Nortel Networks

Nortel VPN Router 600, 1750, 2700, 2750, and 5000

(Hardware Modules with Firmware Version 7_05.100)

FIPS 140-2 Security Policy

Level 2 Validation

Document Version 1.0

Prepared for:

Nortel Networks
600 Technology Park
Billerica, MA 01821
Phone: (800) 466-7835
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 Johnson	Initial draft
0.2	2007-07-25	Xiaoyu Ruan	Added Router 2700
0.3	2007-10-23	Darryl Johnson	Removed references to Router 2700
0.4	2008-02-19	Darryl Johnson	Added references to FIPS physical security kits; added references to Router 2700; updated firmware version number
0.5	2008-02-21	Xiaoyu Ruan	Added algorithm certificate numbers
0.6	2008-04-08	Darryl Johnson	Added text for additional label needed for 600
0.7	2008-06-03	Xiaoyu Ruan	Addressed Lab comments.
0.8	2008-06-18	Xiaoyu Ruan	Addressed Lab comments.
0.9	2008-10-10	Darryl Johnson	Addressed CMVP comments
1.0	2008-10-27	Darryl Johnson	Addressed CMVP comments

Table of Contents

0 INTRODUCTION 5
0.1 PURPOSE 5
0.2 REFERENCES 5
0.3 DOCUMENT ORGANIZATION 5
1 NORTEL VPN ROUTER 600, 1750, 2700, 2750, AND 5000 6
1.1 OVERVIEW 6
1.2 MODULE INTERFACES 7
1.3 ROLES AND SERVICES 12
1.3.1 Crypto Officer Role 12
1.3.2 User Role 13
1.3.3 Authentication Mechanisms 13
1.3.4 Unauthenticated Operator 14
1.4 PHYSICAL SECURITY 14
1.5 OPERATIONAL ENVIRONMENT 14
1.6 CRYPTOGRAPHIC KEY MANAGEMENT 14
1.7 SELF-TESTS 17
1.8 MITIGATION OF OTHER ATTACKS 18
2 SECURE OPERATION 19
2.1 INITIAL SETUP 19
2.1.1 Applying Tamper-Evident Labels 19
2.1.2 Applying Tamper-Evident Shields 20
2.2 CRYPTO OFFICER GUIDANCE 21
2.2.1 Initialization 22
2.2.2 Management 22
2.2.3 Zeroization 22
2.3 USER GUIDANCE 23
3 ACRONYMS 24

Table of Figures

FIGURE 1 – NORTEL VPN ROUTER DEPLOYMENT ARCHITECTURE 6
FIGURE 2 – VPN ROUTER 600 REAR PANEL PHYSICAL PORTS 9
FIGURE 3 – VPN ROUTER 1750 REAR PANEL PHYSICAL PORTS 10
FIGURE 4 – VPN ROUTER 2700 REAR PANEL PHYSICAL PORTS 10
FIGURE 5 – VPN ROUTER 2750 REAR PANEL PHYSICAL PORTS 10
FIGURE 6 – VPN ROUTER 5000 REAR PANEL PHYSICAL PORTS 11
FIGURE 7 – TAMPER-EVIDENT LABEL PLACEMENT FOR 600 19
FIGURE 8 – TAMPER-EVIDENT LABEL PLACEMENT FOR 1750, 2700, AND 2750 19
FIGURE 9 – TAMPER-EVIDENT LABEL PLACEMENT FOR 5000 20
FIGURE 10 – TAMPER-EVIDENT SHIELD PLACEMENT FOR 600 20
FIGURE 11 – TAMPER-EVIDENT SHIELD PLACEMENT FOR 1750 AND 2750 21
FIGURE 12 – TAMPER-EVIDENT SHIELD PLACEMENT FOR 2700 21
FIGURE 13 – FIPS MODE CONFIGURATION 22

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 6
TABLE 2 – NETWORK INTERFACE CARDS AVAILABLE 7
TABLE 3 – ACCELERATOR CARDS SUPPORTED 8
TABLE 4 – VPN ROUTER AND ACCELERATOR CARDS SUPPORTED 8
TABLE 5 – PHYSICAL PORTS AND LOGICAL INTERFACES 9
TABLE 6 – LED STATUS 11
TABLE 7 – CRYPTO OFFICER SERVICES 12
TABLE 8 – USER SERVICES 13
TABLE 9 – AUTHENTICATION MECHANISM USED BY THE MODULES 13
TABLE 10 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 16
TABLE 11 – ACRONYMS 24

0 Introduction

0.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VPN (Virtual Private Network) Router 600, 1750, 2700, 2750, and 5000 from Nortel Networks. This Security Policy describes how the Nortel VPN Router 600, 1750, 2700, 2750, and 5000 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 2 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. 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 Nortel VPN Router 600, 1750, 2700, 2750, and 5000 is referred to in this document as the routers, the cryptographic modules, or the modules.

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 Nortel VPN Router 600, 1750, 2700, 2750, and 5000

1.1 Overview

Nortel is a recognized leader in delivering communications capabilities that secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing routing, firewall, bandwidth management, encryption, authentication, and data integrity for secure tunneling across managed Internet Protocol (IP) networks and the Internet.

Nortel VPN Routers give enterprises a competitive edge by enabling cost-effective, secure connectivity across the entire supply chain, including branch offices, suppliers, distributors, and other business partners. The modules streamline equipment requirements by packaging required VPN firmware and hardware in a single box, without requiring other localized network equipment or servers, minimizing administration costs. A typical deployment of Nortel VPN Routers is shown in Figure 1.

