Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs)

Hardware versions: 3925E (with PCB rev -A0 and -B0), 3945E (with PCB rev -A0 and -B0), [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0], ISR: FIPS-SHIELD-3900=;
Firmware version: 15.1(2)T3

FIPS 140-2 Non-Proprietary Security Policy

Overall Level 2 (Sections 3 and 10 Level 3) Validation

Version 0.8

May 2011

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) from Cisco Systems, Inc. (Hardware Versions: 3925E (with PCB rev -A0 and -B0), 3945E (with PCB rev -A0 and -B0), [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0], ISR: FIPS-SHIELD-3900=; Firmware Version: IOS 15.1(2)T3, 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.

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.

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.

Module Description

Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs)

The Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) are routing platforms that provides VPN functionality, as well as, SIP Gateway Signaling Over TLS Transport. The Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) provide connectivity and security services in a single, secure device. These routers offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

In support of the routing capabilities, the Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) provide IPSec, GetVPN (GDOI), and SSL v3.1 connection capabilities for VPN enabled clients connecting through the Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs).

The tested platforms consist of the following components:

- Cisco 3925E ISR
- Cisco 3945E ISR

Model	Firmware
Cisco 3925E ISR	15.1(2)T3
Cisco 3945E ISR	15.1(2)T3

Table 1: Module Hardware Configurations

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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

Table 2: Module Validation Level

Cryptographic Boundary

The cryptographic boundary for the Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) is defined as the modules' chassis along with the opacity shields.

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 tables:

Physical Interfaces	FIPS 140-2 Logical Interfaces
EHWIC Slots (3) SM Slot (2) GigE Ports (4) Console Port USB Console Port Auxiliary Port	Data Input Interface
EHWIC Slots (3) SM Slot (2) GigE Ports (4) Console Port USB Console Port Auxiliary Port	Data Output Interface
EHWIC Slots (3) SM Slot (2) GigE Ports (4) Console Port USB Console Port Auxiliary Port	Control Input Interface
Activity LED System LED GigE Link LED (1 per GigE port) GigE Speed LED (1 per GigE port) SM LED Compact Flash LED (2) RPS Boost LED Power LED (2) GigE ports (4) Console Port Auxiliary Port USB Console Port	Status Output Interface
Power Plug	Power interface

Table 3: Cisco 3925E ISR Interfaces

Physical Interfaces	FIPS 140-2 Logical Interfaces
EHWIC Slots (3) SM Slot (4) GigE Ports (4) Console Port USB Console Port Auxiliary Port	Data Input Interface
EHWIC Slots (3)	Data Output Interface

Physical Interfaces	FIPS 140-2 Logical Interfaces
SM Slot (4) GigE Ports (4) Console Port USB Console Port Auxiliary Port	
EHWIC Slots (3) SM Slot (4) GigE Ports (4) Console Port USB Console Port Auxiliary Port	Control Input Interface
Activity LED System LED GigE Link LED (1 per GigE port) GigE Speed LED (1 per GigE port) SM LED Compact Flash LED (2) RPS Boost LED Power LED (2) GigE ports (4) Console Port Auxiliary Port USB Console Port	Status Output Interface
Power Plug	Power interface

Table 4: Cisco 3945E ISR Interfaces

NOTE: Each module includes two USB ports and two compact flash slots. These ports and slots are disabled by covering Tamper Evident Labels (TELs) while operating in FIPS-mode.

Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two roles in the router that operators may 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 module supports RADIUS and TACACS+ for authentication. A complete description of all the management and configuration capabilities of the modules can be found in the IOS version 15.1 Configuration Guide Manual and in the online help for the modules.

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). The maximum length of passwords is 25 characters. See the Secure Operation section for more information. The probability of randomly guessing an eight character password would be one (1) in 5,132,188,731,375,616. Thus, in order to successfully guess the sequence in one minute would require the ability to make at least 162,740,637 guesses per second, which far exceeds the operational capabilities of the module.

Additionally, 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 $1.8x10^{21}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

User Services

A User 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 module prompts the User for their username/password combination. If the username/password combination is correct, the User is allowed entry to the module management functionality. The services available to the User role consist of the following:

- Status Functions - View state of interfaces and protocols, firmware version
- 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 memory
- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand
- VPN functions - Negotiation and encrypted data transport via VPN

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 may 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 module - 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 characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Status Functions - View the module configuration, routing tables, active sessions, use get commands to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
- Manage the module - Log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, initiate power-on self tests on demand and restore router configurations.
- Set Encryption/Bypass - Set up the configuration tables for IP tunneling. Set 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
- The Crypto Officer also has access to all User services.

Unauthenticated User Services

The services for someone without an authorized role are to view the status output from the module’s LED and cycle power.

Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE)/Group Domain of Interpretation (GDOI). The module does not output keys or key components in plaintext form.

