

Part No. NN46110-505.01.01
313645-G Rev 01
December 2008

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Router Configuration — FIPS 140-2



Copyright © 2008 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Nortel VPN Router are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft and Windows NT are trademarks of Microsoft Corporation.

NDS and Novell are trademarks of Novell, Inc.

ACE Server and RSA are trademarks of RSA Security, Inc.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

- a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface	11
Before you begin	11
Text conventions	12
Acronyms	13
Related publications	14
How to get Help	15
Finding the latest updates on the Nortel Web site	15
Getting help from the Nortel Web site	15
Getting help over the phone from a Nortel Solutions Center	16
Getting help from a specialist by using an Express Routing Code	16
Getting help through a Nortel distributor or reseller	16
New in this release	17
Features	17
Nortel VPN Router 1010, 1050, and 1100 tamper-evident labels	17
Tamper-evident shields	17
Chapter 1	
Overview of FIPS 140-2 compliance	19
FIPS 140-2 validation	20
Hardware overview	21
Roles and services	22
Role-based authentication	23
Crypto Officer role	23
User role	23
Crypto Officer services	24
User services	25
IPsec	25
PPTP	26

L2TP	26
L2F	27
Key management	28
User passwords	28
Keys	28
Certificates	30
Firewall and advanced routing	31
Self-tests	31
 Chapter 2	
Physically securing the Nortel VPN Router.....	33
 FIPS 140-2 security kit components	34
Tamper-evident labels	35
Before you label the Nortel VPN Router	36
Applying the tamper-evident label (Nortel VPN Router 600)	36
Applying the tamper-evident labels (Nortel VPN Router 1750, 2700, and 2750)	38
Applying the tamper-evident labels (Nortel VPN Router 5000)	39
Applying the tamper-evident label (Nortel VPN Router 1010, 1050, and 1100)	40
Tamper-evident shields	41
Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 600	42
Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 1750/2750	43
Attaching the FIPS 140-2 tamper-evident shields to the Nortel VPN Router 2700	44
Monitoring and controlling FIPS labels	45
 Chapter 3	
Enabling and disabling FIPS mode	47
 Changes enforced by FIPS mode	48
Enabling FIPS mode using the command line interface	49
Disabling FIPS mode using the command line interface	51
Health Check (FIPS)	53
FIPS Health Check status messages	54
Security log	54
Index	57

Figures

Figure 1	Tamper-evident label	35
Figure 2	Damaged tamper-evident label	35
Figure 3	Tamper-evident labels applied to the Nortel VPN Router 600	37
Figure 4	Tamper-evident labels applied to the front bezel of the Nortel VPN Router 1750, 2700, and 2750	38
Figure 5	Tamper-evident label applied to the bezel of the Nortel VPN Router 5000	40
Figure 6	Tamper-evident label applied to the chassis of the Nortel VPN Router 1010, 1050, and 1100	41
Figure 7	Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 600	42
Figure 8	Attaching FIPS 140-2 tamper-evident shield to the Nortel VPN Router 1750/ 2750	43
Figure 9	Attaching FIPS 140-2 tamper-evident shields to the Nortel VPN Router 2700	44
Figure 10	Sample log for monitoring and controlling FIPS labels	45
Figure 11	Health Check screen	53
Figure 12	Security log screen	55

Tables

Table 1	FIPS logical interfaces mapped to Nortel VPN Router physical interfaces	22
Table 2	Contents of the Nortel VPN Router FIPS security kit	34
Table 3	Definitions of sample log terms	45
Table 4	Disabling authentication methods by protocol (FIPS mode)	48
Table 5	FIPS Health Check status messages	54

Preface

This guide provides information about how to configure the Nortel VPN Router to operate in FIPS-compliant mode. This guide includes the following information:

- Roles and services available when using the Nortel VPN Router in FIPS mode
- 140-2 tamper evidence requirements and instructions for applying the tamper evident labels
- Instructions for enabling and disabling FIPS mode

This guide describes Nortel VPN Router only in the context of configuring them for FIPS 140-2 level 2. For more information about Nortel VPN Router hardware and software documentation, see [“Related publications” on page 14](#).

Throughout this guide, the Nortel VPN Router is referred to as *the gateway*.

Before you begin

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

- Experience with system administration
- Familiarity with network management
- Knowledge of FIPS 140-2 concepts and procedures

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	<p>Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is ping <ip_address>, you enter ping 192.32.10.12</p>
bold Courier text	<p>Indicates command names and options and text that you need to enter.</p> <p>Example: Use the show health command.</p>
brackets ([])	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is show ntp [associations], you can enter either show ntp or show ntp associations.</p>
<i>italic text</i>	<p>Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.</p> <p>Example: If the command syntax is ping <ip_address>, <i>ip_address</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates command syntax and system output, for example, prompts and system messages.</p> <p>Example: File not found.</p>
separator (>)	<p>Shows menu paths.</p> <p>Example: Choose Status > Health Check.</p>

Acronyms

This guide uses the following acronyms:

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CSP	critical security parameter
DES	Data Encryption Standard
DTR	Derived Test Requirements
ECMP	equal cost multipath
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HMAC	Hashing Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol, Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
KAT	known answer test
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LED	light emitting diode

MAC	Message Authentication Code
MD5	Message Digest 5
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PCI	peripheral component interconnect
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Services
RIP	Routing Information Protocol
SA	security association
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
WAN	wide area network

Related publications

For complete information about installing and configuring the Nortel VPN Router, refer to the following publications (included on the FIPS 140-2 software CD):

- Release notes
Provide late-breaking information about your hardware and software.
- Hardware installation guide:
 - *Nortel VPN Router Installation— VPN Router 600*
 - *Nortel VPN Router Installation— VPN Router 1700*
 - *Nortel VPN Router Installation— VPN Router 1750*

- *Nortel VPN Router Installation— VPN Router 2700*
- *Nortel VPN Router Installation— VPN Router 2750*
- *Nortel VPN Router Installation— VPN Router 5000*
- Software configuration guides

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortel.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get Help

This section explains how to get help for Nortel Networks products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for **VPN Router**, click one of the following links:

Link to	Takes you directly to the
Latest software	Nortel page for VPN Router software.
Latest documentation	Nortel page for VPN Router documentation.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

New in this release

The following sections details what is new in *Nortel VPN Router Configuration — FIPS 140-2*.

Features

See the following sections for information about feature changes:

Nortel VPN Router 1010, 1050, and 1100 tamper-evident labels

FIPS 140-2 requires that the Nortel VPN Router 1010, 1050, and 1100 receive a level 1 physical compliant label placed over their respective reset configuration holes. For more information see [“Applying the tamper-evident label \(Nortel VPN Router 1010, 1050, and 1100\)” on page 40](#)


Tamper-evident shields

FIPS 140-2 requires the restriction of visual access to the inside of a module. To comply with this standard, you can now seal the Nortel VPN Router by using tamper-evident shields. For more information see [“Tamper-evident shields” on page 41](#).

Chapter 1

Overview of FIPS 140-2 compliance

This chapter introduces Federal Information Processing Standards (FIPS) 140-2 requirements for the Nortel VPN Router.



Note: FIPS 140-2 information applies to these Nortel VPN Router hardware platforms: Nortel VPN Router 600, 1750, 2700, 2750, and 5000.

This chapter contains the following topics:

Topic	Page
FIPS 140-2 validation	20
Hardware overview	21
Roles and services	22
Key management	28
Firewall and advanced routing	31
Self-tests	31

FIPS 140-2 validation

FIPS 140-2 is a U.S. Government federal standard that enhance the security of information when applied to software and hardware. The FIPS 140-2 publication (“Security Requirements for Cryptographic Modules”) specify requirements for the design and implementation of products that perform cryptography.

You can find FIPS 140-2 publications and related information at the <http://csrc.nist.gov/cryptval/> URL

The FIPS 140-2 standard provide four levels of compliance for a cryptographic module. Level 1 is the lowest level, and Level 4 is the highest. The Nortel VPN Router meets Level 2 standards for FIPS 140-2.

Level 2 provides role-based authentication in which a module must authenticate that an operator is authorized to assume a specific role and perform a corresponding set of services. For more information about role-based authentication, see “[Role-based authentication](#)” on page 23.

