Nortel Networks
VPN Router 600, 1700, 1750, 2700, and 5000

(Firmware Version: 5.05_150)

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 0.18

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
0.18	2007-05-10	Xiaoyu Ruan Darryl Johnson	Updated to reflected new version number

Table of Contents

Table of Figures

Table of Tables

0 Introduction

0.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VPN (Virtual Private Network) Router 600, 1700, 1750, 2700, and 5000 from Nortel Networks. This Security Policy describes how the VPN Router 600, 1700, 1750, 2700, 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/cryptval/

The VPN Router 600, 1700, 1750, 2700, and 5000 is referred to in this document as the "routers", "cryptographic modules", or "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/cryptval/) 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 Router 600, 1700, 1750, 2700, 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 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.

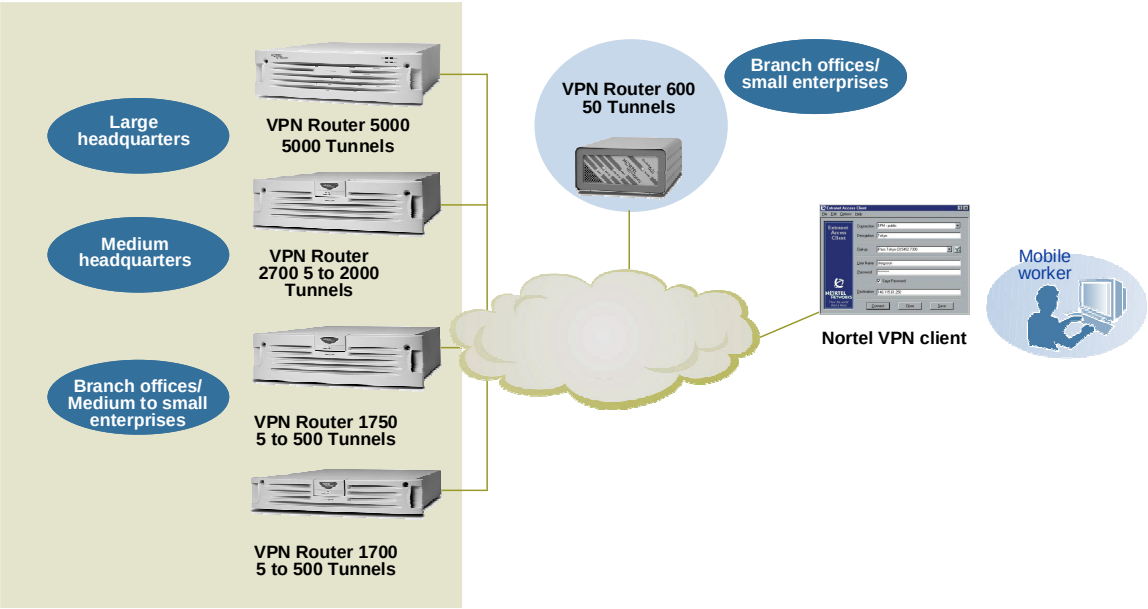

Figure 1 - Nortel VPN Router Deployment Architecture

The VPN Router 600, 1700, 1750, 2700, 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". EMI and EMC refer to Electromagnetic Interference and Electromagnetic Compatibility, respectively.

1.2 Module Interfaces

The VPN Router 600, 1700, 1750, 2700, and 5000 are multi-chip standalone modules that meet overall level 2 FIPS 140-2 requirements. The cryptographic boundary of the VPN Router 600, 1700, 1750, 2700, and 5000 is defined by the outer case of the modules that 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, 1700, 1750, 2700, and 5000.
2. With the Hardware Accelerator card installed in the 1700, 1750, 2700 and 5000 Routers. The hardware version number for this configuration is 1700, 1750, 2700 and 5000 with DM0011052.
3. With the Contivity Security Accelerator card installed in the 1750, 2700 and 5000 Routers. The hardware version number for this configuration is 1750, 2700 and 5000 with DM0011085 and DM0011084.

