Cisco 5921
Embedded Services Router (ESR)

Software Version:
15.2(4)GC

FIPS-140 Non-Proprietary Security Policy

Cisco Systems, Inc.

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco 5921 ESR from Cisco Systems, Inc., referred to in this document as the modules, routers, or by their specific model name. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

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/groups/STM/cmvp/index.html.

1.1 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 Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.2 FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package includes:

Vendor Evidence

- Finite State Machine

- Other supporting documentation as additional references

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See "Obtaining Technical Assistance" section for more information.

2 Module Description

2.1 Cisco 5921 ESR

The Cisco 5921 ESR Embedded Services Router is a software product that runs IOS 15.2(4)GC on an x86-based Linux environment (2.6.32 Kernel or later). For FIPS validation purposes the Cisco 5921 ESR was run on an Intel Desktop Board D2500CC test computer system which utilizes an Intel Atom CPU and runs the CentOS Linux 6.4 32-bit O/S (2.6.32-358 Linux Kernel). The binary is a Router application which allows Linux software connections with virtual and physical Linux interfaces on the host hardware. The binary is the virtual console access application.

2.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**1**

Table 1: Module Validation Level

3 Cryptographic Boundary

For the purposes of the FIPS 140-2 level 1 validation, the logical boundary of the 5921 ESR surrounds the single Linux object module file which executes in the host computer.

The physical cryptographic boundary of the module is the enclosure of the system on which it is executing.

The following diagram illustrates the configuration of the module.
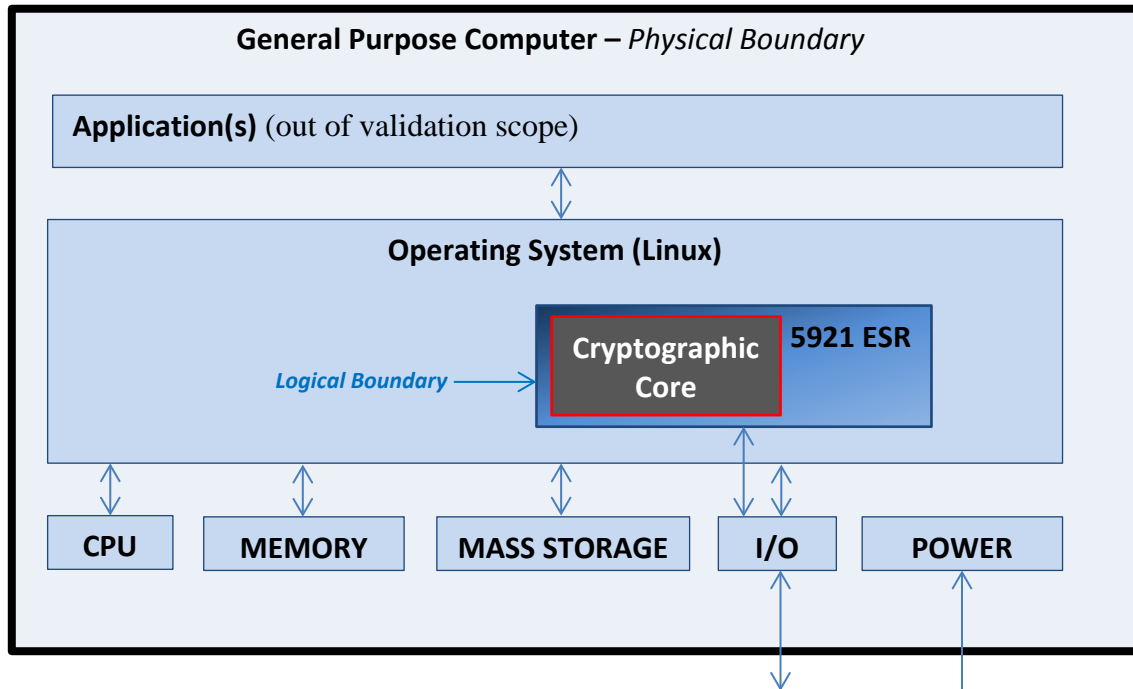
Figure 1: Block Diagram Showing Interfaces

