Cisco 5940 Embedded Services Routers

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.9

January 2013

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco 5940 Embedded Services Router (ESR). This security policy describes how the Cisco 5940 Embedded Services Routers (Hardware Versions: Cisco 5940 ESR air-cooled card and Cisco 5940 ESR conduction-cooled card; Firmware Version: IOS 15.2(3)GC) meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the Cisco 5940 Embedded Services Router.

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/index.html.

1.2 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	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 Module Validation Level

1.3 References

This document deals only with operations and capabilities of the Cisco 5940 Embedded Services routers in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

- The Cisco Systems website contains information on the full line of Cisco Systems routers. Please refer to the following website: http://www.cisco.com/en/US/products/hw/routers/index.html

- The Cisco 5940 Embedded Services Routers is part of the family of Mobile Internet Routers: http://www.cisco.com/en/US/products/hw/routers/products.html#N390A6E

- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

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

1.4 Terminology

In this document, the Cisco 5940 Embedded Services Routers are referred to as the 5940 ESR, router, the module, or the system.

1.5 Document Organization

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

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

This document provides an overview of the Cisco 5940 Embedded Services Router and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco 5940 Embedded Services Routers

The Cisco 5940 is a high-performance, ruggedized router. With onboard hardware encryption, the Cisco 5940 offloads encryption processing from the router to provide highly secure yet scalable video, voice, and data services for mobile and embedded outdoor networks. The Cisco 5940 Embedded Services Routers provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 1 requirements. This section describes the general features and functionality provided by the routers. The Cisco 5940 Router Card uses industrial-grade components and is optimized for harsh environments that require Cisco IOS Software routing technology. The following subsections describe the physical characteristics of the routers.

2.1 The 5940 Embedded Service Router Cryptographic Module Physical Characteristics

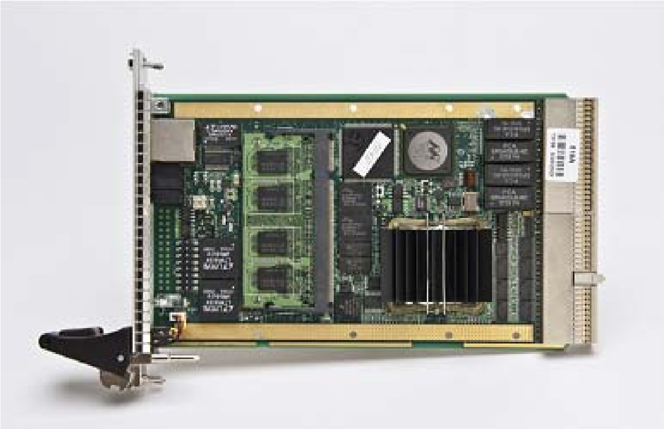


Figure 1 Cisco 5940 Air Cooled Router

Figure 2 Cisco 5940 Conduction Cooled Router

Cisco 5940 Embedded Services Router is a multiple-chip embedded cryptographic module. The router is a cPCI 3U card. These cards are then inserted into a ruggedized enclosure (outside the cryptographic boundary) to protect against the elements.

The physical boundary of the cPCI card is the cryptographic boundary. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

2.2 Module Interfaces

The module features the following interfaces:

1. One serial console port
2. cPCI J1 connector
3. cPCI J2 connector
4. JTAG connectors (via J2 connectors)
5. LEDs

Below are the pin assignments for J1 and J2 connectors:

2.2.1 J1 connector

J1 Pinout

Row	Column A	B	C	D	E	F
1	5V	-12V	TRST#	+12V	5V	GND
2	TCK	5V	TMS	TDO	TDI	GND
3	INTA#	INTB#	INTC#	5V	INTD#	GND
4	IPMB_PWR	HEALTHY#	V(I/O)	INTP	INTS	GND
5	BRSVP1A5	BRSVP1B5	RST#	GND	GNT0#	GND
6	REQ0#	GND	3.3V	CLK0	AD[31]	GND
7	AD[30}	AD[29]	AD[28]	GND	AD[27]	GND
8	AD[26]	GND	V(I/O)	AD[25]	AD[24]	GND
9	C/BE[3]#	GND	AD[23]	GND	AD[22]	GND
10	AD[21}	GND	3.3V	AD[20]	AD[19]	GND
11	AD[18]	AD[17]	AD[16]	GND	C/BE[2]#	GND
12	KEY AREA					
13						
14						
15	3.3V	FRAME#	IRDY#	BD_SEL#	TRDY#	GND
16	DEVSEL#	GND	V(I/O)	STOP#	LOCK#	GND
17	3.3V	IPMB_SCL	IPMB_SDA	GND	PERR#	GND
18	SERR#	GND	3.3V	PAR	C/BE[1]#	GND
19	3.3V	AD[15]	AD[14]	GND	AD[13]	GND
20	AD[12]	GND	V(I/O)	AD[11]	AD[10]	GND
21	3.3V	AD[9]	AD[8]	M66EN	C/BE[0]#	GND
22	AD[7]	GND	3.3V	AD[6]	AD[5]	GND
23	3.3V	AD[4]	AD[3]	5V	AD[2]	GND
24	AD[1]	5V	V(I/O)	AD[0]	ACK64#	GND
25	5V	REQ64#	ENUM#	3.3V	5V	GND

Long Pins
Medium Pins
Short Pins

2.2.2 J2 connector

J2 Pinout

Row	A	B	C	D	E	F
1	N/C [2]	GND	N/C [2]	N/C [2]	N/C [2]	GND
2	N/C [2]	N/C [2]	N/C [2]	N/C [2]	N/C [2]	GND
3	N/C [2]	GND	N/C [2]	N/C [2]	N/C [2]	GND
4	N/C [2]	JTAG/COP TCK	JTAG/COP HRESET#	JTAG/COP TRST#	JTAG/COP VDD_SENSE	GND
5	JTAG/COP COP_CPU_SEL#	JTAG/COP TDI	JTAG/COP SRESET#	JTAG/COP CKSTP_IN#	JTAG/COP NC	GND
6	JTAG/COP JTAG_CPLD_SEL#	JTAG/COP TDO	JTAG/COP TMS	JTAG/COP CKSTP_OUT#	JTAG/COP RUN/STOP#	GND
7	ETH3_DB+	ETH3_DB-	ETH3_LED	ETH3_DD+	ETH3_DD-	GND
8	ETH3_DA+	ETH3_DA-	ETH3_LEDRTN	ETH3_DC+	ETH3_DC-	GND
9	ETH2_DB+	ETH2_DB-	ETH2_LED	ETH2_DD+	ETH2_DD-	GND
10	ETH2_DA+	ETH2_DA-	ETH2_LEDRTN	ETH2_DC+	ETH2_DC-	GND
11	ETH1_DB+	ETH1_DB-	ETH1_LED	ETH1_DD+	ETH1_DD-	GND
12	ETH1_DA+	ETH1_DA-	ETH1_LEDRTN	ETH1_DC+	ETH1_DC-	GND
13	ETH0_DB+	ETH0_DB-	ETH0_LED	ETH0_DD+	ETH0_DD-	GND
14	ETH0_DA+	ETH0_DA-	ETH0_LEDRTN	ETH0_DC+	ETH0_DC-	GND
15	STS_LEDR	STS_LEDRTN	N/C [2]	N/C [2]	N/C [2]	GND
16	STS_LEDG	RTS	N/C [2]	GND	DTR [1]	GND
17	TxD	BMC Console RXD	PRST#	N/C [2]	N/C [2]	GND
18	RxD	BMC Console TXD	BMC DBG TMS	BMC DBG TDO	CTS	GND
19	GND	GND	BMC DBG 3.3VOUT	BMC DBG TDI	BMC DBG ALLPST	GND
20	N/C [2]	GND	Reserved	BMC DBG TCK	BMC DBG RST_IN#	GND
21	N/C [2]	GND	Reserved	BMC DBG TRST#	Reserved	GND
22	N/C [2]	N/C [2]	N/C [2]	N/C [2]	N/C [2]	GND