For a device to be certified as FIPS-compliant, the following actions must take place:

- 1** The applying company submits relevant design documentation, source code, and product executable to a National Voluntary Laboratory Accreditation Program (NVLAP).
- 2** The laboratory executes the tests described in the Derived Test Requirements (DTR).
- 3** The laboratory issues a test report to the National Institute of Standards and Technology (NIST) indicating compliance (PASS or N/A) on all applicable FIPS 140-2 requirements.
- 4** NIST issues an official certificate to the company certifying its compliance with those requirements.

Nortel VPN Router software version 7.05.100 has been certified under FIPS 140-2 level 2, when the provided tamper evident labels are applied on the following platforms:

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



Note: For the FIPS 140-2-certified software version that runs on each Nortel VPN Router platform, go to the <http://csrc.nist.gov/cryptval/> URL. In the left column of the page, click on Validation Lists, then click on the Vendor List link on the resulting page.

Hardware overview

The hardware for the Nortel VPN Router can include the following interfaces:

- One (private) 10/100 Ethernet LAN port provided on the base system
- One serial port for network management
- Depending on the system, expansion slots that can accommodate a combination of optional LAN, WAN, and serial interface cards and hardware encryption accelerator cards



Note: The Nortel hardware encryption accelerator card is an encryption, compression, and authentication processor card with a PCI interface. This option card is certified for operation in FIPS mode.

[Table 1](#) maps the physical interfaces on a Nortel VPN Router to the logical interfaces described by the FIPS 140-2

Table 1 FIPS logical interfaces mapped to Nortel VPN Router physical interfaces

FIPS 140-2 logical interface	Physical interface on the Nortel VPN Router
Data input interface	LAN port WAN port
Data output interface	LAN port WAN port
Control input interface	LAN port WAN port Serial port Power switch Reset switch
Status output interface	Front panel LEDs LAN port LEDs WAN port LEDs Serial port
Power interface	Power plugs

Roles and services

The Nortel VPN Router can support multiple simultaneous users (or “operators”). For FIPS 140-2 Level 2 compliance, the Nortel VPN Router must be able to maintain internally the separation of operator roles and the services performed by each operator. The Nortel VPN Router must also employ access control mechanisms to:

- Authenticate an operator accessing the gateway—either directly or indirectly, via a computer process acting on his or her behalf.
- Verify that the operator is authorized to perform the desired roles and services within that role.

Role-based authentication

To comply with FIPS 140-2 Level 2, the Nortel VPN Router employs *role-based authentication* of users and stores user identity information in an internal Lightweight Directory Access Protocol (LDAP) database. You can optionally configure the Nortel VPN Router as an LDAP proxy server; in this way authentication can be performed against a variety of external servers using LDAP or RADIUS, including Novell* NDS*, Microsoft Windows NT* Domains, RSA* Security and ACE Server*.

FIPS 140-2 Level 2 specifies two main roles that users can assume in the Nortel VPN Router: the *Crypto Officer* role and the *User* role. The Nortel VPN Router administrator assumes the Crypto Officer role to configure and maintain the gateway using Crypto Officer services; other users exercise only User services.

Crypto Officer role

The Crypto Officer role assumes the following rights:

- **Manage Switch** rights (None, View, or Manage): *View* rights allow an administrator to view all configuration and status information on the Nortel VPN Router. *Manage* rights allow an administrator to configure the Nortel VPN Router and change settings.
- **Manage Users** rights (None, View, or Manage): *View* rights allow an administrator to view all user accounts and settings on the gateway. *Manage* rights allow an administrator to create, modify, and delete users.

User role

A user is authenticated and assumes the User role to access the following services:

- Initiate IPsec tunnels.
- Initiate PPTP tunnels.
- Initiate L2TP tunnels.
- Initiate L2F tunnels.
- Change his or her own password.

Crypto Officer services

The Nortel VPN Router has a factory default login ID and password that allow access to the Crypto Officer role. This initial account is the primary administrator's account for the Nortel VPN Router and guarantees that at least one account is able to assume the Crypto Officer role and completely manage the gateway and users. (This initial account always has *manage gateway* and *manage users* rights.) An administrator of the Nortel VPN Router can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional administrators.

Administrators can always access the Nortel VPN Router and authenticate themselves via the serial port. An administrator can also authenticate as a User over a secure tunnel and then authenticate to the gateway as a Crypto Officer in order to manage the gateway. The default configuration allows HTTP management on the private LAN interface of the gateway without requiring a secure tunnel. For FIPS 140-2 level 2 compliance, however, disable HTTP over private non-tunneled interfaces.



Note: You can manage the Nortel VPN Router using an HTTPS connection over a private non-tunneled interfaces and still be in compliance with FIPS 140-2 level 2.

At the highest level, Crypto Officer services include the following:

- **Configure the Nortel VPN Router:** Define network interfaces and settings, set the protocols the Nortel VPN Router will support, define routing tables, set system date and time, load authentication information, etc.
- **Create user groups:** Define common sets of user permissions such as access hours, user priority, password restrictions, protocols allowed, filters applied, and types of encryption allowed. Administrators can define the permission sets for a number of users by creating, editing, and deleting user groups.
- **Create users:** Define user accounts and assign them permissions using user groups. Additionally, an account can be assigned an administrator ID, allowing access to the Crypto Officer role. Each administrator ID is assigned rights to manage the Nortel VPN Router (one of *none*, *view gateway*, or *manage gateway*) and rights to manage users (one of *none*, *view users*, or *manage users*).

- **Define rules and filters:** Create packet filters that are applied to user data streams on each interface. Each filter consists of a set of rules that defines a set of packets to permit or deny. Rules consist of such basic characteristics as protocol ID, addresses, ports, TCP connection establishment, and packet direction. The administrator can use any of the predefined rules or create custom rules to be included in each filter.
- **Monitor status:** View the Nortel VPN Router configuration, routing tables, and active sessions; use Gets to view SNMP MIB II statistics, usage graphs, health, temperature, memory status, voltage, and packet statistics; and review accounting logs.
- **Manage the Nortel VPN Router:** Log off users, shut down or reset the gateway, disable or enable audible alarms, manually back up Nortel VPN Router configurations, restore gateway configurations, or create a recovery diskette.

User services

An administrator (Crypto Officer) who has *manage users* rights assigns each user a name and a user group. The user group defines access permissions and services that the user can exercise, including access hours, call admission priority, forwarding priority, number of simultaneous logins, maximum password age, minimum password length, whether passwords contain only alphabetic characters, whether static IP addresses are assigned, idle timeout, forced logoff for timeout, and filters.

The administrator also assigns each user separate user IDs and passwords for the following services: IPsec, PPTP, L2TP, and L2F tunnels. The user can then authenticate as necessary to initiate secure tunnels using any of these services.

IPsec

IPsec requires authentication through user name and password. IPsec authenticates the user to the gateway and is protected using Internet Key Exchange/Internet Security Association Key Management Protocol (IKE/ISAKMP). Security options for IPsec include using an Encapsulated Security Payload (ESP) with Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, or “40-bit DES” for encryption of data.

Security options also include using an Authentication Header (AH) with Hashing Message Authentication Code Secure Hash Algorithm (HMAC SHA-1) or HMAC Message Digest 5 (MD5) for operator authentication to the module. These security options provide secure communication for a user and prevent sensitive data from traveling over the Internet in the clear.

When operating in FIPS mode, only the IPsec protocol with AES, DES, or Triple DES encryption and HMAC SHA-1 is used to create a secure tunnel.

PPTP

PPTP requires authentication using Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), or Password Authentication Protocol (PAP). Security options for PPTP include using 40-bit RC4 and 128-bit RC4 for encryption of data. Security options also include using SHA-1 or MD5 for operator authentication to the module. These security options provide secure communication for a user and prevent sensitive data from traveling over the Internet in the clear.

When operating in FIPS mode, only SHA-1 is enabled and encryption is disabled. This mode of operation is considered bypass mode, that is, data is forwarded through the gateway in plain-text form and is not encrypted.

L2TP

L2TP requires authentication using MS-CHAP, CHAP, or PAP. Security options for L2TP include using 40-bit RC4 and 128-bit RC4 for encryption of data. Security options also include using SHA-1 or MD5 for operator authentication to the module. These security options provide secure communication for a user.

When operating in FIPS mode, only SHA-1 is enabled and encryption is disabled. This mode of operation is considered bypass mode, that is, data is forwarded through the Nortel VPN Router in plain-text form and is not encrypted.

