Avaya, Inc.

Secure Router 2330

Hardware Version: SR2330; Firmware Version: 10.3.0.100

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.6

Prepared for:

Avaya, Inc.
211 Mt. Airy Road
Basking Ridge, NJ 07920
USA

Phone: +1 (866) 462-8292
http://www.avaya.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
USA

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Secure Router 2330 from Avaya, Inc.. This Security Policy describes how the Secure Router 2330 meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The Secure Router 2330 is referred to in this document as SR2330, the router, or the module.

1.2 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 Avaya website (http://www.avaya.com/usa/products/products-a-z) contains information on the full line of products from Avaya.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

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

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Avaya. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Avaya and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Avaya.

2 Secure Router 2330

2.1 Overview

The Avaya Secure Router 2330 (or SR2330), a converged voice/data branch solution, is a powerful modular system that combines routing, voice gateway, security and multimedia traffic forwarding into a single cost-effective platform for enterprises. The SR2330 delivers fast, secure, reliable, and scalable wide area network (WAN) access, making it ideal for enterprises requiring high-speed IP[1] or Internet access.

The major features of SR2330 are:

- Powerful Routing Services: The SR2330 provides full IPv4 and IPv6, BGP[2]-4, and multicast routing for sophisticated enterprise deployments.
- Bridge Voice and Data: An integrated voice media gateway allows you to connect to the PSTN[3] or traditional telephony devices.
- WAN Connectivity: The SR2330 offers a wide range of WAN connectivity options, including T1/E1, serial, ISDN[4], and ADSL[5]2+.
- Security: A stateful firewall and high-speed VPN[6] encryption allows you to connect securely to the Internet or an IP network.
- Maximum Uptime: Hot-swappable cards, redundant power and port/platform resilience features reduce service interruptions.

The router is a 1U[7] rack-mountable appliance. A picture of the SR2330 is shown below in Figure 1.

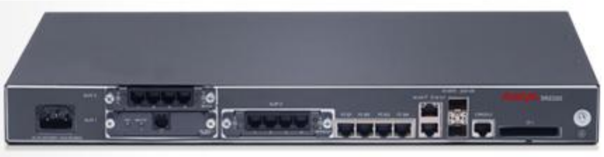

Figure 1 – SR2330 Router

The SR2330 is primarily intended to act as a branch office router that securely communicates with a central office and remote offices. As depicted in Figure 2, the SR2330 is intended to be deployed as the connection between a branch or regional office and a public internet. The SR2330 can connect with other Avaya Secure Router products, or any other compatible VPN devices.

[1] IP – Internet Protocol
[2] BGP – Border Gateway Protocol
[3] PSTN – Public Switched Telephone Network
[4] ISDN – Integrated Services Digital Network
[5] ADSL – Asymmetric Digital Subscriber Line
[6] VPN – Virtual Private Network
[7] U – Unit

