COPYRIGHT COLUBRIS NETWORKS INC.

NON-PROPRIETARY CRYPTOGRAPHIC MODULE SECURITY POLICY FOR THE COLUBRIS CN1050 AND CN1054 WIRELESS LAN ROUTERS VERSION 1.0 (FIRMWARE VERSION 1.24-01-1736)

Document No. 33-00-0001-01
Version 1.7, 22 September 2003

Colubris Networks Inc.
420 Armand-Frappier (Suite 200)
Laval (Quebec) Canada H7V 4B4

COPYRIGHT COLUBRIS NETWORKS INC.
Distribution of this document by the Cryptographic Module Validation Program validation authorities, the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE), is allowed providing the document is copied or printed in its entirety.

COPYRIGHT COLUBRIS NETWORKS INC.

NON-PROPRIETARY CRYPTOGRAPHIC MODULE SECURITY POLICY FOR THE COLUBRIS CN1050 AND CN1054 WIRELESS LAN ROUTERS VERSION 1.0 (FIRMWARE VERSION 1.24-01-1736)

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

1 INTRODUCTION

1.1 PURPOSE

This document defines the security policy for the CN105x Cryptographic Module of the Colubris CN1050 and CN1054 Wireless LAN Routers.

1.2 SCOPE

This document is written in accordance with the requirements of Appendix C of FIPS PUB 140-2, and includes the rules derived from the requirements of FIPS PUB 140-2 and the rules derived from any additional requirements imposed by the vendor.

1.3 INTENDED USE

This document is intended to be used:

a. to provide a specification of the cryptographic security that will allow individuals and organizations to determine whether the CN105x Cryptographic Module, as implemented, satisfies a stated security policy; and

b. to describe to individuals and organizations the capabilities, protection, and access rights provided by the CN105x Cryptographic Module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

1.4 ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CPU	Central Processing Unit
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECB	Electronic CodeBook
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission (US)

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

FIPS	Federal Information Processing Standard
FIPS PUB 140-2	FIPS PUBlication 140 Second Revision (-2)
HMAC	keyed-Hashing for Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol SECurity
KLIPS	KerneL Internet Protocol Security
LAN	Local Area Network
LED	Light Emitting Diode
L2TP	Layer Two (2) Tunnelling Protocol
MSCHPV2	MicroSoft Challenge Handshake Protocol v2
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PAP	Password Authentication Protocol
PCMCIA	Personal Computer Memory Card International Association
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunnelling Protocol
RADIUS	Remote Authentication Dial-In User Service
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SHA1 or SHA-1	Secure Hash Algorithm First Revision (1)
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TMOVS	Triple DES Modes of Operation Validation System
VPN	Virtual Private Network
XAUTH	eXtended AUTHentication
3DES	Triple (3) Data Encryption Standard

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

2 CN105X CRYPTOGRAPHIC MODULE OVERVIEW

Colubris CN105x Secure Wireless LAN Router enables strong security for wireless enterprise networking, using embedded IPSec VPN and firewall functionalities. It is intended for enterprise office environments of differing scales, from the corporate headquarters to remote branch sites, and therefore has been designed with ease of use in mind, making deployment and remote administration as easy as possible.

Supporting up to 50 concurrent sessions, the Colubris 105x Secure Wireless LAN Router enables secure mobile access to IT resources within enterprise environments, remote access and site-to-site VPN services using the IPSec, L2TP and PPTP protocols. It securely delivers enterprise networking without bounds, significantly increasing employee productivity in corporate offices, in decentralized/remote workgroups, and in branch locations with broadband access.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

