Contivity® 600, 1700 and 2700
Secure IP Services Gateways

FIPS 140-2 Non-Proprietary Security Policy

Version 1.3

Level 2 Validated February 2004

Table of Contents

INTRODUCTION 3

PURPOSE 3
REFERENCES 3
DOCUMENT ORGANIZATION 3

CONTIVITY 600, 1700 AND 2700 4

OVERVIEW 4
MODULE INTERFACES 4
ROLES AND SERVICES 5
Crypto-Officer Role 5
User Role 6
Authentication Mechanisms 6
PHYSICAL SECURITY 7
CRYPTOGRAPHIC KEY MANAGEMENT AND ALGORITHMS 7
Key Generation 10
Key Storage 10
Key Protection/Zeroization 11
SELF-TESTS 11
Power-Up Self-Tests 11
Conditional Self-Tests 11
DESIGN ASSURANCE 11
MITIGATION OF OTHER ATTACKS 12

SECURE OPERATION 13

INITIAL SET-UP 13
Configuring the switch for FIPS operating mode 13

ACRONYMS 17

INTRODUCTION

Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Contivity 600, 1700 and 2700 Secure IP Services Gateways from Nortel Networks with a firmware version of V04_75.183 This security policy describes how the Contivity 600, 1700 and 2700 meet the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Nortel Networks website (http://www.nortel.com) contains information on the full line of products from Nortel.

- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Nortel Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Nortel Networks and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Nortel Networks. The Contivity 600, 1700 and 2700 Secure IP Services Gateways will either be referenced as Contivity Modules or Gateways in this document.

CONTIVITY 600, 1700 AND 2700

Overview

The Contivity 600, 1700 and 2700 Secure IP Services Gateways are the ideal solution for enterprises requiring secure, low-cost connectivity across the Internet or managed IP networks. Designed for small sites, the Contivity 600, 1700 and 2700 provide, IP routing, Virtual Private Networking (VPN), stateful firewall, encryption, authentication, directory and policy services, Quality of Service (QoS), and bandwidth management services in a single integrated platform. The Contivity 600, 1700 and 2700 provide options for small sites seeking Internet connectivity, either for secure VPN communications or for basic IP/Internet access.

The Contivity Gateways can be installed in a variety of scenarios to serving the security-conscious, small-user segment of the IP services market. Their advanced routing and built-in VPN capabilities make them ideal either for site-to-site or remote access VPN applications, or for simple Internet connectivity.

The following are the version numbers of the network interface cards that can be used with the module.

Field Installable:
T3 HSSI WAN Interface - DM2111003
T1CSU/DSU WAN interface - DM2111005
Single V.35/X.21 WAN interface - DM2111006
Encryption accelerator - DM0011052
10/100 Ethernet - DM1011002

Factory Installable:
T3 HSSI WAN Interface - DM2104003
T1CSU/DSU WAN interface - DM2111004
Single V.35/X.21 WAN interface - DM2111007
Encryption accelerator - DM0011051
10/100 Ethernet - DM1004002

Module Interfaces

The Contivity 600, 1700 and 2700 have been evaluated as multi-chip standalone modules, and the cryptographic boundary of the module is defined by the outer case of the module. The modules provide a number of physical and logical interfaces to the device.

The physical interfaces provided by the modules are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	10/100BASE-TX LAN Ports, WAN Port
Data Output Interface	10/100BASE-TX LAN Ports, WAN Port
Control Input Interface	10/100BASE-TX LAN Ports, WAN Port, Console Port, Power Button, Reset Button
Status Output Interface	LEDs, 10/100BASE-TX LAN Ports, WAN Port, Console Port
Power Interface	AC power input.

Roles and Services

The modules support role-based authentication. The operators authenticate to the module by entering the appropriate password. The operators are required to enter a user id and password. The passwords conform to FIPS approved security requirements. The module can be accessed in two ways:

1. Through a console port

2. Through a Web-based interface. (Encrypted Ipsec tunnel in a FIPS Mode of operation).

There are two main roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and User role.

Crypto-Officer Role

The Crypto-Officer is the administrator of the Gateway and does the initial set up and maintenance. At the highest level, Crypto-Officer Services include the following:

- Configure the Gateway: define network interfaces and settings, set the protocols the gateway will support, define routing tables, set system date and time, and load authentication information.
- 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 gateway (either *non*e, *view switc*h, or *manage switc*h) and rights to manage Users (either *non*e, *view user*s, or *manage user*s).
- 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, which define a set of

packets to permit or deny basic characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction. The administrator can use any of the predefined rules or create custom rules to be included in each filter.