The firmware version number (5.05_150) is the same for all configurations.

The VPN Routers are designed to be modular. They include a power supply, Dual In-line Memory Module (DIMM) 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[1]:

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 Annex A (ADSL) Option Card.
DM2111017	DM2111018	Asymmetrical Digital Subscriber Line Annex B (ADSL) Option Card.
DM1519006	DM1519003	ISDN - BRI S/T Option Card
DM1519005	DM1519004	ISDN - BRI U (US/Canada Only - ANSI Standard) Option Card
DM2111013	DM2111014	Half Height Single Port T1/FT1 E1 (G.703) w/CSU/DSU Option Card

[1] The option cards are excluded from the security requirements of FIPS 140-2.

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 (HA) Option Card
DM0011084	DM0011085	Contivity Security Accelerator (CSA) Option Card.

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

Table 4 - VPN Router Platform And Hardware Accelerator Cards Supported

VPN Router platform	CSA supported	HA supported
600	No	No
1700	No	Yes
1750	Yes	Yes
2700	Yes	Yes
5000	Yes	Yes

The module's 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 is defined as the packets utilizing the services provided by the modules. These packets enter and exit the modules through the network ports.

Control input consists of data entered into the modules through the web or 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 (CO).

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. Any 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
- Recovery button (to restore the firmware image and file system in the unlikely event that there is a hard disk crash)

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 1700 Physical Port	VPN Router 1750 Physical Port	VPN Router 2700 Physical Port	VPN Router 5000 Physical Port
Data Input	Network ports	Network ports	Network ports	Network ports	Network ports
Data Output	Network ports	Network ports	Network ports	Network ports	Network ports
Control Input	Serial port, Network ports, Recovery button	Serial port, Network ports, Power switch, Reset switch	Serial port, Network ports, Power switch, Reset switch	Serial port, Network ports, Power switch, Reset switch	Serial port, Network ports, Power switch, Reset switch
Status Output	LEDs, Serial port, Network ports	LEDs, Serial port, Network ports	LEDs, Serial port, Network ports	LEDs, Serial port, Network ports	LEDs, Serial port, Network ports
Power	Power connector	Power connector	Power connector	Power connector	Power connectors