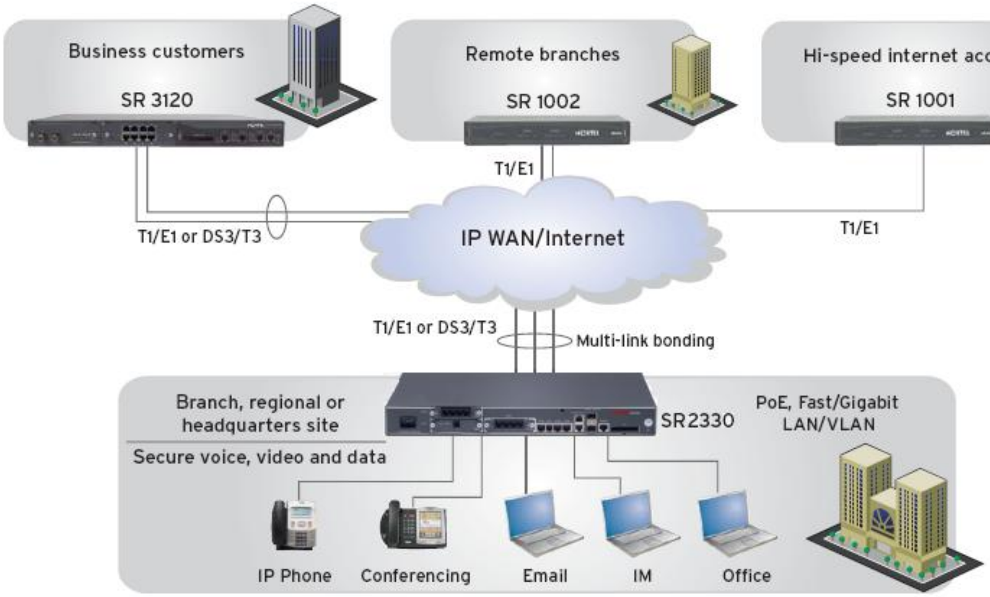

Figure 2 – SR2330 Deployed as a Branch Office Router

The SR2330 allows users to create IP VPNs using Multiprotocol Label Switching (MPLS) or IPsec[8]. Administrators can then locally or remotely manage the SR2330 with a management Command Line Interface (CLI) via the serial console or via Secure Shell (SSH) version 2 (SSH2). The serial console is accessed through an RJ45[9] port on the front of the SR2330.

The Secure Router 2330 is validated at the FIPS 140-2 Section levels listed in Table 1 below. The overall security level of the module is 2.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[10]
7	Cryptographic Key Management	2
8	EMI/EMC[11]	2
9	Self-tests	2
10	Design Assurance	2

[8] IPsec – Internet Protocol Security
[9] RJ45 – a registered jack connector type used in telephone/networking installations
[10] N/A – Not Applicable
[11] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Specification

The Secure Router 2330 is a hardware module Hardware Version: SR2330; Firmware Version: 10.3.0.100 with a multi-chip standalone embodiment. The cryptographic boundary of the Secure Router 2330 is defined by the chassis of the router.

The boundary includes three small card interfaces. A list of cards that can be placed in the small card interface slots is given below:

- 2-port T1/E1 Small Card (Assembly Number: 333-70225-01 Rev 4)
- 2-port Serial Small Card (Assembly Number: 333-70240-01 Rev 02.0011)
- 1-port ADSL2+ Annex A Small Card (Assembly Number: 333-70260-01 Rev 01)

The SR2330 contains a security internal card, which is required for VPN acceleration and IPsec. The SR2330 comes installed with a Safenet 1141/1741 chip as a hardware cryptographic accelerator providing VPN acceleration and some IPsec functionalities.

2.3 Module Interfaces

The SR2330 consists of Ethernet ports, a console port, an external compact flash port, external card interface slots and status LED[12]s. The external compact flash port is disabled. The three small card interface slots (external card interface) are 68-pin PCMCIA[13]-style connectors, which can be used to add/replace networking or communication cards.

The physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Data input/output are the packets utilizing the services provided by the module. These packets enter and exit the module through the network ports (Ethernet ports). Control input consists of Configuration or Administration data entered into the module through the Command Line Interface (CLI) management interface. Any user can be given administrative permissions by the Crypto Officer (CO). Status output consists of the status provided displayed via the LEDs and log information.

The front panel of the SR2330 is shown in Figure 3. Descriptions of all ports present in the front panel are given in Table 2.

[12] LED – Light Emitting Diode

[13] PCMCIA – Personal Computer Memory Card International Association

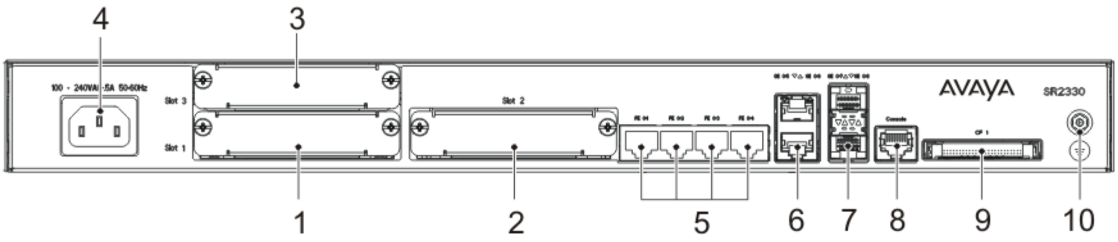

Figure 3 – SR2330 Router Front Panel (with Card Slot Covers Installed)

