Cisco Cloud Services Router 1000 Virtual

FIPS 140-2 Non Proprietary Security Policy

Level 1 Validation

Version 0.5

October 17, 2016

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Cloud Services Router 1000 Virtual (CSR1000v) running Cisco IOS XE 3.16. This security policy describes how the module meets the security requirements of FIPS 140-2 Level 1 and how to run the module 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	2
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 CSR1000v Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Cloud Services Router 1000 Virtual cryptographic module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2IG and additional rules imposed by Cisco Systems, Inc. More information is available from the following Cisco Systems website:

http://www.cisco.com/c/en/us/products/index.html

http://www.cisco.com/en/US/products/ps6120/index.html

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, the Cisco Cloud Services Router 1000 Virtual module identified is referred to as CSR1000v, CSR virtual, CSRv, virtual, module or the system.

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 Cisco Cloud Services Router 1000 Virtual identified in section 1.2 above and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. 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 Cloud Services Router 1000 Virtual

The Cisco® Cloud Services Router 1000V (CSR1000v) is a virtual form-factor router that delivers comprehensive WAN gateway and network services functions into virtual and cloud environments. Using familiar, industry-leading Cisco IOS® XE Software networking capabilities, the CSR1000v enables enterprises to transparently extend their WANs into provider-hosted clouds. Built on the same proven Cisco IOS XE Software platform that powers the Cisco Integrated Services Router (ISR) and Aggregation Services Router (ASR) product families, it offers a rich set of features, including routing, VPN, firewall, Network Address Translation (NAT), QoS, application visibility, failover, and WAN optimization. Additional NFV uses such as virtual route reflector (vRR), virtual broadband network gateway (vBNG), and virtual intelligent services gateway (vISG) are also supported by the CSR1000V platform.

The Cisco CSR1000v is a software router that an enterprise or a cloud provider can deploy as a virtual machine in a provider-hosted cloud or in its own virtual environment. It can run on Cisco Unified Computing System™ (Cisco UCS®) servers as well as servers from leading vendors that support VMware ESXi, Microsoft Hyper-V, Red Hat KVM virtualization, or on the Amazon EC2 cloud. It contains Cisco IOS XE Software networking and security features.

The CSR1000v offers IKE/IPsec, RADIUS/TACACS+, SNMPv3, SSHv2, TLS and GetVPN services along with the Cisco IOS Zone-Based Firewall and access control, meaning an enterprise can connect distributed sites directly to its cloud deployment.

2.1 Cisco Servers

Cisco® Cloud Services Router 1000V runs on many different UCS servers with the VMware vSphere ESXi hypervisor version 5.1 (vendor affirmed) and version 5.5, providing pass through data between the host platform and the module.

For the purposes of this validation, the module was tested in the lab on the following servers:

Platform	Hypervisor	Processor
Cisco EN120E 208	VMware ESXi 5.5	**Intel Xeon**
Cisco EN120S M2	VMware ESXi 5.5	**Intel Xeon**

Table 2 Testing Configuration

The following Cisco UCS servers are Vendor affirmed:

B22 M3
B200 M3
B200 M4
B230 M2
B420 M3
B440 M2
B260 M4

C22 M3
C24 M3
C220 M4
C240 M3
C240 M4
C260 M2
C420 M3

E140S M1
E140S M2
E140D M1
E160D M2
E160D M1
E140DP M1
E160DP M1

B460 M4	C460 M2	EN120E
	C460 M4	EN120SM2

FIPS 140-2 validation compliance is maintained when the module is operated on the other listed environments running in single user mode and no modification to the listed code in this Security Policy has been performed.

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment, which might not be listed on the validation certificate.

2.2 Cryptographic Boundary

The cryptographic module is defined as a multi-chip standalone software module, CSR1000 virtual module (yellow box), while the physical boundary is defined as the hard case enclosure around the Server on which everything runs (blue box). Then the logical boundary is the CSR1000 virtual module, hypervisor, API and processor (red dash box).