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

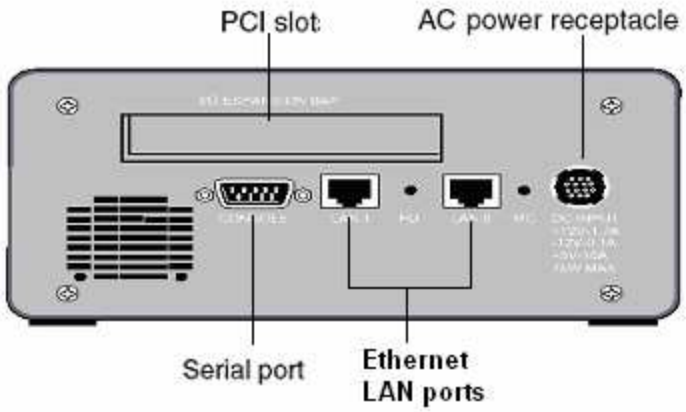

Figure 2 - VPN Router 600 Rear Panel Physical Ports

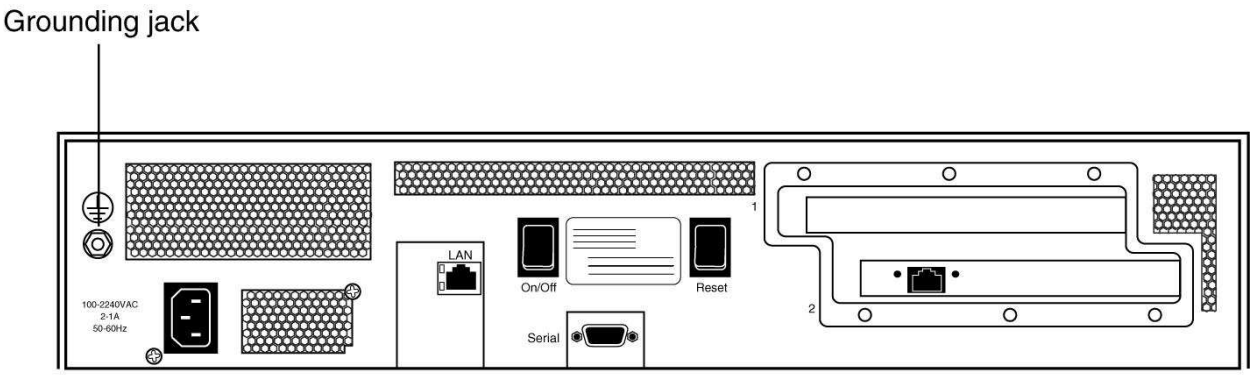

Figure 3 - VPN Router 1700 Rear Panel Physical Ports

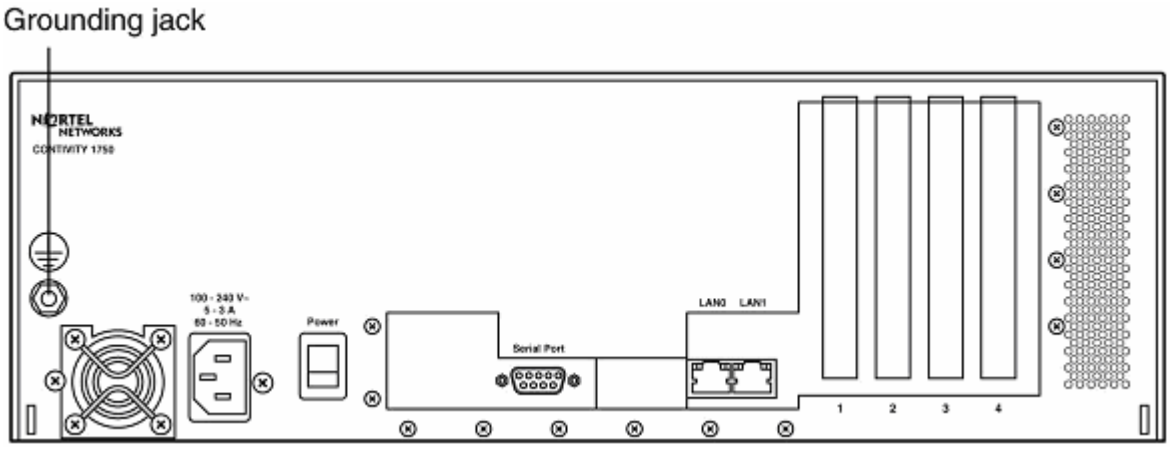

Figure 4 - VPN Router 1750 Rear Panel Physical Ports

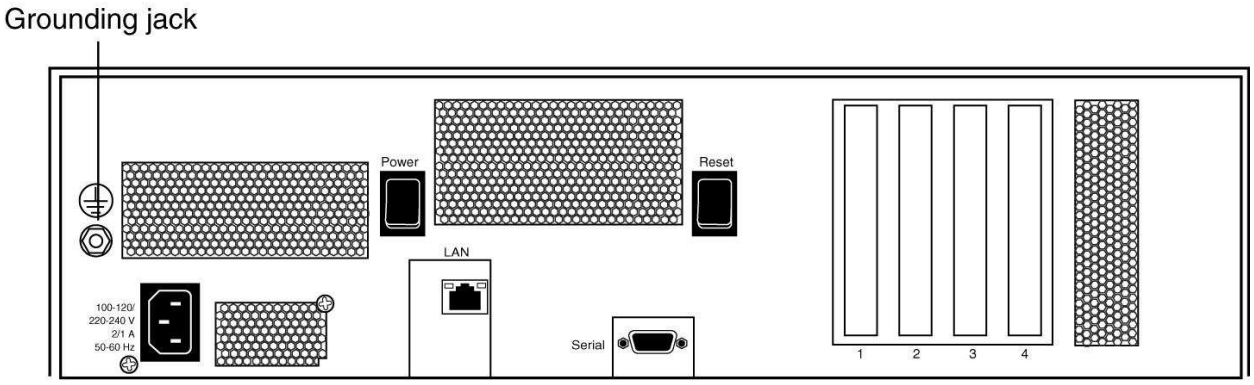

Figure 5 - VPN Router 2700 Rear Panel Physical Ports

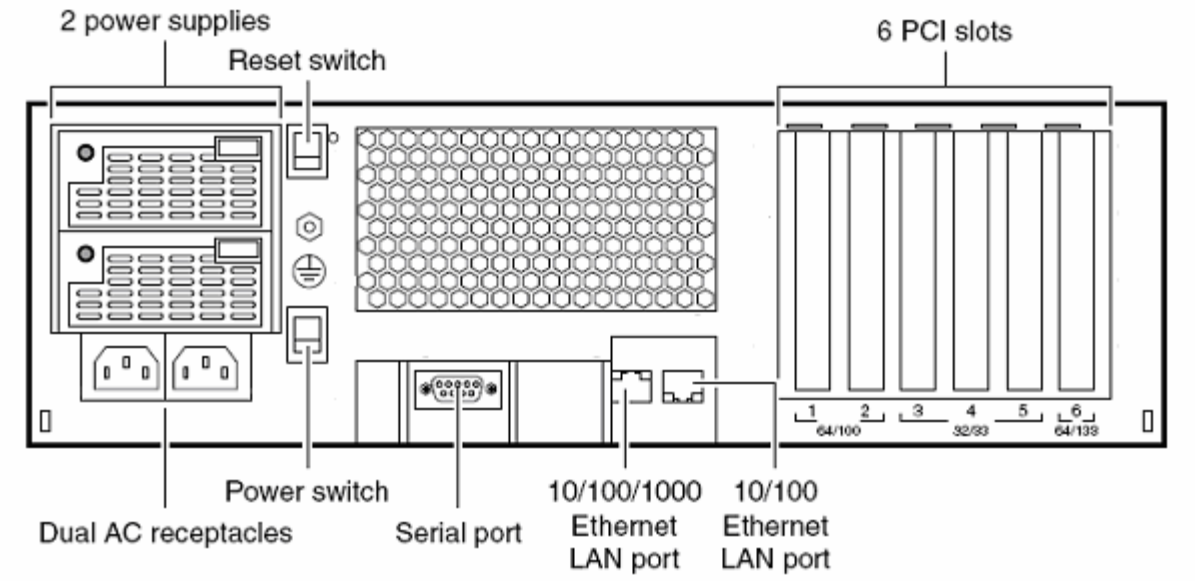

Figure 6 - VPN Router 5000 Rear Panel Physical Ports

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's Description

Model Number	LED	Indicator	Description
600	Power	On	The Router is receiving Alternating Current (AC) power
		Off	The Router is not receiving AC 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 VPN Router 600 is in recovery mode
1700 1750 2700	Power (Nortel Networks logo)	On	The Router is receiving 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.

Model Number	LED	Indicator	Description
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.
	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 module supports 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 performs 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. RADIUS stands for Remote Authentication Dial-In User Service.