2.1 ENCLOSURE AND CONNECTORS

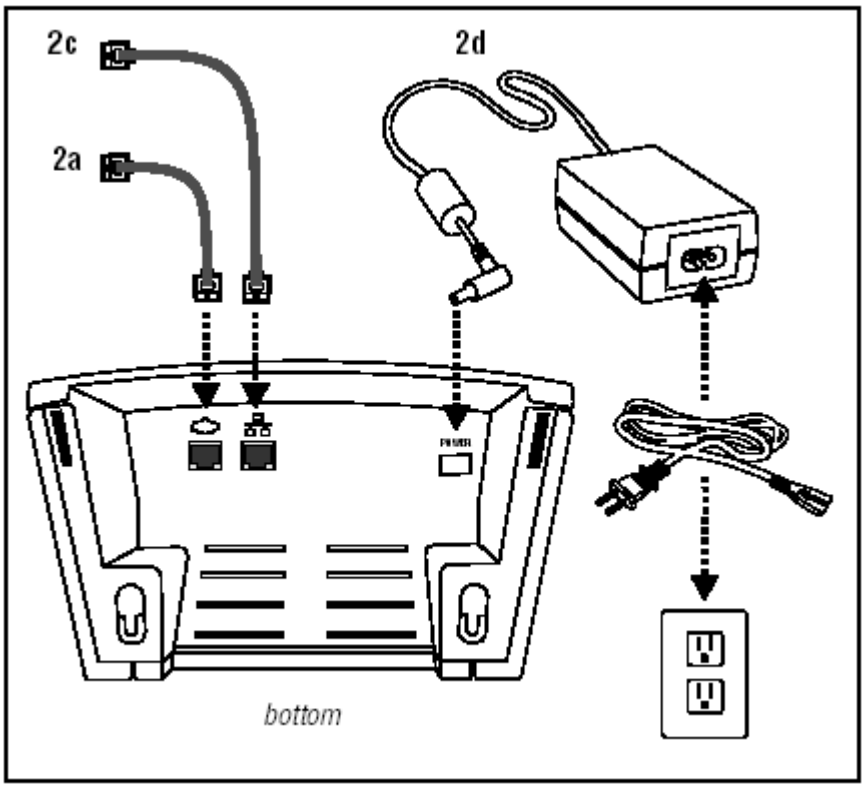


Figure 1

Figure 1 shows the connectors on a CN1050.

2a Internet Port Connection
2c Lan Port Connection
2d Power

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

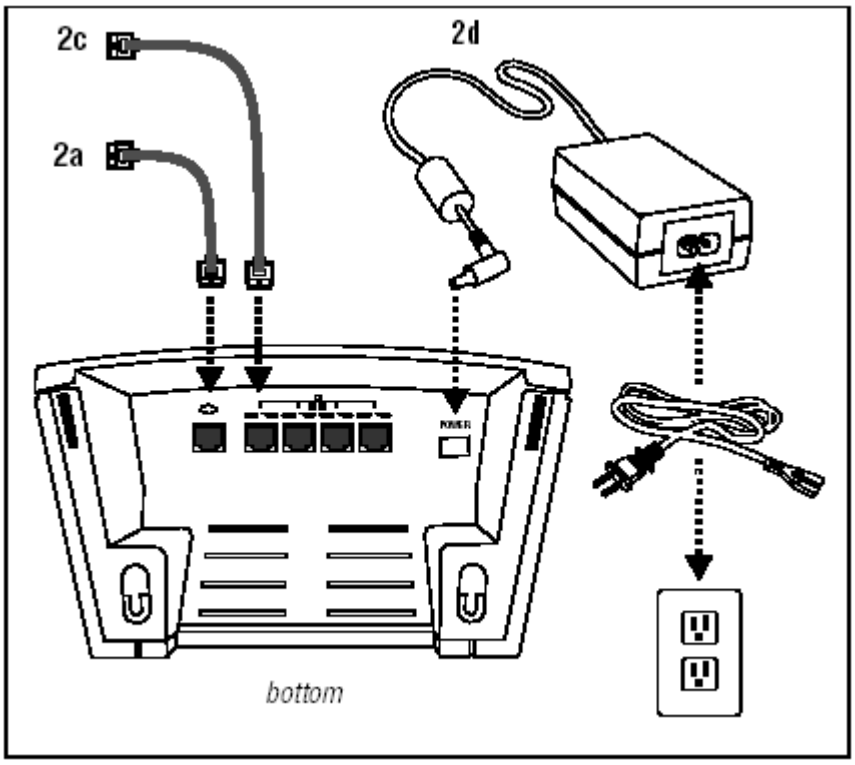


Figure 2

Figure 2 shows the connectors on a CN1054.

2a Internet Port Connection
2c Lan Port Switch
2d Power

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

2.2 TAMPER EVIDENT SEALS

This section describes where the tamper-evident seals must be affixed for the CN105x to meet FIPS 140-2 Physical Security Level 2.

Figure 3 illustrates where the tamper-evident seals must be affixed on the sides of the enclosure. One seal should be affixed on both sides. These seals prevent the sides of the enclosure from being separated without leaving tamper evidence.