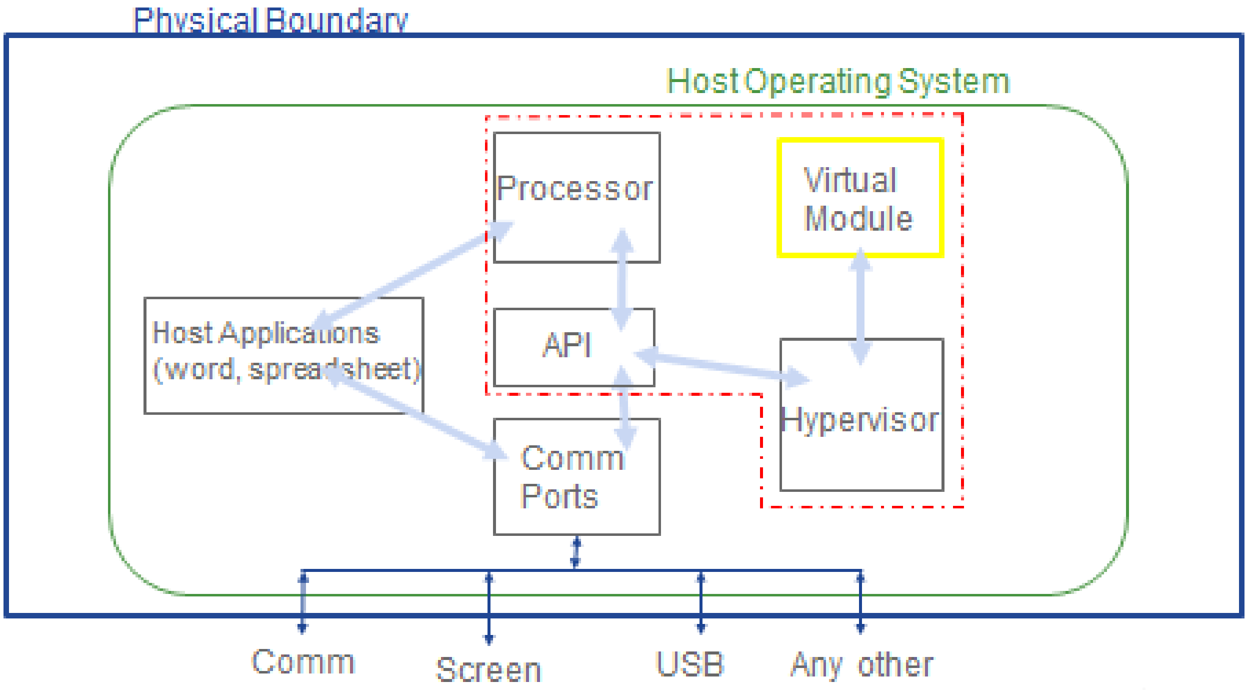

Figure 1 – Block diagram

The module makes use of the physical interfaces of the tested platform(s) hosting the virtual environment upon which the module is installed. The hypervisor, controls and directs all interactions between the CSR1000v and the operator, and is responsible for mapping the module’s virtual interfaces to the GPC’s physical interfaces.

2.3 Module Interfaces

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 logical interfaces and their mapping are described in the following table:

Physical Port/Interface	CSR1000v	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports, Virtual Serial Ports	**Data Input Interface**
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports, Virtual Serial Ports	**Data Output Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Control Input Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Status Output Interface**

Table 3 Module Interfaces

2.4 Roles and Services

The security appliance can be accessed in one of the following ways:

- Console Port
- IPsec
- SSH v2
- HTTPS/TLS

Authentication is role-based. As required by FIPS 140-2, there are two roles that operators may assume: a Crypto Officer role and User role. The module upon initial access to the module authenticates both of these roles. The virtual module also supports RADIUS and TACACS+ as another means of authentication, allowing the storage of usernames and passwords on an external server as opposed to using the module's internal database for storage.

The User and Crypto Officer passwords and the RADIUS/TACACS+ shared secrets must each be at a minimum eight (8) characters long. There must be at least one special character and at least one number character (enforced procedurally) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

Additionally, when using RSA based authentication, an RSA key of 2048 bits is used, thus providing 112 bits of strength. so the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 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 8.65×10^{31} attempts per second, which far exceeds the operational capabilities of the module to support.

When using ECDSA-based authentication, ECDSA has a size of P-256 and P-384, thus providing between 128 and 192 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{128} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. An attacker would not be able to exceed the one in 100,000 probably of successful random key guess in one minute, as it far exceeds the operational capabilities of the module to support.

