Cisco IOS 15.5M Router Security Policy

Cisco Integrated Services Router (ISR) 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR, 5915 ESR and 5940 ESR
Firmware Version: IOS 15.5M

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 1.0

June 2016

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for Cisco IOS 15.5M Router running on Cisco 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR and 5900 ESR
Router (Firmware Version: IOS 15.5M). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

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

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	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 module validation level	**1**

Table 1: Module Validation Level

1.3 References

This document deals only with the capabilities and operations of the Cisco 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR and 5900 ESR routers in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

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

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

1.4 Terminology

In this document, these Cisco Integrated Services Router models identified above are referred to as Routers or the systems.

1.5 Document Organization

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

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

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

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

2 Cisco Routers and Module Description

Cisco 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR and 5900 ESR are multifunctional networking devices delivering fast, reliable, data transfers with a high standard in security. These routers offer full network security, and other capabilities to fill networking needs for a small to medium size network. The Cisco IOS 15.5M Routers provides a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 1 requirements.

Some of the ISRs incorporate the High-Density Packet Voice Digital signal processor (DSP) providing high-density voice connectivity, conferencing and transcoding capabilities.   Two types are part of this validation, the PVDM2 and PVDM3, (Packet Voice Video Digital Signal Processor Module) which are plugged into the router to provide some variant of the conferencing video services associated with the specific type.   The high-density packet voice PVDM2 DSP's are available in five versions: PVDM2-8, PVDM2-16, PVDM2-32, PVDM2-48, and PVDM2-64. The -8, -16, -32, -48 and -64 indicate the maximum number of packet fax and voice channels. While the high-density packet voice PVDM3 DSP modules are available in six versions: PVDM3-16, PVDM3-32, PVDM3-64, PVDM3-128, PVDM3-192, and PVDM3-256 supporting switched-only video with the -128 and higher also supporting video conferencing with transcoding and translating. The -16, -32, -64, -128, -192 and -256 indicate the number of participants.

The Cisco 5900 ESR all optimized for mobile and embedded networks that require IP routing and services. The flexible, compact form factor of the Cisco 5900 routers, complemented by Cisco IOS Software and Cisco Mobile Ready Net capabilities, provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links.

The following configurations listed in Actual Hardware were tested:

<table>
<tr><th>Hardware Model</th><th>Actual Hardware Model Tested</th><th>PVDM</th><th>ISM</th><th>Protocols</th></tr>
<tr><td>1905 ISR</td><td>1905</td><td>N/A</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>1921 ISR</td><td>1921</td><td>N/A</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>1941 ISR</td><td>1941</td><td>N/A</td><td>ISM-VPN-19</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>2901 ISR</td><td>2901</td><td rowspan="8">(Any one of the following:)
PVDM2-8
PVDM2-16
PVDM2-32
PVDM2-48
PVDM2-64
PVDM3-16
PVDM3-32
PVDM3-64
PVDM3-128
PVDM3-192
PVDM3-256</td><td>ISM-VPN-29</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>2911 ISR</td><td>2911</td><td>ISM-VPN-29</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>2921 ISR</td><td>2921</td><td>ISM-VPN-29</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>2951 ISR</td><td>2951</td><td>ISM-VPN-29</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>3925 ISR</td><td>3925</td><td>ISM-VPN-39</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>3945 ISR</td><td>3945</td><td>ISM-VPN-39</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>3925E ISR</td><td>3925E</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>3945E ISR</td><td>3945E</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td rowspan="2">5900 ESR</td><td>Cisco 5915 ESR</td><td>N/A</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
<tr><td>Cisco 5940 ESR</td><td>N/A</td><td>N/A</td><td>SSH, TLS (VPN,Mgt), IPSec, SNMPv3 and CUBE/sRTP</td></tr>
</table>

Table 2 Module Hardware Configurations

The following pictures are representative each of the modules hardware model:

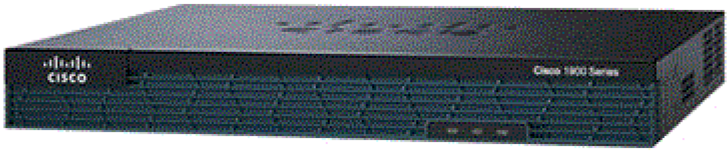

Figure 1 - Cisco 1905 ISR

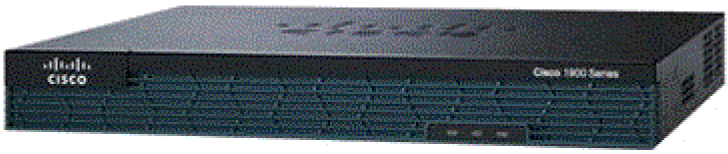

Figure 2 - Cisco 1921 ISR

Figure 3 - Cisco 1941 ISR

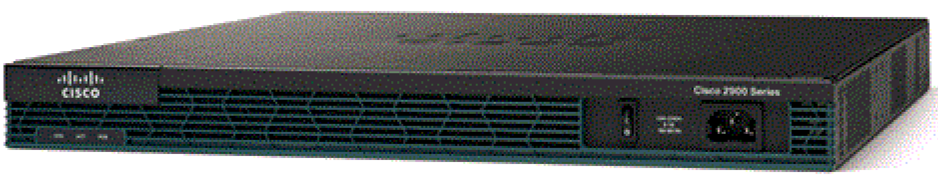

Figure 4 - Cisco 2901 ISR

Figure 5 - Cisco 2911 ISR


Figure 6 - Cisco 2921 ISR


Figure 7 - Cisco 2951 ISR


Figure 8 - Cisco 3925/3925E ISR


Figure 9 - Cisco 3945/3945E ISR

Figure 20 – Cisco 5915/5940 ESR

2.1 Module Interfaces

Each of ISRs is a multiple-chip standalone cryptographic module. The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provided no power to external devices and takes in its power through normal power input/cord. The following table lists all possible logical interface configurations and their associated mapping for all of the various ISR systems detailed in this Security Policy.

	1905, 1921, 1941	**2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E**		**5915, 5940**
Data Input Interface	EHWIC, Gigabit Ethernet (GE) ports, Console Port, USB Console Port, Auxilary Port	EHWIC Slots SM Slot GigE Ports Console Port USB Console Port Auxiliary Port		GigE Ports Console Port
Data Output Interface	EHWIC, Gigabit Ethernet (GE) ports, Console Port, USB Console Port, Auxilary Port	EHWIC Slots SM Slot GigE Ports Console Port USB Console Port Auxiliary Port		GigE Ports Console Port
Control Input Interface	EHWIC, Gigabit Ethernet (GE) ports, Console Port, USB Console Port, Auxilary Port	EHWIC Slots SM Slot GigE Ports Console Port USB Console Port Auxiliary Port		GigE Ports Console Port
Status Output Interface	Activity LED System LED Power LED Console Port, Auxilary Port, USB Console Port, Gigabit Ethernet (GE) ports	Activity LED System LED GigE Link LED (1 per GigE port) GigE Speed LED (1 per GigE port) Compact Flash LED (2) RPS Boost LED Power LED (2) GigE ports (2) Console Port Auxiliary Port USB Console Port		Activity LED System LED GigE Link LED GigE Speed LED GigE Ports Console Port
Power interface	110v ~240v AC power supply, POE power port	Power Plug PoE Port	Power Plug	Power Plug

Table 3 Interfaces

2.2 Cryptographic Boundary

The cryptographic boundary of the module is the physical enclosure of the system on which the module is executed. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

2.3 Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. The module also supports RADIUS or TACACS+ for authentication. There are two roles in the router that operators can assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role and associated services in order to configure the router, while the Users exercise only the basic User services. A complete description of all the management and configuration capabilities of the router can be found in the Performing Basic System Management manual or Configuration Guide Manual and in the online help for the routers.

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 2048-3072 bits, thus providing 112 to 128 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 5.19×10^{28} attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.3.1 User Services

Users enter the system by accessing the console port through a terminal program or via IPsec protected telnet or SSH v2 session to a LAN port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program. 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	View state of interfaces and protocols, version of IOS currently running.	User password (r)
Network Functions	Connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).	User password (r)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	User password (r)
Directory Services	Display directory of files kept in flash memory.	User password (r)
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
SSL VPN (TLSv1.0)	Negotiation and encrypted data transport via SSL VPN (TLSv1.0)	Operator password (r, w, d) and [TLS pre-master secret, TLS Traffic Keys] (d)
IPsec VPN	Negotiation and encrypted data transport via IPSec VPN	Operator password (r, w, d) and [skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key] (d)

Services and Access	Description	Keys and CSPs
SSH Functions	Negotiation and encrypted data transport via SSH	Operator password (r. w. d), SSH Traffic Keys (d)
HTTPS Functions (TLS)	Negotiation and encrypted data transport via HTTPS	Operator password (r, w, d) and [TLS pre-master secret, TLS Traffic Keys] (d)
SNMPv3 Functions	Negotiation and encrypted data transport via SNMPv3	SNMP v3 password, SNMP session key (r,w,d)
CUBE/sRTP Functions	Negotiation and encrypted data transport via CUBE/sRTP	sRTP Traffic Keys (r,w,d)