4 Cryptographic Module Ports and Interfaces

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

Interfaces	FIPS 140-2 Logical Interfaces
API input parameters - plaintext and/or ciphertext data.	Data Input Interface
API output parameters - plaintext and/or ciphertext data.	Data Output Interface
API function calls - function calls, or input arguments that specify commands and control data used to control the operation of the module.	Control Input Interface
API return codes- function return codes, error codes, or output arguments that receive status information used to indicate the status of the module.	Status Output Interface

Table 2: ESR FIPS Logical Interfaces Table

As a software module, control of the physical interfaces and ports is outside of the module's scope. However, when the module is performing self-tests, or is in an error state, all output on the logical data output interface is inhibited.

5   Roles, Services, and Authentication

Authentication in the Cisco ESR is role-based. There are two main roles in the router that operators can assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The configuration of the encryption and decryption functionality is performed only by the Crypto Officer after authentication to the Crypto Officer role by providing a valid Crypto Officer username and password. Once the Crypto Officer configured the encryption and decryption functionality, the User can use this functionality after authentication to the User role by providing a valid User username and password. The Crypto Officer can also use the encryption and decryption functionality after authentication to the Crypto Officer role.

The module supports RADIUS and TACACS+ for authentication. The User and Crypto Officer passwords and all shared secrets must each be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). See the Secure Operation section for more information. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 4,488,223,369,069,440 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. Since it is claimed to be for 8 digits with no repetition, then the calculation should be 94 x 93 x 92 x 91 x 90 x 89 x 88 x 87). In order to successfully guess the sequence in one minute would require the ability to make over 74,803,722,817,824 guesses per second, which far exceeds the operational capabilities of the module.

The RSA digital signature authentication mechanism is used to authenticate the User role via IPSec/IKE protocol implementation.

The security policy stipulates that all user passwords and shared secrets must be 8 alphanumeric characters, so the password space is 2.8 trillion possible passwords. The possibility of randomly guessing a password is thus far less than one in one million. To exceed a one in 100,000 probability of a successful random password guess in one minute, an attacker would have to be capable of 28 million password attempts per minute, which far exceeds the operational capabilities of the module to support.

When using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. An attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8×10^{21} attempts per minute, which far exceeds the operational capabilities of the modules to support.

5.1 User Services

Users can access the system in two ways:

1. By accessing the console port with a terminal program or via IPSec protected telnet or SSH session to an Ethernet port. Please note that the PC used in the situation with the console connection and the terminal program is a non-networked PC. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

2. Via an IPSec session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism.

The services available to the User role consist of the following:

Status Functions	View state of interfaces and protocols, version of IOS currently running.
Network Functions	Connect to other network devices and initiate diagnostic network services (i.e., ping, mtrace).
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).
Directory Services	Display directory of files kept in flash memory.
GetVPN	Negotiation and encrypted data transport via Get VPN
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand
Zeroization Services	Zeroize cryptographic keys stored in Random Access Memory (RAM) via power cycling

Table 3: User Role Services

5.2 Cryptographic Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the 10/100 management Ethernet port. The Crypto Officer authenticates as a User and then authenticates as the Crypto Officer role. During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router.

The Crypto Officer services consist of the following (in addition to all services available to the User Role):

Service	Description

Service	Description
Configure the router	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information. (Includes IPSec/IKE/GDOI configuration)
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 based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
View Status Functions	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
Manage the router	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, zeroize all cryptographic keys or CSPs, view complete configurations, manager user rights, and restore router configurations. In addition, Crypto Officer also has access to all User services.
Set Encryption/Bypass	Set up the configuration tables for IP tunneling. Set pre-shared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
SNMPv3	Non security-related monitoring by the CO using SNMPv3.
SSH	Configure SSH parameter, provide entry and output of CSPs.
SSL VPN (using TLSv1.0)	Configure SSL VPN parameters, provide entry and output of CSPs.
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand

Table 4: Crypto Officer Role Services

5.3 Services Available in a Non-FIPS Mode of Operation

The module supports the following services while in a non-FIPS mode of operation:

Service	Description
SSL VPN (using SSLv3.0)	Configure SSL VPN parameters.
SSHv1	Configure SSH parameters.
SNMPv1; SNMPv2; and SNMPv3 with DES encryption	Non security-related monitoring

5.4 Unauthenticated User Services

The services available to unauthenticated users are:

- Viewing the status output from the module via the Status Output Interface
- Perform bypass services
- Powering the module on and off using the power switch on the third-party chassis

6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. The zeroization method for each individual keys or CSPs can be found in the table below. All cryptographic keys are exchanged and entered electronically or via Internet Key Exchange (IKE)/Group Domain of Interpretation (GDOI), and all CSPs are entered into the module by the Crypto Officer role.

The module supports the following critical security parameters (CSPs):

CSP	Name	Alg.	Size	Description	Storage	Zeroization
1	DRBG V	SP 800-90A CTR_DRBG	128-bits	Generated by entropy source via the SP 800-90A CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Automatically when the router is power cycled
2	DRBG key	SP 800-90A CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG	DRAM (plaintext)	Automatically when the router is power cycled
3	DRBG entropy input	SP 800-90A CTR_DRBG	256-bits	HW based entropy source used to construct seed	DRAM (plaintext)	Automatically when the router is power cycled
4	DRBG seed	SP 800-90A CTR_DRBG	384-bits	Generated by entropy source via the SP 800-90A CTR_DRBG derivation function. Input to the DRBG to determine the internal state of the DRBG	DRAM (plaintext)	Automatically when the router is power cycled
5	Diffie-Hellman private exponent	Diffie-Hellman	2048-bits	The private exponent used in Diffie-Hellman (DH) exchange. Generate by the module. Zeroized after DH shared secret has been generated.	DRAM (plaintext)	Automatically after shared secret generated.
6	Diffie Hellman public key	DH	2048- bits	The p used in Diffie-Hellman (DH) exchange. This CSP is created using the ANSI X9.31 RNG (Nitrox/Octeon II).	DRAM (plaintext)	Automatically after shared secret generated.
7	Diffie-Hellman Shared Secret	Diffie-Hellman	2048-bits	Shared secret derived by the Diffie-Hellman Key exchange	DRAM (plaintext)	Automatically after session is terminated
8	skeyid	Keyed SHA-1	160-bits	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)	Automatically after IKE session terminated.
9	skeyid_a skeyid_d skeyid_e	Keyed SHA-1	160-bits	The IKE key derivation keys for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.

CSP	Name	Alg.	Size	Description	Storage	Zeroization
10	IKE session encryption key	Triple-DES AES	168-bits 128, 192, or 256-bits	The IKE session encrypt key. Derived in the module	DRAM (plaintext)	Automatically after IKE session terminated.
11	IKE session authentication key	SHA-1 HMAC	160-bits	The IKE session authentication key. Derived in the module.	DRAM (plaintext)	Automatically after IKE session terminated.
12	ISAKMP preshared	Secret	At least eight characters	The key used to generate IKE skeyid during preshared-key authentication. It is entered by the Crypto Officer. "no crypto isakmp key" command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext or encrypted)	"# no crypto isakmp key"
13	IKE RSA Authentication private Key	RSA	2048-bits	RSA private key for IKE authentication. Generated by the module, set as IKE RSA Authentication Key with the "crypto keyring" or "ca trust-point" command.	NVRAM (plaintext)	"# crypto key zeroize rsa"
14	IPSec encryption key	Triple-DES AES	168-bits 128, 192, or 256-bits	The IPSec encryption key. Derived in the module. Zeroized when IPSec session is terminated.	DRAM (plaintext)	Automatically when IPSec session terminated.
15	IPSec authentication key	SHA-1 HMAC	160-bits	The IPSec authentication key. Derived in the module. The zeroization is the same as above.	DRAM (plaintext)	Automatically when IPSec session terminated.
16	GDOI Key encryption Key (KEK)	Triple-DES AES	168-bits 128, 192, or 256-bits	This key is generated by using the "GROUPKEY-PULL" registration protocol with GDOI. Generate by the module. It is used protect GDOI rekeying data."	DRAM (plaintext)	Automatically when session terminated.
17	GDOI Traffic Encryption Key (TEK)	Triple-DES AES	168-bits 128, 192, or 256-bits	This key is generated by using the "GROUPKEY-PULL" registration protocol and updated using the "GROUPKEY-PUSH" registration protocol with GDOI. Generate by the module. It is used to encrypt data traffic between Get VPN peers	DRAM (plaintext)	Automatically when session terminated.

