Cisco 4451-X Integrated Services Router (ISR)
(with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 0.4

Date: Oct 30, 2014

.

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco 4451-X Integrated Services Router (ISR) with integrated RP and ESP from Cisco Systems, Inc., referred to in this document as the modules, routers, or by their specific model name. This security policy describes how the module meets the security requirements of FIPS 140-2 and how to run the module 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 ISR4451-X

The Cisco ISR 4451-X is a highly scalable WAN and Internet Edge router platform that delivers embedded hardware acceleration for multiple Cisco IOS XE Software services without the need for separate service blades. In addition, the Cisco ISR 4451-X Router is designed for business-class resiliency, featuring redundant Route and Embedded Services Processors, as well as software-based redundancy.

With routing performance and IPsec VPN acceleration around ten-fold that of previous midrange aggregation routers with services enabled, the Cisco 4400 Series Integrated Services routers provide a cost-effective approach to meet the latest services aggregation requirement. This is accomplished while still leveraging existing network designs and operational best practices.

The router also supports various VPN services (GetVPN, DMVPN, and EasyVPN).

2.2 Embedded Services Processor (ESP)

The Cisco ISR 4451-X Embedded Service Processors (ESP) is based on the innovative, industry-leading Cisco QuantumFlow Processor for next-generation forwarding and queuing in silicon. These components use the first generation of the hardware and software architecture known as Cisco QuantumFlow Processor.

The ESP provides centralized forwarding-engine options for the Cisco ISR 4451-X Router.

The Cisco ISR 4451 ESP is responsible for the data-plane processing tasks, and all network traffic flows through them. The modules perform all baseline packet routing operations, including MAC classification, Layer 2 and Layer 3 forwarding, quality-of-service (QoS) classification, policing and shaping, security access control lists (ACLs), VPN, load balancing, and NetFlow.

It should be noted that the ISR 4451-X uses an integrated ESP and as such does not have a distinct part number.

2.3 Router Processor (RP)

The Cisco ISR 4451-X Route Processor addresses the route-processing requirements of carrier-grade IP and Multiprotocol Label Switching (MPLS) packet infrastructures. Not only does it provide advanced routing capabilities, but it also monitors and manages the other components in the ISR 4451-X Router.

It should be noted that the ISR 4451 employs an integrated RP.

2.4 Packet Voice Digital Signal Processor Module (PVDM)

The Cisco Fourth-Generation Packet Voice Digital Signal Processor Module (PVDM4) enables Cisco 4451-X Integrated Services Routers (ISRs) to provide rich-media capabilities such as high-density voice connectivity, conferencing, transcoding, media optimization, translating, and secure voice in Cisco Unified Communications Solutions.

The fourth-generation packet voice digital-signal-processor (DSP) modules are available in four densities listed under hardware configuration.

The validated platforms consist of the following components shown in Table 1.

#	Base Unit	Image Version	Crypto	Hardware Configuration
1	ISR4451-X	IOS-XE 3.10.2	IC2M(Rel 3) 1.5.2	Integrated RP and ESP, and PVDM4-32
2				Integrated RP and ESP, and PVDM4-64
3				Integrated RP and ESP, and PVDM4-128
4				Integrated RP and ESP, and PVDM4-256

Table 1: Module Hardware Configurations

2.5 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

3 Cryptographic Boundary

The cryptographic boundary for the Cisco ISR 4451-X is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case; all portions of the "backplane" of the case which are not designed to accommodate a removable port adapter; and space within the case that would be occupied by an installed port adapter. The cryptographic boundary includes the connection apparatus between the port adapter and the board that hosts the port adapter, but the boundary does not include the port adapter itself. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular port adapter.

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 tables:

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (6) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Input Interface
Port Adapter Interface (6) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Output Interface
Port Adapter Interface (6) Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port Power Switch	Control Input Interface
Port Adapter Interface (6) LEDs USB Ports (2) Console Port Auxiliary Port 10/100 Management Ethernet Port	Status Output Interface
Power Plug (up to 2)	Power interface

Table 3: ISR 4451-X

5 Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two main 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 Cisco ISR 4400 Integrated Services Routers Software 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). 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.