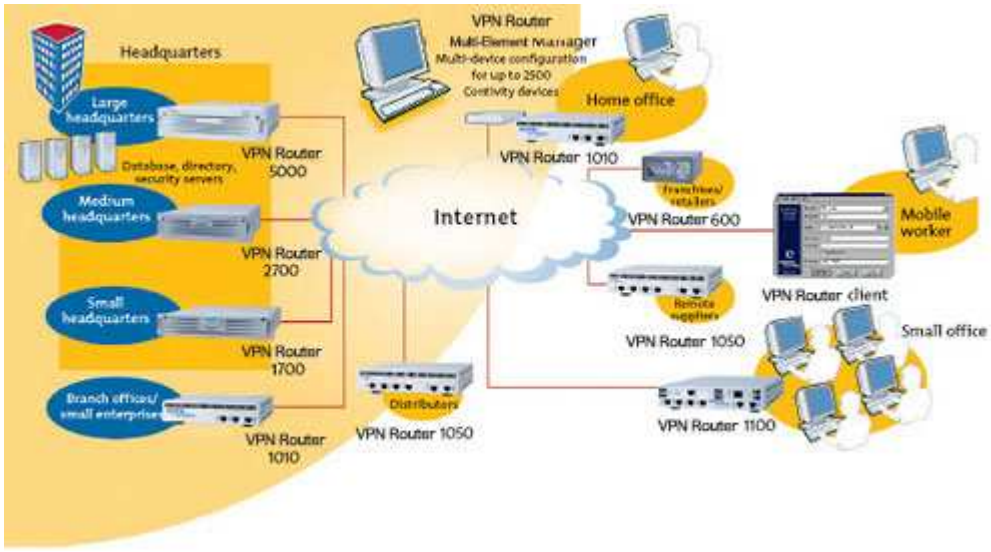

Figure 1 – Nortel VPN Router Deployment Architecture

The Nortel VPN Router 600, 1750, 2700, 2750, and 5000 is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2

Section	Section Title	Level
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Notice that N/A indicates "Not Applicable". EMC and EMI refer to Electromagnetic Compatibility and Electromagnetic Interference, respectively.

1.2 Module Interfaces

The Nortel VPN Router 600, 1750, 2700, 2750, and 5000 are multi-chip standalone modules that meet overall level 2 FIPS 140-2 requirements. The cryptographic boundary of the Nortel VPN Router 600, 1750, 2700, 2750, and 5000 is defined by the outer case of the modules which encloses the complete set of hardware and firmware components.

The VPN Routers are validated in three configurations as follows:

1. With no accelerator cards installed. The hardware version number for this configuration is *600, 1750, 2700, 2750, and 5000*.
2. With the Hardware Accelerator card installed in the 1750, 2700, 2750, and 5000 Routers. The hardware version number for this configuration is *1750, 2700, 2750, and 5000 with DM0011051 or DM0011052*.
3. With the Security Accelerator card installed in the 1750, 2700, 2750, and 5000 Routers. The hardware version number for this configuration is *1750, 2700, 2750, and 5000 with DM0011085 or DM0011084*.

The firmware version number (7_05.100) is the same for all configurations.

The VPN Routers are designed to be modular. They include a power supply, Random Access Memory (RAM), processors, hard disk, floppy drive and Peripheral Component Interconnect (PCI) slots. The VPN Routers communicate with their clients via Local Access Network (LAN) and Wide Access Network (WAN) network interface cards that can be factory installed or field installed. The following network interface cards are available. The option cards are excluded from the security requirements of FIPS 140-2 because they do not provide any security-relevant functionality.

Table 2 – Network Interface cards available

Factory Installable	Field Installable	Description
DM1004002	DM1011002	10/100 Ethernet Option Card
DM3919002	DM3919001	1000Base-SX Option Card
DM3919003	DM3919004	1000Base-T Option Card
DM3811001	DM3811002	56/64K Channel Service Unit/Data Service Unit (CSU/DSU) PCI Option Card
DM2111015	DM2111016	Asymmetrical Digital Subscriber Line (ADSL) Annex A Option Card.
DM2111017	DM2111018	ADSL Annex B Option Card.
DM1519006	DM1519003	Integrated Services Digital Network (ISDN) - BRI S/T Option Card
DM1519005	DM1519004	ISDN - BRI U (US/Canada Only - American National Standards Institute (ANSI) Standard) Option Card
DM2111013	DM2111014	Half Height Single Port T1/FT1 E1 (G.703) w/CSU/DSU Option Card

Factory Installable	Field Installable	Description
DM2119002	DM2119001	Quad T1/FT1 E1 (G.703) w/quad CSU/DSU (4 x RJ48C) Option Card
DM3819002	DM3819004	V.90 Modem Option Card
DM2111027	DM2111006	Single X.21 / V.35 Card Option Card
DM2104003	DM2111003	High Speed Serial Interface (HSSI) option card for external T3/E3 CSU/DSU
DM1004002	DM1011002	10/100 Ethernet Option Card

Additionally, the VPN Router supports the following hardware cryptographic acceleration cards:

Table 3 – Accelerator Cards Supported

Factory Installable	Field Installable	Description
DM0011051	DM0011052	Hardware Accelerator Option Card
DM0011084	DM0011085	Security Accelerator Option Card

The modules support the Hifn 7854 chip on the security accelerator card and the Hifn 7811 chip on the hardware accelerator card, for hardware cryptographic acceleration. Table 4 lists the hardware accelerator cards supported by the modules.

Table 4 – VPN Router and Accelerator Cards Supported

VPN Router platform	Security Accelerator supported	Hardware Accelerator supported
600	No	No
1750	Yes	Yes
2700	Yes	Yes
2750	Yes	Yes
5000	Yes	Yes

After opening the router and installing the cards, the Crypto-Officer has to reapply the tamper-evidence labels as described in section 2 of this document.

The modules' design separates the physical ports into four logically distinct and isolated categories. They are logically divided but are accessed through either the Console port or the network ports. They are:

- Data Input
- Data Output
- Control Input
- Status Output

Data input/output are the packets utilizing the services provided by the modules. These packets enter and exit the modules through the network ports.

Control input consists of Configuration/Administration data entered into the modules through the web interface or the Command Line Interface (CLI) management interface and the input for the power and reset switch. Any user can be given administrative permissions by the Crypto Officer.

Status output consists of the status indicators displayed through the Light Emitting Diodes (LEDs) and log information through the Graphical User Interface (GUI) or CLI. A user with administrative permissions has access to the modules status logs.

