Nortel Networks™ Contivity™ 600

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 2 Validation

March 2002

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic module security policy for the Nortel Networks Contivity 600. This security policy describes how the Contivity 600 meets the security requirements of FIPS 140-1, and how to operate the Contivity 600 in a secure FIPS 140-1 compliant mode of operation. This policy was prepared as part of the FIPS 140-1 level 2 certification of the Contivity 600.

FIPS 140-1 ("Federal Information Processing Standards Publication 140-1 -- *Security Requirements for Cryptographic Modules"*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST web site at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of the Contivity 600 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Contivity 600 and the entire line of Contivity™ products from the following sources:

- The Nortel Networks web site contains information on the full line of Contivity products at www.nortelnetworks.com.
- For answers to technical or sales related questions please refer to the contacts listed on the Nortel Networks web site at www.nortelnetworks.com.

1.3 Document Organization

This document is part of the complete FIPS 140-1 submission package. In addition to this document, the complete submission package contains the following:

- Vendor Evidence Document
- Finite State Machine
- Source code listing
- Other supporting documentation

This document provides an overview of the Contivity 600 and explains the secure configuration and operation of the module. Section 1 provides introductory material, section 2 details the general features and functionality of the Contivity 600 and section 3 addresses configuration of the switch for FIPS-compliant mode of operation, henceforth referred to as FIPS mode.

Corsec Security, Inc. produced this security policy and other certification submission documentation under contract to Nortel Networks. With the exception of this non-proprietary security policy, the FIPS 140-1 certification submission documentation is Nortel-proprietary

and is releasable only under appropriate non-disclosure agreements. Please contact Nortel Networks for access to these documents.

2 The Contivity 600

The Nortel Networks Contivity 600 (referred to as the module, the 600, or Switch in this document) is a scalable, secure, manageable remote access server that meets FIPS 140-1 level 2 requirements. The following sections describe how the Switch addresses FIPS 140-1 requirements.

2.1 Cryptographic Module

The cryptographic boundary for the Contivity 600 includes the entire module. The Contivity 600 combines remote access protocols, security, authentication, authorization, and encryption technologies in a single solution. The Switch can support up to 30 simultaneous user sessions, allowing each user to exercise a variety of secure services. The Switch supports a number of secure network-layer and data-link-layer protocols including Internet Protocol Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), and Layer Two Forwarding (L2F). The architecture for the Switch is user-centric, where an individual user or group of users can be associated with a set of attributes that provide custom access to the Extranet. In effect, you can create a personalized extranet based on the specific needs of a user or group. The unique Quality of Service (QoS) features include call administration and packet forwarding priorities, and support for Resource ReSerVation Protocol (RSVP).

2.2 Module Interfaces

The interfaces for the Switch are located on the rear panel as shown in 1.

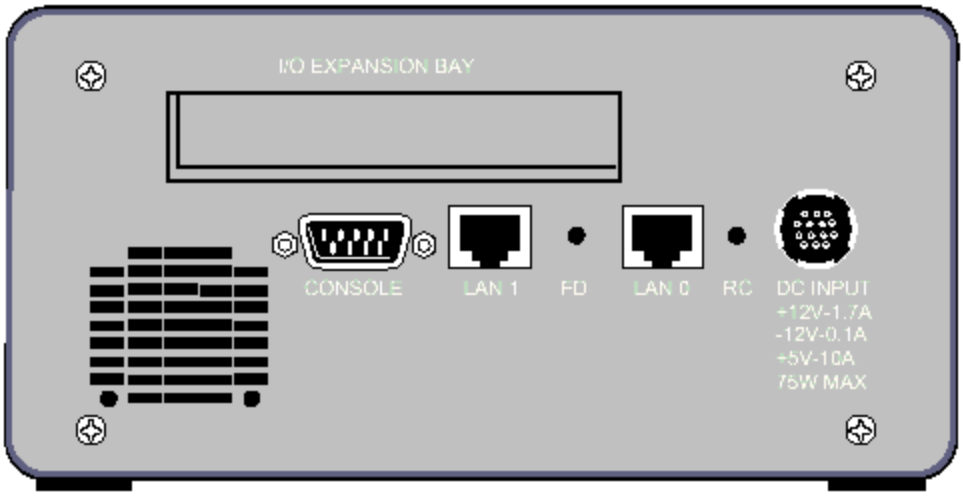

Figure 1 – Physical Interfaces

The physical interfaces include a power input, RC (recovery) switch, a serial port, two 10/100BASE-TX LAN ports, and an optional I/O Expansion Bay. More information on the LAN Port interface can be found in Chapter 2 of *Getting Started with the Contivity 600*.