Table 4: User Services

2.3.2 Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers. The Crypto Officer role is responsible for the configuration 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	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 preshared, Operator password, Enable password] - (r, w, d), [IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key] – (w, d)
Define Rules and Filters	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	Operator password, Enable password - (r, w, d)
View Status Functions	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Enable password - (r, w, d)
Manage the router	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, view complete configurations, manager user rights, firmware upgrade, and restore router configurations.	Operator password, Enable password - (r, w, d)
SNMPv3	Non security-related monitoring by the CO using SNMPv3.	SnmpEngineID, SNMP v3 password - (r, w, d), SNMP session key (w, d)
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	[ISAKMP preshared, Operator password, Enable password] - (r, w, d); [IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key] – (w, d)
SSL VPN (TLSv1.0)	Configure SSL VPN parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys – (r, w, d)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	SSHv2 Private Key, SSHv2 Public Key and SSHv2 session key (r, w, d)
IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_d, IKE session encryption ISAKMP preshared (r, w, d), [skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key] – (w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
Zeroization	Zeroize cryptographic keys	All CSPs (d)
sRTP/CUBE	Configure sRTP parameter, provide entry and output of CSPs.	sRTP Traffic Keys (r,w,d)

Table 5: Crypto Officer Services (r = read w = write d = delete)

2.4 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch
- Sending packets in bypass

2.5 Cryptographic Key/CSP Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are protected by the Crypto Officer role login password-protection, and these keys can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key.

The router is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved).

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel via the Internet Key Exchange (IKE). RSA Public keys are entered into the modules using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

The module supports the following keys and critical security parameters (CSPs).

Name	CSP Type	Size	Description	Storage	Zeroization
DRBG entropy input	SP800-90A DRBG_CTR (using AES-256)	256-bits	This is the entropy for SP 800-90A CTR_DRBG. HW based entropy source used to construct seed.	SDRAM (plaintext)	Power cycle the device
DRBG Seed	SP800-90A 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.	SDRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A 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.	SDRAM (plaintext)	Power cycle the device
DRBG Key	SP800-90A DRBG_CTR	256-bits	Internal Key value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	SDRAM (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.	SDRAM (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 SP800-90A DRBG.	SDRAM (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.	SDRAM (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 SP800-90A DRBG.	SDRAM (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.	SDRAM (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.	SDRAM (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.	SDRAM (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.	SDRAM (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.	SDRAM (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).	SDRAM (plaintext)	Power cycle the device
IKE session authentication key	HMAC-SHA1/256/384/512	160-512 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	SDRAM (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 SP800-90A 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	SDRAM (plaintext)	By running '#crypto key zeroize' command
IPsec encryption 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).	SDRAM (plaintext)	Power cycle the device
IPsec authentication key	HMAC-SHA1/256/384/512	160-512 bits	The IPsec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2).	SDRAM (plaintext)	Power cycle the device
sRTP master key	AES	128/192/256 bits	Key used to generate sRTP session keys	SDRAM (plaintext)	upon end of call or device reset.

Name	CSP Type	Size	Description	Storage	Zeroization
sRTP encryption key	AES	128/192/256 bits	Generated via the sRTP protocol. Key used to encrypt/decrypt sRTP packets	SDRAM (plaintext)	upon end of call or device reset.
sRTP authentication key	HMAC-SHA-1	160-bits	Generated via the sRTP protocol. Key used to authenticate sRTP packets	SDRAM (plaintext)	upon end of call or device reset.
Operator password	Password	8 - 25 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 - 25 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	8 - 25 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	8 - 25 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 SP800-90A 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).	SDRAM (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).	SDRAM (plaintext)	Power cycle the device
TLS server private key	RSA	2048-3072 modulus	Private key used for SSLv3.1/TLS.	NVRAM (plaintext)	"# crypto key zeroize rsa"
TLS server public key	RSA	2048-3072 modulus	Private key used for SSLv3.1/TLS.	NVRAM (plaintext)	"# crypto key zeroize rsa"
TLS pre-master secret	Shared Secret	At least eight characters	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM (plaintext)	Automatically when TLS session is terminated
TLS session encryption key	Triple-DES/AES 128/192/256	192-bits Triple-DES or/ 128/192/256-bits AES	Key used to encrypt TLS session data	SDRAM (plaintext)	Automatically when TLS session is terminated

Name	CSP Type	Size	Description	Storage	Zeroization
TLS session integrity key	HMAC-SHA1/256/384/512	160-512 bits	Used for TLS data integrity protection	SDRAM (plaintext)	Automatically when TLS session is terminated

Table 6: Keys/CSPs Table

2.6 Cryptographic Algorithms

The router is in the approved mode of operation only when FIPS 140-2 approved/allowed algorithms are used. The module implements a variety of approved and non-approved algorithms.