CSP	Name	Alg.	Size	Description	Storage	Zeroization
18	GDOI TEK Integrity key	HMAC SHA-1	160-bits	This key is generated by using the "GROUPKEY-PULL" registration protocol and updated using the "GROUPKEY-PUSH" registration protocol with GDOI. Generate by the module. It is used to ensure data traffic integrity between Get VPN peers.	DRAM (plaintext)	Automatically when session terminated.
19	SSH RSA private key	RSA	2048 bits	This key is used for message signing when performing SSH authentication. Generated by the module.	NVRAM (plaintext or encrypted)	"# crypto key zeroize rsa"
20	SSH RSA Public key	RSA	2048 bits	The SSH public key for the module.	NVRAM (plaintext or encrypted)	"# crypto key zeroize rsa"
21	SSH session key	Triple-DES AES	168-bits 128, 192, or 256-bits	This is the SSH session key. It is used to encrypt all SSH data traffic traversing between the SSH client and SSH server. It is derived in the module.	DRAM (plaintext)	Automatically when SSH session terminated
22	SSH session authentication key	HMAC-SHA-1	160 bits	This key is used to perform the authentication between the SSH client and SSH server. It is derived in the module.	DRAM (plaintext)	Automatically when SSH session terminated
23	User password	Shared Secret	At least eight characters	The password of the User role. It is entered by Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
24	Enable password	Shared Secret	At least eight characters	The plaintext password of the CO role. It is entered by the Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
25	Enable secret	Shared Secret	At least eight characters	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. It is entered by the Crypto Officer. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
26	RADIUS secret	Shared Secret	At least eight characters	The RADIUS shared secret. It is entered by the Crypto Officer. This shared secret is zeroized by executing the "no radius-server key" command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	"# no radius-server key"

CSP	Name	Alg.	Size	Description	Storage	Zeroization
27	TACACS+ secret	Shared Secret	At least eight characters	The TACACS+ shared secret. It is entered by the Crypto Officer. This shared secret is zeroized by executing the "no tacacs-server key" command.	NVRAM (plaintext or encrypted), DRAM (plaintext)	"# no tacacs-server key"
28	TLS Server RSA private key	RSA	2048-bits	Used in TLS negotiations. This CSP is used for SSL/TLS/HTTPS.	NVRAM (plaintext or encrypted)	Automatically when session terminated
29	TLS Server RSA public key	RSA	2048-bits	Used in TLS negotiations. This CSP is used for SSL/TLS/HTTPS.	NVRAM (plaintext or encrypted)	Automatically when session terminated
30	TLS pre-master secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new session keys can be derived. This key was entered into the module via RSA key wrapping.	DRAM (plaintext)	Automatically when session terminated
31	TLS Traffic Keys	Triple-DES AES HMAC SHA-1	168-bits 128, 192, or 256-bits 160-bits	Derived in the module. Used to protect the traffics between SSL/TLS VPN peers.	DRAM (plaintext)	Automatically when session terminated
32	snmpEngineeID	Shared Secret	32-bits	A unique string used to identify the SNMP engine.	NVRAM	Overwrite with new engine ID
33	SNMP v3 password	Shared Secret	8 – 25 characters	The password use to setup SNMP v3 connection.	NVRAM	Overwrite with new password
34	SNMP session key	AES	128-bits	Encryption key used to protect SNMP traffic.	SDRAM	Automatically when session terminated.