More information on the RC switch can be found in Chapter 4 of *Getting Started with the Contivity 600*.

Figure 2 - Front Nozzle Lights

Figure 2 shows the front panel of the Switch, including display lights that provide general status information about the switches current state.

- The **Power LED** is green when DC power is supplied to the unit.
- The **Alert LED** is set to red by the Contivity software to indicate a serious condition. This LED indicates the Health Check status that is described in Health Check reports.
- The **Attention LED** displays yellow to indicate a software attention condition.
- The **Ready LED** displays green to indicate the box has reached a state of readiness.
- The **Boot LED** displays yellow after power is applied. Yellow indicates a boot in process/non-ready state. When both the **Boot** and the **Ready LED** are lit at the same time, this indicates that the unit has entered recovery mode.

The above listed physical interfaces, including the LAN ports, serial port, status LEDs, and RC switch map to the logical interfaces defined in FIPS 140-1 as described in Table 1.

Switch physical interface	FIPS 140-1 Logical Interface
10/100BASE-TX LAN Ports	Data Input Interface
10/100BASE-TX LAN Ports	Data Output Interface
RC Switch Serial Port, 10/100BASE-TX LAN Ports	Control Input Interface
Serial Port Front Panel LEDs	Status Output Interface
Power Plug	Power Interface

Table 1 – FIPS 140-1 Logical Interfaces

2.3 Physical Security

A thick steel case protects the Contivity 600. The Contivity meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for business use (Class A). The case may be removed to allow access to the motherboard, memory, expansion slots, and hard drive. This can be accomplished by:

1. Unscrewing each of the four screws on the bottom of the Switch (see Figure 3)
2. Pulling the cover forward while sliding the rear panel backward (see Figure 4).

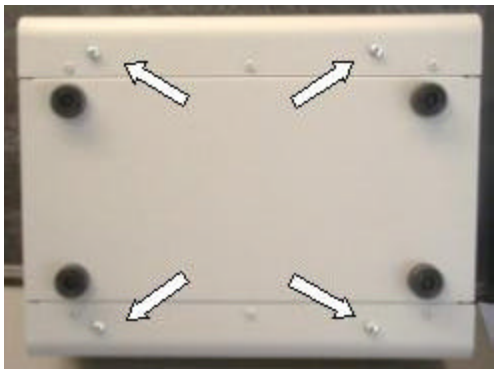

Figure 3

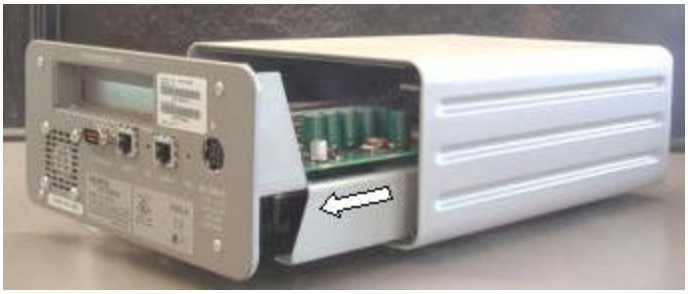

Figure 4

Once the Extranet Switch has been configured in its FIPS 140-1 level 2 mode, the cover may not be removed without signs of tampering. To seal the cover, apply a serialized tamper-evident label as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper-evident label. Alcohol based cleaning pads are recommended for this purpose. The temperature of the switch should be above 10°C.
2. Apply a label on the top overlapping the rear panel as shown in Figure 5.
3. Record the serial numbers of the label applied to the module.
4. Allow 24 hours for the adhesive in the tamper-evident seal to completely cure.