Table 7 - Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP 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 RSA private key - Write Password - Write RADIUS shared secret - Write
Create user groups	Create, edit and delete user groups. Define common sets of user permissions.	Command and parameters	Command response	Password - Read/Write
Create users	Create, edit and delete user. Define user accounts and assign permissions.	Command and parameters	Command response	User password - Read/Write
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

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 - Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	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 Pre-shared key - Write
VPN session	Use the VPN services	Encrypted/decrypted data	Encrypted/decrypted data	Session keys - Read/Write
Change password	Change the user password	Command and parameters	Result of password change	Password - Write

1.3.3 Authentication Mechanisms

The Crypto-Officer can access the module over the console port, Transport Layer Security (TLS) session or an IPSec VPN Client session. The CO authenticates using a 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) database 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. 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.
RSA Public Key Certificates	The module supports RSA digital certificate authentication of users during IPSec/IKE and 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. 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 Physical Security

The VPN Router 600, 1700, 1750, 2700, 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-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the modules. Additionally on all router models except the VPN router 600, an audible alarm can be enabled that is activated when the front cover is removed. All of the modules' components are production grade. The placement of tamper evidence labels can be found in section 3 - 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).

1.3.5 Operational Environment

The operational environment requirements do not apply to the VPN Router 600, 1700, 1750, 2700 and 5000. The modules do not provide a general purpose operating system.

1.3.6 Cryptographic Key Management

The modules implement the following FIPS-approved algorithms:

Firmware:

- AES-CBC (128, 256 bits) – FIPS 197 (certificate 292)
- Triple DES-CBC (168 bits) – FIPS 46-3 (certificate 367)
- RSA(1024, 2048) – PKCS#1 (certificate 83)
- FIPS 186-2 PRNG – General purpose implementation [(X-Original); (SHA-1)] (certificate 116)
- SHA-1 – FIPS 180-2 (certificate 366)
- HMAC-SHA-1 – FIPS 198 (certificate 103)

Contivity 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 FIPS Mode of operation:

Firmware:

- Diffie-Hellman Group 5 (1536 bits)[2]
- Diffie-Hellman Group 2 (1024 bits)[3]

Contivity Security Accelerator:

- Diffie-Hellman Group 5 (1536 bits)[2]
- Diffie-Hellman Group 2 (1024 bits)[3]
- RSA PKCS #1 key wrapping[4]

[2] Group 5 key establishment provides 96 bits of encryption strength.
[3] Group 2 key establishment provides 80 bits of encryption strength.

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

Firmware:

- DES-CBC (56 bits)
- DES-MAC
- Diffie_Hellman Group 8 (ECDH)
- Diffie-Hellman Group 1 (768 bit)
- RC4-CBC (40, 128 bits)
- RC2-CBC (128 bits)
- MD5
- HMAC-MD5
- MD2

Contivity 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.

[4] RSA PKCS #1 key wrapping provides 80-112 bits of encryption strength.

Key	Key Type	Generation / Input	Storage	Zeroization	Use
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[5]	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[5]	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
Passwords	Alphanumeric string (minimum of 8 characters)	Entered into module over an 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 DH key pair	Diffie Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Generated internally during IKE	Not stored - Volatile memory only (plaintext)	Zeroized When no longer used by the module or reboot	Used for session key agreement – public key sent to client
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

[5] Encrypt/Decrypt provides between 80 and 112 bits of encryption strength.

Key	Key Type	Generation / Input	Storage	Zeroization	Use
RADIUS shared secret	Alphanumeric string (minimum of 6 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

The module uses a FIPS Approved FIPS 186-2 PRNG for key generation.

1.3.7 Self-Tests

The VPN Router 600, 1700, 1750, 2700, 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 KAT: Verifying the correct operation of the AES algorithm implementation.
- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementation.
- RSA pair-wise consistency check: Verifying the correct operation of the RSA 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-SHA1 algorithm implementation.
- FIPS 186-2 PRNG KAT: Verifying the correct operation of the FIPS 186-2 PRNG implementation.

CSA (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-SHA1 algorithm implementation.

HA (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-SHA1 algorithm implementation.

