Cisco NCS 5500 Series Routers

Firmware version:
IOS XR 6.3

Hardware versions (chassis):
NCS-5501, NCS-5502, NCS-55A1-36H-SE-S, and NCS-5508

Route Processor (RP) Hardware versions:
NC55-RP

Line Card Hardware versions:
NC55-36X100G-S

FIPS-140 Non-Proprietary Security Policy- Security Level 1

Version 1.0

Cisco Systems, Inc.

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco NCS 5500 Series Routers.

This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

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

1.1 References

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

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

1.2 FIPS 140-2 Submission Package

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

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

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

2 Module Description

2.1 NCS 5500 Series (5501, 55A1, 5502, 5508)

The Network Convergence System 5500 Series is a family of routing platforms including fixed and modular chassis. The platform offers high port density, high performance forwarding, low jitter and the lowest power consumption per Gigabits/sec at a very cost-effective price point.

NCS 5500 series offers industry-leading density of routed 1/10/40/100G ports for high-scale WAN aggregation. It is designed to efficiently scale across Data Centers, Large Enterprise, Web, Service Provider WAN and Aggregation Networks.

Figure 1: NCS-55A1-36H-SE-S

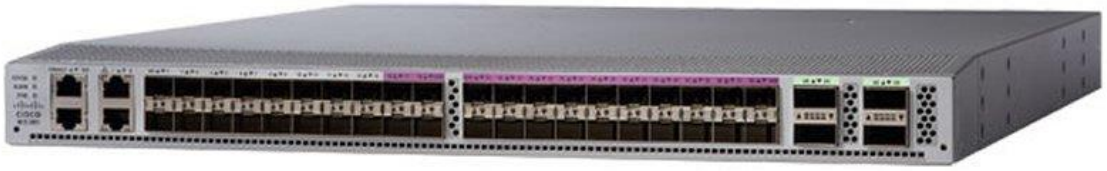

Figure 2: NCS-5501

Figure 3: NCS-5502

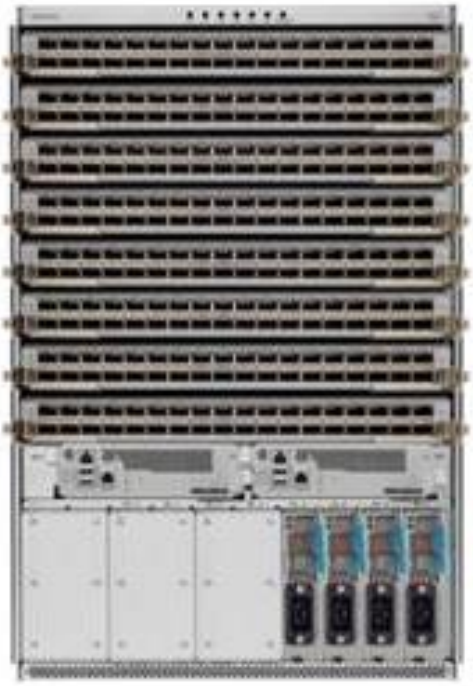

Figure 4: NCS-5508 (populated chassis)

2.2 Line Card and Route Processor for Modular Chassis

The Cisco NCS 5500 Series RPs and LCs included with this module are as follows:

- NC55-36X100GS (36X100GMACsec)

- NC55-RP (Route Processor)

The validated platforms consist of the following components:

Chassis	Hardware Configuration	
	Route Processor	Line Cards
NCS-55A1-36H-SE-S	Fixed Configuration	Fixed Configuration
NCS-5501		
NCS-5502		
NCS-5508	NC55-RP	NC55-36X100G-S

Table 1: Module Validation List

Vendor Affirmed Models	
Chassis	NCS-5504
	NCS-5516

Table 2: Vendor Affirmed Models

It should be noted that all vendor affirmed devices use the same firmware image (IOS XR 6.3) as the modules tested. No claim to conformance is made as these models were not tested by a CSTL or reviewed by the CMVP.

2.3 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

2.4 FIPS and non-FIPS modes of operation

The NCS5500 supports a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode but because the module allows for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. The following services are available in both a FIPS and a non-FIPS mode of operation:

- SSH
- SNMPv3
- MACsec

When the services are used in non-FIPS mode they are considered to be non-compliant.

To determine the mode of operation, the Cryptographic Officer should run the following command:

- Use the "`show logging | i fips`" command to filter FIPS specific logging messages.

If the device is in the non-FIPS mode of operation, the Cryptographic Officer must follow the instructions in section 9.1 of this security policy to transfer into a FIPS approved mode of operation.