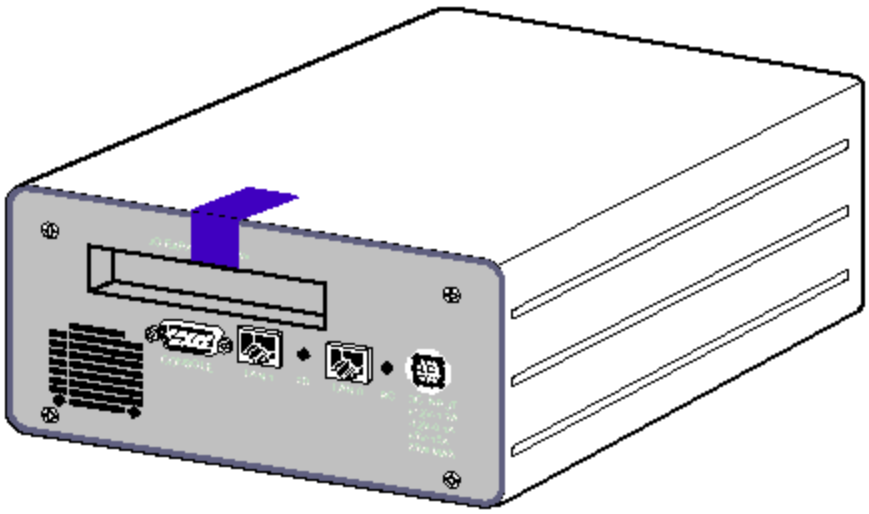

Figure 5 – Tamper-Evident Label

The tamper-evident seal is produced from a special thin gauge white vinyl with self-adhesive backing. Any attempt to open the switch will damage or destroy the tamper-evident seal or the painted surface and metal of the module cover. Since the tamper-evident label has non-repeated serial numbers, the label may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. An intact label is shown in Figure 6, with a visible serial number and no breaks.

Figure 6 – Tamper-Evident Label

Attempting to remove a label breaks it or continually tears off small fragments as depicted in Figure 7. Other signs of tamper-evidence include a strong smell of organic solvents, warped or bent cover metal, and scratches in the paint on the module.

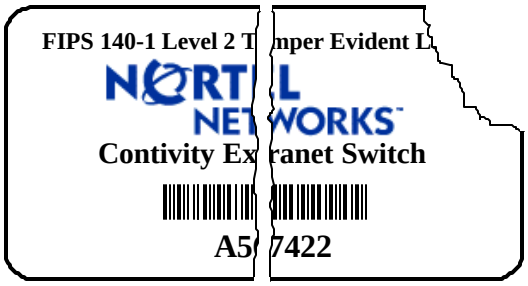

Figure 7 – Damaged Tamper-Evident Label

2.4 Roles and Services

The switch supports up to 30 simultaneous user sessions using Internet Protocol Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), and Layer Two Forwarding (L2F). In addition, an administrator may securely configure the switch either locally or remotely. Remote administration is secured by one of the secure tunneling protocols supported by the box. The administrator selects which protocols are used from the Services-Available menu.

The Switch employs identity-based authentication of users, and stores user identity information in an internal Lightweight Directory Access Protocol (LDAP) database. Authentication can optionally be performed against a variety of external servers using LDAP or Remote Authentication Dial-In User Service (RADIUS), including Novell NDS, Microsoft Windows NT Domains, Security Dynamics ACE Server, and Axent OmniGuard Defender.

Service	Crypto Officer	User
Configure the Switch	✓	
Create User Groups	✓	
Create Users	✓	
Modify User Groups	✓	
Modify Users	✓	
Delete User Groups	✓	
Delete Users	✓	
Define Rules and Filters	✓	
Status Functions	✓	
Self-test Functions	✓	
Manage the Switch	✓	
Encrypted Traffic	✓	✓
Bypassed Traffic	✓	✓
Change Password	✓	✓

Table 2 – Matrix of Services

Users may assume one of two roles: Crypto Officer role or User role. An administrator of the switch assumes the Crypto Officer role to configure and maintain the switch. The Crypto Officer role may have the following rights:

- Switch management rights: (*none*, *view switch*, or *manage switch*). *View switch* permits an administrator to view all the configuration and status information on the switch. *Manage switch* permits an administrator to configure the switch and change critical settings.

- User management rights: (*none*, *view users*, or *manage users*). *View users* permits an administrator to review all user accounts and settings on the switch. *Manage users* rights allows an administrator to create, modify, and delete users.

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

- *Initiate IPSec Protocol Tunnels*
- *Initiate PPTP Protocol Tunnels*
- *Initiate L2TP Protocol Tunnels*
- *Initiate L2F Protocol Tunnels*
- *Change Password*

2.4.1 Crypto Officer Services

There is a factory default login ID and password, which allows access to the Crypto Officer role. This initial account is the primary administrator's account for the Switch, and guarantees that at least one account is able to assume the Crypto Officer role and completely manage the switch and users. The switch can also be configured to authenticate based on RSA digital signatures. An administrator of the switch may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional administrators. Each administrator would have a separate ID and password. Administrators may always access the switch and authenticate themselves via the serial port. They may also authenticate as a User over a secure tunnel (i.e., a LAN connection using either the IPSec, PPTP, or L2TP protocols with encryption) for secure communications and then authenticate to the switch as a Crypto Officer in order to manage the switch. In FIPS mode, only the IPSec protocol with DES or Triple DES encryption is used to create a secure tunnel. An administrator can also configure the switch to allow or disallow management via a private LAN interface, without using a secure tunnel. Initially the default configuration allows HTTP management on the private LAN interface of the Switch without requiring a secure tunnel.