The following is a list of the possible physical ports supported by the modules:

- Power connector
- Power switch
- Network ports (LAN port, WAN port)
- Serial port
- LEDs
- Reset switch

All of these physical interfaces are not available in every Router. Table 5 lists the interfaces available in each Router and also provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2:

Table 5 – Physical Ports and Logical Interfaces

FIPS 140-2 Logical Interface	VPN Router 600 Physical Port	VPN Router 1750, 2700, 2750, and 5000 Physical Port
Data Input	Network ports	Network ports
Data Output	Network ports	Network ports
Control Input	Serial port, Network ports	Serial port, Network ports, Power switch, Reset switch
Status Output	LEDs, Serial port, Network ports	LEDs, Serial port, Network ports
Power	Power connector	Power connector

The physical ports of the modules are depicted in the following figures:

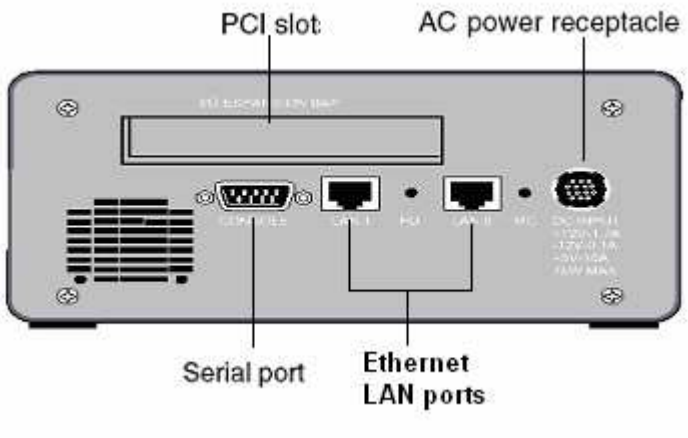

Figure 2 – VPN Router 600 Rear Panel Physical Ports

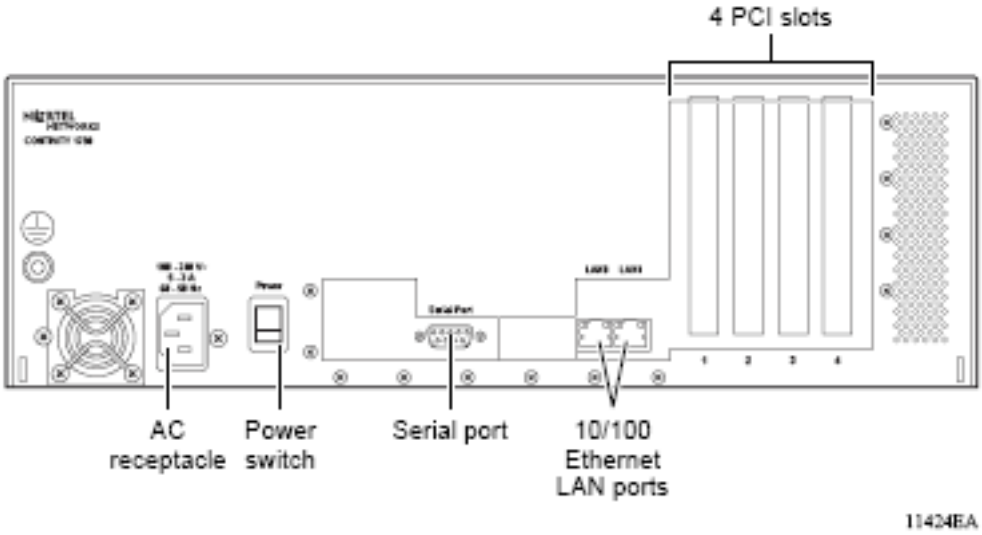

Figure 3 – VPN Router 1750 Rear Panel Physical Ports

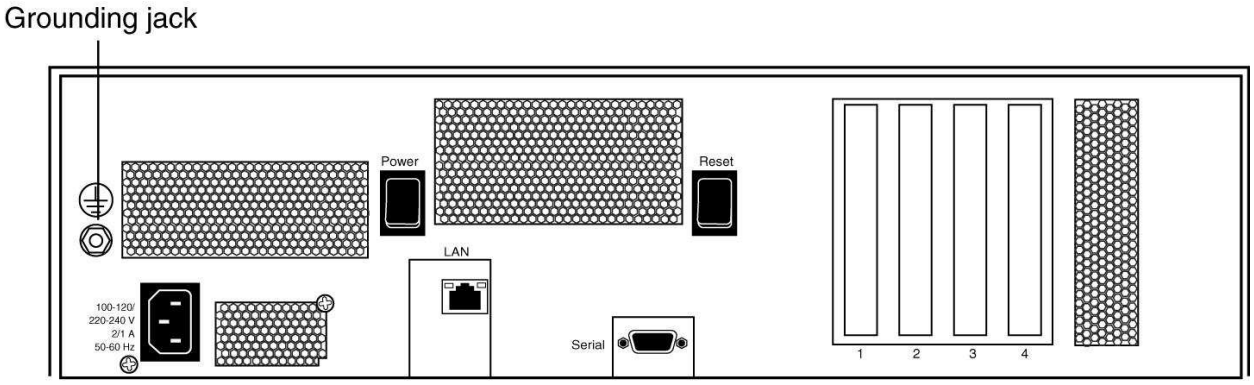

Figure 4 – VPN Router 2700 Rear Panel Physical Ports

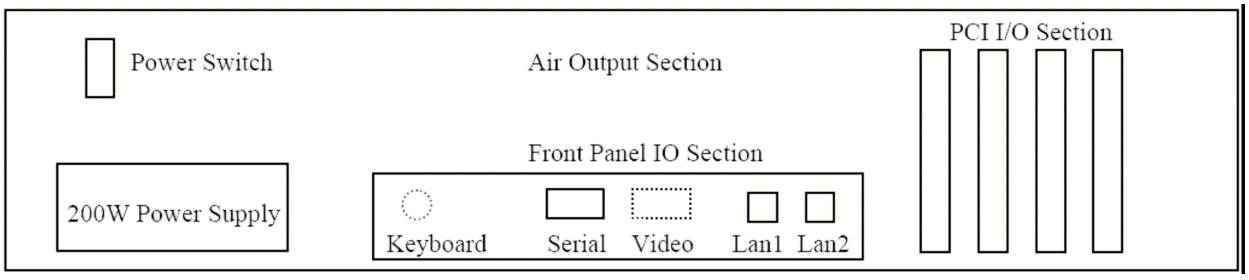

Figure 5 – VPN Router 2750 Rear Panel Physical Ports

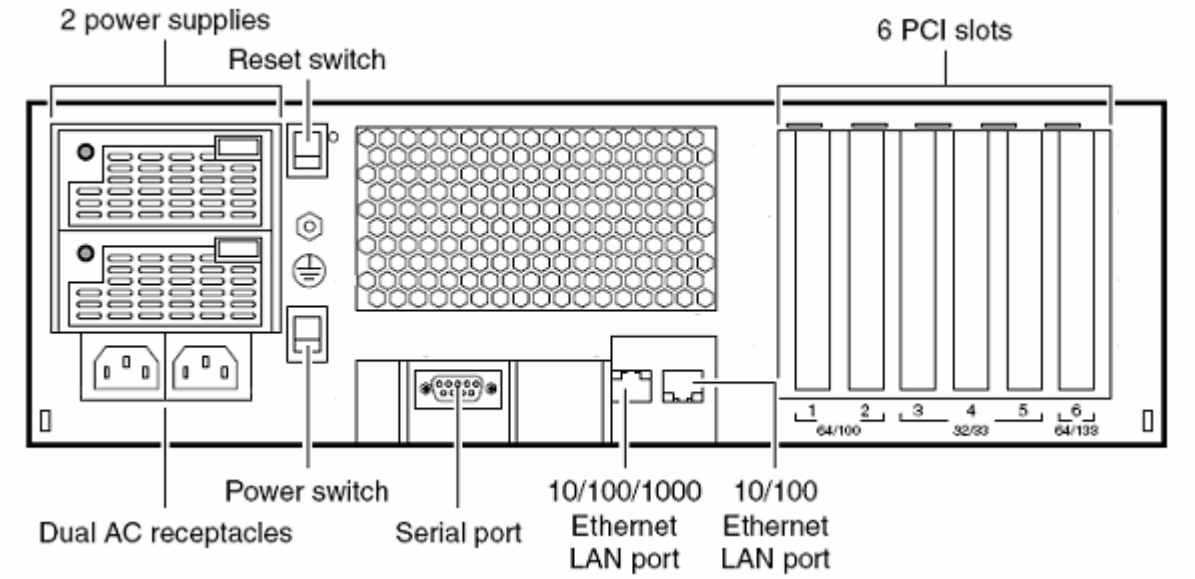

Figure 6 – VPN Router 5000 Rear Panel Physical Ports

The cryptographic modules have a number of LEDs which indicate the state of the modules. The descriptions for the LEDs are listed below for each module.

Table 6 – LED Status

Model	LED	Indicator	Description
600	Power	On	The router is receiving Direct Current (DC) power
		Off	The router is not receiving DC power
	Alert	Red	A serious alarm condition exists that requires attention. A red alert usually indicates a hardware error. The red alert condition is described in the health check display.
	Attention	Amber	A non-fatal alarm condition exists. The yellow alert condition is described in the health check display.
	Ready	Green	The router has booted and is operational.
	Boot	Amber	The router is booting and is in a non-ready state. If the Boot LED and the Ready LED light at the same time, the 600 is in recovery mode
1750 2700 2750	Power (Nortel Networks logo)	On	The router is receiving Alternating Current (AC) power.
		Off	The router is not receiving AC power.
	Alert	Yellow	A non-fatal alarm condition exists. The yellow alert condition is described in the health check display.
	Fail	Red	A serious alarm condition exists that requires attention. A red alert usually indicates a hardware error. The red alert condition is described in the health check display.
	Boot	Yellow	The router is booting and is in a non-ready state.
	Ready	Green	The boot process has completed successfully and the router has reached a state of readiness.
5000	Alert	Yellow	A non-fatal alarm condition exists. The yellow alert condition is described in the health check display.
	Fail	Red	A serious alarm condition exists that requires attention. A red alert usually indicates a hardware error. The red alert condition is described in the health check display.

Model	LED	Indicator	Description
	Boot	Yellow	The system is booting and is in a non-ready state.
	Ready	Green	The boot process has completed successfully and the system has reached a state of readiness.

1.3 Roles and Services

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

1.3.1 Crypto Officer Role

The Crypto Officer role is the administrator for the router and does the initial setup and maintenance. Descriptions of the services available to the Crypto Officer role are provided in the table below. CSP stands for Critical Security Parameter. Crypto Officer services are provided via various protocols including Transport Layer Security (TLS), Secure Shell (SSH), and Remote Authentication Dial-In User Service (RADIUS).