L2F

L2F requires authentication using CHAP or PAP. Security options for L2F include using SHA-1 or MD5 for operator authentication. When operating in FIPS mode, only SHA-1 is enabled. This mode of operation is considered bypass mode, that is, data is forwarded through the Nortel VPN Router in plain-text form and is not encrypted.

Key management

The Nortel VPN Router uses and securely administers these FIPS 140-2 level 2 critical security parameters (CSPs):

- User passwords
- Keys (secret, private, and public)
- Certificates

User passwords

User passwords are created by the Crypto Officer and are stored in the LDAP database in an encrypted format and never released. They are used only for authentication in key exchange protocols. User passwords can be destroyed by Crypto Officers or by users when they overwrite their own passwords. New and changed passwords should have at least five characters.



Note: The Password Authentication Protocol (PAP) transmits password information in the clear; do not enable PAP before you set local policy.

Keys

The Nortel VPN Router uses and manages the following types of keys.

- Session keys: These ephemeral secret keys are created using the gateway's pseudo-random number generator for protocols such as MS-CHAP and ISAKMP, which securely negotiate key exchange and then allow encryption services for PPTP, L2TP, and IPsec. These keys are created during the negotiation of secure tunnels on behalf of operators who have successfully authenticated themselves to the gateway with their user ID and password. The keys are temporarily stored in memory during a tunnel session and are destroyed when the appropriate tunnel, security association (SA), or session is terminated. They are never archived or released from the device.

In FIPS mode, only the IPsec protocol with AES, DES, or Triple DES encryption is used to create a secure tunnel.

- **Pre-shared keys:** These ephemeral secret keys are internally derived for protocols such as MS-CHAP and ISAKMP. The keys are used for authentication purposes with the hashing and encryption services to set up SAs between the gateway and an operator. The keys are temporarily stored in memory during a tunnel session and are destroyed when the appropriate tunnel, SA, or session is terminated. They are never archived or released from the device.

In FIPS mode, only the IPsec protocol with AES, DES, or Triple DES encryption and HMAC SHA-1 is used to create a secure tunnel.

- **Diffie-Hellman keys:** These ephemeral public/private key pairs are used with protocols such as ISAKMP to derive pre-shared secret keys during tunneling sessions. These keys are internally generated using the gateway's pseudo-random number generator during session setup. They are temporarily stored in memory during a tunnel session and destroyed when the appropriate tunnel, SA, or session is terminated. The private key is never output. The public key is output to the respective party during a key agreement procedure.
- **DES password key:** This key is used to encrypt all passwords to be stored in the switch's internal LDAP database. This key is compiled into the Nortel VPN Router device code. For instructions on how to zeroize DES password keys, see the security policy for the Nortel VPN Router model. (Go to this URL for the list of Nortel security policies: (<http://csrc.nist.gov/cryptval/140-1/1401vend.htm>.)
- **3DES password encryption:** When enabled in a one time configuration session, all current DES encrypted passwords are converted to 3DES encryption. This process enables a conversion of DES passwords used in older LDAP versions to the upgraded 3DES encryption type. Once converted to the 3DES type, however, you can no longer use DES encryption. As well, the process does not require a configuration rebuild when upgrading from older releases of code.
- **RSA keys:** These public/private key pairs are used to generate and verify digital signatures for authentication of users during tunneling sessions. The gateway's keys are generated internally according to the PKCS#1 standard using a pseudo-random number generator. The keys are stored in uniquely named directories in PKCS#5 and PKCS#8 formats. The administrator can zeroize all RSA keys by entering commands to delete and zeroize the key directories. The private key is never output. The public key is output to obtain a certificate from a third-party certificate authority (CA).

- **Configurable hash key:** This configurable key enables the entry of a user defined 8 byte character string or hexadecimal value encryption key on the Nortel VPN Router. A SHA1 hash is stored in the LDAP to ensure that the Nortel VPN Routers using a single or external LDAP are using the same password. A hash is created locally to validate with the LDAP version before the new key is accepted and the new password is then stored in the LDAP. When an encryption key is entered from the GUI or the CLI, the passwords currently encrypted are decrypted and re-encrypted with the new encryption key. The SHA1 stored on the LDAP validates the encryption key to ensure there is no corruption of the key before updating the LDAP.

Certificates

RSA certificates are public key-based certificates that are used to authenticate users for tunnel sessions. In addition, the Nortel VPN Router has its own certificate that it uses to authenticate itself to operators. These X.509 certificates are issued by a third-party certificate authority (CA) and are stored in the internal LDAP database. Certificates can be zeroized by the administrator using commands that actively delete the certificates.

Firewall and advanced routing

You can further restrict access to the Nortel VPN Router by enabling the Nortel VPN Router Stateful Firewall. For the Nortel VPN Router Stateful Firewall to function, you must install the Firewall License Key.

Additionally, you can use the advanced routing features of the Nortel VPN Router in FIPS mode. The Advanced Routing License Key is required to enable features such as OSPF and ECMP.

Self-tests

To prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The Nortel VPN Router includes an array of self-tests that are run when power is applied to the Nortel VPN Router and periodically during operation.

The self-tests that run at power-up include the following:

- Cryptographic known answer tests (KATs) on the FIPS-approved cryptographic algorithms (AES, DES, 3DES), on the message digest (SHA-1), and on signatures (RSA with SHA-1)
- Software/firmware integrity tests using a DES MAC per FIPS PUB 113, “Computer Data Authentication”
- Continuous random number generator and pseudo-random number generator tests
- IPSEC and SSL tests that include generated messages indicating pass, failure, or trusted state.

Other tests are run periodically or conditionally, including the following:

- Software/firmware load test for FIPS-approved upgrades using a DES MAC
- Continuous random number generator and pseudo-random number generator tests
- Checksum tests on flash memory that has been updated with flash changes

If any of these self-tests fail, the gateway transitions into an error state. Within the error state, all secure data transmission is halted and the gateway outputs status information indicating the failure.

Chapter 2

Physically securing the Nortel VPN Router

To make your Nortel VPN Router compliant with FIPS 140-2, you must apply the tamper-evident labels and the tamper-evident shields included in the FIPS kit.



Caution: You are responsible for using the FIPS labeling kit and the instructions in this guide to apply the labels and to configure your system for FIPS 140-2 compliance. Nortel Customer Services does *not* apply the labels for you.

This chapter contains the following topics:

Topic	Page
FIPS 140-2 security kit components	34
Tamper-evident labels	35
Before you label the Nortel VPN Router	36
Applying the tamper-evident label (Nortel VPN Router 600)	36
Applying the tamper-evident labels (Nortel VPN Router 1750, 2700, and 2750)	38
Applying the tamper-evident label (Nortel VPN Router 1010, 1050, and 1100)	40
Applying the tamper-evident labels (Nortel VPN Router 5000)	39
Tamper-evident shields	41
Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 600	42
Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 1750/2750	43
Attaching the FIPS 140-2 tamper-evident shields to the Nortel VPN Router 2700	44
Monitoring and controlling FIPS labels	45

After you configure the Nortel VPN Router in FIPS conformant mode (with tamper-evident labels in place), the system cannot be accessed without signs of tampering.

FIPS 140-2 security kit components

[Table 2](#) lists the items in the Nortel VPN Router FIPS 140-2 security kit.

Table 2 Contents of the Nortel VPN Router FIPS security kit

Quantity	Description
2	Sheets of labels (24 labels total). Each sheet has the following labels: <ul style="list-style-type: none">• 8 general FIPS security labels• 3 AC filter input security labels• 1 I/O panel air holes security label
1*	Tamper-evident windowed label- Nortel VPN Router 600 only*
5	Alcohol wipes for cleaning the equipment prior to securing labels
1	Nortel VPN Router software CD (contains software and documentation)
1	Recovery diskette, used to restore the software image and file system (The FIPS kit for the Nortel VPN Router 600 does not contain a recovery diskette.)
1*	Tamper-evident shield - Nortel VPN Router 600 only*
2*	Tamper-evident shields - Nortel VPN Router 2700/2750 only*
3*	Tamper-evident shields - Nortel VPN Router 1750 only*



Caution: If you have not received all the items listed in [Table 2](#), contact Nortel Customer Service (see [“How to get Help”](#) on page 15).

Tamper-evident labels

The FIPS 140-2 labeling kit contains multiple Type C, tamper-evident identification and information labels for resealing your system after maintenance, upgrade of option cards and memory, or required access to the floppy disk drive. Each label has a unique serial number to be recorded by the network manager for control purposes [Figure 1](#).