User Services

A User enters the system by accessing the console port with a terminal program or via IPsec protected telnet or SSH session to a virtual Ethernet port or HTTPS/TLS. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an IPsec session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism. 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	Description	Keys and CSPs Access
Status Functions	View state of interfaces and protocols, version of IOS currently running.	Operator password (r)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r)
Directory Services	Display directory of files kept in flash memory.	Operator password (r)
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
IPsec VPN	Negotiation and encrypted data transport via IPSec VPN	Operator password (r) 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), DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SSH v2 Functions	Negotiation and encrypted data transport via SSH	Operator password (r), Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, SSHv2 Private Key, SSHv2 Public Key, SSHv2 Session Key, SSHv2 Session authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key(r, w, d)
SNMPv3 Functions	Negotiation and encrypted data transport via SNMPv3	SNMPv3 Password, snmpEngineID, SNMP session key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key(r, w, d)

Services	Description	Keys and CSPs Access
GetVPN	Negotiation and encrypted data transport via GetVPN	Operator password (r) and IKE session encrypt key, IKE session authentication, GDOI TEK Integrity key, GDOI Data Security Key (TEK), GDOI Group Key Encryption Key (KEK) (r,w,d) DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
HTTPS Functions (TLS)	Negotiation and encrypted data transport via HTTPS	TLS Server RSA private key, TLS Server RSA public key, TLS pre-master secret, TLS traffic keys, TLS authentication keys, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w,d)

Table 4 - User Services

Crypto Officer Services

A Crypto Officer enters the system by accessing the console port with a terminal program or SSH v2 session to a LAN port or the 10/100/1000 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	Description	Keys and CSPs Access
Configure the Security Blade	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 module configuration, routing tables, active sessions, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Enable password - (r, w, d)
Manage the Security Blade	Log off users, shutdown or reload the module, erase the flash memory, manually back up module configurations, view	Operator password, Enable password - (r, w, d)

	complete configurations, manager user rights, and restore module configurations.	
Configure Remote Authentication	Set up authentication account for users and devices using RADIUS or TACACS+	RADIUS secret, TACACS+ secret (r, 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)
TLS VPN (TLSv1.0 and 1.1)	Configure SSL VPN parameters, provide entry and output of CSPs.	TLS Server RSA private key, TLS Server RSA public key, TLS pre-master secret, TLS session keys, TLS authentication keys, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key(r, w, d)
IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	Operator password (r) 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), DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	Operator password (r), Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman shared secret, SSHv2 Private Key, SSHv2 Public Key, SSHv2 Session Key, SSHv2 Session authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key(r, w, d)
GetVPN	Configure GetVPN parameter, provide entry and output of CSPs.	Operator password (r, w, d) and IKE session encrypt key, IKE session authentication, GDOI TEK Integrity key, GDOI Data Security Key (TEK), GDOI Group Key Encryption Key (KEK) (r,w,d) DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, 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)
SNMPv3	Configure SNMPv3 parameter, provide entry and output of CSPs.	SNMPv3 Password, snmpEngineID, SNMP session key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key(r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 7, Zeroization column.	All CSPs (d)

Table 5 - Crypto Officer Services

All FIPS mode services available can be found at http://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v/model.html. This site lists configuration guides for the CSR1000v systems.

2.5 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 2.5, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Services [1]	**Non-Approved Algorithms**
SSH	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
SNMP	Hashing: MD5, MACing: HMAC-MD5 Symmetric: DES, RC4
TLS	Hashing: MD5, MACing: HMAC-SHA-1, MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

Table 6 – Non-approved algorithms in the Non-FIPS mode services

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

All other non-FIPS mode services available can be found at http://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v/model.html. This site lists configuration guides for the CSR1000v systems.

2.6 Unauthenticated Services

There are no unauthenticated services associated with a virtual module.

2.7 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual

[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.

distribution are used for pre-shared keys whereas protocols such as IKE, TLS and SSH are used for electronic distribution.

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. Only an authenticated Crypto Officer can view the keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol. RSA Public keys are entered into the module 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 CSR1000v harvests entropy through clock drifts collected by the pseudo performance monitor counter provided by the ESXi hypervisor and pulls entropy in 8 bits at a time to create a 1024 bytes entropy pool. Additional information is available in Cisco CSR1000v Entropy Information document.