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

ID	Algorithm	Size	Description	Storage	Zeroization Method
RNG Seed	X9.31	64-bits	This is the seed for X9.31 RNG. Generated by the module.This CSP is stored in DRAM and updated periodically after the generation of 400 bytes – after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this CSP.	DRAM (plaintext)	Automatically every 400 bytes, or turn off the router.
RNG Seed Key	X9.31	168-bits	This is the seed key for the RNG. Generated by the module.	DRAM (plaintext)	Turn off the router
Diffie Hellman private exponent	DH	1024 – 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	DH	1024-bits/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 terminated.	DRAM (plaintext)	Automatically after IKE session 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”	NVRAM (plaintext)	“# crypto key zeroize rsa"

			command.		
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)	AES (128, 192 and 256 bits)	168-bits/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	168-bits/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.
TLS Server RSA private key	RSA	1024/1536 /2048 bits	Identity certificates for module itself and also used in TLS negotiations. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport.	NVRAM (plaintext or encrypted)	“# crypto key zeroize rsa”
TLS pre-master secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created. Generated by the module. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport.	DRAM (plaintext)	Automatically when session terminated.
SSL Traffic Keys	Triple-DES/AES HMAC SHA-1 keys	160-bits/168-bits/256-bits	Generated using the TLS protocol (X9.31RNG + HMAC-SHA1 + either Diffie-Hellman or RSA). Generated by the module. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport.	DRAM (plaintext)	Automatically when session terminated.
Configuration encryption key	AES	256-bits	The key used to encrypt values of the configuration file. This key is entered by the Crypto Officer. This key is zeroized when the “no key config-key” is issued. Note that this command does not decrypt the configuration file, so zeroize with care.	NVRAM (plaintext or encrypted)	“# no key config-key”
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 128/192/256 bits)	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

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: CSP Table

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

	CSP	RNG Seed	RNG Seed 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	Configuration encryption key	TLS Server RSA Private Key	TLS pre-master Secret	SSL Traffic 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	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	r w d	r w d		r w d					
CO Role																												
Configure the module											r w						r w d											
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	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	r w d	r w d	r w d					
Perform Self-tests																												

r = read w = write d= delete

Table 6: Role CSP Access

Cryptographic Algorithms

Approved Cryptographic Algorithms

The Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) support 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 Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) for use in the FIPS mode of operation.

Algorithm	**IOS Cert. #**	**Cavium Accelerator Cert. #**
AES	#1580	#803
SHS (SHA-1, SHA256 and SHA 512)	#1399	#801
HMAC SHA-1	#926	#443
RNG (ANSI X9.31)	#850	N/A
Triple-DES	#1036	#1037
RSA	#771	N/A

Table 7: FIPS-Approved Algorithms for use in FIPS Mode

Non-Approved Algorithms

The Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) cryptographic module implements the following non-Approved algorithms:

- MD5
- DES
- HMAC-MD5
- RC4

The modules support the following key establishment schemes:

- Diffie-Hellman (key establishment methodology provides between 80 and 112 bits of encryption strength)
- RSA key transport (key establishment methodology provides between 80 and 112 bits of encryption strength)
- Internet Key Exchange Key Establishment (IKEv1/IKEv2)
- Group Domain of Interpretation (GDOI)

Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly. The modules implement the power-on self-tests for all implementations of the approved algorithms, detailed as below:

- IOS Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, Triple-DES KAT, RNG KAT, RSA KAT
- Cavium Accelerator Known Answer Tests: AES KAT, HMAC KAT, Triple-DES KAT
- Firmware Integrity Test (32-bit CRC)

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior any other operations; this prevents the module from passing any data during a power-on self-test failure.

In addition, the modules also provide the following conditional self-tests:

- CRNG test for the FIPS-approved RNG
- CRNG tests for the non-approved RNG
- RSA PWCT
- Bypass Test

Physical Security

This module is a multi-chip standalone cryptographic module.

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence.

The tamper evident labels and opacity shields shall be installed for the module to operate in a FIPS Approved mode of operation.

The following sections illustrate the physical security provided by the module.

Module Opacity and Tamper Evidence

All Critical Security Parameters are stored and protected within each module's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (Part Number CISCO-FIPS-KIT=), Revision -B0. The FIPS kit includes 15 of the seals, as well as a document detailing the number of seals required per platform and placement information. Please be aware that the extra tamper evident labels/seals shall be securely stored by the Crypto Officer. These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

The routers also require that a special opacity shield be installed over the side air vents in order to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications. These are obtained by ordering the appropriate FIPS shield, as follows:

- Cisco 3925E ISR: FIPS-SHIELD-3900=
- Cisco 3945E ISR: FIPS-SHIELD-3900=

Once the module has been configured to meet overall FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log. The tamper evident labels shall be applied as shown in the pictures below, for the module to operate in FIPS mode.

Module	Number of Tamper Seals
Cisco 3925E ISR	31 (three FIPS Kits (CISCO-FIPS-KIT=) required)
Cisco 3945E ISR	31 (three FIPS Kits (CISCO-FIPS-KIT=) required)

Install the opacity plates and apply serialized tamper-evidence labels as specified in the pictures below.

NOTE: Prior to applying the serialized labels, the Crypto Officer must ensure that the surface of the module is dry, clear, and free of any dust.

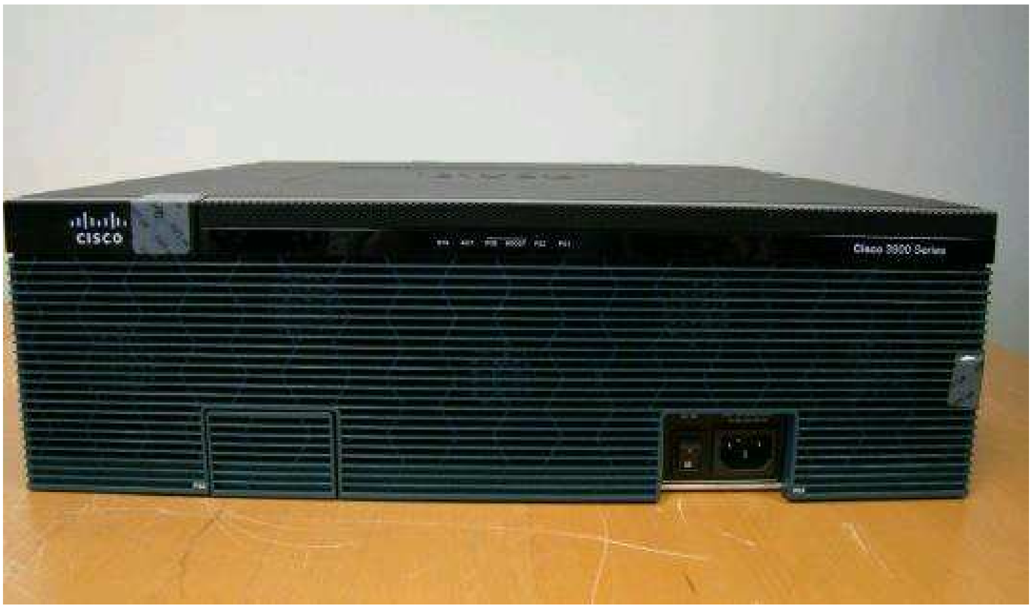

Figure 7: Cisco 3925E ISR Front

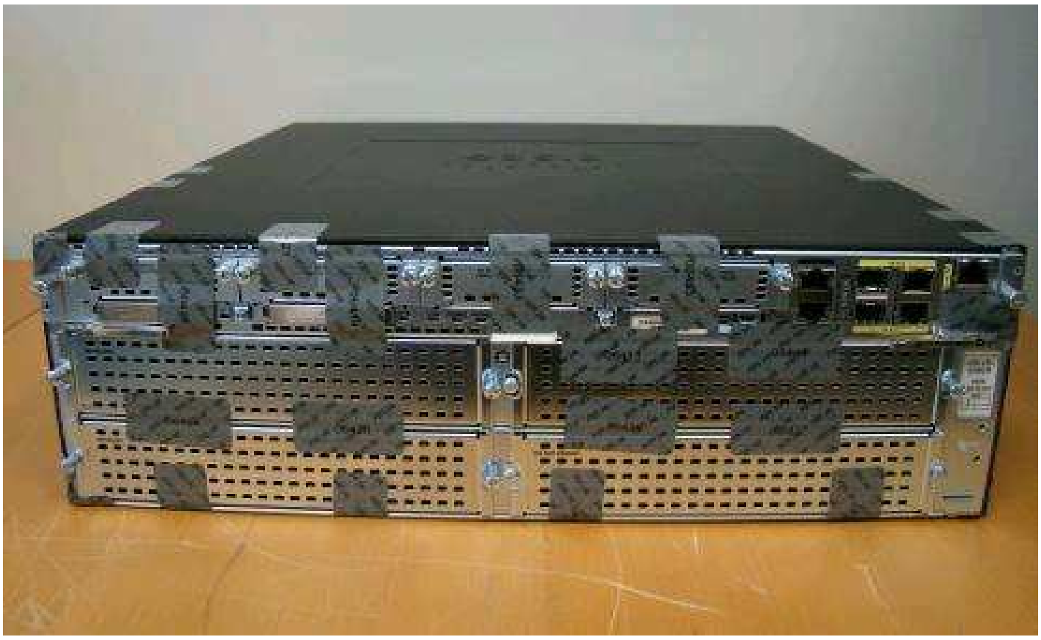

Figure 8: Cisco 3925E ISR Back

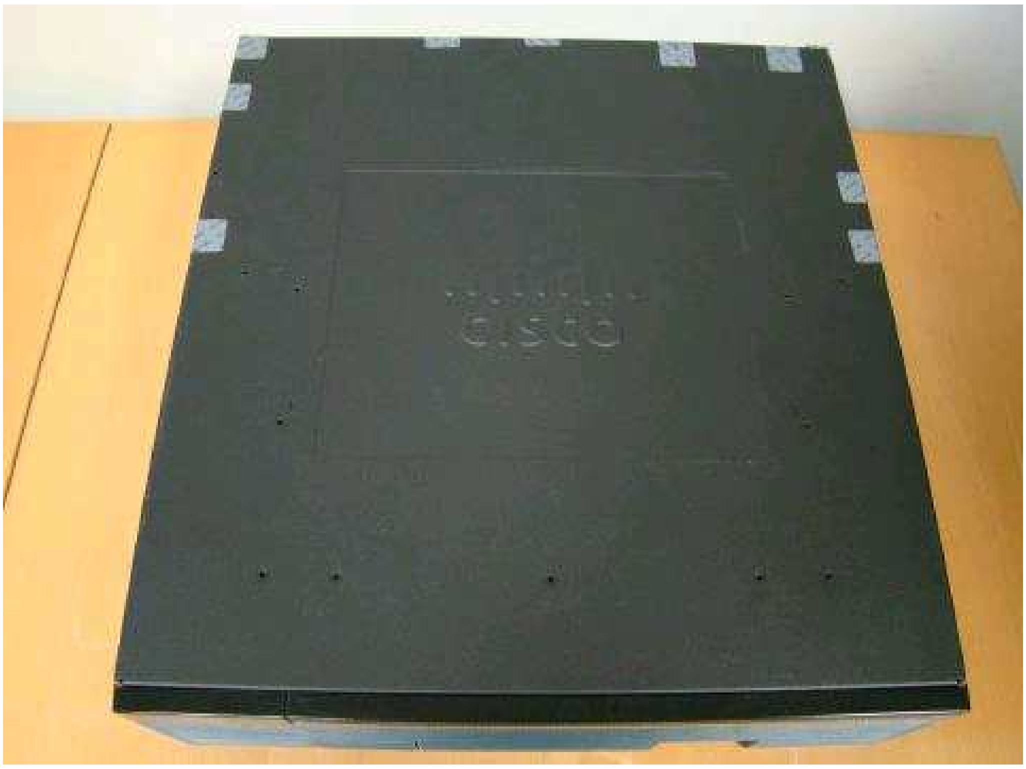

Figure 9: Cisco 3925E ISR Top

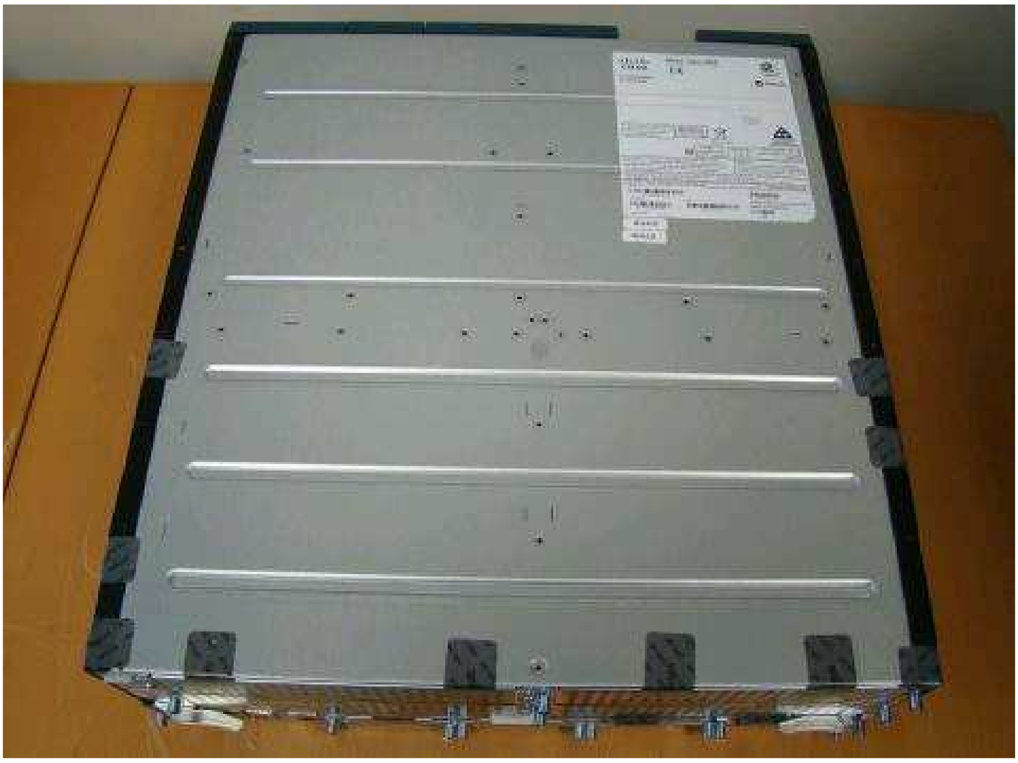

Figure 10: Cisco 3925E ISR Bottom

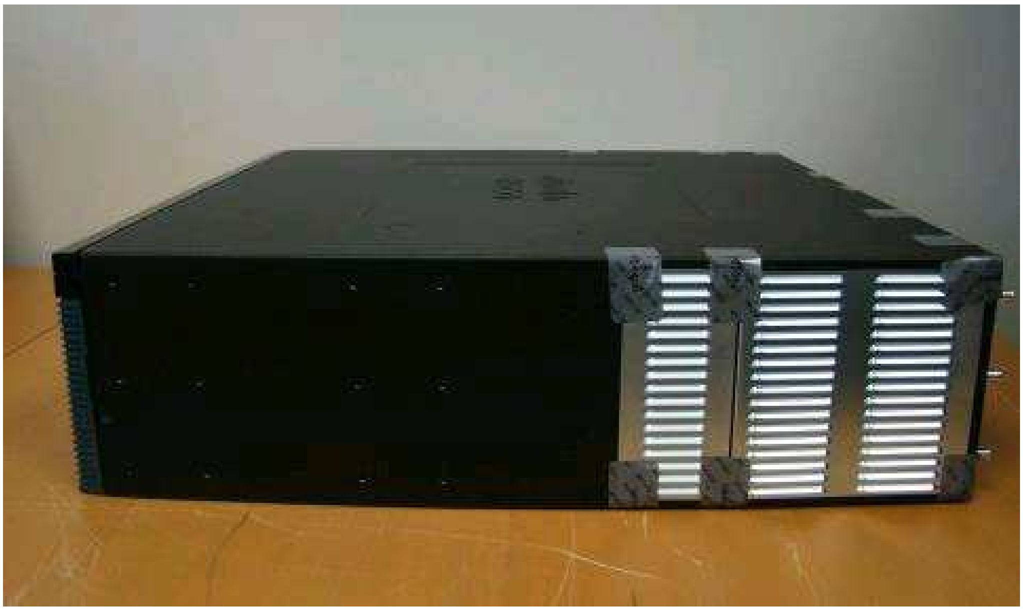

Figure 11: Cisco 3925E ISR Right Side

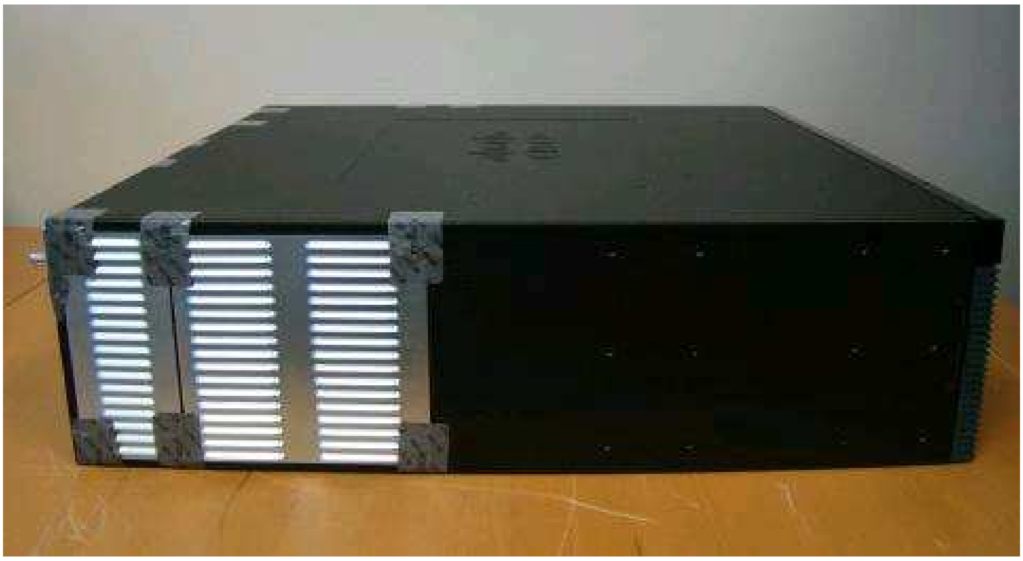

Figure 12: Cisco 3925E ISR Left Side

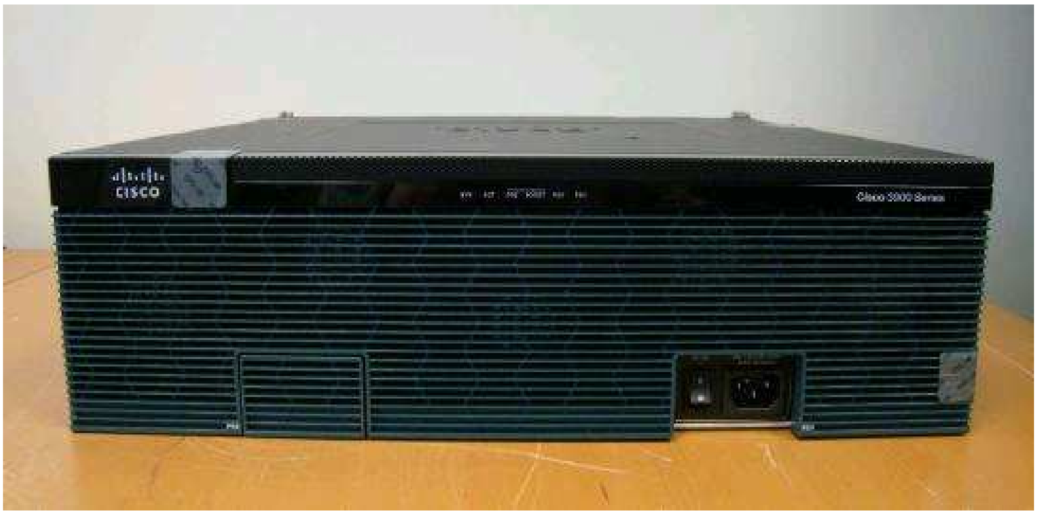

Figure 13: Cisco 3945E ISR Front

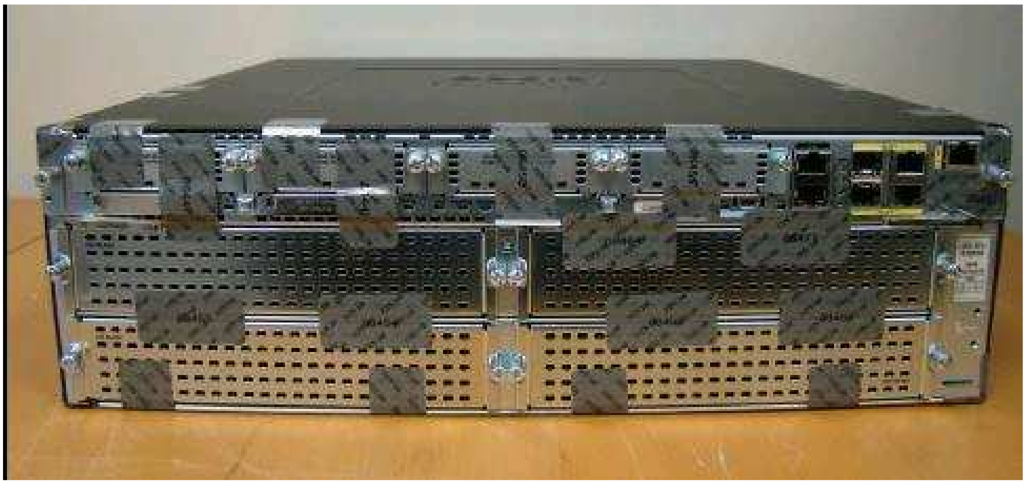

Figure 14: Cisco 3945E ISR Back

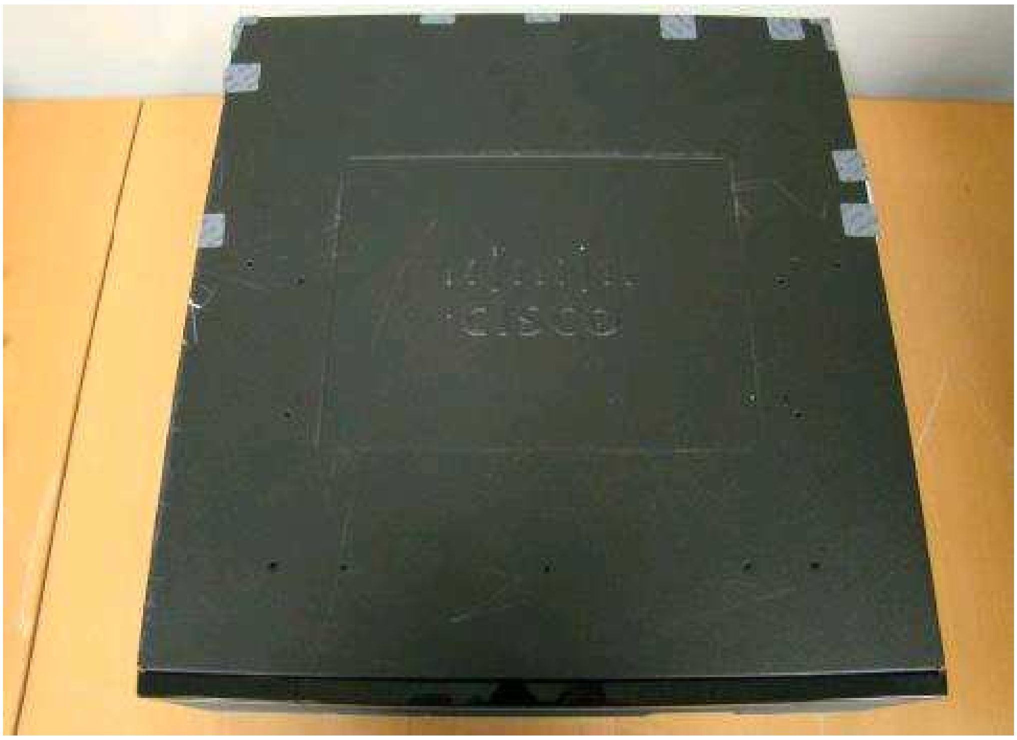

Figure 15: Cisco 3945E ISR Top

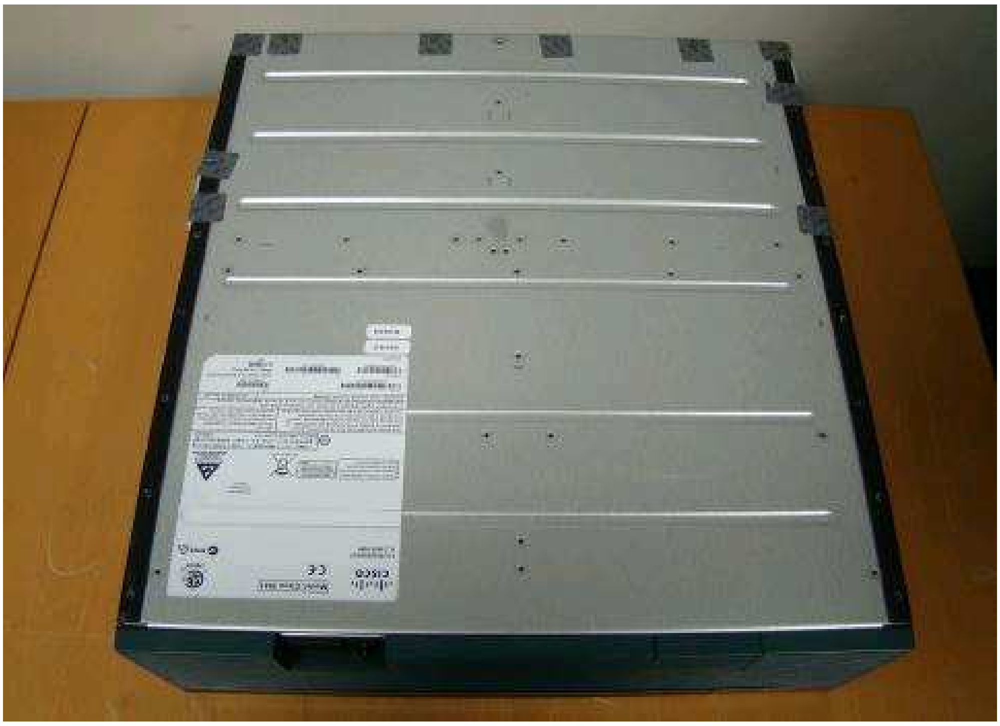

Figure 16: Cisco 3945E ISR Bottom

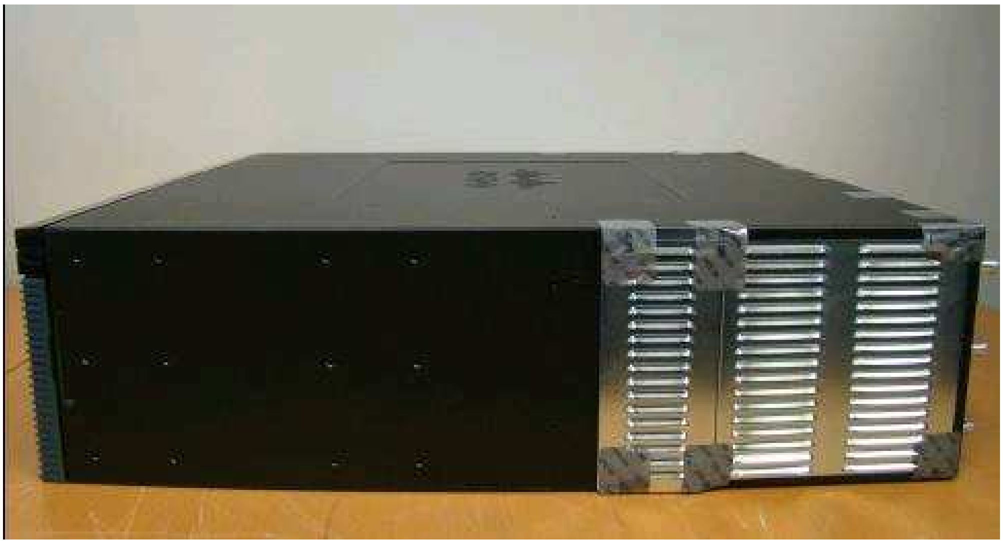

Figure 17: Cisco 3945E ISR Right Side

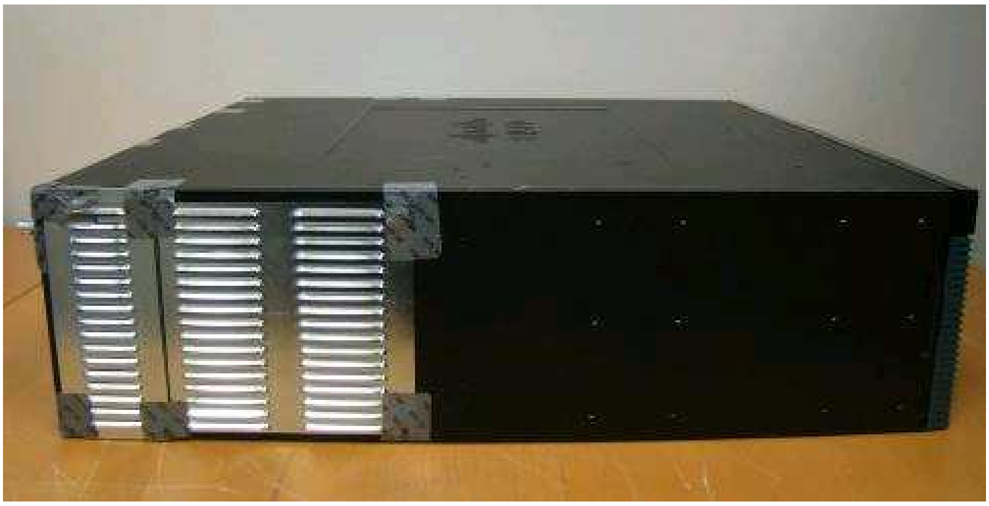

Figure 18: Cisco 3945E ISR Left Side

Secure Operation

The Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) meet all the overall Level 2 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.

Initial Setup

1. The Crypto Officer must install the FIPS opacity shields as described in this document.
2. The Crypto Officer must apply tamper evidence labels as described in this document.
3. The Crypto-Officer must ensure the PC used for the console connection is a non-networked PC.
4. 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.

System Initialization and Configuration

1. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

   config-register 0x0102

2. The Crypto Officer must create the “enable” password for the Crypto Officer role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, 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, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary 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 may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long, including at least one letter and at least one number.
5. Firmware update is not allowed in FIPS mode.

Requirements and Cryptographic Algorithms for IPSec and GetVPN (GDOI) Services

1. Internet Key Exchange (IKE) key management and GDOI group key management are the only two types of key management methods that are allowed in FIPS mode
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
   - esp-aes-192
   - esp-aes-256
3. The following algorithms shall not be used:
   - MD-5 for signing
   - MD-5 HMAC
   - DES

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.

Remote Access

1. SSH access to the module is allowed in FIPS approved mode of operation, using SSH v2 and a FIPS approved algorithm.
2. 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.

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

CUBE TLS Configuration

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

   crypto signaling [strict-cipher]

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 tamper evidence labels and FIPS opacity shields have been properly placed on the module based on the instructions specified in the “Physical Security” and “Secure Operation” sections of this document.
2. 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” section of this document.
3. Issue the following commands: 'show crypto ipsec sa', 'show crypto isakmp policy', and ‘show sip-ua connections tcp tls detail’. Verify that only FIPS approved algorithms are used.

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.

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.

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

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:

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

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.

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.

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://www.cisco.com/en/US/products/products_psirt_rss_feed.html

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 a 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.

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.

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.

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

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.

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

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

Definition List

AES – Advanced Encryption Standard

CMVP – Cryptographic Module Validation Program

CSEC – Communications Security Establishment Canada

CSP – Critical Security Parameter

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

HTTP – Hyper Text Transfer Protocol

KAT – Known Answer Test

LED – Light Emitting Diode

MAC – Message Authentication Code

NIST – National Institute of Standards and Technology

NVRAM – Non-Volatile Random Access Memory

RAM – Random Access Memory

RNG – Random Number Generator

RSA – Rivest Shamir and Adleman method for asymmetric encryption

SHA – Secure Hash Algorithm

TDES – Triple Data Encryption Standard