In the FIPS mode of operation, there are actually two Approved modes of operation as follows:

- Standard Mode
- Recovery Mode

The FIPS Standard mode of operation is entered when the module is configured for FIPS mode and successfully passes all the power on self-tests (POST). The FIPS Standard Mode supports the approved and allowed algorithms, functions and protocols identified in Section 5 of this document.

The FIPS Recovery mode of operation is entered when the module is configured for FIPS mode passes all the power on self-tests (POST) with the exception being that the POSTs related to the MACsec functionality fail. If the module is configured with more than one MACsec line card, then failure of any POST on a line card will cause that line card to be disabled, thus there is the potential for at least some of the MACsec functionality to be available to the module. If module does not have the capability to have more than one MACsec line card, or only has one MACsec line card and a POST failure is detected (related to the MACsec functionality) then the module may still operate except now all MACsec hardware is disabled but the remained crypto functionality and services are still available to the module.

Anyone of these modules, which has MACsec capability, can take on the role of either the Peer or the Authenticator in reference to the MACsec protocol. The link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

When supporting the MACsec protocol in the FIPS approved modes of operation, the module should only be used together with other CMVP-validated modules providing either the remaining Peer or Authenticator functionality.

It should be noted that the module contains two separate and independent versions of the FIPS-approved AES-GCM algorithm.

The implementation contained in software (see CAVP cert C 542) conforms to IG A.5, scenario #3, when operating in a FIPS approved mode of operation. AES GCM, IVs are generated both internally and deterministically and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.1.

The implementation contained in hardware (see CAVP cert AES 4369) is used in support of line rate MACsec functionality and conforms to IG A.5, scenario #2, when operating in a FIPS-approved mode of operation. AES GCM, IVs are generated externally (to the AES-GCM implementation on the chip but still within the module's boundary) using the module's FIPS-approved DRBG (CAVP algorithm cert C 542) and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.2.

3 Cryptographic Boundary

The cryptographic boundaries for the Cisco NCS 5500 series routers are defined as encompassing the "top", “back”, "front", "left", "right", and "bottom" surfaces of the module enclosure.

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:

NCS-5508 Physical Interfaces	NCS-5508 Logical Interfaces
Power Plug (8 slots)	Power Interface
LEDs	Status Output interface

Table 4: NCS 5508 Interfaces

NC55-RP Physical Interfaces	NC55-RP Logical Interfaces
Console Port USB Port (2 slots) Management Ethernet (1)	Data Input Interface
Console Port USB Port (2 slots) Management Ethernet (1)	Data Output Interface
Console Port USB Port (2 slots) Management Ethernet (1)	Control Input Interface
Console Port Management Ethernet (1) LEDs	Status Output interface

Table 5: NC-55 RP Interfaces

NCS-55A1-36H-SE-S Physical Interfaces	NCS-55A1-36H-SE-S Logical Interfaces
Console Port USB Port Management Ethernet (1) 10/25/40/100 GE Ports (36)	Data Input Interface
Console Port USB Port Management Ethernet (1) 10/25/40/100 GE Ports (36)	Data Output Interface
Console Port USB Port Management Ethernet (1) 10/25/40/100 GE Ports (36)	Control Input Interface
Console Port Management Ethernet (1) LEDs 10/25/40/100 GE Ports (36)	Status Output interface
Power Plug	Power Interface

Table 6: NCS-55A1-36H-SE-S Interfaces

NCS-5501 Physical Interfaces	NCS-5501 Logical Interfaces
Console Port Management Ethernet (2) 1/10 GE Ports (48) 40/100 GE Ports (6)	Data Input Interface

NCS-5501 Physical Interfaces	NCS-5501 Logical Interfaces
Console Port Management Ethernet (2) 1/10 GE Ports (48) 40/100 GE Ports (6)	Data Output Interface
Console Port Management Ethernet (2) 1/10 GE Ports (48) 40/100 GE Ports (6)	Control Input Interface
Console Port Management Ethernet (2) LEDs 1/10 GE Ports (48) 40/100 GE Ports (6)	Status Output interface
Power Plug	Power Interface

Table 7: NCS-5501 Interfaces

NCS-5502 Physical Interfaces	NCS-5502 Logical Interfaces
Console Port Management Ethernet (2) 10/40/100 GE Ports (48)	Data Input Interface
Console Port Management Ethernet (2) 10/40/100 GE Ports (48)	Data Output Interface
Console Port Management Ethernet (2) 10/40/100 GE Ports (48)	Control Input Interface

NCS-5502 Physical Interfaces	NCS-5502 Logical Interfaces
Console Port Management Ethernet (2) LEDs 10/40/100 GE Ports (48)	Status Output interface
Power Plug	Power Interface

Table 8: NCS-5502

Line Cards	Physical Interfaces	Logical Interfaces
NC55-36X100G-S	10/40/100 GE Ports (36)	Data Input/Output Interface, Control Input Interface, Status Output Interface
	LED	Status Output Interface

Table 9: Line Card Interfaces

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. A complete description of all the management and configuration capabilities of the modules can be found in the Cisco NCS 5500 Series Routers Software Configuration Guide Manual[1] 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 251,596,800 (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

[1] Software configuration guides are linked in Section 10.

