Cisco Integrated Services Router (ISR) 4351 and 4331 (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Cisco Integrated Services Router (ISR) 4321 (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)

FIPS 140-2 Non Proprietary Security Policy

Level 1 Validation

Version 1.0

Date: December 22, 2015

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Integrated Services Router (ISR) 4351 and 4331 (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and the Cisco Integrated Services Router (ISR) 4321 (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) from Cisco Systems, Inc., referred to in this document as the modules, routers, or by their specific model name. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.1 References

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

- The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.2 FIPS 140-2 Submission Package

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

Vendor Evidence

- Finite State Machine
- Other supporting documentation as additional references

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

2 Module Description

2.1 Cisco ISR 4351, 4331, and 4321

Image 1: ISR 4351 Front and Back

Image 2: ISR 4331 Front and Back

Image 3: ISR 4321 Front and Back

The Cisco ISR 4351, 4331 and 4321 design are based on Cisco ISR 4451-X but scaled down to a single CPU (SOC). The IOS-XE software architecture enables high performance and scalability through leverage of multi-core CPUs, feature inheritance, modularity, fault isolation, and restartability.

1. ISR 4351 will address the aggregated 600Mbps space and/or customers requiring density of services appropriate for two Service Module slots or a Double Wide Service Module.
2. ISR 4331 will address the aggregated 400Mbps space and/or customers requiring density of services appropriate for a Service Module slot.
3. ISR 4321 will address the aggregated 200Mbps market space for customers who desire rich services including support for Unified Communication.

Feature Name	Description
IKE/IPsec	Used for securing data plane traffic
RADIUS	Used for external authentication
SNMPv3	Used for remote management
SSHv2	Used for secure configuration
TACACS+	Used for external authentication
TLS (HTTPS)	Used for secure configuration
GetVPN	Used for data plane traffic
Cube/sRTP	Used for securing data traffic

Table 1: Supported Services

2.2 Packet Voice Digital Signal Processor Module (PVDM)

The Cisco Fourth-Generation Packet Voice Digital Signal Processor Module (PVDM4) enables Cisco 4351, 4331 and 4321 Integrated Services Router (ISR) 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.

http://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet_c78-728307.html

2.3 Next Generation Etherswitch (SM-ES)

SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P are the next Generation Layer 3 Etherswitch Service Modules (ESM) for 29XX/ 39XX/43XX/44XX ISR product families with 16 port, 24 port and 48 port. It is based off of the ESTG's Catalyst 3560-X series switches, with Power Over Ethernet Plus (POE+) providing up to 30 watts of power per port. Additional improvements include IEEE 802.3ae Media Access Control Security (MACSec) port-based, and hop-to-hop. MACSec cannot be used while in FIPS mode of operation.

http://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-730357.html

The validated platforms comprise the main system (Product Model) along with any of the following listed ESM or PVDM4 modules in any configuration. The different configurations only affect the number of ports available. FIPS testing was conducted with each model and the PVDM4 housed.

Product Model	Firmware Image Name	Crypto	Etherswitch Service Modules (ESM)	Packet Voice Digital Signal Processor Module (PVDM4)
ISR 4351	IOS-XE 3.13.2	IC2M(Rel 5)	SM-ES3X-16-P SM-ES3X-24-P SM-D-ES3X-48-P	PVDM4-32: 32-channel DSP Module PVDM4-64: 64-channel DSP Module PVDM4-128: 128-channel DSP Module PVDM4-256: 256-channel DSP Module
ISR 4331	IOS-XE 3.13.2	IC2M(Rel 5)	SM-ES3X-16-P SM-ES3X-24-P SM-D-ES3X-48-P	PVDM4-32: 32-channel DSP Module PVDM4-64: 64-channel DSP Module PVDM4-128: 128-channel DSP Module PVDM4-256: 256-channel DSP Module
ISR 4321	IOS-XE 3.13.2	IC2M(Rel 5)		PVDM4-32: 32-channel DSP Module PVDM4-64: 64-channel DSP Module PVDM4-128: 128-channel DSP Module PVDM4-256: 256-channel DSP Module

Table 2: Module configuration

2.4 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	3
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	3
11	Mitigation of Other Attacks	N/A
Overall	Overall module validation level	1

Table 3: Module Validation Level

3 Cryptographic Boundary

The cryptographic boundary for the Cisco Integrated Services Router (ISR) 4351, 4331 and 4321 is defined as encompassing the "front", "back", "top", "bottom", "left," and "right" surfaces of the case.