- Status functions: view the switch configuration, routing tables, and active sessions; and use Gets to view SNMP MIB II statistics, usage graphs, health, temperature, memory status, voltage, packet statistics, and review accounting logs.
- Manage the switch: log off users, shut down or reset the switch, disable or enable audible alarms, manually back up switch configurations, restore switch configurations, or create a recovery diskette.

User Role

The User can access the services (IPSec, PPTP, L2F and L2TP) on the module to send data through it. The Crypto-Officer manages users' rights and assigns each user a name and a user group. The user group defines access limitations 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. ID and password can be assigned for administration of the switch. The user can then authenticate as necessary to initiate secure tunnels using any of these services.

Authentication Mechanisms

The Contivity modules provide three ways of authentication. The document *Configuring the Contivity in FIPS Mode* makes recommendations and lists guidelines to run the switch in a secure FIPS approved mode.

Authentication Type	Strength	Notes
Password	Meets the FIPS 140-2 requirements.	The module supports password-based authentication for the Crypto-Officer through the password records stored on the module. The minimum size of the password can be chosen by the Crypto-Officer and the module supports password sizes of up to even 16 characters and passwords a minimum of 6 characters in length should be used in FIPS mode. Assuming only 36 characters (A-Z, a-z, and 0-9) with repetition, the chance of a random attempt falsely succeeding is 1 in 56800235584.
Public Key based	An RSA public key based authentication	The module supports authentication using RSA public keys for IPSec. The probability of a random attempt to falsely succeed is much lesser than 1 in 2^512.

Authentication Type	Strength	Notes
Pre-shared keys	Key derived from the user id and password.for each user.	This method of authentication derives the pre-shared keys based on the user id and password using SHA-1. The probability of a random attempt to falsely success is much less than 1 in 2 ^ 160.

Physical Security

The Contivity 600, 1700 and 2700 are multi-chip standalone modules and meet all physical security requirements for FIPS 140-2. The platforms provide production grade equipment, industry-standard and a strong enclosure, and the systems meet Federal Communication Commission (FCC) Electromagnetic Interference (EMI) compatibility requirements. The document *Configuring the Contivity in FIPS Mode* defines the required procedures to apply tamper-evidence labels across the module's cover so that the Crypto-Officer can detect any attempt to open the box. It also details logging all access to the box by logging each time the tamper evidence seals are broken with permission of the Crypto-Officer. The module also implements audible alarm support that activates when the front cover is removed. The Crypto-Officer could configure this through the command line interface.

Cryptographic Key Management and Algorithms

Critical Security Parameters of the Module

Only the Crypto-Officer (Administrator) can log on to the box directly through the console or the web interface. Normal users of the box only access it through the services. So the CSPs are accessed directly only by the Crypto-Officer. All other users access them through protocol.

The following Critical Security Parameters are used in the module:

Cryptographic Key	Description	Key Type	Storage and Zeroization
User and Crypto-officer Passwords	These passwords are used in PAP, CHAP, PPTP, L2TP, L2TF and in generating IPSec pre-shared keys.	An alpha-numeric string with a minimum length of 6 characters.	The passwords of the user and crypto-officer are stored in the LDAP database. They are zeroized by overwriting them with new passwords when the user or Crypto-Officer changes the password.
DES key used for Integrity check and software/firmware	This key is used to perform the integrity check on the module. The key is also used to perform	A DES key of 56 bit length	This key is compiled into the Contivity device code and can

Cryptographic Key	Description	Key Type	Storage and Zeroization
load test for Software upgrades	software/firmware load test for software upgrades.		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.
IPSec pre-shared keys	These are derived from the user name and password. It is the responsibility of the Crypto-Officer to configure the username and password to match on both ends of the connection.		These are generated and stored in the LDAP database if the Crypto-Officer configures to use the pre-shared keys for the particular user. These are zeroized when the module is reset or when the user passwords are changed.
IPSec Session Keys	These are exchanged using IKE protocol and the public-private key pairs.	The type and size of the session keys depend on the algorithm used. So it is an AES, 3DES or DES key.	They are not stored on disk. They are stored in the memory during the session and zeroized immediately after the tunnel is shut down.
X.509 certificates	These include the module's public key and also the certificates of other hosts and users accessing the system. They are used in IPSec key negotiation using Diffie-Hellman and SSL key negotiation.	RSA public key based certificates	They are stored in files in the module. Every certificate is stored in a separate file.
Private Key	This is the module's private key for Diffie-Hellman key exchange for IPSEC and SSL key negotiation	RSA private key	The private key is stored encrypted using a PKCS#5 password based encryption. The password itself is not stored but a MAC of the plaintext private key is stored to verify the password. The encryption is not FIPS

Cryptographic Key	Description	Key Type	Storage and Zeroization
			approved and so for FIPS purposes it is stored in plaintext. These are zeroized when the Crypto-Officer generates new private keys and overwrites the existing keys.