10x9x8x7x6x5x32x52). In order to successfully guess the sequence in one minute would require the ability to make over 4,193,280 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 either 2048 or 3072 bits, thus providing at least 112 bits of strength. Assuming the low end of that range (2048 bits), 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.

It should be noted that the same services are available to both Users and Cryptographic officers, regardless of whether or not they are in a non-FIPS approved mode of operation or a FIPS approved mode of operation.

5.1 User Services

A User enters the system by accessing the console port with a terminal program or SSH v2 session to a LAN port or the 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 consist of the following:

- Status Functions - View state of interfaces and protocols, firmware version
- Terminal Functions - Adjust the terminal session (e.g., lock the terminal, adjust flow control)
- Directory Services - Display directory of files kept in memory
- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand
- Perform Cryptography – Use the cryptography provided by the module:
    - SSH
    - SNMPv3
    - MACsec

5.2 Cryptographic Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the management Ethernet port. The Crypto Officer authenticates in the same manner as a User. The Crypto Officer is identified by accounts that are part of the usergroup “root-lr”. 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 Crypto Officer services consist of the following:

- Configure the module - 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.

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

- Status Functions - View the module configuration, routing tables, active sessions, use get commands to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.

- Manage the module - Log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manage user rights, initiate power-on self-tests on demand and restore router configurations.

- Set Encryption - Set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.

- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand

- Zeroization - Erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

5.3 Unauthenticated User Services

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

6 Cryptographic Key/CSP Management

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

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

CSP#	Name	Key Type	Description	Generation/ Input	Output	Storage	Zeroization
1	DRBG entropy input	not a key (256 bits)	DRBG input used for SP 800-90A CTR_DRBG. This is the entropy for SP 800-90A CTR_DRBG, used to construct the DRBG seed.	Internally generated	Never output from module	DRAM (plaintext)	Power cycle the device
2	DRBG Seed (IOS XR)	not a key (384 bits)	Input to the DRBG that determines the internal state of the DRBG. Derived by using DRBG derivation function that includes the entropy input.	Internally generated	Never output from module	DRAM (plaintext)	Automatically every 400 bytes or turn off the router.

CSP#	Name	Key Type	Description	Generation/ Input	Output	Storage	Zeroization
3	DRBG V	CTR (using AES-256) 256-bit	Internal V value used as part of SP800-90A CTR_DRBG	Internally generated	Never output from module	DRAM (plaintext)	Power cycle the device
4	DRBG Key	CTR (using AES-256) 256-bit	DRBG key used for SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	Internally generated	Never output from module	DRAM (plaintext)	Power cycle the device
5	Diffie-Hellman Shared Secret	DH 2048 – 4096 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	Internally generated	Never output from module	DRAM (plaintext)	Zeroized upon deletion. Overwritten with 0x00
6	Diffie Hellman private exponent	DH 2048 – 4096 bits	The private exponent used in Diffie-Hellman (DH) exchange.	Generated internally via a call to the DRBG.	Never output from the module	DRAM (plaintext)	Zeroized upon deletion. Overwritten with 0x00
7	Diffie Hellman public key	DH 2048 – 4096 bits	The p used in Diffie-Hellman (DH) exchange.	Generated internally via a call to the DRBG.	Never output from the module	DRAM (plaintext)	Zeroized upon deletion. Overwritten with 0x00
8	Operator password	Shared Secret, at least eight characters	The password of the operator.	Externally generated and entered by the User and/or CO when logging in.	Never output from the module	NVRAM (plaintext)	Overwrite with new password

