Cisco Integrated Services Router (ISR) 4451-X (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Integrated Services Router (ISR) 4431 (with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256)

FIPS 140-2 Non Proprietary Security Policy

Level 1 Validation

Version 0.4

Date: June 10, 2015

.

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Integrated Services Router (ISR) 4451-X (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Integrated Services Router (ISR) 4431(with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256), 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

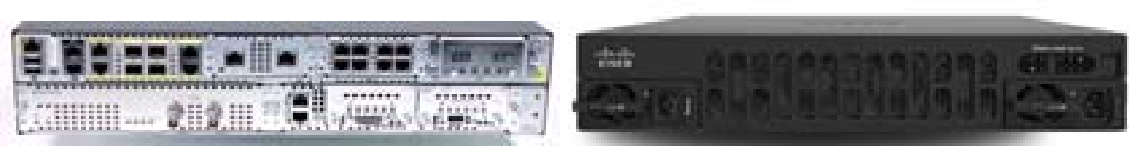
With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See “Obtaining Technical Assistance”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

2 Module Description

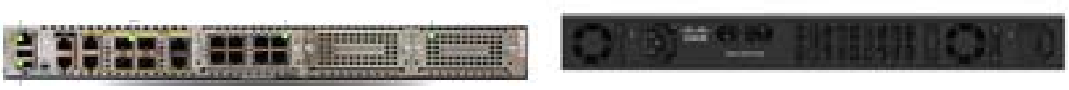
2.1 Cisco ISR4451-X and ISR4431

The Cisco Integrated Services Router (ISR) 4451-X (with SM-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P, PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) and Integrated Services Router (ISR) 4431(with PVDM4-32, PVDM4-64, PVDM4-128 and PVDM4-256) are 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 and 4431Routers are 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.



ISR 4451-X



ISR 4431

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
MACSec (M-ES3X-16-P, SM-ES3X-24-P, SM-D-ES3X-48-P only)	Used for data plane traffic. This service is not allowed in FIPS mode of operation.

Table 1: Supported Services

2.2 Embedded Services Processor (ESP)

The Cisco 4451-X and 4431 Embedded Service Processor (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 4451-X and 4431 Router.

The Cisco 4451-X and 4431 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 Cisco 4451-X and 4431use an integrated ESP and as such does not have a distinct part number.

2.3 Router Processor (RP)

The Cisco 4451-X and 4431 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 Cisco 4451-X and 4431 Router.

It should be noted that the Cisco 4451-X and 4431 employ 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 4431 and 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.

2.5 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/ISR/ESG 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.

Product Model	Firmware Image Name	Hardware Configuration(s)
ISR 4451-X	IOS-XE 3.13	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 4431	IOS-XE 3.13	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 Hardware Configurations

2.6 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 Physical Security Description with Cryptographic Boundary

The Cisco 4451-X and 4431 are dual rack unit (2RU) and single rack unit (1RU) respectfully, housed in a metal case. The Cisco 4451-X and 4431 are classed as a multiple-chip standalone cryptographic module made with production grade components and standard passivation. There cryptographic boundary is defined as the entire unit encompassing the "top," "front," "left," "right," and "bottom" surfaces of the metal case.