The VPN Router 600, 1700, 1750, 2700 and 5000 perform the following conditional self-tests:

Firmware:

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

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

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

1.3.8 Design Assurance

Nortel follows highly stabilized and popular design procedures. The design goes through many phases of review and inspections, and implementations undergo rigorous quality assurance testing. ClearCase Version 5.0 is used to provide configuration management for the modules firmware and documentation.

Additionally, Microsoft Visual Source Safe version 6.0 is used to provide configuration management for the VPN Router 600, 1700, 1750, 2700, and 5000's FIPS documentation. This software provides access control, versioning, and logging.

1.3.9 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 VPN Router 600, 1700, 1750, 2700, 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 FIPS Mode, the tamper evident labels must be applied as shown below. For more details on steps for applying, monitoring and logging the tamper evidence labels see Chapter 2, "Labeling the Contivity Secure IP Services Gateway", of the Using Contivity Secure IP Services Gateways in FIPS Mode document.

The Nortel VPN Router 600 requires one tamper-evident label covering rear panel and the top side.

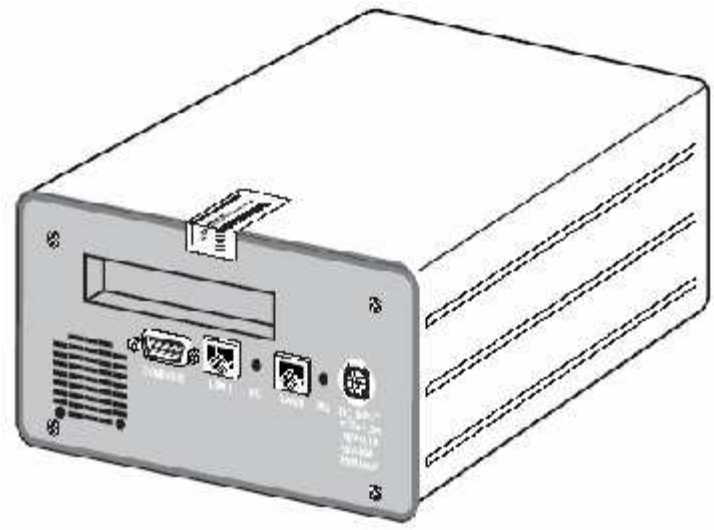

Figure 7 - Tamper evidence label for top cover of 600

To seal the Nortel VPN Router 1700, 1750, and 2700, three tamper-evident labels need to be placed on the front bezel. A label should be put on each of the two bezel screws and another should be overlapped on the center section and bezel.