Table 2 – SR2330 Front Panel Ports and Interfaces

Item	Description
1	Small Card slot 1
2	Small Card slot 2
3	Small Card slot 3
4	Power input
5	Four Fast Ethernet ports (FE[14] 0/1 through FE 0/4)
6	Two 10/100/1000Base-T ports (GE[15] 0/5 and 0/6), which use dual RJ[16]-45 connector with integrated Gigabit Ethernet magnetics
7	Two Small Form-factor Pluggable (SFP) ports (GE 0/7 and 0/8), for plug-in SFP cards
8	Console port (management port)
9	Compact Flash slot (CF1)
10	Ground lug

The rear panel of the SR2330 is shown in Figure 4. Descriptions of all ports present in rear panel are given in

Table 3.

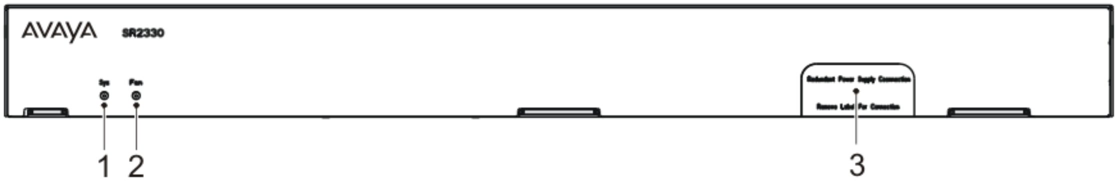
AVAYA
SR2330
Sys
Fan
Redundant Power Supply Connection
Remove Label For Connection
1
2
3

Figure 4 – SR2330 Rear Panel

[14] FE –Fast Ethernet
[15] GE – Gigabit Ethernet
[16] RJ – Registered Jack

Table 3 – SR2330 Rear Panel Ports and Interfaces

Item	Description
1	System LED indicator
2	Fan LED indicator
3	Redundant 12VDC power input

Each Ethernet port has a LED associated with it, which indicates the status of the port. If the cable is not connected or no link is established, then the LED is OFF. When a cable is connected and a link is established, the LED turns GREEN. The System and Fan LED Status indications are described in Table 4.

Table 4 – SR2330 System and Fan LED Status Indications

LED	Color	Definition
System Status LED (SYS)	OFF	The Secure Router 2330 is not powered.
	GREEN	The Secure Router 2330 is powered and is operating normally.
	RED	The Secure Router 2330 is powered, but one or more tasks have failed.
Fan Status LED (FAN)	GREEN	The internal fans are functional.
	RED	There is a fan fault condition.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 5 below.

Table 5 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Ethernet (FE or GE)	4 (FE) 2 (GE)	• Data Input • Data Output • Control Input • Status Output
SFP ports	2	• Data Input • Data Output • Control Input • Status Output
Small Card Interface slots	3	• Data Input • Data Output • Control Input • Status Output
Console	1	• Control Input • Status Output

.

Physical Port/Interface	Quantity	FIPS 140-2 Interface
LEDs	10	• Status Output
Power	2	• Power Input

2.4 Roles and Services

The module supports role-based authentication. Each operator is associated with a specific role. There are two roles in the module (as required by FIPS 140-2) that operators may be assigned: a Crypto Officer role and a User role.

The Crypto Officer (CO) role is the administrator for the router and can perform the setup, module maintenance, and new User management tasks. The User role has the ability to perform configuration and monitoring tasks.