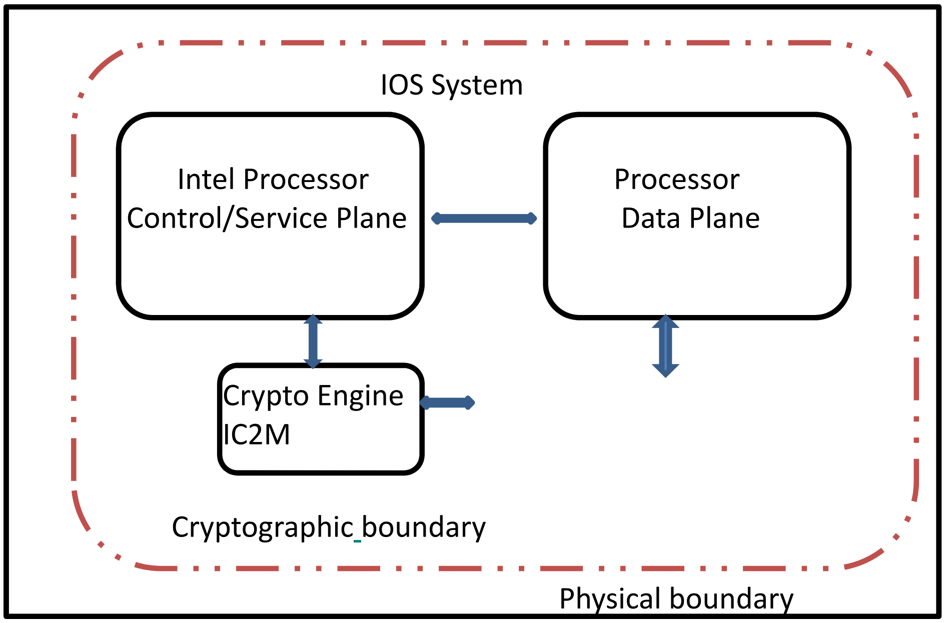


Diagram 1- Block Diagram

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
Service Module 1G Ethernet Ports (on ISR4451-X only) 10/100/1000 Mbps Ethernet Ports Console Port Auxiliary Port Management Port USB Ports	Data Input Interface
Service Module 1G Ethernet Ports (on ISR4451-X only) 10/100/1000 Mbps Ethernet Ports Console Port Auxiliary Port	Data Output Interface

Physical Interfaces	FIPS 140-2 Logical Interfaces
Management Port USB Ports	
Service Module 1G Ethernet Ports (on ISR4451-X only) 10/100/1000 Mbps Ethernet Ports Console Port Auxiliary Port Management Port Power Switch	Control Input Interface
Service Module 1G Ethernet Ports (on ISR4451-X only) 10/100/1000 Mbps Ethernet Ports LEDs USB Ports Console Port Auxiliary Port Management Port	Status Output Interface
Power Plug (up to 2)	Power interface

Table 4: Cisco 4431 and 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 5: User Services

5.2 Crypto Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the 10/100 management Ethernet port. The Crypto Officer authenticates 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 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.

	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 characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	password
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

5.3 Non-FIPS mode Services

The following non-FIPS mode services are available to the User and the Crypto Officer. However neither the User nor the Crypto Officer are allowed to operate these services while in FIPS mode of operation because use of the following non-FIPS mode services are prohibited in a FIPS-approved mode of operation.

- MACSec
- IPSec/IKE with Diffie-Hellman 768-bit/1024-bit modulus, DES, HMAC-MD5 and MD5
- SSHv1 using RC4

5.4 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.

6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer 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	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
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

Name	CSP Type	Size	Description	Storage	Zeroization
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
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	192 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

Name	CSP Type	Size	Description	Storage	Zeroization
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
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	192 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

Name	CSP Type	Size	Description	Storage	Zeroization
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
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	192 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	192 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	192 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

Name	CSP Type	Size	Description	Storage	Zeroization
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
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 7: CSPs Table

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco 4451-X and 4431 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 ISR 4451-X and 4431 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,	1764

Algorithm	Cert. #
384, and 512)	
CVL	253
RSA	1471
SHS (SHA-1, 256, 384, and 512)	2361
Triple-DES	1688/1670
OCTEON II CN6600 Series Die (CN6635 and CN6645)	
AES	2345
HMAC (SHA-1, 224, 256, 384, 512)	1454
SHS (SHA-1, 224, 256, 384, 512)	2022
Triple-DES	1468
Marvell 88E1340	
AES	1024 and 1275

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

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

The Cisco 4431 and 4451-X cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

- RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

- GDOI (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

- NDRNG

7.3 Non-Approved Algorithms

The Cisco 4431 and 4451-X 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:

7.4.1 Power-On Self-Tests (POSTs)

- IC2M (IOS Common Crypto Module) Algorithm Implementation
    - 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) KATs
    - Triple-DES (encrypt and decrypt) KATs

- IOS Common Crypto Module-Extended2 Algorithm Implementation
    - Triple-DES (encrypt and decrypt) KATs
- OCTEON II CN6600 Series Die (CN6635 and CN6645) Algorithm Implementation
    - AES (encrypt and decrypt) KATs
    - HMAC (SHA-1/SHA-256/SHA-384/SHA-512) KATs
    - Triple-DES (encrypt and decrypt) KATs
- Marvell 88E1340 Algorithm Implementation
    - AES-GCM 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 conditional self-tests.

7.4.2 Conditional Self-Tests

- Continuous Random Number Generator test for the FIPS-approved RNG (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
- Conditional IPSec Bypass Test

8 Secure Operation

8.1 System Initialization and Configuration

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

Step 7 - In service software upgrade (ISSU) is not allowed. The operator should not perform in service software upgrade of a FIPS validated firmware image

Step 8 - 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. 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.

8.2 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

8.3 Protocols

SNMP v3 over a secure IPsec tunnel may be employed for authenticated, secure SNMP gets and sets.

8.4 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]
```

8.5 Remote Access

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

9 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.