Name	CSP Type	Size	Description/Generation	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	DRAM (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.	DRAM (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.	DRAM (plaintext)	Power cycle the device
DRBG Key	SP800-90A DRBG_CTR			DRAM (plaintext)	Power cycle the device
Diffie-Hellman Shared Secret	DH	2048, 3072, 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, 256, 379 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048, 3072, 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/Generation	Storage	Zeroization
EC Diffie-Hellman private key	ECDH	Curves: P-256/P-384	256-bits	Internal Key value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	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
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 and 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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IKE authentication public key	RSA/ ECDSA	RSA (2048 and 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 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).	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	8 plus 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 plus 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 and 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 and 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
SSHv2 Session authentication key	HMAC SHA	160/256/384/512-bits.	authenticate all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is internally derived by the module.	DRAM (plaintext)	Automatically when SSH session is terminated.
GDOI Data Security Key (TEK)	Triple-DES/AES	192 bits Triple-DES or/ 128/192/256 bits AES	Generate by calling SP800-90A 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 SP800-90A DRBG in the module. It is used protect Get VPN (GDOI) rekeying data.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
GDOI TEK integrity key	HMAC SHA-1	160 bits	Generate by calling SP800-90A DRBG in the module. It is used to ensure data traffic integrity between Get VPN (GDOI) peers.	DRAM (plaintext)	Power cycle the device
TLS Server RSA private key	RSA	2048 bits	The TLS server private key used in TLS connection. This key is generated by calling SP 800-90A DRBG	NVRAM (plaintext)	By running '# crypto key zeroize rsa' command
TLS Server RSA public key	RSA	2048 bits	The TLS server public key used in TLS connection. This key is generated by calling SP 800-90A DRBG	NVRAM (plaintext)	By running '# crypto key zeroize rsa' command
TLS pre-master secret	Shared Secret	At least eight characters	Shared secret created/derived using asymmetric cryptography from which new HTTPS session keys can be created. This key entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS traffic keys	Triple-DES/AES 128/192/256 HMAC-SHA1/256/384/512	192 bits Triple-DES or 128/192/256 bits AES	Used in HTTPS connections. Generated using TLS protocol. This key was derived in the module.	DRAM (plain text)	Automatically when TLS session is terminated
TLS authentication keys	HMAC SHA	160/256/384/512-bit.	This is the TLS authentication key. It is used to authenticate all TLS data traffics traversing between the TLS client and server. This key is internally generated by the module.	DRAM (plain text)	Automatically when session terminated
SNMPv3 password	Shared Secret	256 bits	The password use to setup SNMPv3 connection. This key is entered by Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
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 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

Table 7 Cryptographic Keys and CSPs

2.8 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm certificates implemented by Cisco Cloud Services Router 1000 Virtual:

CAVP Cert	Algorithm	Standard	Mode/Method
3989	AES 128, 192, 256	FIPS 197, SP80038A	ECB, CBC CFB128 CTR, CMAC(128 only), GCM
2189	Triple-DES 192	SP 800-67	CBC
3293	SHS 1/256/384/512	FIPS 180-4	SHA-1 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512
2604	HMAC SHA1/256/384/512	FIPS 198-1	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512

2047	RSA
	186-4KEY(gen): FIPS186-4_Fixed_e (10001) ;
	PGM(ProvPrimeCondition) (2048 SHA(256)) (3072 SHA(256))
	ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(1 , 256 , 384 , 512))
	SIG(gen) with SHA-1 affirmed for use with protocols only.
	SIG(Ver) (1024 SHA(1 , 256 , 384 , 512)) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(1 , 256 , 384 , 512))
		FIPS 186-4	186-4KEY(gen)
			PKCS1_V1_5
			SIG(gen)
			SIG(Ver)

885	ECDSA	FIPS 186-4	PKG Curves (P-256,P-384), PKV Curves (P-256,P-384), SigGen, SigVer (P-256. P-384)
1181	DRBG	SP 800-90A	CTR_Based w/AES 256
94	KBKDF	SP800-108	CTR_Mode
830	CVL	SP800-135	IKEv1,IKEv2, TLS, SSH, SNMP

Table 8 Approved Cryptographic Algorithms

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec and RFC 5288 for TLS. 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 SNMPv3, SSH, TLS and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode

Algorithms	Caveat	Use
Diffie-Hellman	Provides between 112 and 150 bits of encryption strength	Key Establishment
EC Diffie-Hellman	Provides 128 or 192 bits of encryption strength	Key Establishment
RSA	provides between 112 and 150 bits of encryption strength	Key Establishment
HMAC MD5		TLS1.0/1.1
MD5		TLS1.0/1.1
NDRNG		Entropy source

Table 9 Non-FIPS Approved Cryptographic Algorithms Allowed in FIPS Mode

Non-Approved Cryptographic Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation.

