Contivity™ Extranet Switch 4500

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 2 Validation

February 2000

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Contivity™ Extranet Switch 4500. This security policy describes how the Contivity™ Extranet Switch 4500 meets the security requirements of FIPS 140-1, and how to operate the Contivity™ Extranet Switch 4500 in a secure FIPS 140-1 mode. This policy was prepared as part of the level 2 FIPS 140-1 certification of the Contivity™ Extranet Switch 4500.

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 4500 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Contivity™ Extranet Switch 4500 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 Terminology

In this document the Nortel Contivity™ Extranet Switch 4500 is referred to as the switch, the Contivity™ Switch, module, or system.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Contivity™ Switch and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the Contivity™ Switch. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. 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. For access to these documents, please contact Nortel Networks.

2 The Contivity Extranet 4500 Switch

The Nortel Networks Contivity Extranet Switch 4500 provides a scalable, secure, manageable remote access server that meets FIPS 140-1 level 2 requirements. This section will describe the general features and functionality provided by the Contivity Extranet Switch. Section 3 will provide further details on how the Contivity Switch addresses FIPS 140-1 requirements.

2.1 Cryptographic Module

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

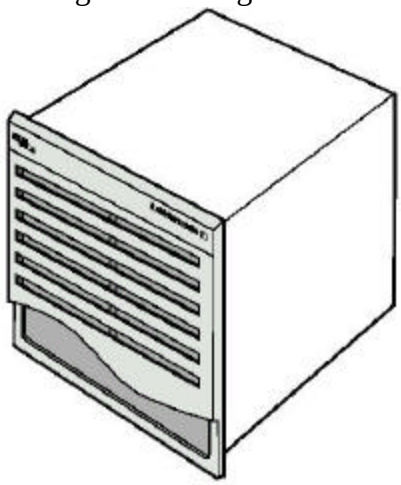

Figure 1 – The Contivity Extranet 4500 Switch

The Switch can support up to 5,000 simultaneous user sessions, allowing each user to exercise a variety of secure connections and 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 personal Extranet based on the special needs of a user or group.

2.2 Module Interfaces

The interfaces for the Switch are located on the rear panel as shown in Figure 2.

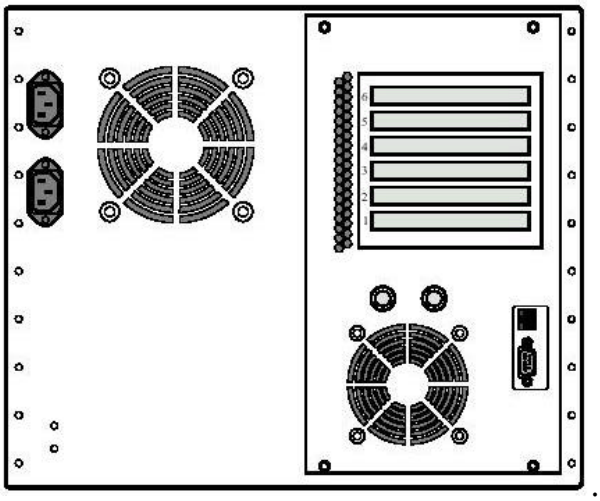

Figure 2 – Physical Interfaces

The physical interfaces include the dual power plugs for the redundant power supplies, the power and reset buttons, the serial port, the LAN Port RJ-45 connector, and up to six slots containing additional network connectors. The power and reset buttons light up to indicate power and hard disk activity respectively. Each RJ-45 connector is accompanied with Light Emitting Diodes (LEDs), including green and orange LEDs on the LAN Port, and Link/Activity and 10/100Mbps LEDs on the 10/100BASE-TX LAN ports.

Figure 3 shows details of the LAN Port LEDs, with the green LED indicating 100Mbps activity, and the orange LED indicating link status and activity. More information on these LEDs and the LAN Port interface can be found in the *Contivity Extranet Switch 4500 Getting Started Guide*, 1C.

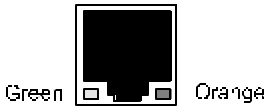

Figure 3 – LAN Port LEDs

Figure 4 shows details of the 10/100BASE-TX LAN Port LEDs, with the link status LED indicating connection to a hub, the activity LED indicating traffic being sent, and the 100TX LED indicating 100Mbps operation. More information on these LEDs and the /100BASE-TX LAN Port interface can be found in the manual *"Getting Started with the Contivity Extranet Switch 4500"*.