Descriptions of the services available to the Crypto Officer and User roles are provided in the Table 6 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 6 – Operator Services*

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Commission the module	✓		Commission the module by following the Security Policy guidelines	None	None	None
Create users	✓		Create, edit; and delete users; define user accounts and assign permissions.	Command	Command response and status output	Crypto Officer password – W
Change CO Password	✓		Change the Crypto Officer password	Command	Command response and status output	Crypto Officer password – W
Change User Password		✓	Change the User password	Command	Command response and status output	User password – W

* Note: For the list of non-approved services, please refer to section 3.2.1 below.

.

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Access the CLI	✓	✓	Access the CLI via Console or Ethernet port to configure or monitor status of the system	Command and parameters	Command response and status output	Crypto Officer password – W Preshared key – X IKE[17] Phase 1 Session key – W IPSec Phase 2 Session key – W SSH Session key – W DSA[18] private keys – X DH[19] private keys – X
Configure routing services	✓	✓	Configure IP stack and firewall related features	Command and parameters	Command response	Preshared key – X IKE Phase 1 Session key – W IPSec Phase 2 Session key – W SSH Session key – W DSA private keys – X DH private keys – X
Employ SSH service	✓	✓	Manage the module using SSH2 protocol.	Command and parameters	Command response	SSH Session key – W DSA private keys – X
Employ VPN service	✓	✓	Establish VPN session, authenticate and use VPN services	Command and parameters	Command response	Preshared key – X IKE Phase 1 Session key – W IPSec Phase 2 Session key – W DSA private keys – X DH private keys – X
Zeroize Keys	✓	✓	Zeroize unprotected keys and CSPs	Command and parameters such as "reboot", "password" or file delete commands	Command response	Crypto Officer password – W User password – W
Perform Self Tests	✓	✓	Perform Power-up Self Tests on demand.	Command	Command response	None

[17] IKE – Internet Key Exchange
[18] DSA – Digital Signature Algorithm
[19] DH – Diffie Hellman

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Show Status	✓	✓	Facilitates the user to check whether the module is in FIPS-Approved mode or not	None	None	None

All services provided by the module require the operator to assume a role, and the module authenticates the role before providing any services. The module performs role-based authentication.

Operators authenticate to the module using a username and password. When authenticating with a Crypto Officer role credential, the operator explicitly assumes both the Crypto Officer and User roles. When authenticating with a User role credential, the operator explicitly assumes the User role. Table 7 lists the authentication mechanisms used by the module. A Crypto Officer or a User communicating via SSH client can be authenticated via public-key authentication or password based authentication.

Table 7 – Authentication Mechanism

Authentication Type	Strength
Password	The minimum length of the password is eight, with 62 different case-sensitive alphanumeric characters and symbols possible for usage. The chance of a random attempt falsely succeeding is $1{:}62^8$, or 1:218,340,105,584,896. The fastest network connection supported by the module is 100 Mbps. Hence at most $(100 \times 10^6 \times 60 = 6 \times 10^9 =)$ 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than $1{:}\ (62^8 / 6\times 10^9)$, or 1: 291,120, which is less than 100,000 as required by FIPS 140-2.
Public key certificates	The module supports RSA and DSA digital certificate authentication of users during IPsec/IKE. Using conservative estimates and equating a 1024 bit RSA or DSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is $1{:}2^{80}$ or 1: 1,208,925,819,614,629,174,706,176. The fastest network connection supported by the module is 100 Mbps. Hence at most $(100 \times 10^6 \times 60 = 6 \times 10^9 =)$ 6,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than $1{:}\ (2^{80} / 6\times 10^9)$, or 1: 201,487,636,602,438, which is less than 100,000 as required by FIPS 140-2.

The Simple Network Management Protocol (SNMP) services are provided without authentication. An unauthenticated operator uses a community string to access the SNMP services. The SNMP implemented in the routers only allows the unauthenticated operator to get non-security-relevant system condition information. The SNMP services do not affect the security of the module.

2.5 Physical Security

The Secure Router 2330 is a multi-chip standalone cryptographic module. It is enclosed in a hard and opaque metal case that completely encloses all of its internal components. There are only a limited set of vent holes provided in the case, and the view of the internal components of the module is obscured by the baffling provided by the power supply unit (on the left hand side) and the Fan unit (on the right hand side). Tamper-evident labels are applied to the case as well as all removable cards and covers to provide physical evidence of attempts to gain access to the module's internal components. All of the module's components are production grade. The placement of tamper-evident labels can be found in Section 3.1 of this document.