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

- **Configure the Switch**: to define network interfaces and settings, set the protocols the switch will support, define routing tables, set system date and time, load authentication information, etc.
- **Create User Groups**: to 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 create, edit and delete User Groups, which effectively defines the permission sets for a number of Users.
- **Create Users**: to define User accounts and assign them permissions using User Groups. Every User may be assigned a separate ID and password for IPSec, PPTP, L2TP, and L2F, which allow access to the User roles. Additionally, an account may be assigned an Administration ID, allowing access to the Crypto Officer role. Each Administrator ID is assigned rights to manage the Switch (either

none, *view switch*, or *manage switch*) and rights to manage users (either *none*, *view users*, or *manage users*). Administrators can create, edit and delete Users, which effectively defines the profiles for each User.

- **Define Rules and Filters**: to create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction. The administrator may use any of the pre-defined Rules or create custom Rules to be included in each Filter.
- **Status Functions**: to view the switch configuration, routing tables, active sessions, use Gets to view SNMP MIB II statistics, usage graphs, health, temperature, memory status, voltage, packet statistics, and review accounting logs.
- **Manage the Switch**: to log off users, shut down or reset the switch, disable or enable audible alarms, manually back up switch configurations, restore switch configurations, create a virtual recovery diskette, run self-tests, etc.

A complete description of all the management and configuration capabilities of the Contivity Extranet switch can be found in the *Contivity Extranet Switch Administrator's Guide* and in the online help for the switch.

2.4.2 User Services

An administrator (who has *manage users* rights) assigns each User a name and a User Group. The User Group defines access limitations and services that the User may exercise, including access hours, call admission priority, forwarding priority, number of simultaneous logins, maximum password age, minimum password length, whether passwords may contain only alphabetic characters, whether static IP addresses are assigned, idle timeout, forced logoff for timeout, filters, and whether Internetwork Packet Exchange (IPX) is allowed.

The administrator also assigns each user separate User IDs and passwords for the following services: IPSec, PPTP, L2TP, and L2F tunnels (a fifth ID and password may be assigned for the optional creation of a second Crypto-Officer role for Administration of the switch, which would then have the services available to it as described in 2.4.1.). The User may then authenticate as necessary to initiate secure tunnels using any of these services.

- IPSec: Requires authentication through User Name and Password. This authenticates the User to the switch and is protected using Internet Key Exchange (IKE)/Internet Security Association Key Management Protocol (ISAKMP). Security options for IPSec include using an Encapsulated Security Payload (ESP) with Triple-DES, Data Encryption Standard (DES), or "40-bit DES" for encryption of data. Security options also include using an Authentication Header (AH) with Message Authentication Code Secure Hash Algorithm (HMAC SHA-1) or HMAC 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 Triple DES ESP, DES ESP, and HMAC SHA-1 AH options are enabled.

- PPTP: Requires authentication using Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP), Challenge Handshake Authentication Protocol (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.
- 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.
- 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.

These four protocols (L2TP, L2F, PPTP, and IPSec) are industry standard protocols used for creating secure tunnels. Full explanations of the protocols are beyond the scope of the security policy. However, the following sources will provide additional information on each of the tunneling protocols described above:

IPSec: The IETF website http://www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html provides links to all Internet RFCs that comprise the IPSec standards.

PPTP: Details on PPTP can be found at http://infodeli.3com.com/infodeli/tools/remote/general/pptp/draft-00.pdf. Although this is classified as an Internet draft, it was never registered with the IETF.

L2TP: This protocol is specified in the Internet Request for Comment (RFC) 2661. More information can be found at http://www.ietf.org/rfc/rfc2661.txt?number=2661.

L2F: This protocol is specified in Internet RFC 2341. More information can be found at http://www.ietf.org/rfc/rfc2341.txt?number=2341.

More information on the authentication protocols can be found in Internet RFCs 2433 and 2759.

2.5 Key Management

There are five types of critical security parameters (CSPs) in the Contivity Switch: passwords, secret keys, private keys, public keys, and certificates. All passwords are created by the Crypto Officer and stored in the internal LDAP database encrypted with DES. User passwords can be destroyed by the Crypto Officer or by Users overwriting their own passwords. These passwords are used for authentication purposes and never released. The details of their use are governed by the protocol and mechanism by which an operator is attempting authentication to the switch. (Crypto Officers should be aware that PAP transmits password information in the clear and should not be enabled before deciding local policy. See notes on PAP in the *Contivity Extranet Switch Administrator's Guide*.)