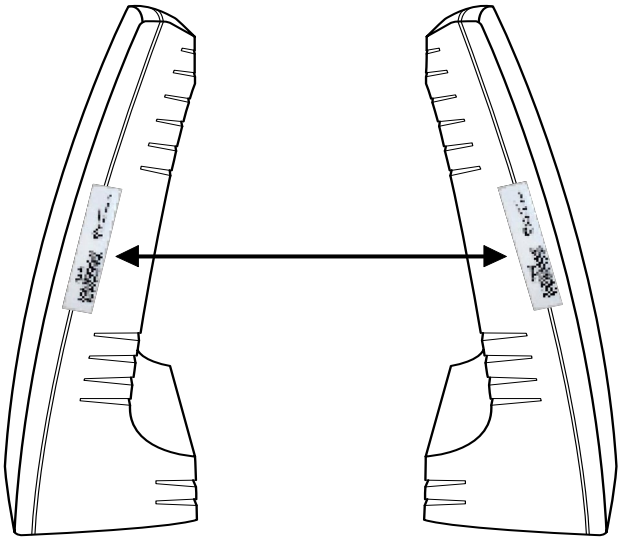


Figure 3 – Placement of Tamper-Evident Seals on Sides of Enclosure

Figure 4 shows where a tamper-evident seal must be affixed on the bottom of the enclosure. This seal prevents the bottom part of the enclosure from being opened to allow access to the internals of the CN105x without the presence of tamper evidence.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

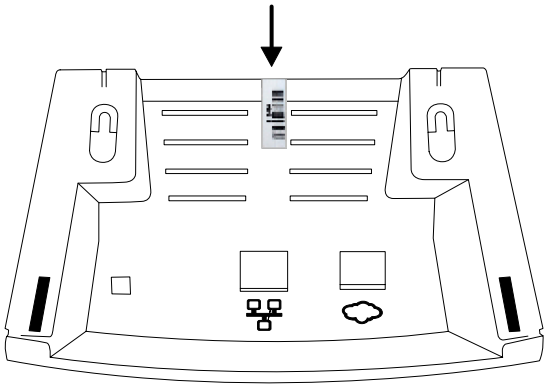


Figure 4 – Placement of Tamper-Evident Seal on Enclosure Bottom

Figure 5 illustrates how a tamper-evident seal should be affixed to the wireless LAN card and the enclosure to prevent the card from being removed without leaving evidence. Notice that the seal covers one of the screws.

Figure 5 - Placement of Tamper-Evident Seal on Wireless LAN Card and Enclosure

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

2.3 FEATURES

The CN105x Cryptographic Module provides:

a. secure storage for passwords and CSPs;
b. an IPSec capability, consisting of IKE and ESP;
c. cryptographic libraries, including a FIPS-compliant one, with an API that allows other modules to call upon these libraries; and
d. hardware cryptography (Hifn 7901).

2.4 CN105X CRYPTOGRAPHIC MODULE BOUNDARY

The CN105x Cryptographic Module boundary is the hard plastic enclosure with a PCMCIA card in its slot. The CN105x Cryptographic Module is a multiple-chip standalone cryptographic module.

The primary components of the CN105x Cryptographic Module are the main CPU, the Hifn 7901 encryption accelerator chip, memory, the reset switch, and the LED array.

The following physical components have been excluded from the requirements of the FIPS 140-2 standard: the power management components, the Ethernet transceiver(s), the Ethernet switch (CN1054 Secure Wireless LAN Router only), the PCMCIA wireless card, and the boot ROM.

Some of the firmware providing firewall or router services have been excluded from the requirements of FIPS PUB 140-2.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

2.5 FIPS PUB 140-2 TARGETED LEVELS

Table 1 specifies the level targeted for each of the requirements groups of FIPS 140-2.

FIPS 140-2 Section	Target Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	Not Applicable
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	Not Applicable

Table 1 - FIPS 140-2 Section Targeted Levels

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

3 PRODUCT OPERATION

3.1 OVERVIEW

The CN1050 and CN1054 Wireless LAN Routers are general-purpose devices whose operational mode is configurable through an administrative interface. This section describes how to operate the device, and the cryptographic module, in FIPS Approved Mode. The *CN1050 Wireless Access Point Administrator's Guide* or the *CN1054 Wireless Access Point Administrator's Guide* should be consulted if a complete discussion of the product's operation is required.