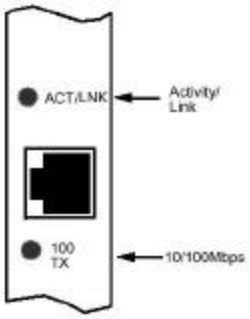

Figure 4 – 10/100BASE-TX LAN LEDs

These physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

Switch physical interface	**FIPS 140-1 Logical Interface**
10/100BASE-TX LAN Port, LAN Port, Serial Port	Data Input Interface
10/100BASE-TX LAN Port, LAN Port, Serial Port	Data Output Interface
Power Button, Reset Button, Serial Port, LAN Port	Control Input Interface
LAN Port LEDs, 10/100BASE-TX LAN Port LEDs Serial Port Power Button Light Reset Button Light	Status Output Interface
Dual Power Plugs	Power Interface

Table 1 – FIPS 140-1 Logical Interfaces

2.3 Redundancy and Physical Security

With up to 5,000 simultaneous users accessing critical information, network managers can rest assured that the Contivity Extranet Switch is designed for high availability. Auto switching redundant power supplies and a redundant storage system protect against failure. Multilevel authentication methods and automatic backup of all system and accounting data ensure maximum reliability and management peace of mind. The Switch meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for business use (ClassA), and is labeled in accordance with FCC requirements.

The Contivity™ Extranet Switch 4500 is entirely encased by a thick steel chassis. The system has three removable portions: the front bezel, the top cover, and the I/O Panel. Removing the

front bezel allows access to the dual power supplies, hard drives, and floppy drive. Removing the top cover or the I/O panel allows access to the motherboard, memory, and expansion slots.

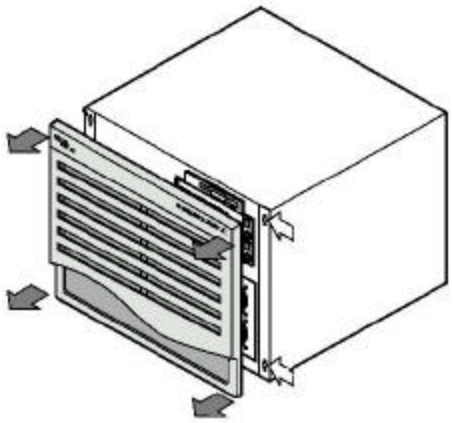

Figure 5 – The Steel Cover of the Extranet Switch 4500

Once the Extranet Switch 4500 has been configured in its FIPS 140-1 level 2 conformant mode, the system cannot be accessed without signs of tampering. To seal the system, apply 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 sides overlapping the top cover and the main chassis as shown in Figure 6.
3. Apply two (2) labels on the top and bottom overlapping the bezel and the main chassis as shown in Figure 6.
4. Apply one (1) label over the air holes on the rear I/O Panel as shown in Figure 7
5. Apply one (1) label over the keyboard button cover as shown in Figure 7
6. Apply one (1) label over the gap between the I/O Panel and the main chassis as shown in Figure 7
7. Apply 2 labels over the AC filter input module screws as shown in Figure 7
8. Record the serial numbers of the labels applied to the module.
9. Allow 24 hours for the adhesive in the tamper-evident seals to completely cure.