Additionally, when using RSA-based authentication, RSA key pair has a modulus size of 2048 bits, thus providing between 112 bits of strength. Assuming the low end of that range, 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 $5.19x10^{28}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

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

Services and Access	Description	Keys and CSPs
Status Functions (r)	View state of interfaces and protocols, version of IOS currently running.	User password
Terminal Functions (r)	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	User password
Directory Services (r)	Display directory of files kept in flash memory.	User password
Self-Tests (r)	Execute the FIPS 140 start-up tests on demand	N/A
IPsec VPN (r, w, d)	Negotiation and encrypted data transport via IPSec VPN	User password
GetVPN (GDOI) (r, w, d)	Negotiation and encrypted data transport via GetVPN	User password
SSH Functions(r, w, d)	Negotiation and encrypted data transport via SSH	User password
HTTPS Functions (TLS) (r, w, d)	Negotiation and encrypted data transport via HTTPS	User password
SNMPv3 Functions(r, w, d)	Negotiation and encrypted data transport via SNMPv3	User password
CUBE/sRTP Functions (r, w, d)	Negotiation and encrypted data transport via CUBE/sRTP	User password

Table 4: User 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 in the same manner as a User. The Crypto Officer is identified by accounts that have a privilege level 15 (versus the privilege level 1 for users). 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 services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below.

Services and Access	Description	Keys and CSPs
Configure the router (r,w)	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.	ISAKMP pre-shared keys, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, User passwords, Enable password, Enable secret,
Define Rules and Filters (r,w,d)	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	password

	characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	
View Status Functions (r)	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.	password
Manage the router (r,w,d)	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.	password
SNMPv3 (r)	Non security-related monitoring by the CO using SNMPv3.	SnmpEngineID, SNMP v3 password, SNMP session key
Configure Encryption/Bypass (r,w,d)	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.	ISAKMP pre-shared keys, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, Enable secret,
TLS VPN (TLSv1.0) (r,w,d)	Configure SSL VPN parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys
SSH v2 (r, w, d)	Configure SSH v2 parameter, provide entry and output of CSPs.	SSH Traffic Keys
sRTP/CUBE (r, w, d)	Configure CUBE/sRTP parameter, provide entry and output of CSPs.	CUBE/sRTP Traffic Keys
IPsec VPN (r, w, d)	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, ISAKMP pre-shared, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key
GetVPN (GDOI) (r, w, d)	Configure GetVPN parameters, provide entry and output of CSPs.	GDOI key encryption key (KEK), GDOI traffic encryption key (TEK), GDOI TEK integrity key
Self-Tests (r)	Execute the FIPS 140 start-up tests on demand	N/A
User services (r,w,d)	The Crypto Officer has access to all User services.	Password
Zeroization (d)	Zeroize cryptographic keys	All Keys and CSPs will be destroyed

Table 5: Crypto Officer Services

5.3 Unauthenticated User Services

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

6 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 operator logins, 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).

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

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
DRBG entropy input	DRBG_CTR (using AES-256)	256-bit	This is the entropy for SP 800-90 CTR_DRBG.	DRAM (plaintext)	Power cycle the device	Manage the Security Appliance And Set Encryption
DRBG Seed	DRBG_CTR (using AES-256)	384-bits	This DRBG seed is collected from the onboard Cavium cryptographic processor.	DRAM (plaintext)	Automatic-ally every 400 bytes, or turn off the router.	Manage the Security Appliance And Set Encryption
DRBG V	DRBG_CTR (using AES-256)	256-bit	Internal V value used as part of SP 800-90 CTR_DRBG	DRAM (plaintext)	Power cycle the device	Manage the Security Appliance And Set Encryption
DRBG Key	DRBG_CTR (using AES-256)	256-bit	Internal Key value used as part of SP 800-90 CTR_DRBG	DRAM (plaintext)	Power cycle the device	Manage the Security Appliance And Set Encryption
Diffie-Hellman Shared Secret	DH	2048 – 4096 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	DRAM (plaintext)	Zeroized upon deletion.	Manage the Security Appliance And Set Encryption