3.2 FIPS APPROVED MODE OF OPERATION

3.2.1 Description

The FIPS Approved Mode of Operation is a special configuration of the CN105x, in which:

a. the unit is configured to operate in the FIPS 140-2 mode;
b. the Wireless LAN is configured to use IPSec or L2TP over IPSecVPN;
c. RADIUS authentication operates over an IPSec protected link; and
d. SNMP management of the unit operates over an IPSec protected link

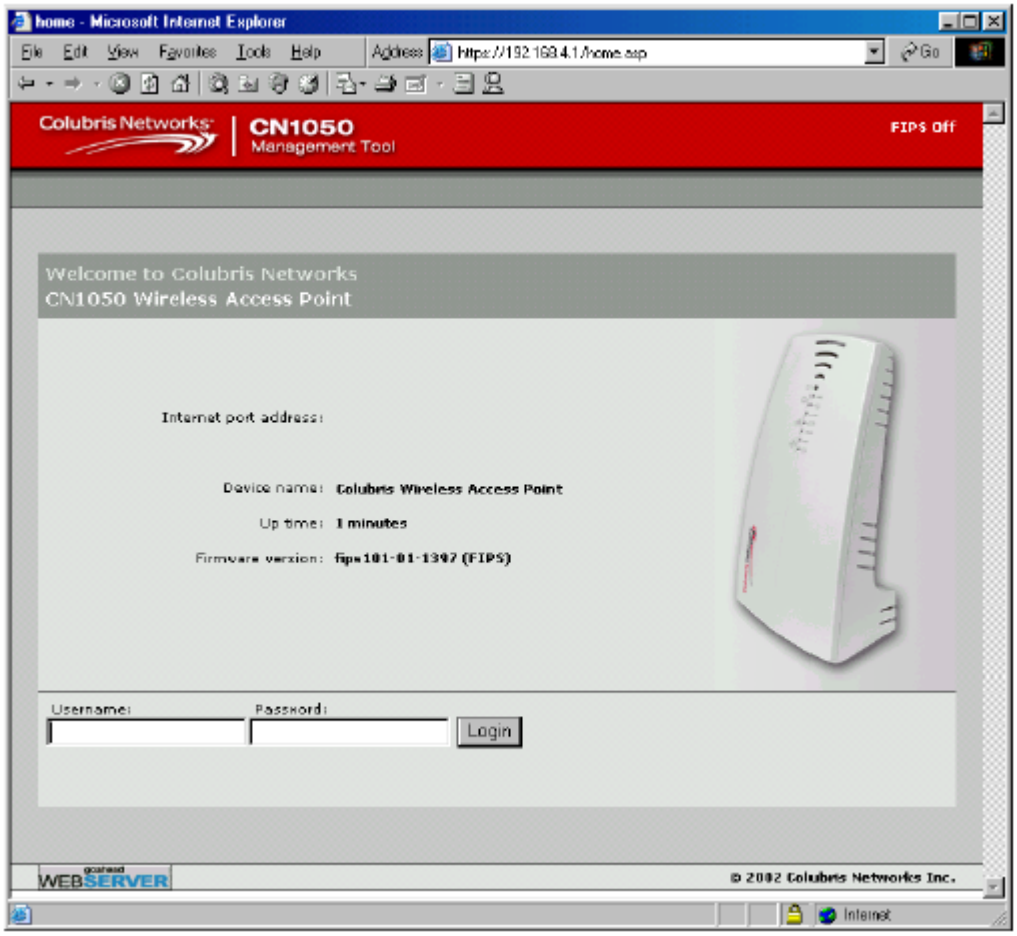
The instructions for configuring the unit in FIPS mode are provided in section 3.2.2.

COPYRIGHT COLUBRIS NETWORKS INC.

3.2.2 Instructions for Invoking FIPS Approved Mode of Operation

To enable FIPS 140-2 mode

1. Start your web browser and connect to the management tool.



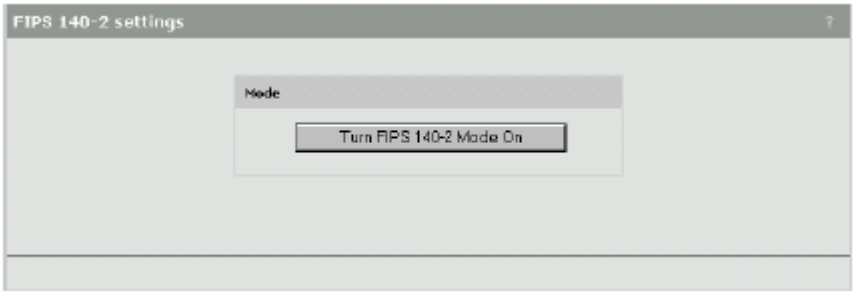
2. Login with username *admin* and password *admin*.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

3. If this is the first time you are logging in, you will be prompted to change the default administrator password. Click **Cancel**.