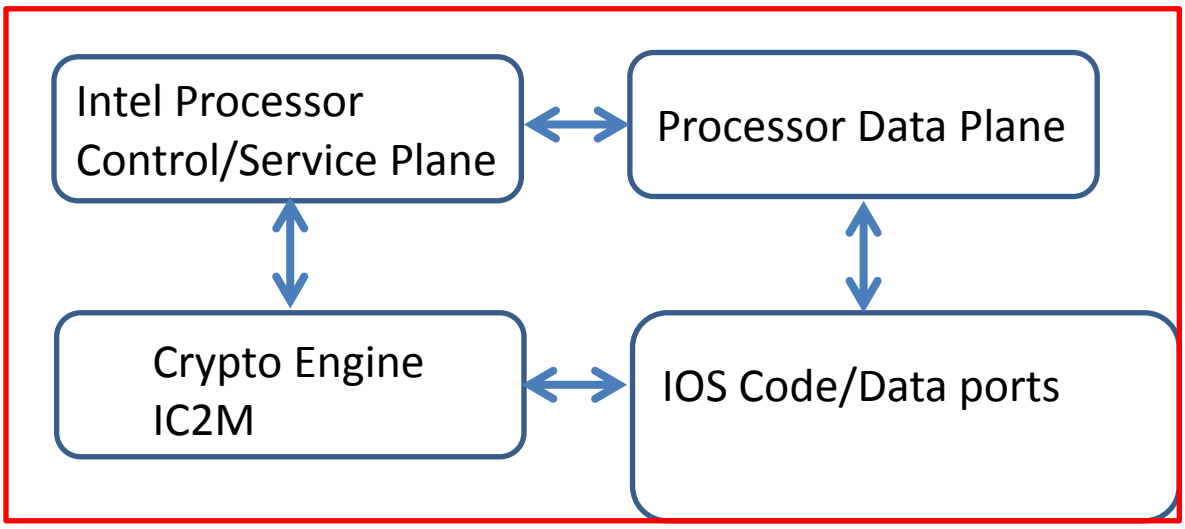

Diagram 1- Block Diagram (Cryptographic boundary and Physical boundary in red)

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 Interface For 4351,4331,4321	Logical Interface
10/100/1000 RJ-45 Ethernet port USB port Console Port AUX port	Data Input
10/100/1000 RJ-45 Ethernet port USB port Console Port AUX port	Output Interface
10/100/1000 RJ-45 Ethernet port USB port Console Port AUX port Power Switch	Control Input
10/100/1000 RJ-45 Ethernet port USB port Console Port AUX port	Status Output Interface
Power Plug	Power Interface

Table 4: ESG 4351, 4331, and 4221

5 Physical Security

The Module is a multi-chip embedded cryptographic module and conforms to Level 1 requirements for physical security. The cryptographic module consists of production-grade components in that the components have standard industry acceptable coating applied to them.

6 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 (which covers ISR 4400 and ISR 4300 Series) 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 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.

P-256 and P-384 curves are supported for ECDSA based authentication. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^128, which is less than 1 in 100,000 required by FIPS 140-2.

6.1 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 5 - User Services

6.2 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 of the router. 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
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	password

	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 (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, SKEYSEED, 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/CSPs by running the zeroization methods classified in table 7, Zeroization column.	All CSPs

Table 6 - Crypto Officer Services

6.3 Non-FIPS mode Services

The cryptographic module in addition to the above listed FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved

algorithms and non-approved key sizes a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the Non-Approved services in Section 6.3 the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Non-Approved Service [1]	Non-Approved Algorithms and non-approved key/curve sizes[2]
IPsec	Hashing: MD5, MACing: HMAC-SHA-1, MD5 Symmetric: Triple-DES, AES, DES, RC4 Asymmetric: RSA (key transport), ECDSA, Diffie-Hellman, EC Diffie-Hellman
SSH	Hashing: MD5, MACing: HMAC MD5 Symmetric: Triple-DES, AES, DES Asymmetric: RSA (key transport), Diffie-Hellman, EC Diffie-Hellman
TLS	Hashing: MD5, MACing: HMAC-SHA-1, MD5 Symmetric: AES, DES, RC4 Asymmetric: RSA (key transport), Diffie-Hellman, EC Diffie-Hellman
SNMP	Hashing: MD5, MACing: HMAC-SHA-1, MD5 Symmetric: AES, DES, RC4 Asymmetric: RSA (key transport), Diffie-Hellman, EC Diffie-Hellman

[1] These approved services become non-approved when using any of non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

[2] When using a non-approved keys as part of a non-Approved function or service approved algorithms like AES and Triple-DES become non-approved by association to these Non-Approved keys. The other algorithms listed are non-approved FIPS algorithms.

MACSec	Symmetric: AES Key Derivation: NIST SP 800-108 KBKDF

Table 7 – Non-FIPS Services

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

The Crypto Officer must zeroize all CSPs prior to utilizing the MACSec services in Table 7.