The module employs a FIPS compliant password scheme; it has a configurable password mechanism where the Crypto-Officer can set a maximum password length of 16 characters. It is required that the minimum length is 6. The CSPs are accessible only to the Crypto-Officer.

IKE

The Switch performs Internet Key Exchange (IKE) (ISAKMP-Oakley) in both main-mode and aggressive mode key exchanges. These are protocols based on Diffie-Hellman key exchanges. IPSec explicitly negotiates a common key during the ISAKMP exchange, and also refreshes it periodically. The switch can also use the pres-shared key option of IPSec for aggressive mode for authentication purposes. Key generation is done per ISAKMP-Oakley.

Algorithms

The switch supports the following cryptographic algorithms.

The Contivity switches support the following Approved cryptographic algorithms:

Symmetric Key Algorithms

Algorithm	Modes Implemented	Key Sizes
▪ AES (FIPS 197)	CBC	128 Bits
▪ DES (FIPS 46-3)	CBC	56Bits (to be used for legacy systems only), 40Bits (may not be used in FIPS mode)
▪ Triple DES (FIPS 46-3)	CBC	112 Bits

Hashing Algorithms

▪ SHA-1 (FIPS 180-1)

Message Authentication Algorithms

▪ DES-MAC (FIPS 113)	▪ HMAC SHA-1 (FIPS 198)

Public Key Algorithms

▪ RSA (PKCS#1) (FIPS 186-2)	512, 768, 1024, 2048

On the 2700 the algorithm implementations are there in the hardware accelerator also. The algorithms that are in the hardware are DES, 3DES, SHA-1 and HMAC SHA-1. AES is not implemented in the hardware accelerator.

The certificate numbers for the algorithms are given below:

Algorithm	Software Implementation	Hardware Implementation
DES	48	101
3DES	53	29
AES	50	Not implemented
SHA-1	31	51

Non-FIPS Approved Algorithms

- Symmetric Key Algorithms

Algorithm	Modes Implemented	
▪ RC2	CBC	128 Bits
▪ RC4	CBC	40Bits, 128Bits

- Hashing Algorithms

▪ MD5	▪ HMAC MD5
▪ MD2	

- Key Exchange Algorithm

▪ Diffie-Hellman

Key Generation

The module implements the FIPS 186-2 based PRNG. All key generation functions use the approved PRNG implementation. The module generates private-public key pairs. It also uses the PRNG implementation to generate keys for IPSec negotiations.

Key Storage

The module stores keys internally. The keys are shielded from outside access and only Crypto-Officers can access them. The private keys are stored encrypted with a password based string based on PKCS#5 specification. User passwords are stored in the switch in an encrypted form in the internal LDAP database. A fixed key/pass-phrase string (which is compiled into the module code) is used to encrypt the passwords. For FIPS purposes, these keys are considered to be in plaintext form. The access rights set on each of the CSPs do not matter because only the Crypto-Officer has direct access to them.

Key Protection/Zeroization

Only the Crypto-Officer can access the keys. The module has a password-based authentication mechanism for the administrator. Also the interface through which the administrator logs in is different from the user interface for additional security.

The switch securely administers both cryptographic keys and other critical security parameters, such as operator passwords. Ephemeral session 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. Private keys are always overwritten by new keys if need to be changed. 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 are never released. They are used only for authentication in key exchange protocols. Crypto Officers should be aware that Password Authentication Protocol (PAP) transmits password information in the clear and should not be enabled before deciding local policy. See *Configuring the Contivity VPN Switch* for more information on PAP.

Self-Tests

The module performs power-up and conditional self-tests to ensure the secure and proper operation, and the sections below provide details on the module's self-tests.

Power-Up Self-Tests

The power-up self tests implemented include known answer tests for AES, DES, 3DES, SHA-1, HMAC SHA-1 and RSA. Also executed at power-up are the PRNG KAT and the software/firmware integrity check. Power-up self tests are executed automatically when the module is started.