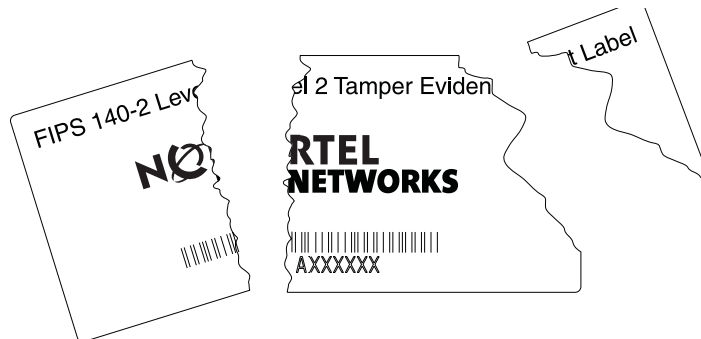
Figure 1 Tamper-evident label



CS450001A

The tamper-evident labels are made of a special thin-gauge white vinyl with a self-adhesive backing. Any attempt to access the NVR will damage or destroy these labels. An attempt to remove a label breaks it or continually tears off small fragments, as shown in [Figure 2](#).

Figure 2 Damaged tamper-evident label



CS450001B

Other signs of tampering include warped or bent metal cover, scratches in the paint of the module, and possibly, a smell of organic solvents.

Because each tamper-evident label has a unique serial number, the labels can be inspected for damage and verified against the network manager's log files (see [“Monitoring and controlling FIPS labels” on page 45](#)).



Caution: To ensure the security of the system, surplus maintenance labels *must* be controlled and locked.

Before you label the Nortel VPN Router

Before you apply the tamper-evident labels to your system, note the following:

- The FIPS 140-2 security labels are very fragile and require careful handling.
- You must press the label firmly onto the chassis to ensure proper adhesion. Do not rub.
- You must allow *72 hours* for the adhesive on the tamper-evident seals to cure completely.



Note: Your system is not fully FIPS 140-2 compliant until the adhesive has completely cured (72 hours).

Applying the tamper-evident label (Nortel VPN Router 600)

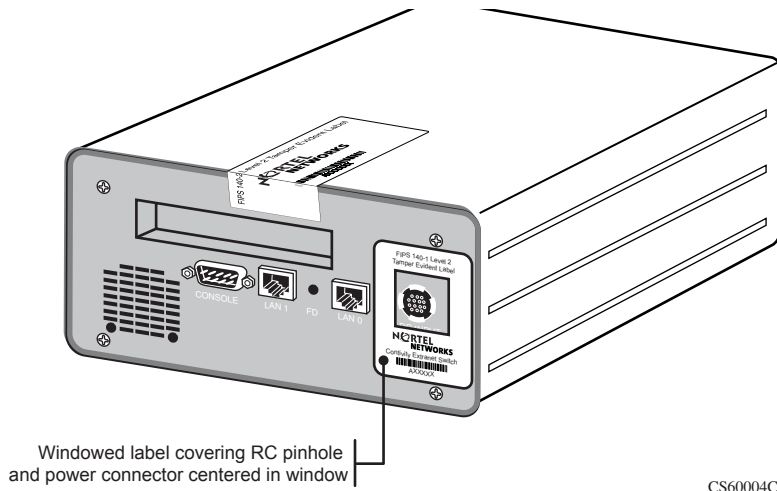
The Nortel VPN Router 600 has one removable portion. Removing the system from the chassis allows access to the system board, memory, and expansion slots.

To seal the cover of the Nortel VPN Router 600, you must apply the tamper-evident labels as follows:

- 1 Ensure that the temperature of the NVR is above 10°C (50°F).
- 2 Clean the chassis of any grease, dirt, or oil. Use the alcohol-based cleaning pads that are shipped in the FIPS 140-2 security kit.
- 3 Affix the solid label to the top of the chassis, making sure that the label overlaps the rear panel [Figure 3 on page 37](#).

- 4 Affix the windowed label to the rear panel by centering the window over the chassis's power connector while ensuring that the left side of the label covers the RC pinhole [Figure 3](#).

Figure 3 Tamper-evident labels applied to the Nortel VPN Router 600



- 5 Record the serial number of the label applied to the Nortel VPN Router 600 in a security log (for an example of a security log, see [Figure 10 on page 45](#)).



Note: Allow *72 hours* for the adhesive in the tamper-evident seals to cure completely.

- 6 For instructions on configuring the Nortel VPN Router 600 for FIPS mode, see [Chapter 3, “Enabling and disabling FIPS mode,” on page 47](#).

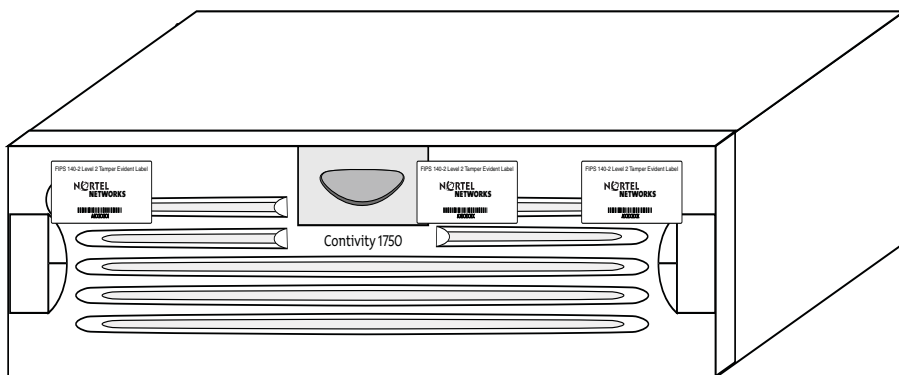
Applying the tamper-evident labels (Nortel VPN Router 1750, 2700, and 2750)

The Nortel VPN Router 1750, 2700, and 2750 have two removable portions: the front bezel and the top cover. Removing the front bezel allows access to the floppy disk drive. Removing the top cover allows access to the system board, memory, and expansion slots.

To seal the Nortel VPN Router 1750, 2700 or 2750, you must apply the serialized, tamper-evident labels as follows.

- 1 Ensure that the temperature of the Nortel VPN Router is above 10°C (50°F).
- 2 Clean the front bezel of any grease, dirt, or oil. Use the alcohol-based cleaning pads that are shipped in the FIPS 140-2 security kit.
- 3 Affix two labels over the bezel screw holes completely covering the holes and affix one label overlapping the center piece and the bezel (Figure 4).

Figure 4 Tamper-evident labels applied to the front bezel of the Nortel VPN Router 1750, 2700, and 2750



- 4 Record the serial numbers of the labels applied to the Nortel VPN Router in a security log (for an example of a security log, see [Figure 10 on page 45](#)).



Note: Allow *72 hours* for the adhesive in the tamper-evident seals to cure completely.

- 5 For instructions on configuring the Nortel VPN Router for FIPS mode, see [Chapter 3, “Enabling and disabling FIPS mode,” on page 47](#).

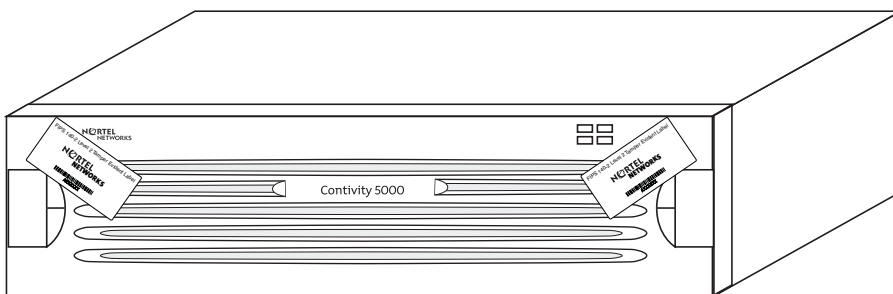
Applying the tamper-evident labels (Nortel VPN Router 5000)

The Nortel VPN Router 5000 has two removable portions: the front bezel and the top cover. Removing the front bezel allows access to the hard disk drives and the floppy disk drive. Removing the top cover allows access to the system board, memory, and expansion slots.

To seal the Nortel VPN Router 5000, you must apply the serialized, tamper-evident labels as follows.

