NORTEL NETWORKS

Contivity™ Extranet Switch 4600

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 2 Validation

June 2001

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic module security policy for the Contivity™ Extranet Switch 4600. This security policy describes how the Contivity™ Extranet Switch 4600 meets the security requirements of FIPS 140-1, and how to operate the Contivity™ Extranet Switch 4600 in a secure FIPS 140-1 compliant mode of operation. This policy was prepared as part of the FIPS 140-1 Level 2 multi-chip stand alone certification of the Contivity™ Extranet Switch 4600.

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™ Extranet Switch 4600 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Contivity™ Extranet Switch 4600 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™ Switch 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™ Switch 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 Extranet 4600 Switch

The Nortel Networks Contivity Extranet Switch 4600 (referred to as the module, or Switch in this document) provides a scalable, secure, manageable remote access server that meets FIPS 140-1 level 2 requirements for a multiple-chip standalone module. The following sections describe how the Switch addresses FIPS 140-1 requirements.

2.1 Cryptographic Module

The Contivity Extranet Switch combines remote access protocols, security, authentication, authorization, and encryption technologies in a single solution.

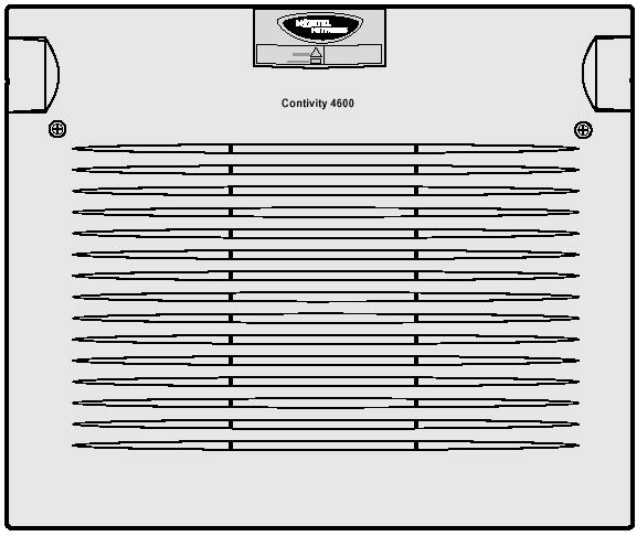

Figure 1 – The Contivity Extranet 4600 Switch

The Switch can support up to 5000 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 Figure 2.

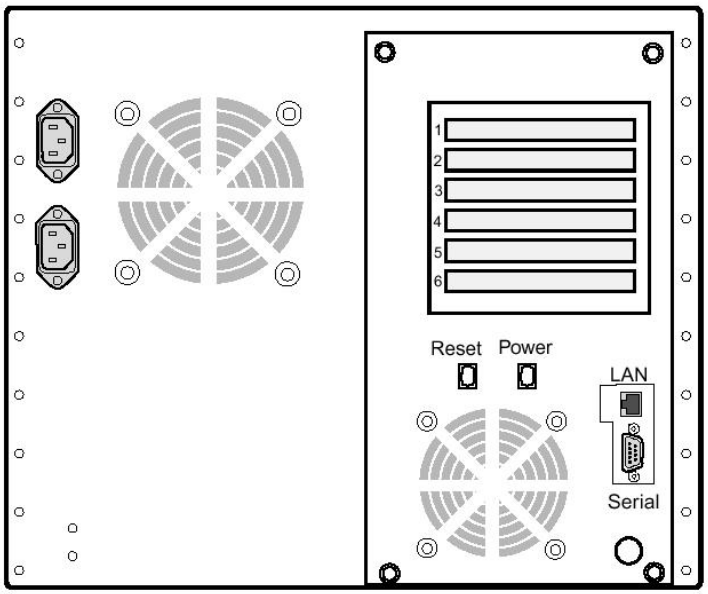

Figure 2 – Physical Interfaces

The physical interfaces include a power plug, power and reset switches, a serial port, a LAN Port RJ-45 connector and up to two additional network connectors. Each RJ-45 connector is accompanied by light emitting diodes (LEDs). The LAN Port LEDs, with the green LED indicating 100Mbps activity and the orange LED indicating link status and activity, are located on the back panel of the module. More information on the LEDs and the LAN Port interface can be found in *Getting Started with the Contivity Extranet Switch 4600*.