Conditional Self-Tests

The module performs two conditional self-tests: a pair-wise consistency test each time a module generates RSA public/private key, a continuous random number generator test each time the module produces random data and a software load test for upgrades.
If any of the self tests fail the module logs them in a file and forcibly crashes and reboots the machine, thus preventing access to the system in an error state.

Design Assurance

Nortel Networks follows highly stabilized and popular design procedures for both Software and Hardware implementations. The design for the Contivity follows FIPS provided guidelines. The software and hardware design both go through many phases of review and inspections. The code and design documents are securely stored and the delivery is also secure.

Mitigation of Other Attacks

The module does not attempt to mitigate any attacks in the FIPS mode of operation.

SECURE OPERATION

This section describes the steps required to run the switch in a FIPS approved mode of operation. It also suggests standard security principles to ensure a more secure operation.

Initial Set-Up

Configuring the switch for FIPS operating mode

A number of protocols and features of the switch are not part of the permitted functions in a FIPS-compliant system. The web-based management interface provides a button to enable FIPS mode. Place the module in FIPS mode by clicking on the FIPS Enabled button on the 'Services...Available management' screen, and restart the module. Enabling FIPS mode disables these protocols and features.

The following are performed by the system after pushing the button to enable FIPS mode:

- Must have an *internal* LDAP server to be FIPS compliant. The external LDAP server is disabled in FIPS mode.
- Enabling FIPS automatically disables FTP
- Either enabling or disabling FIPS requires a system reboot.
- The 'NULL' encryption option should be disabled for the IPSec services. This ensures that the module is not in a bypass mode in a FIPS mode of operation.

These additional actions must be performed by the Crypto-Officer to put the module in a FIPS mode.

- The Crypto-officer passwords configured in the switch should have a minimum length of at least 6 characters.
- Maximum number of login attempts must be set to five (5)
- Apply the tamper-evident labels.
- Disable cryptographic services (PPTP, L2TP, L2F) that employ non-FIPS approved algorithms. This includes SSL, and so all services using SSL should be disabled.
- All access to the web based management interface should be done over an IPSec tunnel.

A number of configuration options are required when you are operating the switch in a FIPS 140-2-compliant manner.

Configuration:

- Change the default administrator password on the switch.
- Debugging scripts are disabled.
- The administrator is given additional authority to reset the default administrator's password and username.
- Configure audible alarms so as to sound when the front cover is removed. This is done through the command line interface (accessed through the serial port interface) using the command 'audible alarm'.

Crypto Officer and User Guidance

The document *Configuring the Contivity for FIPS Mode* gives a detailed list of actions that must be run to place the module in FIPS mode and also outlines the steps needed to perform them. This document is the Crypto Officer Guidance document. There is no specific User Guidance, as the configuration and management of the module are services of the Crypto Officer; thus, the User documentation for the module is sufficient User Guidance.

Applying Tamper Evidence Labels

Once the Contivity module has been configured in the FIPS 140-2 level 2 mode, the cover may not be removed without signs of tampering.

To seal the cover for the 600, apply a serialized tamper-evident label 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 a label on the top overlapping the rear panel as shown in Figure 5.
3. Record the serial numbers of the labels applied to the module.
4. Allow 24 hours for the adhesive in the tamper-evident seals to completely cure.

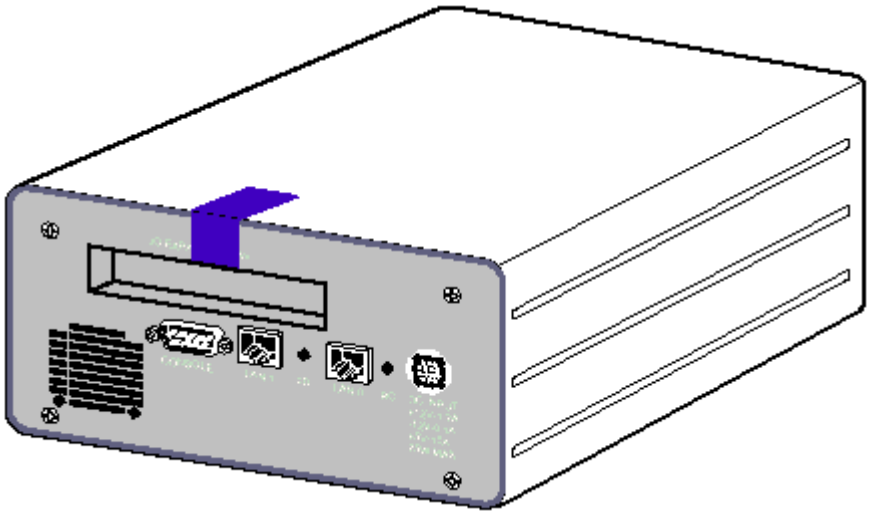


Figure 5 – Tamper-Evident Label

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.