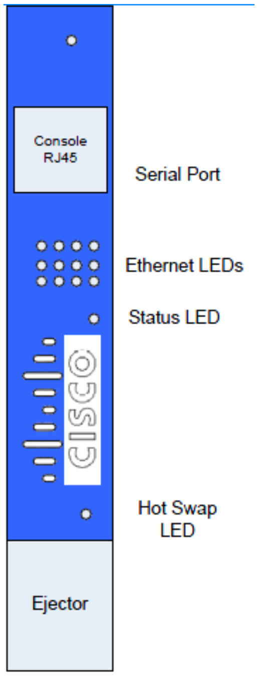
Notes:
1) DTR permanently asserted
2) Assigned by cPCI specification, but unused in RTM

Color Code:

GbE	Console
JTAG/COP	BMC
Status LED	cPCI Spec

These interfaces are depicted in the figures below:

The interface for the router is located on the front and rear panels as shown in Figure 3 and Figure 5, respectively.



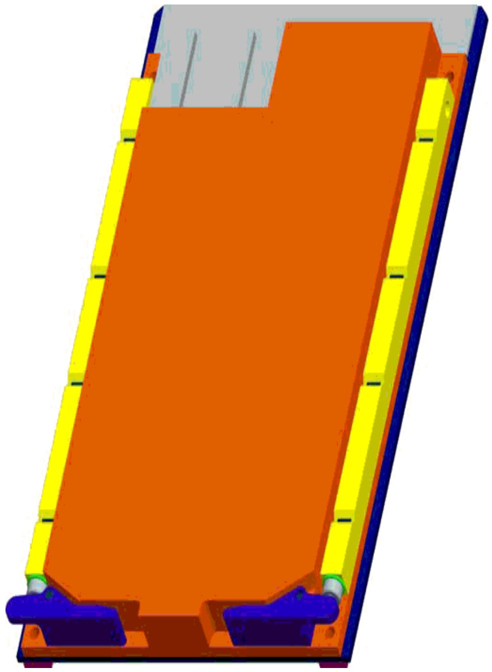


Figure 3: Faceplate **Figure 4: Conduction Cooled cover**

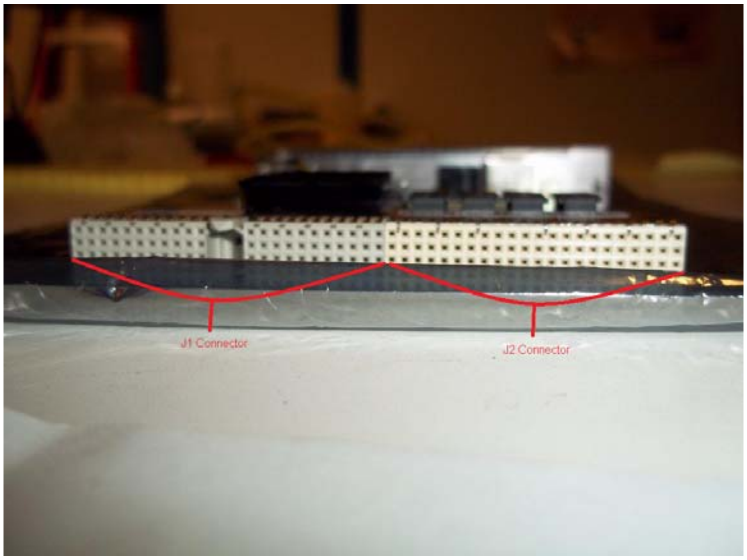


Figure 5: Connector pins

The following tables provide more detailed information conveyed by the LEDs on the front and rear panel of the router:

Name	State	Description
Ethernet LEDs	Active	Used to show activity on Ethernet ports in the RTM
Status LED	Active	Bicolor user LED to assist location of the device in a rack.
Hot Swap	Active	BLUE LED indicates hot swap status based on ejector handle position