- 1 Ensure that the temperature of the Nortel VPN Router is above 10°C (50°F).
- 2 Clean the bezel of any grease, dirt, or oil. Use the alcohol-based cleaning pads that are shipped in the FIPS 140-2 security kit.
- 3 Affix two labels over the bezel screw holes, making sure that the labels completely cover the holes [Figure 4 on page 38](#).

Figure 5 Tamper-evident label applied to the bezel of the Nortel VPN Router 5000



- 4 Record the serial numbers of the labels applied to the Nortel VPN Router 5000 in a security log (for an example of a security log, see [Figure 10 on page 45](#)).



Note: Allow *72 hours* for the adhesive in the tamper-evident seals to cure completely.

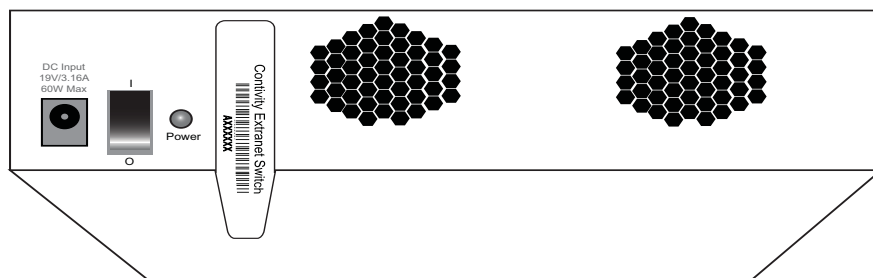
- 5 For instructions on configuring the gateway for FIPS mode, see [Chapter 3](#), “Enabling and disabling FIPS mode,” on page 47

Applying the tamper-evident label (Nortel VPN Router 1010, 1050, and 1100)

Nortel VPN Router 1010, 1050, and 1100 chassis require a FIPS 140-2 label for level 1 physical compliancy. In this procedure you place the tamper-evident label over the reset configuration pinholes at the back of the chassis.

- 1 Ensure that the temperature of the Nortel VPN Router is above 10°C (50°F).
- 2 Clean the chassis of any grease, dirt, or oil. Use the alcohol-based cleaning pads that are shipped in the FIPS 140-2 security kit.
- 3 Affix the label over the reset configuration holes at the back of the Nortel VPN Router 1010, 1050, or 1100 chassis [Figure 6 on page 41](#).

Figure 6 Tamper-evident label applied to the chassis of the Nortel VPN Router 1010, 1050, and 1100



- 4 Record the serial numbers of the labels applied to the Nortel VPN Router 1010, 1050, and 1100 in a security log (for an example of a security log, see [Figure 10 on page 45](#)).



Note: Allow *72 hours* for the adhesive in the tamper-evident seals to cure completely.

- 5 For instructions on configuring the gateway for FIPS mode, see [Chapter 3](#), “Enabling and disabling FIPS mode,” on page 47.

Tamper-evident shields

FIPS 140-2 requires the restriction of visual access to the inside of a module. To comply with this standard, the Nortel VPN Router is sealed by using tamper-evident shields supplied with the FIPS 140-2 security kit onto the Nortel VPN Router chassis.

The tamper-evident shield is a solid opaque metal bracket that has legs, or stand-offs, which when inserted, prevent any visual access into the chassis. Tamper-evident shields are inserted into the front air vents of the Nortel VPN Router 600 and the rear air vents of the Nortel VPN Router 1750, 2700, and 2750 chassis.

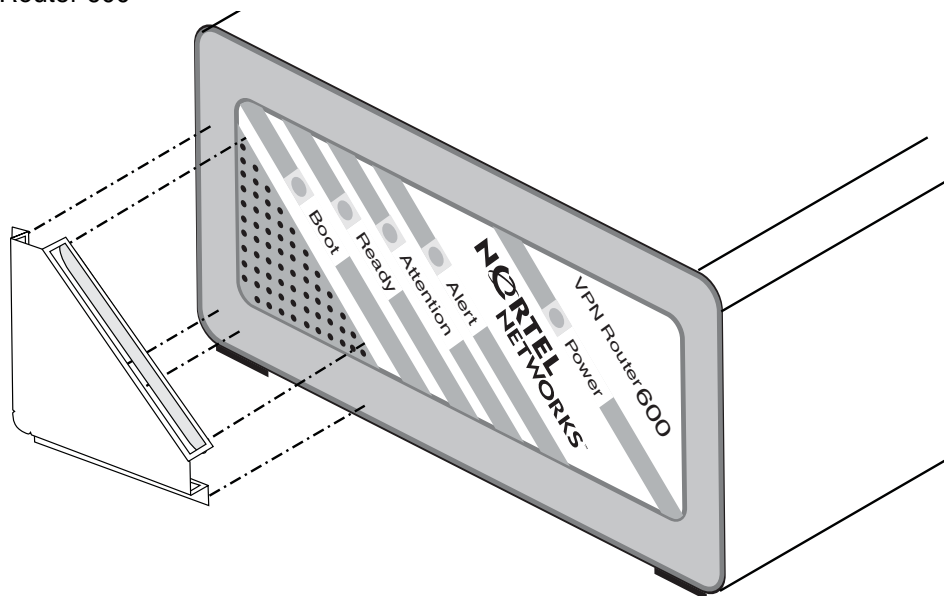
Any attempt to remove the shield results in one or more of the stand-offs breaking and thereby revealing evidence of tampering.

Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 600

To attach the tamper-evident shields to the Nortel VPN Router 600 chassis, complete the following:

- 1 Remove the protective paper from the adhesive strips affixed to the flanges of the tamper-evident shield.
- 2 Align the flanges to the chassis surface surrounding the air vents found on the front of the chassis as shown in [Figure 7](#). Ensure the flanges do not cover the air vents.
- 3 Press firmly on the tamper-evident shield to ensure a secure attachment to the chassis.

Figure 7 Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 600

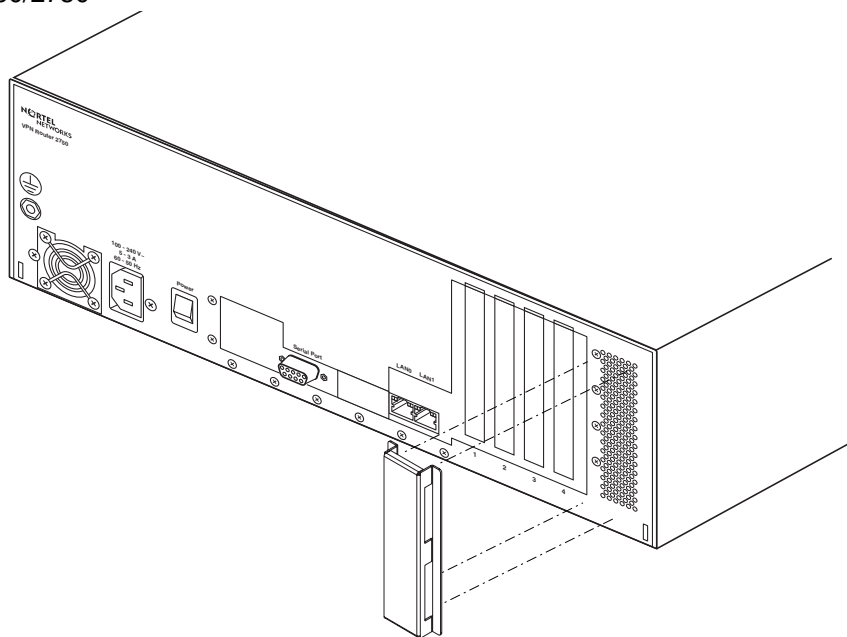


Attaching the FIPS 140-2 tamper-evident shield to the Nortel VPN Router 1750/2750

To attach the tamper-evident shield to the Nortel VPN Router 1750 or 2750 chassis air vents, complete the following:

- 1 Remove the protective paper from the adhesive strips affixed to the flanges of the tamper-evident shield.
- 2 Align the flanges to the chassis surface surrounding the air vents found on the back of the chassis as shown in [Figure 8](#). Ensure the flanges do not cover the air vents.
- 3 Press firmly on the tamper-evident shield to ensure a secure attachment to the chassis.