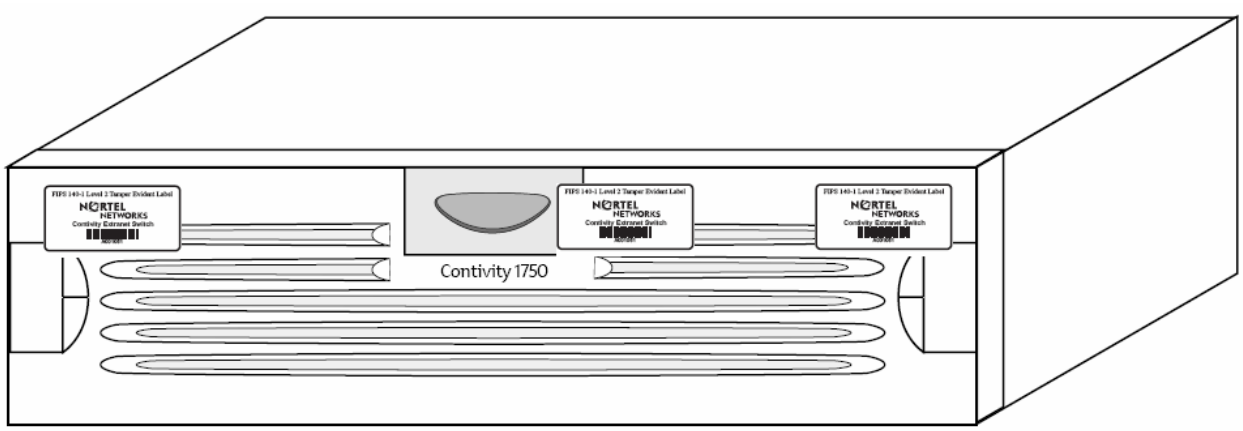

Figure 8 - Tamper evidence label for 1700, 1750, and 2700

The Nortel VPN Router 5000 router requires a tamper-evident label on each of the two bezel screws to seal the module. For the VPN router 5000, labels should be placed in an angle to avoid molding the labels over the curved handles which would also hide the front LEDs.

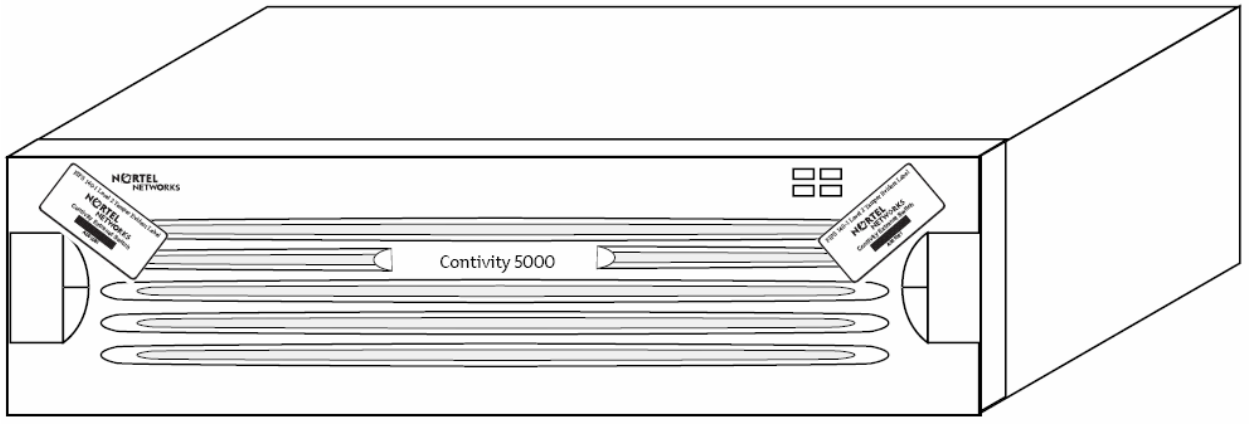

Figure 9 - Tamper evidence label for 5000

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

- Debugging scripts are disabled
- File Transfer Protocol (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 configured to a minimum length of 8 characters
- RADIUS shared secret must be a minimum length of 6 characters
- 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 or PPTP, Layer 2 Tunneling Protocol or L2TP, Layer 2 Forwarding or 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.

For more details on the initial configuration of the routers see *Configuring the Contivity 600/1700/1750/2700/5000.*

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 TLSv1 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. The CO must 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. If there is a concern that the firmware has been modified during operation in Non-FIPS mode then the Crypto Officer should reinstall the Nortel firmware from a trusted media such as the Nortel installation compact disc or the Nortel website.

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 the FIPS Mode the module automatically reboots zeroizing all CSP's in volatile memory. 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 minimum 8 characters or greater), 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
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CSA	Contivity Security Accelerator
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CSU	Channel Service Unit
DES	Data Encryption Standard
DIMM	Dual In-line Memory Module
DSU	Data Service Unit
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	Hardware Accelerator
HMAC	(Keyed-) Hash MAC
HSSI	High Speed Serial Interface
HTTPS	Secure Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
KAT	Known Answer Test
L2F	Layer 2 Forwarding

Acronym	Definition
L2TP	Layer 2 Tunneling Protocol
LAN	Local Access Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
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
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WAN	Wide Access Network
VPN	Virtual Private Network