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.6 Operational Environment

The operational environment requirements do not apply to the Secure Router 2330, because the module does not provide a general-purpose operating system (OS) to the user. The Secure Router 2330 employs a VxWorks-based kernel; it is a non-modifiable OS that provides only a limited operational environment, and only the module's custom written image can be run on the system. All firmware updates are digitally-signed using RSA and a self-test is performed during each update.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 8 below.

Table 8 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	Firmware	Hardware
Advanced Encryption Standard (AES) in CBC[20]mode (128, 192, 256-bit keys)	1606	96
Triple Data Encryption Standard (TDES) in CBC mode (Three-Key)	1051	210
Secure Hash Algorithm (SHA)-1	1419	187
Keyed-Hash Message Authentication Code (HMAC) using SHA-1	942	N/A
RSA[21] signature verification (PKCS[22]#1 v1.5) (2048, 3072, 4096-bits)	788	N/A
Digital Signature Algorithm (DSA) key generation, signature generation/verification	497	N/A
SP[23] 800-90 Hash-Based DRBG[24] (SHA-256)	80	N/A
SHA-256 for DRBG	1419	N/A

The module uses the FIPS-Approved SP 800-90 Hash DRBG to generate cryptographic keys. It uses a DRBG implementation from Network Security Services (NSS), release version 3.12.8. The module does not receive a seed value for PRNG from outside; rather, it is seeded via a Non-Deterministic Random Number Generator (NDRNG), which is generated from cryptographic hardware accelerator chip, Safenet 1140/1741. The SHA-256 is used only for DRBG implementation and it is not accessible for any other purposes.

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementations:

- MD5[25] used in TACACS+[26], VoIP[27], and routing services

[20] CBC – Cipher Block Chaining
[21] RSA – Rivest Shamir Adleman
[22] PKCS – Public-Key Cryptography Standards
[23] SP – Special Publication
[24] DRBG – Deterministic Random Bit Generator

.

- Hardware random number generator – for seeding the FIPS-Approved DRBG
- Blowfish
- DES
- RSA key-pair generation
- RSA signature generation
- Diffie-Hellman for key agreement during IPsec: 1024, 1536, 2048 or 3072-bit keys (provides 80, 96, 112 or 128 bits of security, respectively).
- Diffie-Hellman for key agreement during SSH: 1024-bit key (provides 80 bits of security).

The module utilizes the following algorithm implementations that are FIPS-Allowed but deprecated (the user must accept some risks). For further details regarding deprecation please refer to NIST special publication, SP800-131A.

- Diffie-Hellman for key agreement during IPsec (1024 and 1536-bit keys).
- Diffie-Hellman for key agreement during SSH (1024-bit key).
- SHA-1 for digital signature generation and verification.
- HMAC (with key length >= 80-bits but < 112-bits)
- DSA (1024-bit).

[25] MD5 – Message Digest 5

[26] TACACS – Terminal Access Controller Access Control Systems Plus

[27] VoIP – Voice Over Internet Protocol

.

The module supports the critical security parameters (CSPs) listed below in Table 9.