Figure 8 Attaching FIPS 140-2 tamper-evident shield to the Nortel VPN Router 1750/2750

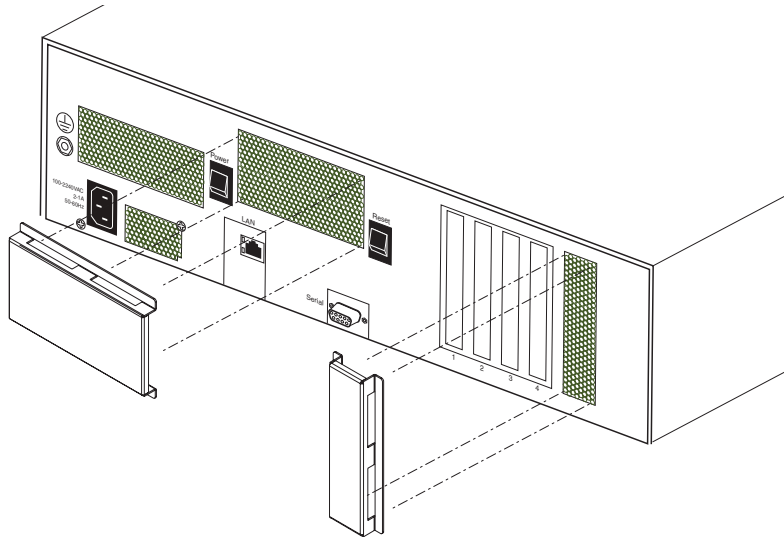


Attaching the FIPS 140-2 tamper-evident shields to the Nortel VPN Router 2700

To attach the tamper-evident shields to the Nortel VPN Router 2700 chassis air vents, complete the following:

- 1 Remove the protective paper from the adhesive strips affixed to the flanges of the tamper-evident shields.
- 2 Align the flanges to the chassis surface surrounding the air vents found on the back of the chassis as shown in [Figure 9](#). Ensure the flanges do not cover the air vents.
- 3 Press firmly on the tamper-evident shield to ensure a secure attachment to the chassis.

Figure 9 Attaching FIPS 140-2 tamper-evident shields to the Nortel VPN Router 2700

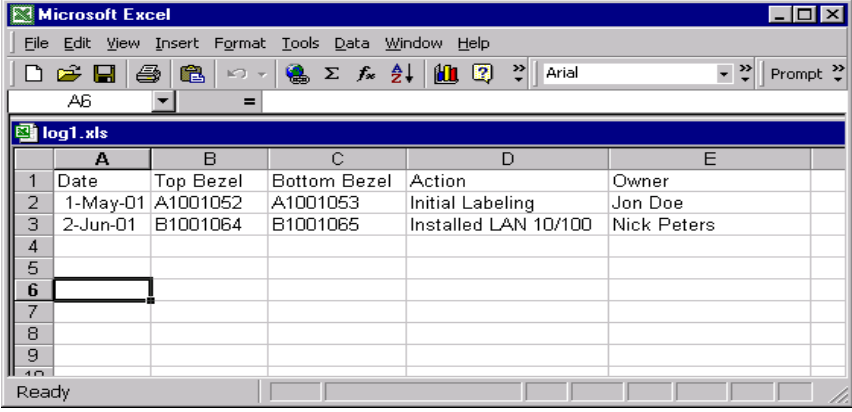


Monitoring and controlling FIPS labels

After you configure the Nortel VPN Router for FIPS mode with the tamper-evident labels and shields in place, the Nortel VPN Router cannot be accessed without signs of tampering or intrusion. For this reason, all access to the FIPS-compliant system must be documented.

A log can identify the date, access area, reason for access, and the person who accessed the system. [Figure 10](#) shows an example of how the FIPS administrator could use Microsoft® Excel to document, monitor, and control use of the FIPS tamper-evident labels to maintain security for a Nortel VPN Router.

Figure 10 Sample log for monitoring and controlling FIPS labels



	A	B	C	D	E
1	Date	Top Bezel	Bottom Bezel	Action	Owner
2	1-May-01	A1001052	A1001053	Initial Labeling	Jon Doe
3	2-Jun-01	B1001064	B1001065	Installed LAN 10/100	Nick Peters
4					
5					
6					
7					
8					
9					
10					



Note: If you have more than one Nortel VPN Router, add a line at the top of the log to identify the gateway by its model and serial number.

[Table 3](#) defines the terms used in the sample log shown in [Figure 10](#) on page 45.

Table 3 Definitions of sample log terms

Term	Definition
Date	Date that the system was accessed
Top bezel	Top bezel labels (2 places)
Bottom bezel	Bottom bezel labels (2 places)

Table 3 Definitions of sample log terms (continued)

Term	Definition
A1001052, A1001053, B1001064, B1001065	Unique numbers assigned to each label
Action	Reason the system was accessed
Owner	Name of the person accessing the system

Chapter 3

Enabling and disabling FIPS mode

The Nortel VPN Router can run in normal operating mode or in FIPS operating mode. In FIPS operating mode, the Nortel VPN Router meets all Level 2 requirements for FIPS 140-2. (You can find FIPS 140-2 publications and related information at the <http://csrc.nist.gov/cryptval/> URL. For the list of Nortel security policies, click on Validation Lists in the left column of the page.)



Note: Before you enable FIPS mode, apply the tamper-evident labels and the o the Nortel VPN Router gateway as described in [Chapter 2](#), “Physically securing the Nortel VPN Router,” on page 33.

This chapter contains the following topics:

Topic	Page
Changes enforced by FIPS mode	48
Enabling FIPS mode using the command line interface	49
Disabling FIPS mode using the command line interface	51
Health Check (FIPS)	53
Security log	54

Changes enforced by FIPS mode

Changing a FIPS mode, from enabled to disabled or disabled to enabled, resets the Nortel VPN Router to the factory default configuration and all connectivity to the NVR is lost. As well, all data that you configured prior to changing a FIPS mode is completely wiped from disk memory. Nortel recommends that you use the Command Line Interface through the console port whenever changing the FIPS mode. After the reset a simple configuration allows you to access the management interface for further configuration..



Caution: Changing FIPS modes causes a loss of all configuration data stored in non-volatile memory (disk) and resets the Nortel VPN Router to factory default configuration. Nortel recommends that you use the Command Line Interface through the console port whenever changing FIPS modes.

The following changes are strongly recommended:

Table 4 Disabling authentication methods by protocol (FIPS mode)

Protocol	Authentication methods for FIPS mode
IPsec	MD5 is not an approved FIPS algorithm. (For example, you can select Triple DES with SHA1 integrity, but <i>not</i> Triple DES with MD5 integrity.) On the Services, IPsec Settings screen, deselect any encryption option with MD5 as the integrity option.
L2F	You cannot enable CHAP. On the Services, L2F Settings screen, disable (uncheck) the CHAP option and click on OK.
L2TP	You cannot enable MS-CHAP, CHAP, or RC4 encryption. On the Services, L2TP Settings screen, disable (uncheck) MS-CHAP, CHAP, RC4-128, and RC4-40 and click on OK.
OSPF	MD5 is not an approved FIPS algorithm. To change the OSPF authentication type, choose Routing, Interfaces, then click on the Configure button next to OSPF. On the Configure OSPF screen, change the Authentication option from MD5 to None or Simple.
PPTP	You cannot enable MS-CHAP, CHAP, or RC4 encryption. On the Services, PPTP Settings screen, disable (uncheck) MS-CHAP, CHAP, RC4-128, and RC4-40 and click on OK.
RIP	MD5 is not an approved FIPS algorithm. To change the RIP authentication type, choose Routing, Interfaces, then click on the Configure button next to RIP. On the Configure RIP screen, change the Authentication option from MD5 to None or Simple.

- Change the default administrator password on the gateway.
- Disable all management protocols other than HTTPS—for example, HTTP and SNMP—over private non-tunneled interfaces. (NIST permits the use of HTTPS over a private non-tunneled interface.)

To disable management protocols, choose **Services, Available** and deselect the protocols.



Note: After you disable HTTP, you can manage the gateway using an IPsec tunnel or using an HTTPS connection over a private non-tunneled interface.

Enabling FIPS mode using the command line interface

Enabling FIPS mode resets the Nortel VPN Router to the factory default configuration and all connectivity to the NVR is lost. As well, all data that you configured prior to changing a FIPS mode is completely wiped from disk memory. Nortel recommends that you use the Command Line Interface through the console port whenever changing the FIPS mode. After the reset a simple configuration allows you to access the management interface for further configuration..



Caution: Changing FIPS modes causes a loss of all configuration data stored in non-volatile memory (disk) and resets the Nortel VPN Router to factory default configuration. Nortel recommends that you use the Command Line Interface through the console port whenever changing FIPS modes.