4. On the main menu, click **Security** and then click **FIPS 140-2**. The *FIPS 140-2 settings* page opens.

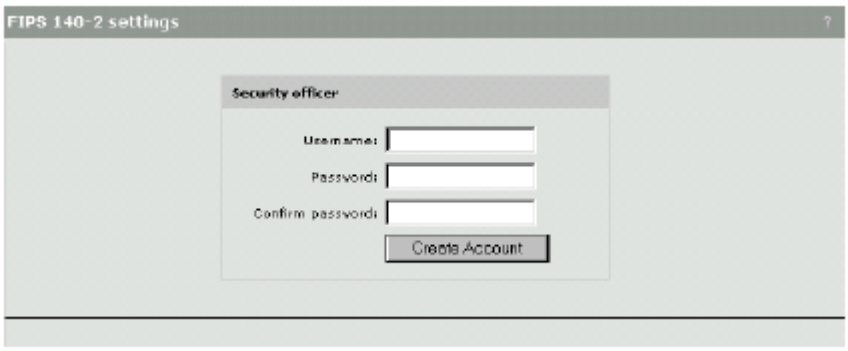


5. Click **Turn FIPS 140-2 Mode On**. The CN105x will reset to factory default settings and restart. Note that this resets the IP address of the LAN port to 192.168.4.1.
6. After the CN105x restarts, login with username *admin* and password *admin*.
7. You will be prompted to change the default administrator password. Specify a new password and click **Save**.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

8. You will be prompted to define the security officer account (This can also be done by clicking **Security** and then **FIPS 140-2)**.



9. Define a username and password for the security officer account. Both must be at least six characters long and contain at least four unique characters.
10. Log out.
11. The CN105x Cryptographic Module is now in FIPS 140-2 mode.
12. Log in using the security officer username and password.
13. You now have access to all configuration and security settings and can configure the CN105x as required.

Important notes:

When in FIPS 140-2 mode, the CN1050 uses TLS, with 3DES-SHA1, rather than SSL, to secure communication with the management tool. To communicate with the management tool, your web browser must be configured with TLS support.

When using a RADIUS server for authentication, the link between the CN105x and the RADIUS server must be protected by IPSec. An IPSec transport mode connection for the RADIUS server can be configured on the Security/IPSec page. Information on how to do this is provided in the *CN1050 Wireless Access Point Administrator's Guide* and the *CN1054 Wireless Access Point Administrator's Guide*.

In the FIPS Approved Mode of Operation of the CN105x, only FIPS-approved algorithms in the CN105x Cryptographic Module are called. Single DES must only be used for communicating with legacy systems.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

4 SECURITY RULES DERIVED FROM THE REQUIREMENTS OF FIPS PUB 140-2

4.1 FINITE STATE MODEL

The finite state model for the CN105x Cryptographic Module is shown and described in the *Finite State Model for the Colubris CN105x Wireless Access Point.*

4.2 ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC)

The CN105x is a wireless LAN device with an antenna providing 802.11 wireless signals. It is thus an intentional emitter.

The CN1050 Wireless LAN Router was tested as meeting FCC 47 CFR Part 15, Subpart B: 1999 Class B by Nemco Canada Inc.

The PCMCIA wireless card inserted into the CN1050 is an OEM product from Agere, and bears FCC ID: IMRWLPCE2411R.