Table 2 – 5940 ESR LED Indicators

Each 5940 ESR provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

Router Physical Interface	FIPS 140-2 Logical Interface
J2 Connector Console Port JTAG Connector	Data Input Interface
J2 Connector Console Port JTAG Connector	Data Output Interface
J2 Connector Console Port JTAG Connector	Control Input Interface
J2 Connector Console Port JTAG Connector LEDs	Status Output Interface
J1 Connector	Power Interface

Table 3 – 5940 ESR FIPS 140-2 Logical Interfaces

2.3 Roles and Services

Authentication in Cisco 5940 ESR is role-based. There are two main roles in the router that operators can assume: the Crypto Officer role and the User role. There is also a maintenance role available through the JTAG connector. 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 RSA digital signature authentication mechanism is used to authenticate the User role via IPSec/IKE protocol implementation.

The maintenance role does not include authentication, and it has the capability to read and write memory, reset the board, program the Complex Programmable Logic Device (CPLD), and debug Rommon.

2.3.1 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 for the console connection 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 Dynamic Random Access Memory (DRAM) via power cycling

2.3.2 Crypto 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:

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.
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 preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
Perform Self-Tests	Perform the FIPS 140 start-up tests on demand

2.3.3 Maintenance Role

The module supports a Maintenance role while operating in FIPS mode of operation. The maintenance role can be accessed via the JTAG connector. The services available to this role include reading and writing memory, resetting the board, programming the Complex Programmable Logic Device (CPLD), and debugging Rommon. The entity entering the maintenance role must zeroize all plaintext keys and CSPs before entering and exiting the Maintenance role.

2.3.4 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch on the third-party chassis

2.3.5 Strength of Authentication

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 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} 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.

2.4 Physical Security

The module is being validated at physical security level 1. As such apart from using production grade material, the module does not implement any physical security mechanisms.

2.5 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

2.5.1 Approved Cryptographic Algorithms

The routers support the following FIPS-2 approved algorithm implementations:

Algorithm	**Algorithm Certificate Number**	
	IOS	**MPC8548E**
AES	#1643	#962 and #1535
Triple-DES	#1073	#757
SHS	#1444	#933
HMAC	#965	#537
DRBG	#89	N/A
RSA	#811	N/A

Table 4: Approved Cryptographic Algorithms

2.5.2 Non-Approved Cryptographic Algorithms

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

- DES
- DES MAC
- MD5
- MD4
- HMAC MD5
- RC4

The modules support the following key establishment/derivation schemes:

- Diffie-Hellman (key establishment methodology provides between 80 and 112 bits of encryption strength)
- Internet Key Exchange Key Establishment (IKEv1/IKEv2)
- GDOI (key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength)

2.6 Cryptographic Key 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 table 4 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 keys and critical security parameters (CSPs):

ID	Algorithm	Size	Description	Storage	Zeroization Method
DRBG V	SP 800-90 CTR_DRBG	128-bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Automatically when the router is power cycled
DRBG Key	SP 800-90 CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90 CTR_DRBG	DRAM (plaintext)	Automatically when the router is power cycled
Diffie-Hellman private exponent	Diffie-Hellman	1024 /1536/ 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.
Diffie-Hellman Shared Secret	Diffie-Hellman	1024/1536 /2048-bits	Shared secret generated by the Diffie-Hellman Key exchange	DRAM (plaintext)	Automatically after session is terminated
Skeyid	Keyed SHA-1	160-bits	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is	DRAM (plaintext)	Automatically after IKE session