- Session Keys: These ephemeral secret keys are created using the switch's pseudo-random number generator for protocols like 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 switch with their ID and password. The keys are temporarily stored in memory during a tunnel session and 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 DES or Triple DES encryption is used to create a secure tunnel.

- Pre-shared Keys: These ephemeral secret keys are internally derived for protocols like MS-CHAP and ISAKMP. The keys are used for authentication purposes with the hashing and encryption services to setup Security Associations (SAs) between the switch and an operator. The keys are temporarily stored in memory during a tunnel session and 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 DES or Triple DES encryption and HMAC SHA-1 are used to create a secure tunnel.

- Diffie-Hellman Keys: These ephemeral public/private key-pairs are used with protocols like ISAKMP to derive pre-shared secret keys during tunneling sessions. These keys are internally generated using the switch'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 switch's code and can be zeroized using the Recovery (RC) switch located on the rear of the module. In order to zeroize this key, the Crypto-Officer must select the format option from

the module's management interface and then depress the RC switch. The format utility then causes the firmware to be erased, effectively zeroizing the key.

- RSA Keys: These public/private key-pairs are used for generating and verifying digital signatures for authentication of users during tunneling sessions. The switch'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 while the public key is output to obtain a certificate from a third party Certification Authority (CA).

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

2.6 Self-tests

It is important to test the cryptographic components of a security module to insure all components are functioning correctly. The Contivity Switch includes an array of self-tests that are run during startup and periodically during operations. The self-tests run at power-up include a cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms implemented in both Hardware and Software (DES, 3DES), on the message digest (SHA-1), and on signatures (RSA with SHA-1). Additional self-tests performed at startup include software integrity tests using a DES MAC per FIPS 113 and a continuous random number generator test. Other tests are run periodically or conditionally such as a software load test for FIPS-approved upgrades using a DES MAC and the continuous random number generator test. In addition, there are checksum tests on the flash memory that are updated with flash changes.

If any of these self-test fail the switch will transition into an error state. Within the error state, all secure data transmission is halted and the switch outputs status information indicating the failure.

3 Secure Operation of the Contivity 600

The Contivity Switch is a versatile machine; it can be run in a Normal Operating Mode or a FIPS Operating Mode. In FIPS operating mode, the switch meets all the level 2 requirements for FIPS 140-1. To place the module in FIPS mode, click the "FIPS Enabled" button on the Services Available management screen and restart the module. A number of configuration settings are recommended when operating the Contivity Switch in a FIPS 140-1 compliant manner. Other changes are required in order to maintain compliance with FIPS 140-1 requirements. These include the following:

Recommended

- Change the default administrator password on the switch.
- Disable all management protocols over private non-tunneled interfaces

Required

- Select the "FIPS Enabled" button on the Service Available Management screens and restart the module.
- Apply the tamper evident label as described in section 2.3
- Disable cryptographic services that employ non-FIPS approved algorithms.
    - For IPSec: When operating the device in a FIPS 140-1 compliant manner, only the Triple DES ESP, DES ESP, and HMAC SHA-1 AH may be enabled.
    - For PPTP, L2TP, and L2F: When operated in a FIPS 140-1 compliant manner, MS-CHAP and CHAP are not enabled with RC4 encryption. MD5 must be disabled and SHA-1 is enabled.
    - The internal LDAP database must be used in place of an external LDAP server.
    - Secure Sockets Layer (SSL) cannot be used to establish secure connections
    - For Routing Information Protocol (RIP) – In FIPS mode, MD5 must be disabled.

There are several services that are affected by transitioning the module into FIPS compliant mode. When the module is restarted in FIPS mode, several administrative services accessing the shell, including the debugging scripts, are disabled. When the module is in FIPS mode, the administrator is given additional authority to reset the default administrator's password and username. The integrated firewall program, by Checkpoint, and the restore capabilities are disabled during FIPS mode. The FTP demon is also turned off, preventing any outside intruder from FTPing into the server. In order to transition the mode out of FIPS mode, the FIPS disable button, on the Services Available management screen, must be clicked and the module must be restarted.

When transitioning the module from Non-FIPS mode to FIPS mode, the Crypto Officer should ensure that the module is running only the Nortel supplied, FIPS 140-1 validated firmware. If there is a concern that the firmware has been modified during operation in

Non-FIPS mode (This might be done by an unauthenticated malicious remote user who has the capability to submit shell commands) then the Crypto Officer should reinstall the Nortel firmware from a trusted media such as the installation CD or the Nortel website.