To enable FIPS mode:

- 1 Access the command line interface in one of two ways:
 - Connect a terminal or PC to the serial port on the gateway. From the Serial Port menu, enter **L** to access the command line interface.
 - Establish a Telnet session with the gateway's management IP address.

- 2 At the Login prompt, log in to the gateway using an account with administrator privileges, for example:

```
Login: admin
Password: <password>
CES>
```

- 3 At the User mode prompt (CES>), go to Privileged EXEC mode and then to Global Configuration mode.

```
CES> enable
Password: <password>
CES# configure terminal
CES(config)#
```

- 4 Enter the **fips enable** command.

```
CES(config)# fips enable
```

To be FIPS compliant, you must be running a FIPS certified software version and be protected by FIPS tamper proof labels. FIPS kits, which include full instructions on how to be FIPS compliant, are available from Nortel Networks sales and resellers. A list of switch hardware models and software versions that have been FIPS certified is available from Nortel Networks and from the US Government NIST Web site.

Enabling FIPS will initiate a reset to the factory default configuration.

Do you want to proceed? [no]:

- 5 Type **yes** (or **y**) and press Return.

```
Please wait. System will reboot.
CES(config)#
```

```
Your connection has been terminated
```

After the Nortel VPN Router gateway reboots, FIPS is enabled and the gateway runs in FIPS mode.



Note: Telnet is automatically disabled on the private interface when you enable FIPS. You can use Telnet to access the command line interface only after you connect to the gateway over a secure tunnel. You can still access the command line interface using the serial port.

Disabling FIPS mode using the command line interface

Disabling FIPS mode resets the Nortel VPN Router to the factory default configuration and all connectivity to the NVR is lost. As well, all data that you configured prior to changing a FIPS mode is completely wiped from disk memory. Nortel recommends that you use the Command Line Interface through the console port whenever changing the FIPS mode. After the reset a simple configuration allows you to access the management interface for further configuration..



Caution: Changing FIPS modes causes a loss of all configuration data stored in non-volatile memory (disk) and resets the Nortel VPN Router to factory default configuration. Nortel recommends that you use the Command Line Interface through the console port whenever changing FIPS modes.



Caution: Upgrade and Downgrade: Because of the changes now enforced by FIPS mode at 7.05.100, when upgrading or downgrading a FIPS enabled NVR, ensure that FIPS mode remains enabled through the entire process. Perform any upgrades or downgrades through a control tunnel with FIPS enabled to ensure that the FIPS enabled configuration remains intact and to avoid the scenario where changing FIPS mode now forces a factory default of the unit

To disable FIPS mode:

- 1 Access the command line interface in one of two ways:
 - Connect a terminal or PC to the serial port on the gateway. From the Serial Port menu, enter **L** to access the command line interface.
 - Establish a Telnet session with the gateway's management IP address.



Note: After you enable FIPS mode, you can use Telnet only after you connect to the gateway over a secure tunnel.

- 2 At the Login prompt, log in to the gateway using an account with administrator privileges, for example:

```
Login: admin
Password: <password>
CES>
```

- 3 At the User mode prompt (CES>), go to Privileged EXEC mode and then to Global Configuration mode.

```
CES> enable
Password: <password>
CES# configure terminal
CES(config)#
```

- 4 Enter the **no fips** command.

```
CES(config)# no fips
Disabling FIPS will initiate a reset to the factory
default configuration.
Do you want to proceed? [no]:
```

- 5 Type **yes** (or **y**) and press Return.

```
Please wait. System will reboot.
CES(config)#
```

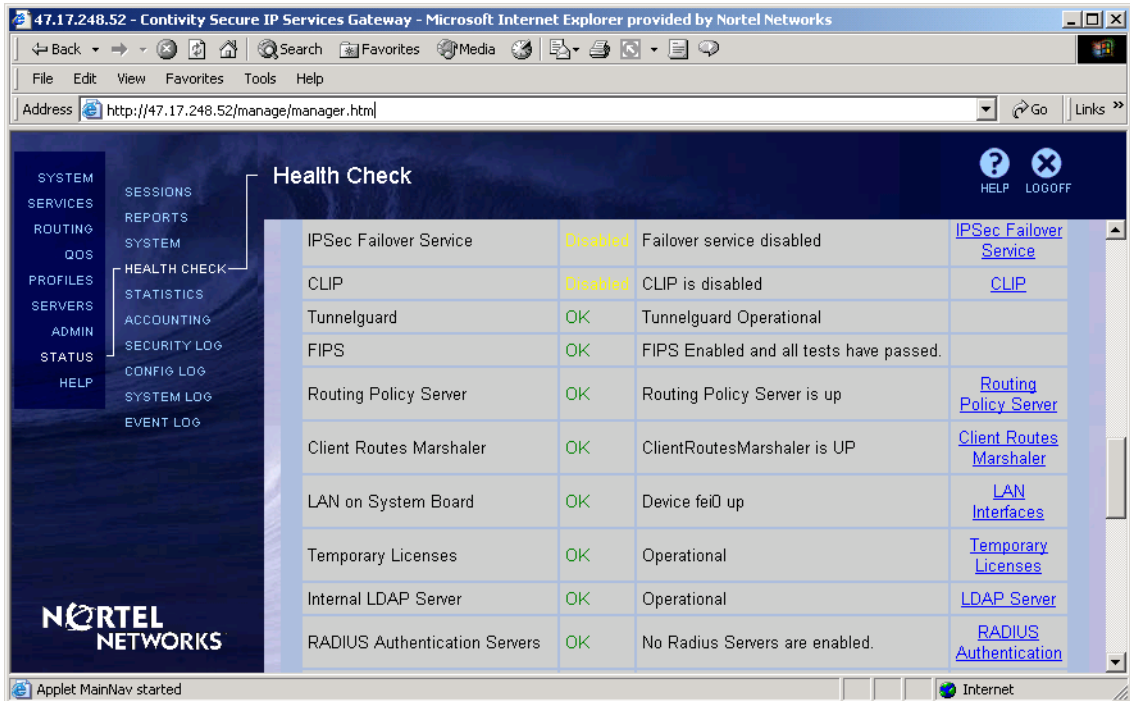
```
Your connection has been terminated.
```

After the gateway reboots, FIPS is disabled and the gateway runs in normal operating mode. You can reenables FTP, Telnet, and other protocols and services that are not FIPS compliant (see [“Changes enforced by FIPS mode” on page 48](#)).

Health Check (FIPS)

A FIPS status entry appears on the Status, Health Check screen (Figure 11).

Figure 11 Health Check screen



The cause of an unhealthy Health Check status can be determined by consulting the gateway's event log or system log. Note that the Health Check page has an audible alarm enable feature.

FIPS Health Check status messages

The Health Check screen displays the results of test/self-test functions. SNMP traps are sent based on FIPS warnings or failures. An SNMP trap is sufficient notification according to FIPS requirements for a failed self-test. [Table 5](#) lists the FIPS Health Check status messages.