Table 7 – Crypto Officer Services

Service	Description	Input	Output	Keys/CSPs and Type of Access
Configuring the router	Define network interfaces and settings, set the protocols the router will support and load authentication information	Command and parameters	Command response	RSA public key - write, read RSA private key - write, read Password - write, read RADIUS shared secret - write, read
Create user groups	Creating, editing and deleting user groups, define common sets of user permissions.	Command and parameters	Command response	Password - write, read IPsec pre-shared keys - write, read
Create users	Creating, editing and deleting user, Define user accounts and assign permissions.	Command and parameters	Command response	Password - write, read
Define rules and filters	Create packet filters that are applied to user data streams on each interface.	Command and parameters	Command response	None
Monitor status	View the router configuration, active sessions and logs.	Command	Status information	None
Manage the router	Log off users, shut down or reset the router, backup or restore the router configuration, create recovery diskette or zeroize.	Command and parameters	Command response	All - write, read, delete
RADIUS service	RADIUS server logs in and performs User authentication.	RADIUS shared secret	Status information	RADIUS shared secret - read
TLS service	Manage the module using with TLS protocol.	Command, username, password	Status information	RSA public key - read RSA private key - read Password - read TLS Session Keys - write, read, delete ANSI X9.31 PRNG key - write, read, delete

Service	Description	Input	Output	Keys/CSPs and Type of Access
SSH service	Manage the module using with SSH protocol.	Command, username, password	Status information	SSH DSA public key - read SSH DSA private key - read Password - read SSH Diffie-Hellman key pair - write, read, delete ANSI X9.31 PRNG key - write, read, delete SSH Session Key - write, read, delete

1.3.2 User Role

The User role has the ability to access the VPN services provided by the modules which can be exercised by authenticating during the establishment of an IPsec session using a pre-shared key or digital certificate. Descriptions of the services available to the User role are provided in the table below. API stands for Application Programming Interface.

Table 8 – User Services

Service	Description	Input	Output	Keys/CSP and Type of Access
VPN session establishment	Establish VPN session and authenticate	API calls, including proper messages to authenticate	Result of negotiation and session key	RSA private key - read Password - read IPsec pre-shared keys - read IKE Diffie-Hellman key pair - write, read, delete FIPS 186-2 PRNG Seed key - write, read, delete
VPN session	Use the VPN services	Encrypted/decrypted data	Encrypted/decrypted data	IPsec Session Keys - write, read, delete
Change password	Change the user password	Command and parameters	Result of password change	Password - write, read, delete

1.3.3 Authentication Mechanisms

The Crypto Officer can access the module over the console port, TLS session, or an IPsec VPN Client session. The Crypto Officer authenticates using user ID and password. The user authenticates using a pre-shared key or digital certificate during Internet Key Exchange (IKE). In addition to these mechanisms, authentication maybe performed by the internal Lightweight Directory Access Protocol (LDAP) or external LDAP or external LDAP proxy or RADIUS servers.