Table 9 –Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IKE Preshared key	Shared secret	Entered by the CO or User	Can be exported by the CO or User in plaintext over the console port	Plaintext in internal NVRAM[28]	File deletion using CLI commands	Peer Authentication of IKE session
IKE Phase 1 Symmetric key	1024, 1536, 2048, 3072 bits symmetric keys generated via DH key agreement	Generated internally during IKE negotiation	Never exit the module	Plaintext in internal NVRAM	Reboot or session termination	Exchanging shared secret during IKE
IPsec Phase 2 Symmetric key	AES-128, 192, 256 or TDES key	Generated internally during IKE negotiation	Never exit the module	Plaintext in internal NVRAM	Reboot or session termination	Encryption or decryption of IPSec packets
SSH Symmetric key	1024-bit Symmetric key generated via DH key agreement	Diffie-Hellman key agreement	Never exit the module	Plaintext in NVRAM	Reboot or session termination	Encryption or decryption during SSH
HMAC key	Shared key generated via DH key agreement	Generated internally during IKE negotiation	Never exit the module	Plaintext in NVRAM	Reboot or session termination	IKE negotiation and support isakmp messages
DRBG seed C value	Random value	Generated internally by the hardware NDRNG.	Never exit the module	Plaintext in NVRAM	Reboot or session termination	Generate random number
DRBG seed V value	Random value	Generated internally by the hardware NDRNG.	Never exit the module	Plaintext in NVRAM	Reboot or session termination	Generate random number
Password for Private-key file	Passphrase used to obscure the DSA private-key files	Entered by the CO or User	Never exit the module	Plaintext in NVRAM	Zeroized when the password is updated with a new one	To obscure the DSA private key files using AES-128

[28] NVRAM – Non Volatile Random Access Memory

.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
RSA public key	1024, 2048, 3072, 4096 bits	Enters the module in plaintext.	The module's Public key exits the module in plaintext.	Plaintext in NVRAM	File deletion using CLI commands	Keys used during SSH authentication and Firmware load tests
DSA public key	1024 bits	The module's Public key is generated internally for PKI authentication, IKE authentication and SSH key negotiation; while public key of a peer enters the module in plaintext.	The module's Public key exits the module in plaintext.	Plaintext in NVRAM	File deletion using CLI commands	Keys used for PKI authentication and during IPsec/IKE and SSH key negotiation
DSA private key	1024 bits	Generated internally for PKI authentication, IKE authentication and SSH key negotiation	Never exits the module	Plaintext or encrypted in NVRAM	File deletion using CLI commands	Private key used for PKI authentication , and during IPsec/IKE and SSH key negotiation
DH public key	1024, 1536, 2048, 3072 bits	The module's Public key is generated internally; while public key of a peer enters the module in plaintext.	The module's Public key exits the module in plaintext.	Plaintext in NVRAM	Reboot or session termination	Generation of IKE Key Agreement key and SSH Session key
DH private key	1024, 1536, 2048, 3072 bits	Generated internally	Never exits the module	Plaintext in NVRAM	Reboot or session termination	Generation of IKE Key Agreement key and SSH Session key
Crypto Officer password	Minimum of eight characters of alphanumeric string	Entered into module via a console port or over SSH	Never exits the module	Plaintext in NVRAM	Zeroized when the password is updated with a new one	Used for authenticating the Crypto Officer
User password	Minimum of eight characters of alphanumeric string	Entered into module via a console port or over SSH	Never exits the module	Plaintext in NVRAM	Zeroized when the password is updated with a new one	Used for authenticating the User

2.8 Self-Tests

The module implements cryptographic algorithms using firmware (OpenSSL and NSS) as well as hardware accelerator, and the module performs various Self-Tests (Power-Up Self-Tests and Conditional Self-Tests) to verify their functionality and correctness. Upon self-test failure, the module goes into “Critical Error state” and it disables all access to cryptographic functions and CSPs. All data outputs are inhibited upon a self-test failure. A permanent error status will be recorded to the system log file and/or event audit log file. The task that invoked the failed self-test will be suspended. The current operation will not complete and the module goes into “Critical Error state”, which halts the module. This error state is visible via the console or terminal, where the module does not respond to any commands. The CO must reboot the machine to clear the error condition and return to a normal operational state.