All services available can be found in the ISR data sheet; along with instructions on configuration can be found in ISR software configuration guide.

6.4 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.

7 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer 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). Keys/CSPs can be zeroized by running the zeroization methods classified in table 7, Zeroization column. The module supports the following critical security parameters (CSPs):

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90 DRBG_CTR (using AES-256)	256-bits	This is the entropy for SP 800-90 CTR_DRBG. HW (onboard Cavium cryptographic processor) based entropy source used to construct seed.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG Seed	SP800-90 DRBG_CTR	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90 DRBG_CTR	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG Key	SP800-90 DRBG_CTR	256-bits	Internal Key value used as part of SP 800-90 CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman Shared Secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie Hellman private key	DH	224-379 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90 DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048 – 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman private key	ECDH	Curves: P-256/P-384	Used in establishing the session key for an IPSec session. The private key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is generated by calling SP800-90 DRBG.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
EC Diffie-Hellman public key	ECDH	Curves: P-256/P-384	Used in establishing the session key for an IPSec session. The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman shared secret	ECDH	Curves: P-256/P-384	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
skeyid	Shared Secret	160 bits	A shared secret known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1) and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Power cycle the device
skeyid_d	Shared Secret	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Power cycle the device
SKEYSEED	Shared Secret	160 bits	A shared secret known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Power cycle the device
IKE session encrypt key	Triple-DES/AES	168 bit Triple-DES or 128/192/256 bits AES	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	DRAM (plaintext)	Power cycle the device
IKE session authentication key	HMAC SHA-1	160 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
ISAKMP preshared	Pre-shared key	Variable 8 plus characters	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	By running '# no crypto isakmp key' command
IKE authentication private Key	RSA/ ECDSA	RSA (2048 – 3072 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA private key used in IKE authentication. This key is generated by calling SP800-90 DRBG.	NVRAM (plaintext)	By running '#crypto key zeroize' command
IKE authentication public key	RSA/ ECDSA	RSA (2048 – 3072 bits) or ECDSA (Curves: P-256/P-384)	RSA/ECDSA public key used in IKE authentication. Internally generated by the module	NVRAM (plaintext)	By running '#crypto key zeroize' command
IPsec encrypt-ion key	Triple-DES/AES	168 bits Triple-DES or 128/192/256 bits AES	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	DRAM (plaintext)	Power cycle the device
IPsec authentication key	HMAC SHA-1	160-bits	The IPsec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	DRAM (plaintext)	Power cycle the device
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
Enable password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
RADIUS secret	Shared Secret	16 characters	The RADIUS shared secret. Used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext),	By running '# no radius-server key' command
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext),	By running '# no tacacs-server key' command

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SSHv2 Private Key	RSA	2048 – 3072 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP800-90 DRBG.	NVRAM (plaintext)	By running '# crypto key zeroize rsa' command
SSHv2 Public Key	RSA	2048 – 3072 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module.	NVRAM (plaintext)	By running '# crypto key zeroize rsa' command
SSHv2 Session Key	Triple-DES/AES	168 bits Triple-DES or 128/192/256 bits AES	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Power cycle the device
GDOI Data Security Key (TEK)	Triple-DES/AES	168 bits Triple-DES or/ 128/192/256 bits AES	Generate by calling SP800-90 DRBG in the module. It is used to encrypt data traffic between Get VPN (GDOI) peers.	DRAM (plaintext)	Power cycle the device
GDOI Group Key Encryption Key (KEK)	Triple-DES/AES	168 bits Triple-DES or/ 128/192/256 bits AES	Generate by calling SP800-90 DRBG in the module. It is used protect Get VPN (GDOI) rekeying data.	DRAM (plaintext)	Power cycle the device
GDOI TEK integrity key	HMAC SHA-1	160 bits	Generate by calling SP800-90 DRBG in the module. It is used to ensure data traffic integrity between Get VPN (GDOI) peers.	DRAM (plaintext)	Power cycle the device
snmpEngineID	Shared Secret	32 bits	A unique string used to identify the SNMP engine. This key is entered by Crypto Officer.	NVRAM (plaintext)	Overwrite with new engine ID
SNMPv3 password	Shared Secret	256 bits	The password use to setup SNMP v3 connection. This key is entered by Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
SNMPv3 session key	AES	128 bits	Encryption key used to protect SNMP traffic. This key is derived via key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
sRTP Master Key	AES	128/196/256 bits	This key is transported into the module protected by a TLS session. This Key is used to derived sRTP Encryption key and sRTP Authentication keys.	DRAM (plaintext)	Power cycle the device
sRTP Encryption key	AES	128/196/256 bits	Derived from sRTP Master Key via key derivation function defined in SP800-135 KDF (sRTP). This key is used to encrypt/decrypt sRTP packets.	DRAM (plaintext)	Power cycle the device
sRTP Authentication key	HMAC SHA-1	160 bits	Derived from sRTP Master Key via key derivation function defined in SP800-135 KDF (sRTP). This key is used to authenticate sRTP packets.	DRAM (plaintext)	Power cycle the device

Table 8: CSP Table

8 Cryptographic Algorithms

8.1 Approved Cryptographic Algorithms

The Cisco Integrated Services Router (ISR) 4351, 4331 and 4321 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 4351, 4331 and 4321 for use in the FIPS mode of operation.