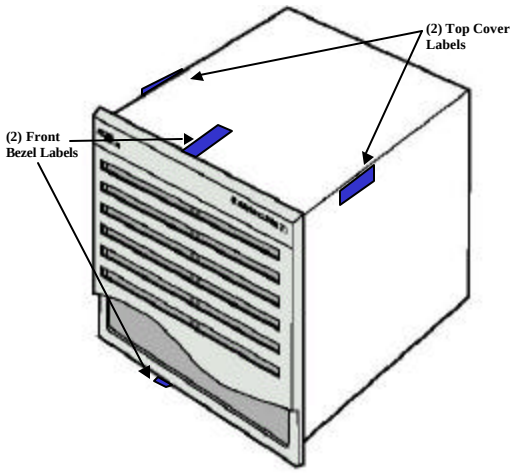

Figure 6 – Tamper-Evident Labels Applied to Switch Front Bezel and Top Cover

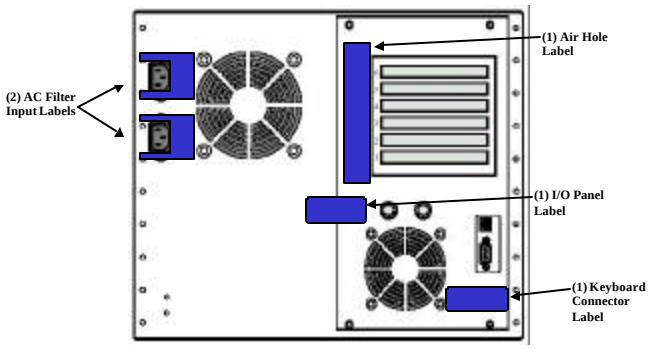

Figure 7 – Tamper Evident Labels Applied to Rear Panel

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 with. An intact label is shown in Figure 8, with a visible serial number and no breaks.

FIPS 140-1 Level 2 Tamper Evident Label

NORTEL NETWORKS

Contivity Extranet Switch

Serial Number: 5673422

Figure 8 – Tamper-Evident Label

Attempting to remove a label breaks it or continually tears off small fragments as depicted in Figure 9. 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.

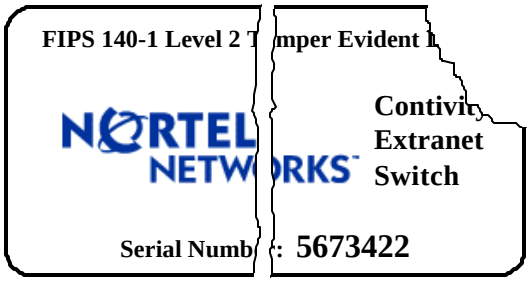

Figure 9 – Damaged Tamper-Evident Label

2.4 Roles and Services

The Switch supports up to 5000 simultaneous users sending packets 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.

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

There are two main roles in the Switch (as required by FIPS 140-1) that users may assume: Crypto Officer role and User role. The administrator of the switch assumes the Crypto Officer role in order to configure and maintain the switch using Crypto Officer services, while the Users exercise only the User services. The Crypto Officer role is assumed with the following rights:

- Manage Switch rights: (either *none*, *view switch*, or *manage switch*). V*iew switch* rights allow an administrator to view all the configuration and status information on the switch. *Manage switch* rights allow an administrator to configure the switch and actually change settings.
- Manage Users rights: (either *none*, *view users*, or *manage users*). *View users* rights allow an administrator to review all user accounts and settings on the Switch while *manage users* rights actually allow an administrator to create, modify, and delete users.

A User authenticates and assumes the User role in order to have rights 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. (This initial account always has *manage switch* and *manage users* rights.) An administrator of the switch may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional administrators. 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 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{ XE "SNMP" } MIB II{ XE "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 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 administrators manual, *Managing the Contivity Extranet Switch,* 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, whether 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 an LDAP directory or using AXENT or a SecureID token). This authenticates the User to the switch and is protected using 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{ XE "SHA" } Algorithm{ XE "secure hash algorithm" } (HMAC-SHA) or HMAC-MD5.
- PPTP: Requires authentication using MS-CHAP, CHAP, or PAP. MS-CHAP can use no encryption, 40-bit RC4, 128-bit RC4 encryption.
- L2TP: Requires authentication using MS-CHAP CHAP, or PAP. MS-CHAP can use no encryption, 40-bit RC4, 128-bit 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, SA, or session is terminated and are never archived or released from the device. User passwords can be destroyed by Crypto Officers, 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 each protect 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 *Managing the Contivity Extranet Switch (page 3-32)*.

2.6 Self Tests

In order to prevent any secure data being released, 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 which are run during startup and periodically during operations. The self-test run at power-up include a cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES) and on the message digest (SHA-1). Also performed at startup are software integrity tests using a DES MAC per FIPS 113 and a continuous random number generator test. Other test are run periodically or conditionally such as a software load test for upgrades using a DES MAC and the continuous random number generator test. In addition, there are checksum tests on the flash memory which 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. In FIPS operating mode, the switch meets all the Level 2 requirements for FIPS 140-1. In order 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-tunnelled 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 disable to operate in a FIPS compliant manner.
    - The internal LDAP database must be used in place of an external LDAP server.
    - SSL cannot be used to establish secure connections
    - For RIP – In FIPS mode, MD5 must be disabled.

Note: *A switch that has a Hardware Accelerator installed cannot be run in FIPS mode.*

There are several services that are effected 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. RSA digital signatures are disabled in FIPS mode, because RSA digital signature is not a FIPS approved algorithm. 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.