2.8.1 Power-Up Self-Tests

The Secure Router 2330 performs the following self-tests at power-up to verify the integrity of the firmware binaries and the correct operation of the FIPS-Approved algorithm implementations employed by the module:

- Firmware integrity check using 32-bit CRC[29] for boot ROM[30] image
- Firmware integrity check using 32-bit CRC for run-time application image
- Cryptographic algorithm tests:
    - AES-CBC-256 Known Answer Tests (KAT) for OpenSSL and Safenet chip implementations.
    - Triple-DES[31] KATs for both OpenSSL and Safenet chip implementations.
    - RSA sign/verify test for OpenSSL implementation.
    - DSA sign/verify test for OpenSSL implementation.
    - DSA pairwise consistency test for OpenSSL implementation.
    - SP 800-90 DRBG KAT for NSS implementation.
    - SHA-1 KATs for both OpenSSL and Safenet chip implementations.
    - HMAC SHA-1 KATs for both OpenSSL and Safenet chip implementations.
- Critical function tests for DRBG instantiation and reseed, as specified in SP 800-90. DRBG will go through reseed process only when its lifetime gets expired.

The CO can perform the power-up self-tests at any time by power-cycling the module or issuing a reboot command over the module’s CLI.

2.8.2 Conditional Self-Tests

The Secure Router 2330 performs the following conditional self-tests:

- DSA Pairwise consistency test for OpenSSL implementation.
- Continuous DRBG test for NSS implementation.
- Continuous RNG test for non-approved NDRNG, which is used to seed DRBG.
- Bypass mode test
- Firmware update test

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

[29] CRC – Cyclic Redundancy Check

[30] ROM – Random Access Memory

[31] DES – Data Encryption Standard

3 Secure Operation

The Secure Router 2330 meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Initial Setup

The CO is responsible for commissioning the router and powering it up. Before powering-up the router, the CO must ensure that the required tamper-evident labels (included in the FIPS kit) are correctly applied to the router enclosures following the instructions below.

It is the responsibility of the Crypto Officer to apply the tamper-evident labels to the module. The instructions for applying the tamper evident labels are as follows:

1. The surface must be cleaned with isopropyl alcohol (99%) to remove surface contaminants.
   a. Rubbing alcohol is not acceptable because it may contain oils to minimize the drying effect on skin; these oils can interfere with the adhesion.
   b. Lower concentrations of alcohol (90%, 70%, etc) are not recommended, because the non-alcohol portion is not a cleaning agent and may inhibit optimum adhesion.
2. The surface must be dried using a clean paper towel or cotton cloth (allowing to air dry is not recommended).
3. The surface temperature must be minimum +50F.
4. The labels must be applied 72 hours before the module is placed into operation.

Four tamper evident labels must be placed as follows to provide the required physical security:

1. Two small-sized labels must be applied horizontally between the front panel chassis and the front panel removable cards (or blanks, in case the cards are not present) in slot 1 and slot 3, as shown by the red-dotted lines in Figure 5.
2. One small-sized label must be applied vertically between the bare-metal bottom chassis and the front panel removable card (or blank, in case the card is not present) in slot 2, as shown by blue-dotted lines in Figure 5.
3. One big-sized label must be applied between the rear panel and bare-metal bottom chassis (in horizontal position), covering the center screw head as shown in Figure 6.

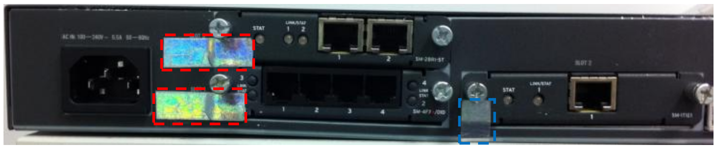

Figure 5 - Tamper Evident Labels 1, 2, 3

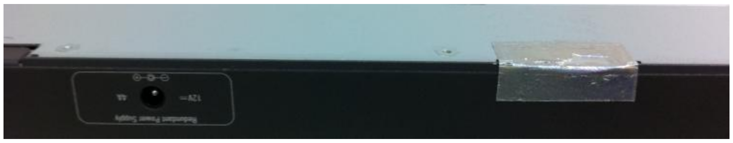

Figure 6 - Tamper Evident Label 4

3.2 Secure Management

The SR2330 has a non-modifiable OS and by default it is in FIPS-Approved mode of operation.

.