The CN1054 Wireless LAN Router was tested as meeting FCC Part 15: 1998 Subpart B applicable radio standards by the Centre de Recherche Industrielle du Quebec.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

4.3 SELF-TESTS

4.3.1 Power-Up Self-Tests

The CN105x Cryptographic Module implements the following power-up self-tests that are initiated on the application of power:

- Firmware integrity test verifying the SHA-1 hash on all executables, shared libraries, and kernel loadable modules;

- Statistical random number generator tests monobit, poker, runs and long runs, according to Section 4.9.1 of FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* and Change Notice 1 for this standard, run on the output from the FIPS-approved deterministic random number generator from ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, section A.2;

- Known answer test on both implementations of SHA-1 in software;
- Encryption and decryption known answer tests on DES CBC in software;
- Encryption and decryption known answer tests on DES ECB in software;
- Encryption and decryption known answer tests on both implementations of 3DES CBC in software;
- Encryption and decryption known answer tests, with 128 and 256 bit keys, on both implementations of AES CBC in software;
- RSA in software tested with 1024 and 2048 bit keys;
- Known answer test on HMAC-SHA-1 in software;
- Encryption and decryption known answer tests on the Hifn 7901 implementation of 3DES CBC; and
- Known answer test on the Hifn 7901 implementation of SHA-1.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

4.3.2 Conditional Self-Tests

The CN105x Cryptographic Module implements the following conditional self-tests:

- Firmware load test, verification of a HMAC-SHA-1 signature, on the entire firmware loaded on to the CN1050 or CN1054;
- Pair-wise consistency tests on generated RSA key pairs;
- Cryptographic bypass test on peer-to-peer policies defined in the IPSec policy database; and
- Continuous random number generator tests on the FIPS-approved deterministic random number generator and on /dev/random, which provides random data for the seed key and seed value for the FIPS-approved RNG.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

4.4 DESIGN ASSURANCE

4.4.1 Delivery and Operation

Colubris tracks each shipment and is able to provide confirmation to the customer that a product with a FIPS-validated CN105x Cryptographic Module has been received. The *CN1050 Wireless Access Point Administrator's Guide* and the *CN1054 Wireless Access Point Administrator's Guide* describe how the user can validate the receipt of a CN105x Wireless LAN Router device with a FIPS 140-2 validated CN105x Cryptographic Module.

4.4.2 Functional Specification

The functional specification for the CN105x and the CN105x Cryptographic Module is contained in the *Functional Specification for the Colubris CN105x Wireless Access Point* document.

4.4.3 Guidance Documents

User and Crypto Officer guidance is contained for the CN105x Cryptographic Module in the *CN1050 Wireless Access Point Administrator's Guide* or the *CN1054 Wireless Access Point Administrator's Guide*.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

5 ADDITIONAL SECURITY RULES

1. The local certificate, CA certificate and SSL certificates may only be imported if the key length of the RSA public key is equal to or greater than 1024 bits.

2. The RSA public key entered for Building-to-Building mode is checked to verify it has a key length greater than or equal to 1024 bits.

3. IPSec client connections with X.509 certificates will only be allowed if the received certificate has been signed with RSA-SHA1 with an RSA key greater than or equal to 1024 bits.

4. IPSec Security Associations are restricted to transforms 3DES-SHA1 or AES-SHA1.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

6 IDENTIFICATION AND AUTHENTICATION POLICY

The identification and authentication policy includes specification of all roles, the associated type of authentication, the authentication data required of each role or operator, and the corresponding strength of the authentication mechanism.

Role	Type of Authentication	Authentication Data
Basic IPSec VPN User	Role-Based	IPSec Preshared Secret
XAUTH Basic IPSec VPN User	Identity-Based	IPSec Preshared Secret plus XAUTH Name and Password
X.509 IPSec VPN User	Identity-Based	X.509 Certificate
XAUTH X.509 IPSec VPN User	Identity-Based	X.509 Certificate plus XAUTH Name and Password
IPSec VPN User (Agressive Mode)	Identity-Based	IPSec Preshared Secret and group name
XAUTH IPSec VPN User (Aggressive Mode)	Identity-Based	IPSec Preshared Secret, group name and XAUTH Name and password
L2TP Over IPSec VPN User	Identity-Based	X.509 Certificate or IPSec Preshared Secret plus PPP user name and password (PAP, MSCHAPV2)
Security Officer (Crypto Officer)	Identity-Based	Security Officer Password
Administrator (Crypto Officer)	Identity-Based	Administrator Password

Table 2 - Roles and Required Identification and Authentication

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

Authentication Mechanism	Strength of Mechanism
IPSec Preshared Secret	6 characters per password with 4 unique; 82 different characters; probability of guessing password; 1 in 2.55 X 10^{11}
XAUTH Password	6 characters per password with 4 unique; 82 different characters; probability of guessing password; 1 in 2.55 X 10^{11}
Group Password	6 characters per password with 4 unique; 82 different characters; probability of guessing password; 1 in 2.55 X 10^{11}
X.509 Certificates	1024-bit RSA keys
Security Officer Password	6 characters per password with 4 unique; 82 different characters; probability of guessing password; 1 in 2.55 X 10^{11}
Administrator Password	6 characters per password with 4 unique; 82 different characters; probability of guessing password; 1 in 2.55 X 10^{11}