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
Diffie Hellman private key	DH	224 – 379 bits	The private exponent used in Diffie-Hellman (DH) exchange. This CSP is created using SP800-90 DRBG	DRAM (plaintext)	Zeroized upon deletion.	Manage the Security Appliance And Set Encryption
Diffie Hellman public key	DH	2048 – 4096 bits	The p used in Diffie-Hellman (DH) exchange. This CSP is created using SP800-90 DRBG	DRAM (plaintext)	Zeroized upon deletion.	Manage the Security Appliance And Set Encryption
EC Diffie-Hellman private key	ECDH	P-256/P-384	The p used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	DRAM	Automatically after shared secret generated.	Key exchange in IPsec
EC Diffie-Hellman public key	ECDH	P-256/P-384	The p used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	DRAM	Automatically after shared secret generated.	Key exchange in IPsec
EC Diffie-Hellman shared secret	ECDH	P-256/P-384	The shared key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Created per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM	Zeroized upon deletion.	Key exchange in IPsec
skeyid	Keyed SHA-1	160-bits	Value derived per the IKE protocol based on the peer authentication method chosen.	DRAM (plaintext)	Automatically after IKE session terminated.	Set Encryption
skeyid_d	Keyed SHA-1	160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.	Set Encryption
IKE session encrypt key	Triple-DES /AES	-168 bits/ 128, 192, or 256 bits	The IKE session encrypt key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically after IKE session terminated.	Set Encryption

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
IKE session authentic-cation key	HMAC SHA-1	160-bits	The IKE session authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically after IKE session terminated.	VPN functions And Configure the Module and Set Encryption
ISAKMP preshared	Secret	At least eight characters	The key used to generate IKE skeyid during preshared-key authentication. **# 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. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	# no crypto isakmp key	VPN functions And Configure the Module and Set Encryption
IKE authentication private Key	RSA/ ECDSA	2048 – 4096 bits and P-256/P-384	The key used in IKE authentication. **# crypto key zeroize rsa** command zeroizes it.	NVRAM (plaintext)	# crypto key zeroize rsa	Set Encryption
IKE authentication public key	RSA/ ECDSA	2048 – 4096 bits and P-256/P-384	The key used in IKE authentication. **# crypto key zeroize rsa** command zeroizes it.	NVRAM (plaintext)	# crypto key zeroize rsa	Set Encryption
IPsec encrypt-ion key	Triple-DES /AES	168 bits/ 128, 192, or 256 bits	The IPsec encryption key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically when IPsec session terminated.	VPN functions And Configure the Module And Manage the Security Appliance and Set Encryption

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
IPsec authentication key	HMAC SHA-1	160-bits	The IPsec authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically when IPsec session terminated.	VPN functions And Configure the Module And Manage the Security Appliance and Set Encryption
Operator password	Shared Secret	At least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password	Status Function And Terminal function And VPN Function And Perform Cryptography And Configure the Module and Define Rules and filters And Status Function and Manage the Security Appliance and Set Encryption
Enable password	Shared Secret	At least eight characters	The plaintext password of the CO role. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password	Configure the Module and Set Encryption And Zeroization

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
Enable secret	Shared Secret	At least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Cryptographic Operator optionally configures the module to obfuscate the Enable password. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password	Manage the Security Appliance
RADIUS secret	Shared Secret	16 characters	The RADIUS shared secret. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	# no radius-server key	Manage the Security Appliance
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	# no tacacs-server key	Manage the Security Appliance
SSH Private Key	RSA	2048 – 4096 bits	The SSH private key for the module. RSA key sizes 1024 - 4096 bits.	NVRAM (plaintext)	SSH private key is zeroized by either deletion (via **# crypto key zeroize rsa**) or by overwriting with a new value of the key	Manage the Security Appliance
SSH Public Key	RSA	2048 – 4096 bits	The SSH public key for the module. RSA key sizes 1024 - 4096 bits.	NVRAM (plaintext)	Zeroized upon deletion.	Manage the Security Appliance
SSH Session Key	Triple-DES /AES	168 bits/ 128, 192, or 256 bits	The SSH session key. This key is created through SSH key establishment.	DRAM (plaintext)	Automatically when the SSH session is terminated.	Manage the Security Appliance
GDOI Data Security Key (TEK)	Triple-DES /AES	168 bits/ 128, 192, or 256 bits	This key is created using the “GROUPKEY-PULL” registration protocol with GDOI.	DRAM (plaintext)	Automatically when session terminated.	Manage the Security Appliance