The physical interfaces, the LAN port, the 10/100Base-TX ports, serials port and status LEDs, 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, LAN Port	Data Input Interface
10/100BASE-TX LAN Ports, LAN Port	Data Output Interface
Power Switch, Reset Switch, Serial Port, LAN Port	Control Input Interface
LAN Port LEDs, 10/100BASE-TX LAN Port LEDs Serial Port	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™ Extranet Switch 4600. The switch meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (ClassB). The case has two removable portions: the front bezel and the top cover. Removing the front bezel allows access to the floppy drive. The following diagram shows how to remove the front bezel.

Note: The steps required to remove the front bezel are the same whether or not the Switch is rack mounted.

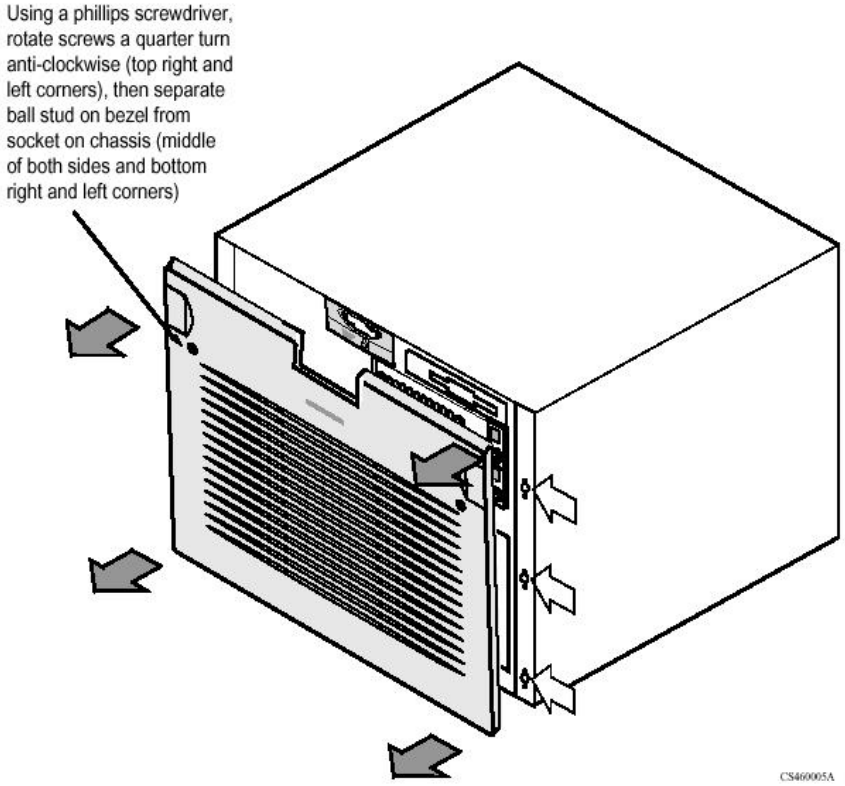

Figure 3 - Removing the front bezel

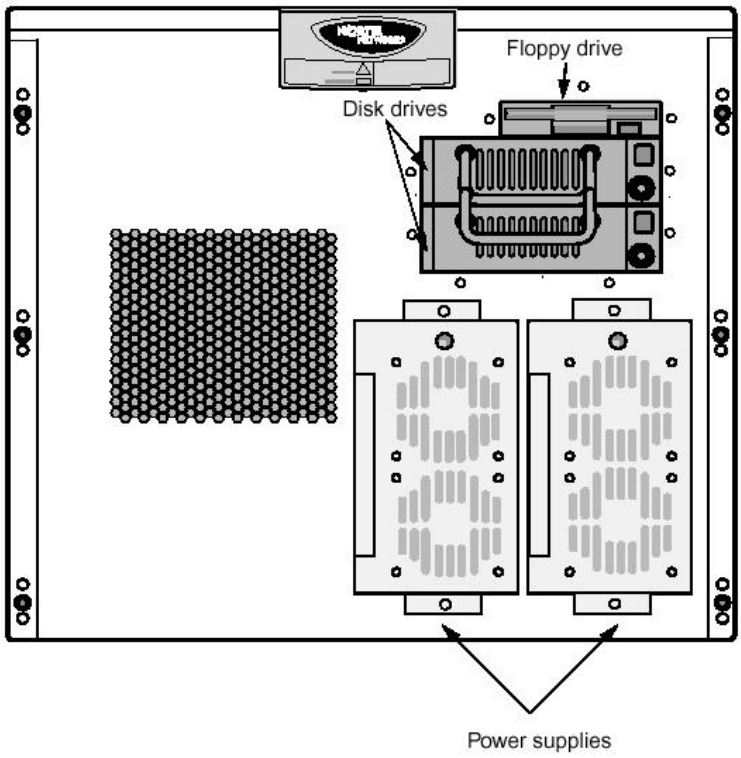

Figure 4 – Front view without front bezel

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 three serialized tamper-evident labels as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol based cleaning pads are recommended for this purpose. The temperature of the switch should be above 10°C.