Table 3 - Strengths of Authentication Mechanisms

The User Role is assumed by providing one of the following sets of identification and authentication data from a computer connected via the wireless LAN, the wired LAN, or the Internet through IKE: IP address and IPSec preshared key; IP address and XAUTH password plus IPSec preshared key; X.509 certificate; and X.509 certificate plus XAUTH password.

The Security Officer Role, a Crypto Officer type role, is assumed by executing the Web Configurator and logging in with the Security Officer username and password. The Administrator Role, another Crypto Officer type role, is assumed by executing the Web Configurator and logging in with the Administrator username and password.

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

7 ACCESS CONTROL POLICY

7.1 OVERVIEW

This section discusses the access that operator X, performing service Y while in role Z, has to security-relevant data item W for every role, service, and security-relevant data item contained in the cryptographic module.

The specification is of sufficient detail to identify the cryptographic keys and CSPs that the operator has access to while performing a service, and the type(s) of access the operator has to the parameters.

7.2 CRYPTOGRAPHIC MODULE SERVICES

7.2.1 Show Status

Purpose:	Provide an indication that the cryptographic module is operating correctly.
Approved Functions:	SHA-1, DES, 3DES, AES, RSA, HMAC-SHA-1
Service Inputs:	Power-On
Service Outputs:	LED Array

Status lights indicate the operational status of the CN105x.

The Management Tool home page of the Web Configurator provides a quick overview of the operational status of the CN105x Cryptographic Module and provides a means of selecting more detailed status of the ports and connections.

7.2.2 Perform Power-Up Self-Tests

Purpose:	Verify that the CN105x Cryptographic Module is operating correctly.
Approved Functions:	SHA-1, DES, 3DES, AES, RSA, HMAC-SHA-1
Service Inputs:	Self-Test Command
Service Outputs:	Self-Test Result

COPYRIGHT COLUBRIS NETWORKS INC.

7.2.3 Perform IPSec IKE

Purpose:	Complete the IPSec IKE Exchange in preparation for ESP data transfer
Approved Functions:	Signature Verification, Diffie-Hellman Key Establishment, FIPS-Approved Random Number Generation
Service Inputs:	IKE Inputs
Service Outputs:	IKE Outputs

.

7.2.4 Perform IPSec ESP Transfers

Purpose:	Transfer data securely using the IPSec Encapsulating Security Payload packets.
Approved Functions:	AES, 3DES, SHA-1, HMAC-SHA-1
Service Inputs:	Packet to be Processed
Service Outputs:	Processed Packet

The Packet to be Processed may be an outgoing plaintext packet that is to be converted into an IPSec Packet before transmission or an incoming IPSec Packet that is to be converted into a plaintext packet.

7.2.5 Firmware Load

Purpose:	Upgrade Firmware
Approved Function:	HMAC-SHA-1
Service Inputs:	New Firmware to be Loaded on CN105x
Service Outputs:	New Firmware Loaded on CN105x

7.2.6 Configuration File Export

Purpose:	Export Configuration File for Backup
Approved Function:	3DES
Service Inputs:	Backup Selected
Service Outputs:	Configuration File with Encrypted Preshared Secrets, Passwords, Session Key, and Local RSA Private Key

COPYRIGHT COLUBRIS NETWORKS INC.

7.2.7 Plaintext Key and CSP Zeroization

Purpose:	Zeroize Plaintext Cryptographic Keys and CSPs
Approved Function:	Zeroization
Service Inputs:	Holding of Reset Button
Service Outputs:	Factory Defaults Reset, Flash Memory Zeroized

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

7.3 SECURITY DATA

7.3.1 General

Security data comprises all cryptographic keys and CSPs employed by the cryptographic module, including secret, private, and public cryptographic keys (both plaintext and encrypted), authentication data such as passwords or PINs, and other security-relevant information (e.g., audited events and audit data).

The CN105x Cryptographic Module implements the following non-FIPS approved cryptographic algorithms: RC4, MD5, MD4, HMAC-MD5, and Diffie-Hellman (for key agreement). The CN105x Cryptographic Module also implements SHA-2, which cannot be used in the FIPS-approved mode of operation.