Table 5 FIPS Health Check status messages

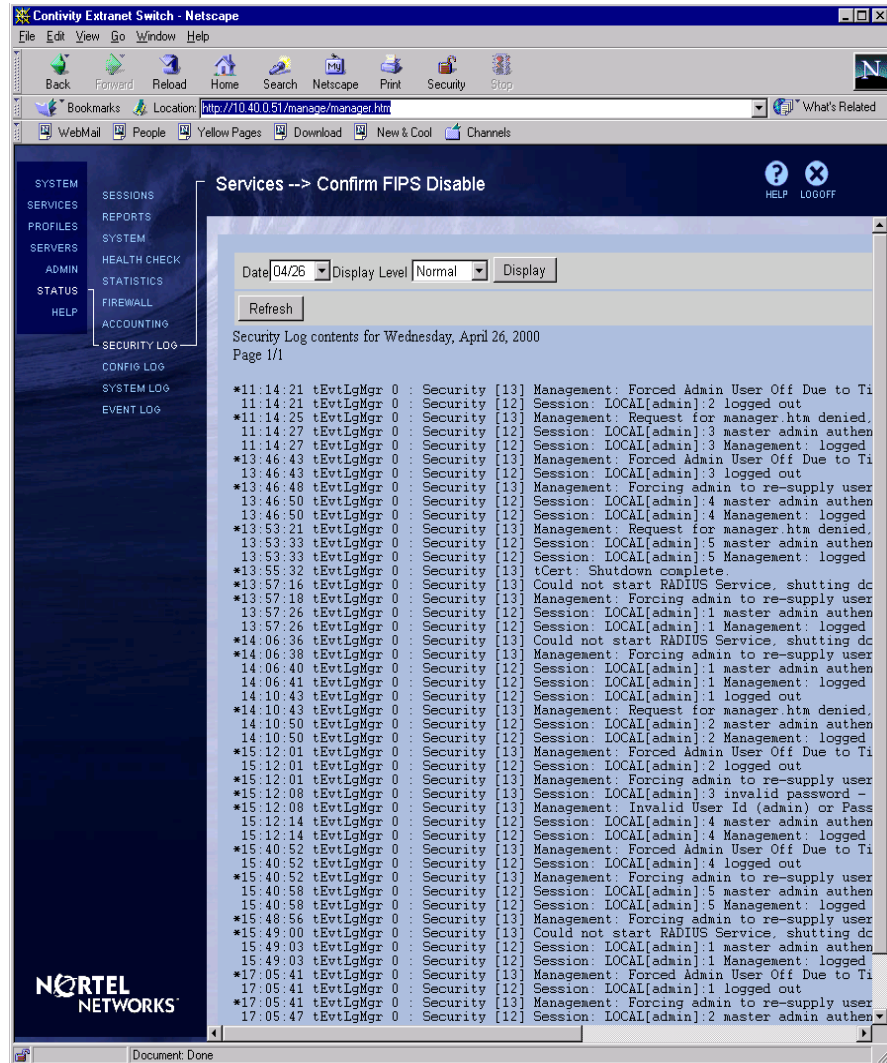
Health Check status (Healthy/Warning/Alert)	Description
Healthy	FIPS: Disabled
Healthy	FIPS: Enabled and all tests passed
Warning	FIPS: Random generator test failed
Warning	FIPS: DES MAC check on executables Failed
Warning	FIPS: DES KAT Test Failed
Warning	FIPS: SHA1 Self Test Failed
Alert	FIPS: Status not known

Security log

The Security log records all activity about system or user security. The Security log shown in [Figure 12 on page 55](#) lists all security events, both failures and successes. The events can include authentication and authorization events, such as:

- Tunnel or administration requests
- Encryption, authentication, or compression
- Hours of access
- Number of session violations
- Communications with servers
- LDAP
- RADIUS
- FIPS messages

Figure 12 Security log screen



Index

A

- acronyms 13
- administrator login, Nortel VPN Router
 - changing default password 49
 - default 24
- advanced routing license 31
- authentication of users, role-based 23

C

- certificates, used by Nortel VPN Router 30
- checksum tests 31
- command line interface
 - disabling FIPS mode 52
 - enabling FIPS mode 49
- compliance levels, FIPS 20
- components list, FIPS kit 34
- continuous random number generator test 31
- control input interfaces, FIPS 22
- conventions, text 12
- critical security parameters (CSPs) 28
- Crypto Officer
 - role defined 23
 - services 24
- cryptographic keys, Nortel VPN Router 28
- CSP (critical security parameter) 28

D

- data input interfaces, FIPS 22
- data output interfaces, FIPS 22
- Derived Test Requirements (DTR) 20

- DES MAC integrity check 31
- DES password keys, described 29
- Diffie-Hellman keys, described 29
- DTR (Derived Test Requirements) 20

E

- encryption accelerator card 21
- error states 32
- event log, Nortel VPN Router 54

F

- FIPS 140-2
 - defined 20
 - key management 28
 - levels of compliance 20
 - logical interfaces mapped to Nortel VPN Router
 - physical interfaces 22
 - Nortel VPN Router platforms certified under 20
 - role-based authentication of users 23
 - self-tests 31, 54
- FIPS 140-2 Derived Test Requirements 20
- fips enable** command 50
- FIPS kit components 34
- FIPS labels. *See* tamper-evident labels
- FIPS mode
 - defined 47
 - disabling
 - using command line interface 52
 - displayed in Health Check 53
 - enabling
 - using command line interface 49
- FIPS operating mode. *See* FIPS mode

FIPS security kit components 34

Firewall, Nortel VPN Router Stateful 31

H

hardware encryption accelerator card 21

hardware interfaces

 Nortel VPN Router 21

 Nortel VPN Router physical mapped to FIPS
 logical 22

Health Check 53

HTTP (Hypertext Transfer Protocol), disabling 49

I

integrity tests, software 31

interfaces

 FIPS logical 22

 Nortel VPN Router physical 21

IPsec

 described 25

 disabling authentication methods for FIPS mode
 48

 options available in FIPS mode 26

K

KATs (known answer tests) 31

key management for FIPS compliance 28

keys, cryptographic

 DES password 29

 Diffie-Hellman 29

 pre-shared 29

 RSA 29

 session 28

keys, license 31

kit, FIPS, contents 34

known answer tests (KATs) 31

L

L2F

 described 27

 disabling authentication methods for FIPS mode
 48

 options available in FIPS mode 27

L2TP

 described 26

 disabling authentication methods for FIPS mode
 48

 options available in FIPS mode 26

labels, tamper-evident. *See* tamper-evident labels

LDAP (Lightweight Directory Access Protocol) 23

levels of compliance for FIPS 140-2 20

license keys

 advanced routing 31

 firewall 31

Lightweight Directory Access Protocol (LDAP) 23

log for tamper-evident labels 45

log, security 54

login ID, default for Nortel VPN Router
 administrator 24

M

management protocols, disabling on private
 interfaces 49

MD5 authentication

 IPsec 48

 RIP and OSPF 48

N

National Institute of Standards and Technology
 (NIST) 20

National Voluntary Laboratory Accreditation
 Program (NVLAP) 20

NIST (National Institute of Standards and
 Technology) 20

no fips command 52

normal operating mode 47

Nortel VPN Router

 administrator login 24

- applying tamper-evident labels 33
- certificates 30
- certified for FIPS 140-2 20
- cryptographic keys 28
- disabling FIPS mode 51
- hardware encryption accelerator card 21
- hardware interfaces 21
- license keys 31
- operating modes 47
- physical interfaces mapped to FIPS logical interfaces 22
- See also* Nortel VPN Router
- user passwords 28
- Nortel VPN Router 1700, 1750 2700, and 2750
 - See also* Nortel VPN Router
- Nortel VPN Router 1700, 1750, 2700 and 2750
 - applying tamper-evident labels 38
- Nortel VPN Router 5000
 - applying tamper-evident labels 39
 - See also* Nortel VPN Router
- Nortel VPN Router 600
 - applying tamper-evident labels 36
- Nortel VPN Router Stateful Firewall 31
- NVLAP (National Voluntary Laboratory Accreditation Program) 20

O

- operating modes, Nortel VPN Router 47
- OSPF (Open Shortest Path First), disabling MD5 authentication 48

P

- PAP (Password Authentication Protocol) 28
- passwords
 - Nortel VPN Router administrator 24, 49
 - user 28
- power interfaces, FIPS 22
- PPTP
 - described 26

- disabling authentication methods for FIPS mode
 - 48
 - options available in FIPS mode 26
- pre-shared keys, described 29
- processor card 21
- pseudo-random number generator test 31
- publications
 - hard copy 15
 - related 14

R

- random number generator test 31
- RIP (Routing Information Protocol), disabling MD5 authentication 48
- role-based authentication of users 23
- routing, advanced 31
- RSA certificates 30
- RSA keys, described 29

S

- security kit for FIPS, contents 34
- security log, Nortel VPN Router 54
- security parameters 28
- self-tests, FIPS
 - described 31
 - results displayed in Health Check screen 54
- services
 - Crypto Officer 24
 - User 25
- session keys, described 28
- SNMP (Simple Network Management Protocol), disabling 49
- SNMP traps 54
- software integrity tests 31
- status messages, FIPS 54
- status output interfaces, FIPS 22

T

tamper-evident labels

- applying to the hardware

 - Nortel VPN Router 5000 39

 - Nortel VPN Router 600 36

 - Nortel VPN Router, 1700, 1750, 2700 and
2750 38

- described 35

- obtaining additional 36

- tracking 36, 45

- usage notes 36

technical publications 15

text conventions 12

traps, SNMP 54

U

User (FIPS)

- role defined 23

- services 25

user passwords 28

X

X.509 certificates 30