Algorithm	Use
Diffie-Hellman	key establishment methodology; non-compliant less than 112-bits of encryption strength
RSA	key establishment; non-compliant less than 112-bits of encryption strength
DES	Encryption/Decryption
HMAC-MD5	Keyed Hash
MD5	Hash
RC4	Encryption/Decryption
HMAC-SHA1	Keyed Hash, less then 112-bits key size

Table 10 Non-Approved Cryptographic Algorithms

2.9 Self-Tests

The module includes 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.

Self-tests performed

- POSTs - IOS Common Crypto Module
  - Software 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

- Conditional Tests - (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

- Critical Function Tests
  - NIST 800-90A DRBG Instantiate Health Check;
  - NIST 800-90A DRBG Generate Health Check;
  - NIST 800-90A DRBG Reseed Check; and
  - NIST 800-90A DRBG Uninstantiate Check.

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

- Continuous Random Number Generator Test (CRNGT) for SP800-90A DRBG
- CRNGT for the NDRNG
- Pairwise Consistency Test for RSA
- Conditional IPSec Bypass Test

The module performs all power-on self-tests automatically at boot when the power is applied. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the security appliance from passing any data during a power-on self-test failure. In the unlikely event that a power-on or conditional self-test fails, an error message is displayed on the console followed by a security appliance reboot.

3 Secure Operation

System setup is detailed in “Cisco CSR1000V Series Cloud Services Router Software Configuration Guide”. The Cisco CSR1000V was validated with software version 3.16 (File name: csr1000v-universalk9.03.16.03.S.155-3.S3-ext.ova). This is the only allowable image for FIPS-approved mode of operation.

CSR1000V configuration Guide
http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg.pdf

Installing the Cisco CSR 1000v in VMware ESXi
http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg/installesxi.html

Listing of commands can be found in the Master Command List:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

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:

```
Router# dir bootflash:
Router# configure terminal
Router(config)# no boot system
Router(config)# boot system  bootflash:system-image-filename .bin
Router(config)# boot system bootflash:csr1000v-universalk9.03.10.00.S.153-
3.S-ext.SPA.bin
Router(config)# exit
Router#write memory
Router# show version
Router# configure terminal
Router(config)# config-register 0x2102
Router(config)# exit
Router# copy running-config startup-config
Router# write memory
Router# reload
```

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:

```
Device> enable
```

```
Device# configure terminal
Device(config)# enable secret password
```

Step 3 - To establish a username-based authentication system, use the username command in global configuration mode. To remove an established username-based authentication, use the no form of this command. 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:

username *name* [**password** *secret*]

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.
Note: Since this only uses MD5 it is recommend that some secure tunnel be established like IPsec, SSH or TLS.

Step 6 - Dual IOS mode is not allowed. ROMMON variable IOSXE_DUAL_IOS must be set to 0.

Step 7 - 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.

Step 8 – Execute the “platform ipsec fips-mode” command.

```
   Router(config)# platform ipsec fips-mode
```

(enable FIPS mode will take effect after reboot)

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.

3.1 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

3.2 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.

3.3 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 when SNMP v3 is configured with AES encryption.

3.4 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]
```

3.5 SNMP Configure

1. enable (Device> enable)

2. configure terminal (Device# configure terminal)

3. snmp-server user username group-name [remote host [udp-port port]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [priv { aes {128 | 192 |256}} privpassword] [access [ipv6 nacl] {acl-number | acl-name}] (Device(config)# snmp-server user new-user new-group v3 auth SHA secureone priv aes 256 privatetwo access 2)

4. exit (Device(config)# exit)

3.6 Remote Access

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

3.7 Zeroization

In addition to zeroization commands and power cycling mentioned in Table 7 above all CSPs may also be zeroized by reinstalling the virtual module. The CO must wait until the virtual module has successfully installed and host platform rebooted to verify the zeroization has completed successfully.