Table 6: CSPs

The services accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below.

Role/Service	DRBG V	DRBG Key	DRBG Entropy Input	DRBG Seed	Diffie Hellman private exponent	Diffie Hellman public key	Diffie Hellman Shared Secret	Skeyid	skeyid_a, skeyid_d, skeyid_e	IKE session encrypt key	IKE session authentication key	ISAKMP preshared	IKE RSA Authentication private Key	IPSec encryption key	IPSec authentication key	GDOI Key encryption Key (KEK)	GDOI Traffic Encryption Key (TEK)	GDOI TEK Integrity Key	SSH RSA Private Key	SSH RSA Public Key	SSH session key	SSH session authentication key	User password	Enable password	Enable secret	RADIUS secret	TACACS+ secret	TLS Server RSA private key	TLS Server RSA public key	TLS pre-master secret	TLS Traffic Keys	snmpEngineID	SNMP v3 password	SNMP session key
User Role																																		
Status Function																																		
Network Function	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r											
Terminal Function																																		
Directory Services																																		
Perform Self-tests																																		
VPN Function					rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd		rwd													
CO Role																																		
Configure the module														rw	rw	rw	rw	rw	rw															
Define Rules and Filters																																		
Status Functions																																		
Manage the module	d	d	d	d																			rwd	rwd	rwd	rwd	rwd							
Set Encryption/ Bypass	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd																
SNMPv3																																r	r	r
SSH																			rwd	rwd	rwd	rwd												
SSL VPN (using TLSv1.0)																												rwd	rwd	rwd	rwd	rwd	rwd	rwd
Perform Self-tests																																		

Table 7: Role CSP Access

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco ESR supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms included in the ESR for use in the FIPS mode of operation.

Algorithm	Supported Mode	Algorithm Cert. #
		IOS
AES	CBC (128, 192, 256) CTR (256) GCM (128, 192, 256)	2785
Triple-DES	KO 1, CBC	1673
SHS (SHA-1, 256, and 512)	Byte Oriented	2340
HMAC SHA-1	Byte Oriented	1744
DRBG	CTR (using AES-256)	472
RSA	2048-3072 bit key	1457
ECDSA	P-256, P-384	486
CVL (as per SP 800-135)	IKEv1, IKEv2, SNMP, SSH, TLS	237

Table 8: FIPS-Approved Algorithms for use in FIPS Mode

7.2 Non-Approved Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- DES
- DES MAC
- HMAC MD4
- HMAC MD5
- MD4
- MD5 (*but ALLOWED for use in the TLS protocol in FIPS mode)

- NDRNG
- RC4

The modules support the following key establishment/derivation schemes:

- Diffie-Hellman (key establishment methodology provides 112 bits of encryption strength)

- RSA key transport (key establishment methodology provides 112 bits of encryption strength)

- GDOI (key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength)

7.3 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. All self-tests are implemented by the firmware and associated hardware component. An example of self-tests run at power-up is a cryptographic known answer test (KAT) on each of the FIPS-approved cryptographic algorithms and on the Diffie-Hellman algorithm. Examples of tests performed at startup are a software integrity test using an RSA signature. Examples of tests run periodically or conditionally include: a bypass mode test performed conditionally prior to executing IPSec, and a continuous random number generator test. If any of self-tests fail, the router transitions into an error state. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Examples of the errors that cause the system to transition to an error state:

- IOS image integrity checksum failed
- Known answer test failed

7.3.1 Self-tests performed by the IOS

- IOS Self Tests
    - POST tests
        - Firmware Integrity test - (RSA PKCS#1 v1.5 (2048 bits)
        - AES Known Answer test (encrypt)
        - AES Known Answer test (decrypt)
        - DRBG Known Answer test
        - HMAC-SHA-1 Known Answer test
        - RSA Known Answer Test (sign)
        - RSA Known Answer Test (verify)
        - ECDSA PWCT test
        - SHA-1/256/512 Known Answer test
        - Triple-DES Known Answer test (encrypt)