Table 9 – Authentication Mechanism Used by the Modules

Authentication Type	Strength
Password	Passwords are required to be at least 8 characters in length, and the module supports lengths of up to 32 characters. Considering only the case sensitive English alphabet and the numerals 0-9 using an 8 digit password with repetition, the number of potential passwords is 62^8, which equates to a 1 in 62^8 chance of false positive.
Pre-shared key	The module authenticates the user during IKE using pre-shared keys. Pre-shared keys are generated based on user credentials. The probability of a random attempt to succeed is $1:2^{160}$.

Authentication Type	Strength
RSA Public Key Certificates	The module supports RSA digital certificate authentication of users during IPsec/IKE. The module also supports RSA digital certificate authentication of LDAP servers during TLS. Using conservative estimates and equating a 1024 bit RSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is $1:2^{80}$.
RADIUS shared secret	The RADIUS server authenticates to the module using a hash of the secret key with other information. The shared secret should be at least 8 characters in length, and the module supports lengths of up to 32 characters. Considering only the case sensitive English alphabet and the numerals 0-9 using an 8-digit password with repetition, the number of potential passwords is 62^8, which equates to a 1 in 62^8 chance of false positive.

1.3.4 Unauthenticated Operator

The Simple Network Management Protocol (SNMP) services are provided without authentication. An unauthenticated operator uses a community string to access the SNMP services. The SNMP implemented in the routers is version 1 and it only allows the unauthenticated operator to get non-security-relevant system condition information. The SNMP services do not affect the security of the module.

1.4 Physical Security

The Nortel VPN Router 600, 1750, 2700, 2750, and 5000 are multi-chip standalone cryptographic modules and are enclosed in a hard and opaque metal case that completely encloses all of the internal components of the modules. There are only a limited set of vent holes provided in the case, and these obscure the view of the internal components of the module. Tamper-evidence labels are applied to the case to provide physical evidence of attempts to remove the case of the modules. Additionally an audible alarm can be enabled that is activated when the front cover is removed, except for the VPN router 600. All of the modules' components are production grade. The placement of tamper-evidence labels can be found in section 2 - Secure Operation.

The modules were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

1.5 Operational Environment

The operational environment requirements do not apply to the VPN Router 600, 1750, 2700, 2750, and 5000. The modules do not provide a general purpose operating system.

1.6 Cryptographic Key Management

The modules implement the following FIPS-approved algorithms:

Firmware:

- AES[1]-CBC[2] (128, 256 bits) – FIPS 197 (certificates #718 and #719)
- Triple DES[3]-CBC (168 bits) – FIPS 46-3 (certificates #641 and #642)
- RSA[4] (1024, 2048) – PKCS[5]#1 (certificates #338 and #339)

[1] Advanced Encryption Standard
[2] Cipher Block Chaining
[3] Data Encryption Standard
[4] Rivest, Shamir, and Adleman
[5] Public Key Cryptography Standard

- DSA[6] (1024) – FIPS 186-2 (certificate #272)
- FIPS 186-2 PRNG[7] – General purpose implementation [(x-Original); (SHA[8]-1)] (certificate #420)
- ANSI X9.31 Appendix A.2.4 PRNG (certificate #419)
- SHA-1 – FIPS 180-2 (certificates #738 and # 739)
- HMAC[9]-SHA-1 – FIPS 198 (certificates #387 and #388)

Security Accelerator:

- AES-CBC (128 bits) – FIPS 197 (certificate #48)
- Triple DES-CBC (168 bits) – FIPS 46-3 (certificate #158)
- SHA-1 – FIPS 180-2 (certificate #143)
- HMAC-SHA-1 – FIPS 198 (certificate #102)

Hardware Accelerator:

- Triple DES-CBC (168 bits) – FIPS 46-3 (certificate #29)
- SHA-1 – FIPS 180-2 (certificate #51)
- HMAC-SHA-1 – FIPS 198 (certificate #101)

The module utilizes the following non-FIPS-approved algorithm implementation in the FIPS mode of operation:

Firmware:

- Hardware RNG[10] – for seeding the FIPS 186-2 PRNG
- Non-approved RNG – for seeding the ANSI X9.31 PRNG
- RSA PKCS #1 key wrap (1024 and 2048 bits), providing 80 and 112 bits of encryption strength; non-compliant less than 80 bits (when using key sizes less than 1024 bits)
- Diffie-Hellman Group 5 (1536 bits), providing 96 bits of encryption strength
- Diffie-Hellman Group 2 (1024 bits), providing 80 bits of encryption strength

Security Accelerator:

- RSA PKCS #1 key wrapping (1024 and 2048 bits), providing 80 and 112 bits of encryption strength; non-compliant less than 80 bits (when using key sizes less than 1024 bits)
- Diffie-Hellman Group 5 (1536 bits)[2]
- Diffie-Hellman Group 2 (1024 bits)[3]

Additionally, the following algorithms are disabled within the module in the FIPS mode of operation:

Firmware:

- DES-CBC (56 bits)
- DES MAC[11]
- Diffie-Hellman Group 8 (Elliptic Curve Diffie-Hellman)
- Diffie-Hellman Group 1 (768 bit)
- RC4-CBC (128, 40 bits)

---

[6] Digital Signature Algorithm
[7] Pseudo Random Number Generator
[8] Secure Hash Algorithm
[9] Keyed-Hash Message Authentication Code
[10] Random Number Generator
[11] Message Authentication Code

- RC2-CBC (128 bits)
- MD5
- HMAC MD5
- MD2

Security Accelerator:

- Hardware RNG – for seeding the FIPS-approved ANSI X9.31 PRNG
- ANSI X9.31 PRNG – Appendix A.2.4 of ANSI X9.31 (certificate #82)
- MD5
- HMAC MD5

Hardware Accelerator:

- DES-CBC (56 bits)
- MD5
- HMAC MD5

The module supports the following critical security parameters:

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Storage	Zeroization	Use
Firmware integrity check key	DES MAC (56 bits)	Externally generated predetermined value hard coded into the module	Non-volatile memory (hard drive – plaintext) in module binaries	Zeroized by formatting the hard drive	This key is used to perform the integrity check on the module.
ANSI X9.31 PRNG key	Triple DES key	Generated internally by non-approved RNG	Volatile memory only (plaintext)	Zeroized when the module reboots	Used by ANSI X9.31 PRNG
FIPS 186-2 PRNG Seed key	160 bits	Generated internally by gathering system entropy	Volatile memory only (plaintext)	Zeroized when the module reboots	Used by FIPS 186-2 PRNG
RSA public key	1024, 2048 bits (X.509 certificate)	Server public key is internally generated using PKCS #1; User public key is sent to the module during IPsec/IKE and TLS session key negotiation.	Non-volatile memory	Zeroized when the certificate is deleted; User public key is zeroized when tunnel is disconnected	Public key used for IPsec/IKE and TLS key negotiation
RSA private key	1024-2048 bits	Generated internally using PKCS #1.	Non-volatile memory (PKSC#5 – plaintext)	Zeroized when the certificate is deleted	Private key used for IPsec/IKE and TLS key negotiation
SSH RSA public key	1024, 2048 bits (X.509 certificate)	Server public key is internally generated using PKCS #1; User public key is sent to the module during SSH sessions.	Non-volatile memory	Zeroized when the certificate is deleted; User public key is zeroized when SSH session is disconnected	Public key used for SSH key negotiation

Key	Key Type	Generation / Input	Storage	Zeroization	Use
SSH RSA private key	1024-2048 bits	Generated internally using PKCS #1.	Non-volatile memory (PKSC#5 – plaintext)	Zeroized when the certificate is deleted	Private key used for SSH key negotiation
Passwords	Alphanumeric string (8 - 32 characters)	Entered into module over a console port, TLS or IPsec session	Non-volatile memory (internal LDAP database – plaintext)	Zeroized when the password is updated with a new one	Used for authenticating the Crypto Officer and Users
IPsec pre-shared keys	160 bits	Generated internally using user id and password	Not stored - in volatile memory only (plaintext)	Zeroized when not needed or when the module reboots	Mutual authentication between the server and the client
IKE Diffie-Hellman key pair	Diffie-Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Generated internally using FIPS 186-2 PRNG during IKE	Not stored - Volatile memory only (plaintext)	When no longer used by the module or reboot	Used for session key agreement – public key sent to client
SSH Diffie-Hellman key pair	Diffie-Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Generated internally using ANSI X9.31 PRNG during SSH sessions	Not stored - Volatile memory only (plaintext)	When no longer used by the module or reboot	Used for session key agreement – public key sent to client
SSH DSA public key	1024 bits	Generated internally using ANSI X9.31 PRNG	Not stored - Volatile memory only (plaintext)	Zeroized by formatting the hard drive	Used for client to verify SSH traffic
SSH DSA private key	1024 bits	Generated internally using ANSI X9.31 PRNG	Not stored - Volatile memory only (plaintext)	Zeroized by formatting the hard drive	Used for server to sign SSH traffic
SSH Session Key	128-bit AES key	Diffie-Hellman key agreement, Group 2 or Group 5	Not stored - Volatile memory only (plaintext)	Upon session termination or when a new key is generated (after a certain timeout)	Encrypt and decrypt SSH traffic
IPsec Session Keys	AES (128, 256 bits) Triple-DES (168 bits), HMAC-SHA-1 keys (160 bits)	Negotiated during IKE using Diffie-Hellman key agreement	Not stored - in volatile memory only (plaintext)	Zeroized when not needed or when the module reboots	Used to encrypt/decrypt/MAC tunnel traffic
TLS Session Keys	AES (128, 256 bits) Triple-DES (168 bits), HMAC-SHA-1 keys (160 bits)	Negotiated during TLS session establishment.	Not stored - in volatile memory only in plaintext	Zeroized when not needed or when the module reboots	Used to encrypt/decrypt/MAC the TLS session
RADIUS shared secret	Alphanumeric string (minimum of 8 - 32 characters)	Entered into module over an console port, TLS or IPsec session	Non-volatile memory (internal LDAP database – plaintext)	Zeroized when the RADIUS server setup is deleted	Used to authenticate RADIUS server

1.7 Self-Tests

The VPN Router 600, 1750, 2700, 2750, and 5000 performs the following self-tests at power-up:

Firmware:

- Firmware integrity check: Verifying the integrity of the firmware binaries of the module using a DES MAC error detection code.
- AES Known Answer Test (KAT): Verifying the correct operation of the AES algorithm implementations.
- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementations.
- RSA sign/verify test: Verifying the correct operation of the RSA implementations.
- DSA sign/verify test: Verifying the correct operation of the DSA implementation.
- SHA-1 KAT: Verifying the correct operation of the SHA-1 algorithm implementations.
- HMAC-SHA-1 KAT: Verifying the correct operation of the HMAC-SHA-1 algorithm implementations.
- FIPS 186-2 PRNG KAT: Verifying the correct operation of the FIPS 186-2 PRNG implementations.
- ANSI X9.31 PRNG KAT: Verifying the correct operation of the ANSI X9.31 PRNG implementations.

Security accelerator (if installed):

- AES 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-SHA-1 KAT: Verifying the correct operation of the HMAC-SHA-1 algorithm implementation.

Hardware accelerator (if installed):

- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementation.
- HMAC-SHA-1 KAT: Verifying the correct operation of the HMAC-SHA-1 algorithm implementation.

The VPN Router 600, 1750, 2700, 2750, and 5000 perform the following conditional self-tests:

Firmware:

- Continuous test for the FIPS 186-2 PRNG: Verifying the correct operation of the FIPS 186-2 algorithm implementation.
- Continuous test for the entropy gathering RNG: Verifying the correct operation of the seeding mechanism for the FIPS 182-2 PRNG.
- Continuous test for the ANSI X9.31 PRNG: Verifying the correct operation of the ANSI X9.31 algorithm implementation.
- Continuous test for the non-approved RNG: Verifying the correct operation of the seeding mechanism for the ANSI X9.31 PRNG.
- RSA sign/verify pair-wise consistency test: Verifying that a newly generated RSA key pair works properly.
- DSA sign/verify pair-wise consistency test: Verifying that a newly generated DSA key pair works properly.

If any of the hardware accelerator cards self-tests fail, then the module forces the corresponding card to enter an error state, logs the error to a file, and shuts down the card. Cryptographic operations then failover to firmware.

If any of the firmware self-tests fail, then the module enters an error state, logs the error to the event log, forces a controlled crash, and then reboots itself.

1.8 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 level 2 requirements for this validation.

2 Secure Operation

The Nortel VPN Router 600, 1750, 2700, 2750, and 5000 meets Level 2 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

Before enabling the FIPS mode, tamper-evident labels and the tamper-evident shields (included in the FIPS kit) must be applied to the VPN Router enclosures as shown in the following sections.