7.3.2 Keys

3DES Secret Keys
DES Secret Keys
AES Secret Keys
RSA Public and Private Keys

RSA public keys in X.509 certificates are stored by the CN105x Cryptographic Module.

7.3.3 Critical Security Parameters

IPSec Preshared secret
Security Officer password
Administrator password
XAUTH password
Group password

COPYRIGHT COLUBRIS NETWORKS INC.

7.4 ROLES, SERVICES AND ACCESSES

7.4.1 Role-Based Services

This section discusses, for each role, the services an operator is authorized to perform within that role, and for each service within each role, the type(s) of access to the cryptographic keys and CSPs.

Role	Authorized Services
IPSec VPN User (independent of authorization type)	Perform IPSec IKE Perform IPSec ESP Transfers
Security Officer (Crypto Officer)	Show Status Perform Self-Tests (Command)
Administrator (Crypto Officer)	Firmware Load Configuration File Export

Table 4 - Services Authorized for Roles

Service	Cryptographic Keys and CSPs	Type(s) of Access (e.g. Read, Write, Execute)
Show Status	Administrator Password, Security Officer Password	E
Perform Self-Tests	3DES, DES, AES, RSA (Self-Test Only Keys)	E
Perform IPSec IKE	IPSec Preshared Key	E
	RSA Public Key	R, E
	3DES, AES	W
Perform IPSec ESP Transfers	3DES, AES	E
Firmware Load	Administrator Password	E
	3DES, AES	E
Configuration File Export	Administrator Password	E
	3DES Master Key	E
	3DES, AES	W
	Local RSA Key	W
Plaintext Key and CSP Zeroization	Administrator Password, Security Officer Password, IPSec Preshared Keys, 3DES, DES, AES, RSA Keys, Local RSA Key	None

Table 5 - Access Rights Within Services

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

7.4.2 Anonymous Services

The following services are provided to users without requiring them to assume an authorized role.

Service	Description	Security Considerations
Perform Self-Test	The Initial Self-Test of the cryptographic module does not require the operator to assume a role. It requires only that the reset button be pressed or the system power be changed from OFF to ON	The Initial Self-Test does not use operational keys or CSPs and therefore does not affect the security of the module.
Plaintext Key and CSP Zeroization	The reset button is pressed and held for approximately 5 seconds until the lights start flashing.	Plaintext keys and CSPs are zeroized; therefore this service prevents access.

Table 6 - Anonymous Services

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

8 PHYSICAL SECURITY POLICY

8.1 OVERVIEW

This section discusses the physical security mechanisms that are implemented to protect the Colubris CN105x Cryptographic Module and the actions that are required to ensure that the physical security of the module is maintained.

8.2 PHYSICAL SECURITY MECHANISMS

8.2.1 Tamper-Evident Seals

The CN105x Cryptographic Module is completely enclosed with a hard plastic production-grade enclosure and a PCMCIA wireless LAN card.

The CN105x is protected by tamper-evident seals on the sides and bottom of the enclosure and by a tamper-evident seal affixed to the PCMCIA card and the enclosure. The seal affixed to the PCMCIA card and enclosure also covers one of the screws holding the top of the enclosure together. Figure 3, Figure 4, and Figure 5 show the locations of the four affixed seals.

The tamper-evident seals provided by Colubris should be kept in a locked cabinet accessible only by the CN105x Cryptographic Module Security Officer (Crypto Officer). The CN105x should be kept in a locked cabinet until the tamper-evident seals are affixed.

8.3 INSPECTION AND TESTING

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Weekly	Examine visually for evidence that any seal has been damaged, broken, says “VOID”, or is missing.

Table 7 - Inspection/Testing of Physical Security Mechanisms

COPYRIGHT COLUBRIS NETWORKS INC.

COPYRIGHT COLUBRIS NETWORKS INC.

9 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS

9.1 OVERVIEW

The Colubris CN105x Cryptographic Module does not mitigate against specific attacks for which testable requirements are not defined in FIPS 140-2.

9.2 MECHANISMS IMPLEMENTED

Not applicable

9.3 MITIGATION SUMMARY

Other Attacks	Mitigation Mechanisms	Specific Limitations
None	N/A	N/A

Table 8 - Mitigation of Other Attacks

COPYRIGHT COLUBRIS NETWORKS INC.