- Triple-DES Known Answer test (decrypt)
  o Conditional tests
    - RSA PWCT (pairwise consistency test)
    - ECDSA PWCT
    - Conditional bypass test
    - CRNG test on DRBG
    - CRNG tests on non-approved RNGs

8 Physical Security

The module is comprised of software only and thus does not claim any physical security.

9 Secure Operation

The Cisco ESR meets all the Level 1 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

9.1 Initial Setup

1. The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal

no service password-recovery

end

show version
```

NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

9.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 15.2(4)GC, filename: c59XX-adventerprisek9-mz.SPA.152-4.GC.bin is the only allowable image; no other image should be loaded.

2. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except '?' are accepted) and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

3. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
line con 0

password [PASSWORD]

login local
```

4. The Crypto Officer shall only assign users to a privilege level 1 (the default).

5. The Crypto Officer shall not assign a command to any privilege level other than its default.

6. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long.

9.3 IPSec Requirements and Cryptographic Algorithms

1. The only type of IPSec key establishment methods that is allowed in FIPS mode are Internet Key Exchange (IKE) and Group Domain of Interpretation (GDOI).

2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

   ah-sha-hmac
   esp-sha-hmac
   esp-3des
   esp-aes

3. The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:

   DES
   DES MAC
   HMAC MD4
   HMAC MD5
   MD4
   MD5
   RC4

9.4 SSLv3.1/TLS Requirements and Cryptographic Algorithms

When negotiating TLS cipher suites, only FIPS approved algorithms must be specified. All other versions of SSL except version 3.1 must not be used in FIPS mode of operation. The following algorithms are not FIPS approved and should not be used in the FIPS-approved mode:

- MD5
- RC4
- DES

9.5 Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

2. SSH v2 access to the module is only allowed if SSH v2 is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH v2 uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.

3. SNMP access is only allowed when SNMP v3 is configured with AES encryption.

9.6 Cisco Unified Border Element (CUBE) TLS Configuration

When configuring CUBE TLS connections, the following configuration command option must be
 executed to limit the TLS session options to FIPS-approved algorithms.

sip-ua

crypto signaling [strict-cipher]

9.7 Identifying Operation in an Approved Mode

The following activities are required to verify that that the module is operating in an Approved mode of operation.

1. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the "Secure Operation of the Cisco 59XX ESR" section of this document.

2. Issue the following commands: 'show crypto ipsec sa', 'show crypto isakmp policy',

and 'show crypto gdoi policy'. Verify that only FIPS approved algorithms are used.

10 Related Documentation

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

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.

11 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

11.1 Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

11.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

11.3 Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

12 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

> Cisco Systems
> Attn: Customer Document Ordering
> 170 West Tasman Drive
> San Jose, CA 95134-9883

We appreciate your comments.

13 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://tools.cisco.com/security/center/rss.x?i=44

13.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302

- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

14 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco

Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

14.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

14.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)EMEA: +32 2 704 55 55USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

14.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) – Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

15 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links

Page 23 of 25

to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

16 Definition List

AES – Advanced Encryption Standard

CMVP – Cryptographic Module Validation Program

CSE – Communications Security Establishment

CSP – Critical Security Parameter

ECDSA – Elliptic Curve Digital Signature Algorithm

ESR – Embedded Services Router

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

HTTP – Hyper Text Transfer Protocol

KAT – Known Answer Test

MAC – Message Authentication Code

NIST – National Institute of Standards and Technology

PWCT – Pairwise Consistency Test

QoS – Quality of Service

RAM – Random Access Memory

RNG – Random Number Generator

RSA – Rivest Shamir and Adleman method for asymmetric encryption

SHA – Secure Hash Algorithm