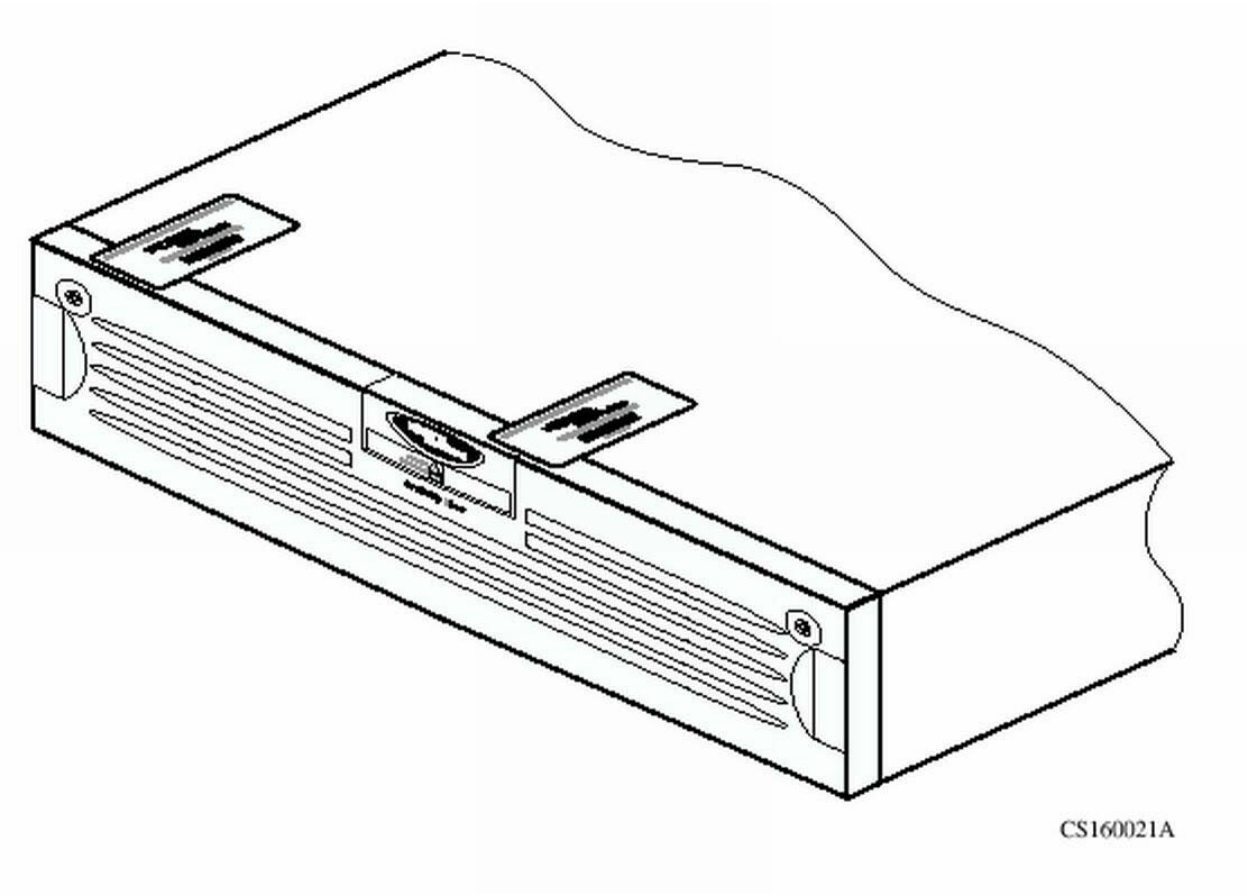
Attempting to remove a label breaks it or continually tears off small fragments. Other signs of tamper-evidence include a strong smell of organic solvents, warped or bent cover metal, and scratches in the paint on the module.