Name	Alg.	Key Size	Description	Storage	Zeroization	Service and Access
GDOI Group Key Encryption Key (KEK)	Triple-DES /AES	-168 bits/ 128, 192, or 256 bits	This key is created using the “GROUPKEY-PUSH” registration protocol with GDOI.	DRAM (plaintext)	Automatically when session terminated.	Manage the Security Appliance
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	DRAM (plaintext)	Automatically when session terminated.	Manage the Security Appliance
snmpEngineID	Shared Secret	-32-bits	A unique string used to identify the SNMP engine.	NVRAM	Overwrite with new engine ID	Manage the Security Appliance
SNMPv3 password	Shared Secret	-8 – 25 characters	The password use to setup SNMP v3 connection.	NVRAM	Overwrite with new password	Manage the Security Appliance
SNMPv3 session key	AES	-128-bits	Encryption key used to protect SNMP traffic.	DRAM (plaintext)	Automatically when session terminated.	Manage the Security Appliance
sRTP Master Key	AES	AES (128/196/ 256 bits)	Generated by the CUCM and sent to phone in TLS session. Key used to generate sRTP session keys	DRAM	upon end of call or device reset.	Manage the Security Appliance and seesions
sRTP Encryption key (AES)	AES	AES (128/196/ 256 bits)	Generated via the sRTP protocol. Key used to encrypt/decrypt sRTP packets	DRAM	upon end of call or device reset.	Set encryption
sRTP Authentication key (HMAC)	HMAC SHA-1	-160 bits	Generated via the sRTP protocol. Key used to authenticate sRTP packets	DRAM	upon end of call or device reset.	Authentication

Table 6: CSP Table

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco ISR 4451 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 ISR 4451 for use in the FIPS mode of operation.

Algorithm	Supported Mode	Cert. #
IC2M(IOS XE) IOS Common Crypto Module/Common Crypto Module-Extended2		
AES	CBC (128, 192, 256), CMAC, GCM	2817
SHS (SHA-1, 256, 384, and 512)	Byte Oriented	2361
HMAC SHA (1, 256, 384, and 512)	Byte Oriented	1764
ECDSA	KeyGen, SigGen/Ver	493
DRBG	CTR (using AES-256)	481
RSA	PKCS#1 v.1.5, 2048-4096 bit key	1471
Triple-DES	KO 1,2; CBC	1688/1670
KAS	Component Test KAS FFC/ECC	252
KDF	Component Test KDF-135	253
Cavium Octeon II CN6645 (Embedded Services Processor (ESP))		
AES	ECB, CBC (128, 192, 256), GMAC	2345
SHS (SHA-1, 256, 384, 512)	Byte Oriented	2022
HMAC SHA-1, 256, 384, 512	Byte Oriented	1454
Triple-DES	KO 1,2 - ECB, CBC	1468

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

Note: Each of Triple-DES certs (#1468, #1688 and #1670) supports two-key and three-key Triple-Des options, but only three-key Triple-DES is used in FIPS mode.

7.2 Non-Approved Algorithms allowed for use in FIPS-mode

The ISR 4451 cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Diffie-Hellman – provides between 112 and 150-bits of encryption strength
- RSA Key Wrapping – provides between 112 and 150-bits of encryption strength
- EC Diffie-Hellman (key establishment methodology provides between 128 and 192 bits of encryption strength)
- GDOI (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)
- Non-approved RNG for seeding the DRBG.

7.3 Non-Approved Algorithms

The ISR 4451 cryptographic module implements the following non-Approved algorithms:

- MD5
- DES
- HMAC MD5
- RC4

7.4 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 following power-on self-tests:

- IC2M(IOS XE)
    - POSTs - IOS Common Crypto Module
        - Firmware Integrity Test (HMAC SHA-256)
        - AES encrypt and decrypt KATs
        - AES GCM KAT
        - AES-CMAC KAT
        - DRBG KAT
        - ECDSA Sign/Verify
        - HMAC-SHA-1 KAT
        - HMAC-SHA-256 KAT
        - HMAC-SHA-384 KAT
        - HMAC-SHA-512 KAT
        - KAS ECC Primitive “Z” KAT
        - KAS FFC Primitive “Z” KAT
        - RSA KAT
        - SHA-1 KAT

        - SHA-256 KAT
        - SHA-512 KAT
        - Triple-DES encrypt and decrypt KATs
    - POSTs - IOS Common Crypto Module-Extended2
        - Triple-DES encrypt and decrypt KATs

- Cavium Octeon II CN6645 (Embedded Services Processor (ESP))
    - AES encrypt and decrypt KATs
    - AES-GMAC encrypt and decrypt KATs
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-512 KAT
    - Triple-DES encrypt and decrypt KATs

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:

- IC2M(IOS XE)
    - Continuous Random Number Generator test for the FIPS-approved DRBG
    - Continuous Random Number Generator test for the non-approved RNG
    - Pair-Wise Consistency Test for RSA
    - Pair-Wise Consistency Test for ECDSA keys

8 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 following sections illustrate the physical security provided by the module. The module relies upon Tamper Evident Labels and Opacity Shields with the following Cisco part numbers:

- ISR4451-FIPS-Kit

8.1 Module Opacity

To install an opacity shield on the ISR 4451 routers, follow these steps:

1. The opacity shield is designed to be installed on an ISR 4451 router chassis that is already rack-mounted. If your ISR 4451-X router chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the ISR 4451 router Installation Guide. If your ISR 4451-X router chassis is already rack-mounted, proceed to step 2.
2. Open the FIPS kit packaging.
3. Open the protective packaging and remove the opacity shield and the two bags of installation hardware. Select the bag of installation hardware appropriate for your installation. Set the second bag of fasteners aside; you will not need them for this installation.
4. Open the bag of installation hardware (Bag with part number 69-1497) and remove the following: Two M4 thumbscrews, four M4 snap rivet fastener sleeves, and four M4 snap rivet pins.

Note: Extra snap fasteners are included in the bags of installation hardware in case of loss or damage.

Note: Installation hardware from one bag is not interchangeable with the installation hardware from the second bag.

The figures in the following section illustrate the installation of the opacity shields for each platform.

8.2 Tamper Evidence

The tamper evident seals (hereinafter referred to as tamper evident labels (TEL)) shall be installed on the security devices containing the module prior to operating in FIPS mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

Should the CO have to remove, change or replace TELs (tamper-evidence labels) for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth.

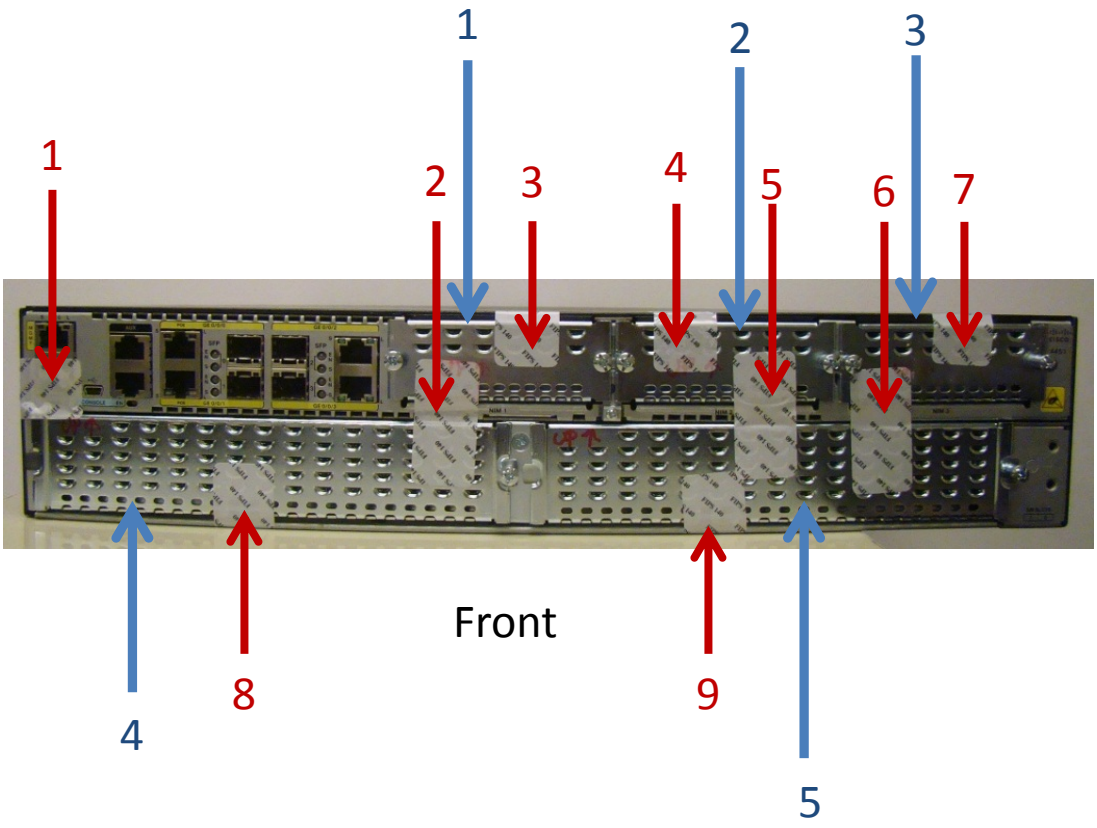
Any deviation of the TELs placement such as tearing, misconfiguration, removal, change, replace or any other change in the TEL's from its original configuration as depicted below by unauthorized operators shall mean the module is no longer in FIPS mode of operation. Returning the system back to FIPS mode of operation require the replacement of the TEL as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy.