2.6.1 Approved Cryptographic Algorithms

The routers support the following FIPS 140-2 approved algorithm implementations:

	IOS	Router HW Accelerator
AES	#2817 (128,192,256) (ECB, CBC, CFB,CTR,CMAC, GCM)	#2343 (128,192,256)(ECB, CBC, GCM)
Triple-DES	#1688 (192) (CBC)	#1466 (192) (ECB, CBC)
SHS	#2361 (SHA1,256,384,512)	#2020 (SHA1,256,384,512)
HMAC	#1764 (HMAC SHA1,256,384,512)	#1452 (HMAC SHA1,256,384,512)
RSA	#1471 (Gen, PKCS1_V1_5, Sig-GEN, SIG-VER) (2048, 3072) Note 1: The module supports 1024-bit RSA Signature Generation. This may not be used in FIPS mode Note 2: The module supports RSA Signature Generation with SHA-1. This may only be used in protocols as defined in SP 800-52 and SP 800-57.	N/A
ECDSA	#493 (P-256, P-384)	N/A
CVL	#252 and 253 (IKE, TLS, IPsec, SSH, SNMP, SRTP, ECDH, DH)	N/A
DRBG	#481 (CTR-AES-256)	N/A

Table 7: Algorithm Certificates

Note:

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec. The module uses a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.
- The TLS, IKEv1/IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.

2.6.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

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

2.6.3 Non-FIPS Approved Algorithms

Integrated Services Routers (ISRs) cryptographic module implements the following non-Approved algorithms:

Service	Non-Approved Algorithm
SSH*	Hashing: MD5, MACing: HMAC MD5, Symmetric: DES, Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
TLS*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
IPsec*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
SNMP*	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman

Table 8 Non-Approved Services

Note: Services marked with a single asterisk (*) have the listed non-approved cryptographic algorithms available to be used. Use of these algorithms are prohibited in a FIPS-approved mode of operation. The services may be used with FIPS-approved algorithms.

2.7 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

2.7.1 Power-On Self-Tests (POSTs)

- IOS Algorithm Self-Tests
    - AES (encrypt/decrypt) Known Answer Tests
    - AES GCM Known Answer Test
    - DRBG Known Answer Test
    - ECDSA Sign/Verify
    - HMAC-SHA-1 Known Answer Test
    - HMAC-SHA-256 Known Answer Test
    - HMAC-SHA-384 Known Answer Test
    - HMAC-SHA-512 Known Answer Test
    - RSA Known Answer Test
    - SHA-1 Known Answer Test
    - SHA-256 Known Answer Test
    - SHA–384 Known Answer Test
    - SHA-512 Known Answer Test
    - Triple-DES (encrypt/decrypt) Known Answer Test
    - ECC Primitive “Z” KAT
    - FFC Primitive “Z” KAT

- Hardware Accelerator Self-Tests

- AES (encrypt/decrypt) Known Answer Tests
- Triple-DES (encrypt/decrypt) Known Answer Tests
- HMAC (SHA-1) Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA–384 Known Answer Test
- SHA-512 Known Answer Test

- Firmware Integrity Test
  - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-512

2.7.2 Conditional tests

- Conditional Bypass test
- Continuous random number generation test for SP800-90A DRBG
- Continuous Random Number Generator test for NDRNG
- Pairwise consistency test for ECDSA
- Pairwise consistency test for RSA
- Firmware load test

3 Secure Operation

The Cisco 1905 ISR, 1921 ISR, 1941 ISR, 2901 ISR, 2911 ISR, 2921 ISR, 2951 ISR, 3925 ISR, 3925E ISR, 3945 ISR, 3945E ISR and 5900 ESR routers meet all the Level 1 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Initial Setup

The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal
no service password-recovery
end
show version
```

NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.2 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 15.5M (cXXXX-universalk9-mz.SPA.155-3.Mbin or cXXXX-adventerprisek9-mz.SPA.155-3.M.bin), Advanced Security build (advsecurity) is the only allowable image; no other image should be loaded. Once this image has been installed, no updates to software or firmware are permitted in FIPS mode of operations.
2. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0102
   ```

3. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except '?' are accepted) and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

   ```
   enable secret [PASSWORD]
   ```

4. The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

   ```
   line con 0
   password [PASSWORD]
   login local
   ```

5. If using a Radius/TACACS+ server for authentication, it is recommended that an IPsec tunnel or some other secure tunnel between the Router and the RADIUS/TACACS+ be set up.

   The pre-shared key must be at least 8 characters long.

3.3 IPSec Requirements and Cryptographic Algorithms

1. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

   - ah-sha-hmac

- esp-sha-hmac
- esp-Triple-DES
- esp-aes

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

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

3.4 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

3.5 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.

3.6 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]
```