2.1.1 Applying Tamper-Evident Labels

To provide evidence of tampering, the Nortel VPN Router 600, 1750, 2700, 2750, and 5000 requires the use of tamper-evident labels. The Nortel VPN Router 600 requires two tamper-evident labels: one overlapping the rear panel and top side and one covering the Recovery pinhole (see Figure 7).

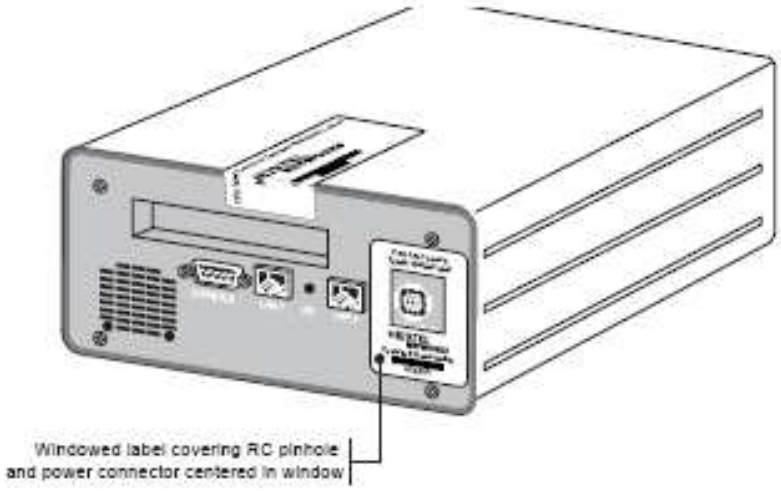

Figure 7 – Tamper-Evident Label Placement for 600

For sealing the Nortel VPN Routers 1750, 2700, and 2750, three tamper-evident labels need to be placed on the front bezel. A label should be placed on each of the bezel screws and another should be overlapped on the center section and bezel (see Figure 8).

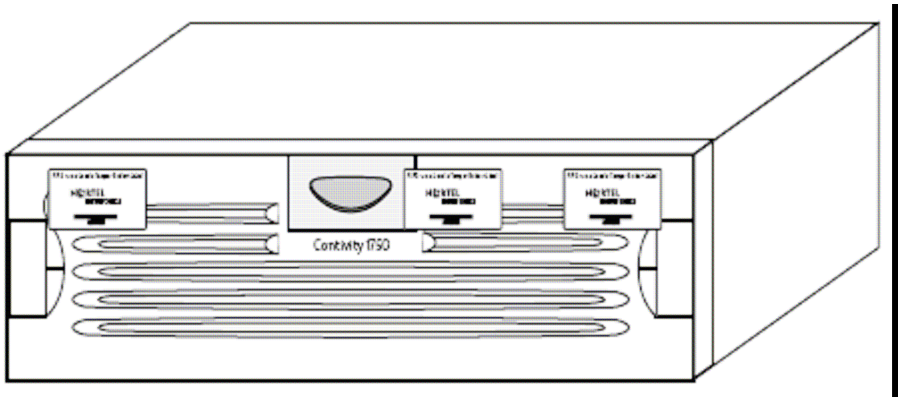

Figure 8 – Tamper-Evident Label Placement for 1750, 2700, and 2750

The Nortel VPN Router 5000 requires two tamper-evident labels on both bezel screws to seal the module. Labels should be placed in an angle to avoid molding the labels over the curved handles and also hide LEDs at front (see Figure 9).

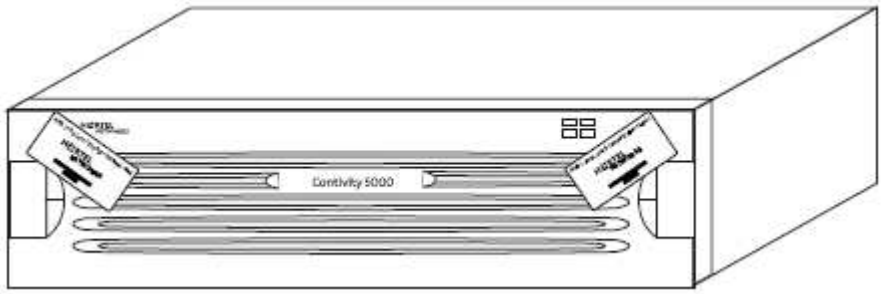

Figure 9 – Tamper-Evident Label Placement for 5000

2.1.2 Applying Tamper-Evident Shields

To prevent visual access to the internal components of the module, shielding must be applied to the VPN Router enclosures. The Nortel VPN Router 600 requires placement of one tamper-evident shield covering rear panel and the top side (see Figure 10).

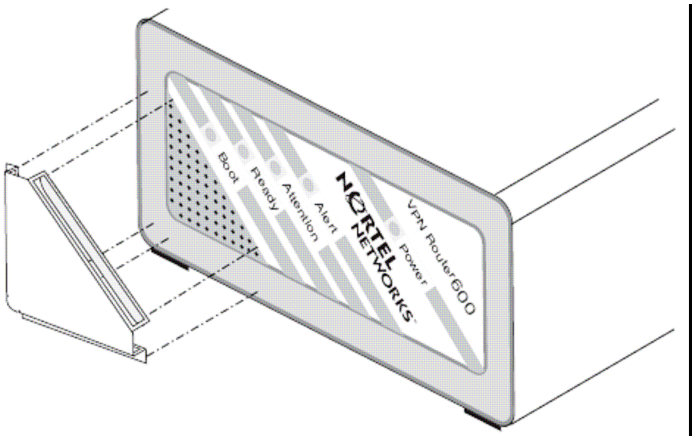

Figure 10 – Tamper-Evident Shield Placement for 600

For protecting the Nortel VPN Routers 1750, 2700, and 2750, one tamper-evident shield needs to be affixed over the ventilation holes at the right of the rear panel (see Figure 11).