			terminated.		terminated.
skeyid_d	Keyed SHA-1	160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session encrypt key	Triple-DES/AES	168-bits/256-bits	The IKE session encrypt key. Generate by the module	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	SHA-1 HMAC	160-bits	The IKE session authentication key. Generate by the module.	DRAM (plaintext)	Automatically after IKE session terminated.
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”
IKE RSA Authentication private Key	RSA	1024 – 2048 bits	RSA private key for IKE authentication. Generated or entered like any RSA key, set as IKE RSA Authentication Key with the “crypto keyring” or “ca trust-point” command.	NVRAM (plaintext)	“# crypto key zeroize rsa"
IPSec encryption key	Triple-DES/AES	168-bits/256-bits	The IPSec encryption key. Generate by the module . Zeroized when IPSec session is terminated.	DRAM (plaintext)	Automatically when IPSec session terminated.
IPSec authentication key	SHA-1 HMAC	160-bits	The IPSec authentication key. Generate by the module. The zeroization is the same as above.	DRAM (plaintext)	Automatically when IPSec session terminated.
GDOI Key encryption Key (KEK)	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256-bits)	This key is created 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.
GDOI Traffic Encryption Key (TEK)	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256-bits)	This key is created 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.
GDOI TEK Integrity key	HMAC SHA-1	160-bits	This key is created 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.
SSH RSA private key	RSA	1024/1536/2048	This key is used for message signing when performing SSH authentication. Generated by the module.	NVRAM (plaintext or encrypted)	“# crypto key zeroize rsa”
SSH session key	TDES /AES	TDES (Key Size 168 bits)/AES (Key Size	This is the SSH session key. It is used to encrypt all SSH data traffics traversing between the SSH client and SSH server. It is generated by the module	DRAM (plaintext)	Automatically when SSH session terminated

		128/192/256 bits)			
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 generated by the module.	DRAM (plaintext)	Automatically when SSH session terminated
User password	Shared Secret	At least eight characters	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
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
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
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”
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”

Table 5: Cryptographic Keys and CSPs

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below.

	CSP	DRBG V	DRBG Key	Diffie Hellman private exponent	Diffie Hellman Shared Secret	Skeyid	skeyid_d	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 session key	SSH session authentication key	User password	Enable password	Enable secret	RADIUS secret	TACACS+ secret
Role/Service																								
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				
Terminal Function																								
Directory Services																								
Perform Self-tests																								
VPN Function						r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d					
CO Role																								
Configure the module											r w													
Define Rules and Filters																								
Status Functions																								
Manage the module		d	d																	r w d	r w d	r w d	r w d	r w d
Set Encryption/ Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w d	r w d	r w d					
Perform Self-tests																								

r = read w = write d= delete

Table 6: CSP/Role/Service Access Policy

2.7 *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 EDC. 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
- Microprocessor overheats and burns out
- Known answer test failed
- NVRAM module malfunction.

2.7.1 Self-tests performed by the IOS and Hardware

- IOS Self Tests
  - POST tests
    - Firmware Integrity test
    - AES Known Answer test
    - DRBG Known Answer test
    - HMAC-SHA-1 Known Answer test
    - RSA Known Answer Test (both signature/verification)
    - SHA-1/256/512 Known Answer test
    - Triple-DES Known Answer test
  - Conditional tests
    - RSA PWCT test
    - Conditional bypass test
    - DRBG CRNG test
    - CRNG test on non-approved RNGs

- Hardware Self Tests
  - POST tests
    - AES Known Answer Test
    - HMAC-SHA-1 Known Answer Test
    - Triple-DES Known Answer Test

3 Secure Operation of the Cisco 5940 ESR

The Cisco 5940 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.

3.1 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.

3.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 15.2(3)GC, filename: c5940-adventerprisek9-mz.SPA.152-3.GC.bin is the only allowable image; no other image should be loaded.
2. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0102
   ```

3. 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]
   ```

4. 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
   ```

5. The Crypto Officer shall only assign users to a privilege level 1 (the default).
6. The Crypto Officer shall not assign a command to any privilege level other than its default.
7. 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.
8. Loading any IOS image onto the router is not allowed while in FIPS mode of operation.

3.3 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-Triple-DES

esp-aes

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

   DES

   DES-MAC

   HMAC MD-5

   MD-4

   MD-5

   RC4

3.4 Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.

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

3.6 HTTPS/TLS management is not allowed in FIPS mode.

3.7 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 5940 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.