2. Apply two (2) labels on the top cover overlapping the side and the rear of the chassis as shown in Figure 5.
3. Apply two (2) labels on the top and bottom overlapping the front bezel as shown in Figure 5.
4. Apply one (1) label over the keyboard button cover as shown in Figure 5.
5. Record the serial numbers of the labels applied to the module.
6. Allow 24 hours for the adhesive in the tamper-evident seals to completely cure.

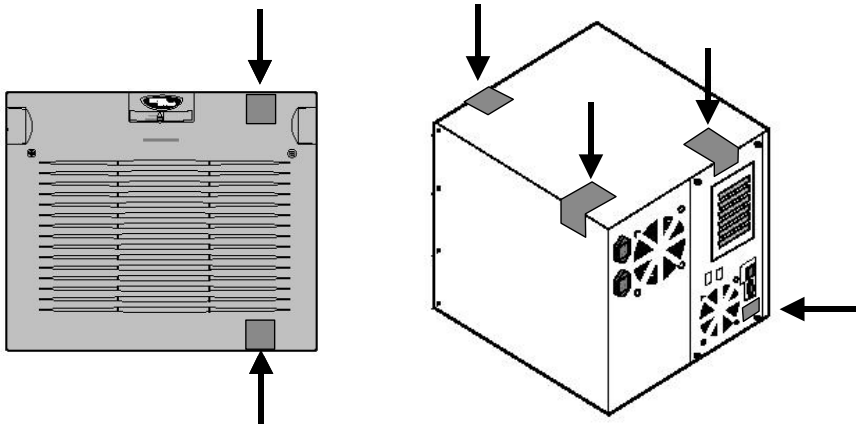

Figure 5 – Tamper-Evident Labels Applied to Switch

The tamper-evident seals are 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 seals or the painted surface and metal of the module cover. Since the tamper-evident labels have non-repeated serial numbers, the labels 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.

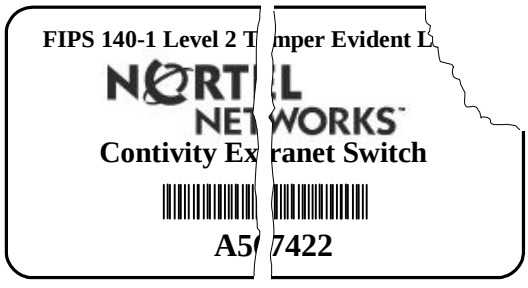

Figure 7 – Damaged Tamper-Evident Label

2.4 Roles and Services

The switch supports up to 5000 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 role-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 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	✓	
Manage the Switch	✓	
Encrypted 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:

- *IPSec Protocol Tunnels*
- *PPTP Protocol Tunnels*
- *L2TP Protocol Tunnels*
- *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 and then authenticate to the switch as a Crypto Officer in order to manage the switch. 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*).
- **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 Simple Network Management Protocol (SNMP) Management Information Base (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 recovery diskette, 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 Internet Protocol (IP) addresses are assigned, idle timeout, forced logoff for timeout, filters, 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 Administration of the switch 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 (checked against a Lightweight Directory Access Protocol (LDAP) directory or using AXENT or a SecureID token). This authenticates the User to the switch and is protected using Internet Security Association and Key Management Protocol (ISAKMP). The Switch may be configured to additionally require authentication through RADIUS with a Group Name and Password. Security options for IPSec include using an Encapsulated Security Payload (ESP) with Triple-DES, Data Encryption Standard (DES), or "40-bit DES", and an Authentication Header (AH) with Message Authentication Code Secure Hash Algorithm (HMAC-SHA) or HMAC-MD5. When operating the device in a FIPS 140-1 compliant manner, only the Triple DES ESP, DES ESP, and HMAC-SHA AH may be enabled.
- PPTP: Requires authentication using the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Challenge Handshake Authentication Protocol (CHAP), or Password

Authentication Protocol (PAP). MS-CHAP can use no encryption, 40-bit RC4, 128-bit RC4 encryption. When operated in a FIPS 140-1 compliant manner, MS-CHAP is not enabled with RC4 encryption.

- L2TP: Requires authentication using MS-CHAP CHAP, or PAP. MS-CHAP can use no encryption, 40-bit RC4, 128-bit RC4 encryption. When operated in a FIPS 140-1 compliant manner, MS-CHAP is not enabled with RC4 encryption.
- L2F: Requires authentication using CHAP, or PAP.

2.5 Key Management

The switch securely administers both cryptographic keys and other critical security parameters such as User passwords. Ephemeral sessions keys are created during the negotiation of secure tunnels on behalf of Users who have successfully authenticated themselves to the switch with their user ID and password. These keys are created for protocols like MS-CHAP and ISAKMP, which securely negotiate key exchange and then allow encryption services for PPTP, L2TP, and IPSec.

Keys are destroyed when the appropriate tunnel, Security Association (SA), or session is terminated and are never archived or released from the device. User passwords can be destroyed by the Crypto Officer or by Users overwriting their own passwords. All passwords are stored in the LDAP database in an encrypted format, and never released. They are used only for authentication in key exchange protocols, which protect Critical Security Parameters (CSPs) according to their protocol. (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 are ephemeral encryption keys used by the module for encrypting packets during IPSec tunneling. These keys are derived during the setup of the tunnel and used only during a secure tunnel session. The IPSec tunnel may use either 56-bit DES or TDES for encryption. These keys are created by setting odd parity and checking for known weak keys. The session keys are internally derived from the Internet Key Exchange (IKE)/ Internet Security Association Key Management Protocol (ISAKMP-Oakley). These protocols are based on Diffie-Hellman Key Agreement. IPSec "Pre-shared keys" may optionally be used with Diffie-Hellman to negotiate a shared session key from the concatenated and SHA-1 hashed value of the user ID and password.

- DES password key: This key is used to encrypt user passwords to be stored in the module's internal LDAP database. This key is compiled into the module's code and can be zeroized using a floppy to erase the firmware. The floppy disk unit holds a "format" utility. In order to zeroize the DES key (hard-coded into the module firmware), the crypto officer must run the format utility

contained on the floppy disk via the module's management interface. The format utility then causes the firmware of the module to be erased

- RSA keys: These RSA public/private key-pairs are used for generating and verifying digital signatures for authentication of users during IPSec tunneling sessions. The module's keys are generated internally by 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, respectively. All RSA keys can be zeroized by the administrator by entering commands to delete and zeroize the key directories. The private key is never output from the module while the module's public key is output to obtain a certificate from a third party Certificate Authority (CA).

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

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 Switch

The Contivity Switch is a versatile machine; it can be run in a Normal Operating Mode or a FIPS Operating Mode (FIPS mode). In FIPS 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 labels 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 AH may be enabled. MD5 is not an approved FIPS algorithm.
    - For PPTP and L2TP: When operated in a FIPS 140-1 compliant manner, MS-CHAP and CHAP are not enabled with RC4 encryption.
    - For L2P: CHAP must be disabled to operate in a FIPS compliant manner.
    - 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.