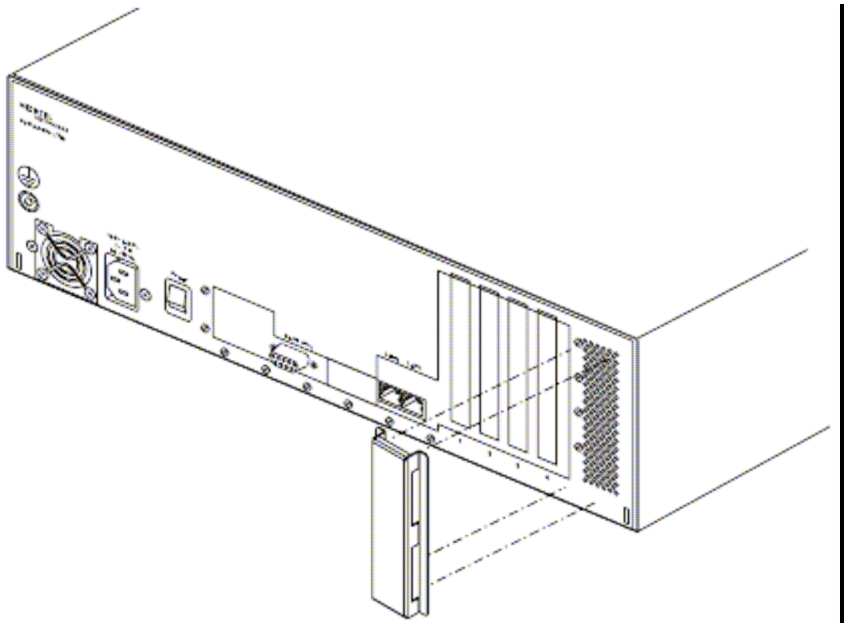

Figure 11 – Tamper-Evident Shield Placement for 1750 and 2750

The Nortel VPN Router 2700 requires two tamper-evident shields to be affixed over the large ventilation areas on the rear panel (see Figure 12).

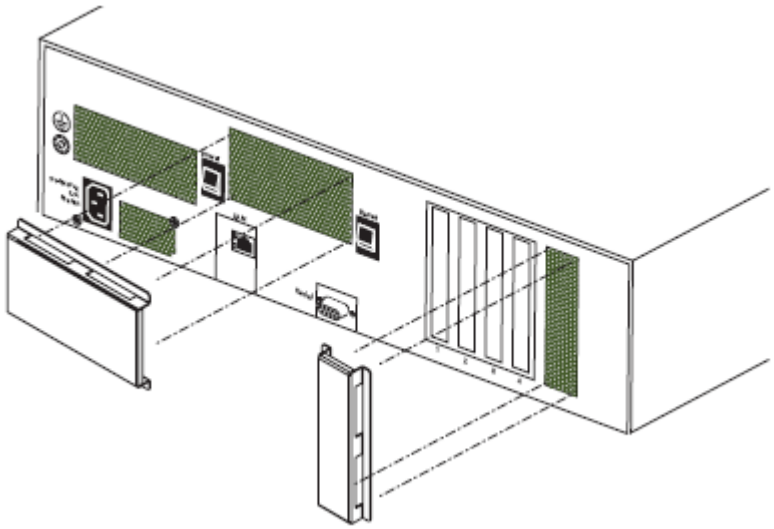

Figure 12 – Tamper-Evident Shield Placement for 2700

2.2 Crypto Officer Guidance

The Crypto Officer is the administrator for the router and does the initial setup and maintenance.

2.2.1 Initialization

The modules are shipped with a default administrator ID and password. The FIPS mode of operation can be enabled from the CLI or web GUI. In CLI, use “fips enable” to enable the FIPS mode and use “no fips” to disable the FIPS mode. In GUI, the FIPS configuration is on the Services → Available page.

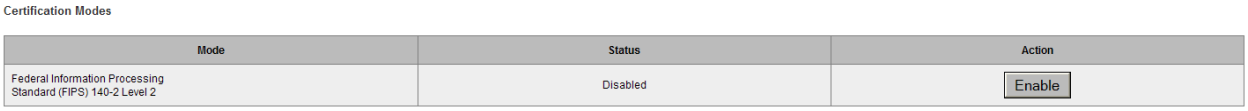

Figure 13 – FIPS Mode Configuration

When FIPS mode is enabled, the modules automatically reboot and disable the following features/services.

- Debugging scripts are disabled
- FTP is disabled on the public interface
- Telnet is disabled on the public interface
- The ‘NULL’ encryption option is disabled for IPsec services

Additionally the Crypto Officer must perform these additional actions to put the modules in a FIPS mode:

- Change the default administrator password
- The Crypto Officer password must be between 8 and 32 characters in length
- RADIUS shared secret must be between 8 and 32 characters in length
- Maximum number of login attempts must be configured to five
- RSA key size of 1024 bits or greater should be used
- All cryptographic services (Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F) etc.) that employ Non-FIPS Approved algorithms must be disabled
- All access to the web based management interface should be over a TLS session (Secure Hypertext Transfer Protocol or HTTPS) or IPsec VPN Client connection
- Use only TLS and enable Ciphers 1 and 2 from services -> ssltls
- LDAP and LDAP Proxy must be over a TLS session
- The backup interface should be over an IPsec session
- Disable DES (56 and 40 bits)
- Do not perform any firmware upgrades

At this point, the module must be rebooted to enable all of the changes. Upon reboot, initialization of the module in FIPS mode is complete and the module is now configured securely.

2.2.2 Management

The Crypto Officer must be sure to only configure cryptographic services for the module using the FIPS Approved algorithms, as listed in the Cryptographic Key Management section above. IPsec and TLS must only be configured to use FIPS Approved cipher suites, and only digital certificates generated with FIPS Approved algorithms may be utilized. RSA key size must be a minimum of 1024 bits in length. Do not perform any firmware upgrades.

When transitioning the modules from Non-FIPS mode to FIPS mode, the Crypto Officer should ensure that the module is running only the Nortel supplied FIPS 140-2 validated firmware.

2.2.3 Zeroization

At the end of its life cycle or when taking the modules out of FIPS mode, the modules must be fully zeroized to protect CSPs. When switching between FIPS mode the module automatically reboots zeroizing all the CSPs. The

Crypto Officer must wait until the modules have successfully rebooted in order to verify that zeroization has completed.

2.3 User Guidance

The User does not have the ability to configure sensitive information on the modules, with the exception of their password. The User must be diligent to pick strong passwords (alphanumeric with a length between eight and 32 characters), and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as IPsec session keys.

3 Acronyms

Table 11 – Acronyms

Acronym	Definition
AC	Alternating Current
ADSL	Asymmetrical Digital Subscriber Line
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSU	Channel Service Unit
DC	Direct Current
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSU	Data Service Unit
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HSSI	High Speed Serial Interface
HTTPS	Secure Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
KAT	Known Answer Test
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Access Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code

Acronym	Definition
N/A	Not Applicable
NIST	National Institute of Standards and Technology
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standards
PPTP	Point-to-Point Tunneling Protocol
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security
WAN	Wide Access Network
VPN	Virtual Private Network