Algorithm	Cert. #
IC2M(IOS XE) IOS Common Crypto Module/Common Crypto Module-Extended2	
AES	2817
DRBG	481
ECDSA	493
HMAC SHA (1, 256, 384, and 512)	1764
CVL(SP800-56A KAS)	252
CVL(SP800-135 KDF)	253

Algorithm	Cert. #
RSA	1471
SHS (SHA-1, 256, 384, and 512)	2361
Triple-DES	1688/1671
Intel Rangeley	
AES	3032

Table 9: FIPS-Approved Algorithms for use in FIPS Mode

Note: Each of Triple-DES certs (#1688 and #1671) supports two-key and three-key Triple-Des options, but only three-key Triple-DES is used in FIPS mode.

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

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

- Diffie-Hellman (key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key establishment methodology provides 128 or 192 bits of encryption strength)
- NDRNG

8.3 Non-Approved and Non-Allowed Algorithms

The cryptographic module can implement the following non-Approved and non-Allowed algorithms for use outside of FIPS-mode:

- AES (non-Approved)[3]
- MD5
- DES

[3] The validated AES algorithm implantation is considered non-Approved when utilized in with the MACSec protocol.

- HMAC MD5
- RC4
- Diffie-Hellman (non-Approved)[4]
- RSA key transport (non-Approved)[5]
- SP 800-108 Key-Based Key Derivation Function (non-Approved)

8.4 IPsec protocol IV Generation

The IV is constructed in compliance with the IPSec protocol and is only used in the context of the AES GCM mode encryption within the IPSec protocol. Furthermore this IV Generation is in compliance with the IPsec specifications outlined in RFC 6071. Additionally the IKEv2 protocol (RFC 7296) is used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. All of this is IKE key establishment is performed *entirely within* the cryptographic boundary of the module.

8.5 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 Pair-Wise Consistency Test
        - HMAC (SHA-1,SHA-256, SHA-384, SHA-512) KATs
        - RSA (sign and verify) KAT
        - Triple-DES (encrypt and decrypt) KATs
    - POSTs - IOS Common Crypto Module-Extended2

[4] The allowed Diffie-Hellman implementation is considered non-Approved when utilizing key sizes which provide less than 112-bits of encryption strength

[5] The validated RSA implementation is considered non-Approved when utilizing key sizes which provide less than 112-bits of encryption strength

- Triple-DES (encrypt and decrypt) KATs

- Rangeley
  - AES (encrypt and decrypt) KAT

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)
  - Conditional IPsec Bypass test
  - Continuous Random Number Generator test for the FIPS-approved DRBG (SP800-90a DRBG)
  - Continuous Random Number Generator test for the non-approved RNG
  - Pair-Wise Consistency Test for RSA
  - Pair-Wise Consistency Test for ECDSA

9 Secure Operation

9.1 System Initialization and Configuration

System setup is detailed in “Cisco 4000 Series ISRs Software Configuration Guide “Cisco 4400 Series ISRs and Cisco 4300 Series ISRs Software Configuration Guide”

Step1 - 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.

Step 2 - 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:

Router# configure terminal
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot Router# copy running-config startup-config
Router# reload
after install is complete
Router>enable
Router#show version

Step 3 - 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:

Router> fips enable
Router# configure terminal
Router (config)#
Router (config) # enable secret [PASSWORD]

Example: `Router(config)# enable secret cr1ny5ho`

Step 4 - 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 5 – 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:

Router(config)# line console 0
Router(config-line)# password [PASSWORD]
Router(config-line)# login

Step 6 - The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. 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 7 - In service software upgrade is not allowed. The operator should not perform in service software upgrade of a validated firmware image

Step 8 - Use of the debug.conf file is not allowed while in FIPS mode of operation.

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. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

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).

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 SSLv3.1/TLS Requirements and Cryptographic Algorithms

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

- MD5
- RC4
- DES

When the Crypto Office sets fips enable during the initial set-up. Diffie-Hellman negotiations will not accept any key sizes less than 2048. Negotiations with key sizes offered with less than 2048 will not be complete.

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

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

9.5 Cisco Unified Border Element (CUBE) TLS Configuration

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

sip-ua
crypto signaling [strict-cipher]

9.6 Remote Access

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