3.2.1 Initialization

As soon as the module is powered-up, it boots and performs start-up self-tests and enters in to FIPS-Approved mode of operation. The following features/services shall not be used in the FIPS-Approved mode of operation:

- Debugging services
- Telnet
- FTP[32] services
- RSA key-pair generation
- RSA signature generation
- External Compact Flash slot

It is the Crypto Officer's responsibility to ensure that the module boots correctly, to verify that the services/features that are supposed to be disabled as mentioned above, are disabled, and configure the module properly. The module is shipped with a default administrator ID and password. The CO is required to change the default password as part of initial configuration. The Crypto Officer password must be at least 8 characters in length. If the CO had to change any configurations to make the module FIPS compliant, then the CO must follow the zeroization procedure as mentioned in section 3.2.3, save the configuration and perform a reboot. Upon reboot, initialization of the module in FIPS compliant mode is complete and the module is now configured securely. The CO should not enable any of the disabled services mentioned previously, if any of the non-approved services are enabled then the module is not in the FIPS-Approved mode of operation. In that case, the CO must disable the non-approved services and perform a reboot.

3.2.2 Management

The Crypto Officer must be sure to only configure cryptographic services for the module using the FIPS-Approved algorithms as listed in the Cryptographic Key Management section above. IPsec and SSH must only be configured to use FIPS-Approved cipher suites, and only digital certificates generated with FIPS-Approved algorithms may be utilized. The module implements RSA key-pair generation method that is non-conformant to the FIPS 140-2 standard and hence shall not be used in the FIPS-Approved mode of operation. The CO shall not import or export keys via the FTP client. The CO can modify the bypass functionality by modifying the configuration of the IPsec tunnel and then enabling the IPsec tunnel.

If any catastrophic event (such as high power surge) results in damaging the removable cards, the module should be sent back to the manufacturing factory or the CO is allowed to replace a removable card. The CO must power down the module, replace the required removable card/s, re-apply the tamper evident label, following the procedure as described in section 3.1 and power-up the module. The CO must ensure at all times that the labels do not show any signs of tampering. Evidence of tampering can be indicated by any of the following:

- Deformation of the label
- Label appearing broken or torn
- Missing label (in parts of full) from its expected position
- Label showing "OPENED" or "VOID" text

3.2.3 Zeroization

The module stores the preshared key and the security keys as plaintext in Flash memory.

There are many critical security parameters (CSP) within the Secure Router cryptographic boundary, including private keys, certificate secret credentials, system configuration files and logon passwords. All ephemeral keys used by the module are zeroized on reboot or session termination. CSPs reside in multiple

[32] FTP – File Transfer Protocol

storage media including the system memory, non-volatile memory, and device private memory. These keys are zeroized when the module is rebooted. The Crypto Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed. Other keys and CSP such as public and private keys that are stored in the Flash within a file can be zeroized by the Crypto Officer by deleting the files using CLI commands.

3.3 User Guidance

The User is capable of making configuration changes, but configuration changes must be approved by a Crypto Officer before implementation. The module implements RSA key-pair generation method that is non-conformant to the FIPS 140-2 standard and hence shall not be used in the FIPS-Approved mode of operation. The user shall not use DH with key size 768-bits. The User shall not import or export keys via the FTP client. The User must be diligent to pick strong passwords (alphanumeric with minimum 8 characters), and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as IPsec session keys. The User should report to the Crypto Officer if any irregular activity is noticed.

4 Acronyms

This section describes the acronyms used throughout this document.

Table 10 – Acronyms

Acronym	Definition
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CAMA	Centralized Automatic Message Accounting
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie Hellman
DID	Direct Inward Dial
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FE	Fast Ethernet
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GE	Gigabit Ethernet
HMAC	(Keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network

.

Acronym	Definition
KAT	Known Answer Test
LED	Light Emitting Diode
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
NVRAM	Non Volatile Random Access Memory
OS	Operating System
PCMCIA	Personal Computer Memory Card International Association
PKCS	Public-Key Cryptography Standards
PSTN	Public Switched Telephone Network
RJ	Registered Jack
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control Systems
TDES	Triple Data Encryption Standard
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
USA

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com