To seal the system on the 1700 or 2700, you must apply serialized, tamper-evident labels as follows:

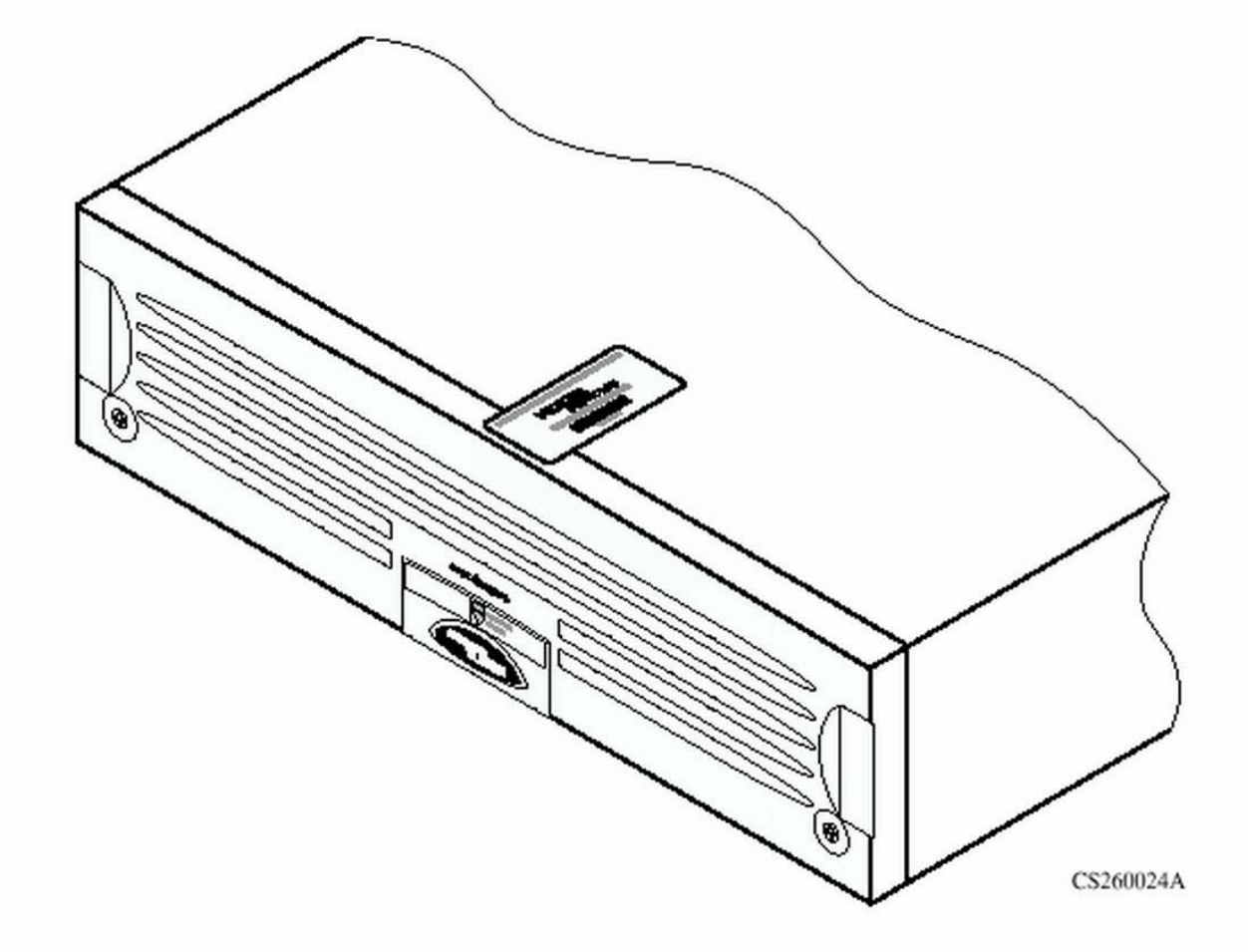
1. Ensure that the temperature of the switch is above 10°C (Nortel Networks recommends a temperature of approximately 20°C).
2. Turn off and unplug the system.
3. Clean the chassis of any grease, dirt, or oil. The supplied alcohol-based cleaning pads are recommended for this purpose.
4. Apply one of the general labels to the bottom front, overlapping the bezel and the main chassis.
5. Apply a label on the top overlapping the rear panel.
6. Record the serial numbers of the labels applied to the Contivity switch in a security log.
7. Allow *72 hours* for the adhesive in the tamper-evident seals to completely cure.

The following are diagrams illustrating where the tamper evidence labels are applied.

- Figure 1. Tamper Evidence Labels applied to top cover



- Figure 2. Tamper Evidence Labels to the bottom front.



ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer