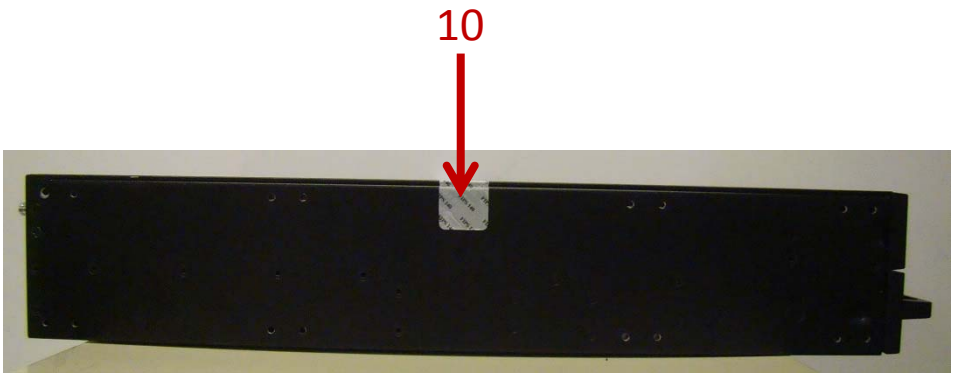
The modules shall require the following number of labels to be affixed:

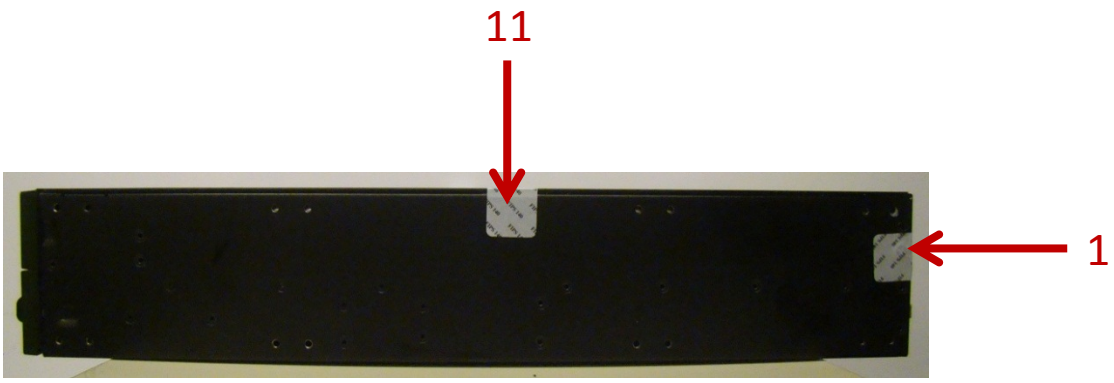
Model	Number of Tamper Labels Affixed	Opacity Shields
ISR 4451-X	13 (indicated in red)	5 (indicated in blue)

Table 8: TELs Table

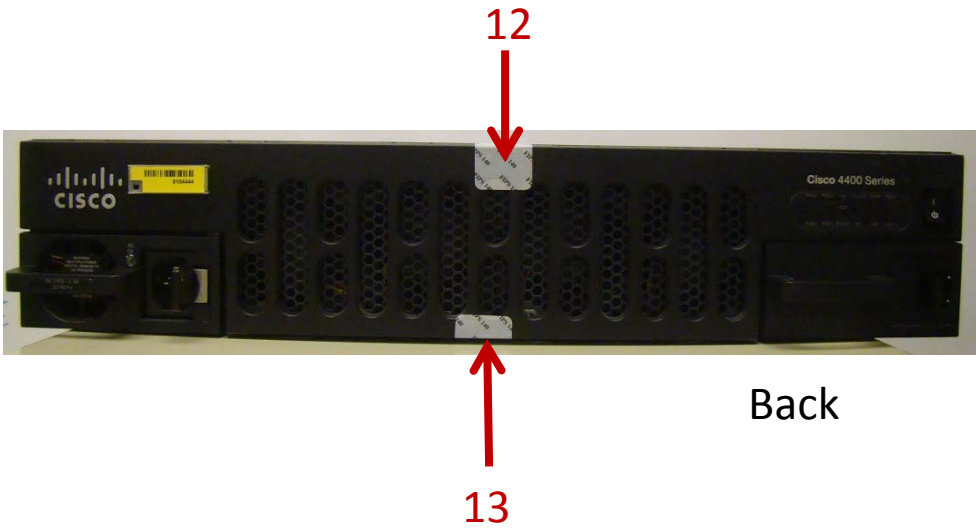
The following figures illustrate the installation of the TELs for each platform.



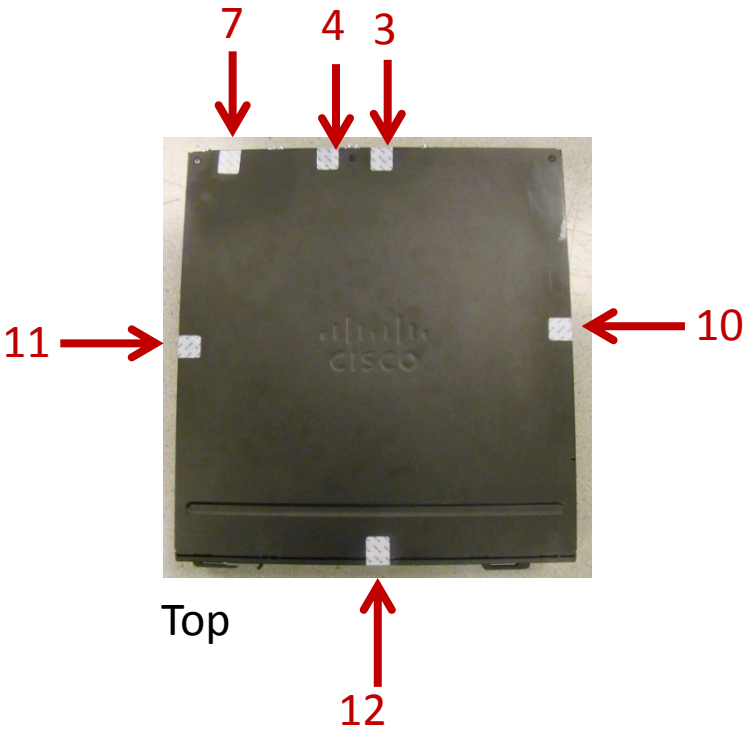




Left side



Back



9 Secure Operation

9.1 System Initialization and Configuration

Prior to system operational initialization and configuration the Crypto Officer must install the opacity shields and tamper evidence seals as specified in section 8 above.

Step1 - 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

Step 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]

Step 3 - The Crypto Officer must set up the operators of the module. The Crypto Officer enters the following syntax at the “#” prompt:

Username [USERNAME]

Password [PASSWORD]

Step 4 – For the created operators, 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

Step 5 - 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.

Step 6 - The Crypto Officer must apply tamper evidence labels as described earlier in this document.

Step 7 - Dual IOS mode is not allowed. ROMMON variable IOSXE_DUAL_IOS must be set to 0.

Step 8 - In service software upgrade (ISSU) is not allowed. The operator should not perform in service software upgrade of an ISR 4451-X FIPS validated firmware image

Step 9 - Use of the debug.conf file is not allowed. The operator should not create the bootflash:/debug.conf file and use it for setting environment variables values.

NOTE: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. Although key separation is maintained by the module so that FIPS mode keys are not used in non-FIPS mode or vice versa, it is recommended that keys be zeroized by the Crypto Officer prior to the module transition from FIPS to non-FIPS mode or from non-FIPS to FIPS mode.

9.2 IPsec Requirements and Cryptographic Algorithms

Step 1 - The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE) (non-compliant).

Step 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

Step 3 - The following algorithms shall not be used:

- MD-5 for signing
- MD-5 HMAC
- DES

9.3 Protocols

Step 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.

Step 2 - Secure DNS is not allowed in FIPS mode of operation and shall not be configured.

9.4 Remote Access

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

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.