CSP#	Name	Key Type	Description	Generation/ Input	Output	Storage	Zeroization
9	SSH Private Key	RSA 2048 – 3072 bits EC Diffie-Hellman P-256, 384 and 521	The SSH private key for the module.	Generated internally via a call to the DRBG.	Never output from the module	NVRAM (plaintext)	SSH private key is zeroized by either deletion (via **# crypto key zeroize rsa**) or by overwriting with a new value of the key
10	SSH Public Key	RSA 2048 – 3072 bits EC Diffie-Hellman P-256, 384 and 521	The SSH public key for the module.	Generated internally via a call to the DRBG.	Never output from the module	NVRAM (plaintext)	Zeroized upon deletion. Overwritten with 0x00
11	SSH Session Key	Triple-DES 168-bits AES 128-, 192-, or 256-bits	The SSH session key.	Agreed using SSH key establishment using Diffie-Hellman	Never output from the module	DRAM (plaintext)	Automatically when the SSH session is terminated.
12	EC Diffie-Hellman Shared Secret	EC Curves: P-256, P-384, and P-521	The shared secret used in EC Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	Internally generated	Never output from module	DRAM (plaintext)	Zeroized upon deletion. Overwritten with 0x00
13	SNMPv3 Password	Secret 256 bits	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication	Externally generated and entered by the CO.	Never output from the module	DRAM	Power cycle

CSP#	Name	Key Type	Description	Generation/ Input	Output	Storage	Zeroization
14	snmpEngineID	Not a key	Unique string to identify the SNMP engine	Externally generated and entered by the CO.	Never output from the module	NVRAM	# no snmp-server engineID local engineid-string, overwritten with new engine ID
15	SNMP session key	AES 128-bit Triple-DES 168-bits	Encrypts SNMP traffic	Internally generated via SNMP KDF	Never output from the module	DRAM	Power cycle
16	MACsec Connectivity Association Key (CAK)	AES-GCM	128/256 bits. A CO configured pre-shared secret key possessed by members of a MACsec connectivity association (via MKA) to secure control plane traffic.	Externally generated and entered by the CO.	Never output from the module	DRAM (plaintext)	Automatically when session expires.
17	MACsec Integrity Check Key (ICK)	AES-CMAC	128/256 bits. Used to prove an authorized peer sent the message.	Derived from the CAK using the SP800-108 KDF.	Never output from the module	DRAM (plaintext)	Automatically when session expires.
18	MACsec Key Encryption Key (KEK)	AES-CMAC	128/256 bits. Used to transmit SAKs to other members of a MACsec connectivity association.	Derived from the CAK using the SP800-108 KDF.	Never output from the module	DRAM (plaintext)	Automatically when session expires.

CSP#	Name	Key Type	Description	Generation/ Input	Output	Storage	Zeroization
19	MACsec Security Association Key (SAK)	AES-GCM	128/256 bits. Used for creating Security Associations (SA) for encrypting/decrypting the MACsec data plane traffic.	Derived from the CAK using the SP800-108 KDF.	Output from the module to other members of a MACsec connectivity association when encrypted by the KEK	DRAM (plaintext)	Automatically when session expires.

Table 10: CSPs

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

	User Role				CO Role				
CSP#	Network	Status	Terminal	Directory	Configure	Define Rules and Filter	Status	Management	Set Encryption
1	r							d	rwd
2	r							d	rwd
3	r							d	rwd
4	r							d	rwd
5	r								rwd
6	r								rwd
7	r								rwd
8	r							rwd	
9								rwd	
10								rwd	
11								rwd	
12								rwd	
13								rwd	
14								rwd	
15								rwd	
16								rwd	
17								rwd	
18								rwd	
19								rwd	

Table 11: Role CSP Access

6.1 Triple-DES Keys

In accordance with CMVP IG A.13, when operating in a FIPS approved mode of operation, the same Triple-DES key shall not be used to encrypt more than 2^{20} 64-bit data blocks.

The SSH protocols governs the generation of the respective Triple-DES keys. Please refer to IETF RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring that the module limits the number of encrypted blocks with the same key to no more than 2^{20} when utilized as part of the recognized IETF protocol.

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco NCS 5500 series routers 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 NCS 5500 series routers for use in the FIPS mode of operation. Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

Algorithm	Supported Mode	Cert. #
IOS XR		
AES	ECB (128, 192, 256) CBC (128, 192, 256) CTR (128, 192, 256) GCM (128, 256) CMAC (128, 256)	C 542
SHS	SHA-1, -256, -384, and -512 (Byte Oriented)	C 542
HMAC	SHA-1, -256, -384, and -512	C 542
DRBG	CTR (using AES-256)	C 542
KBKDF (SP 800-108)	HMAC SHA-1, HMAC SHA-2-224, -256, -384, -512	C 542
RSA	PKCS#1 v.1.5, 1024-4096 bit key (SigVer, KeyGen and SigGen) 1024-bit keys allowed for signature verification only	C 542
Triple-DES	TCBC (KO 1)	C 542
CVL (SP800-135)	SSH KDF, SNMP KDF	C 542
CVL (KAS-ECC CDH-Component)	Curves: P-256, P-384, P-521	C 542
MACsec H/W Crypto Acceleration Chip on NC55-36X100G-S		
AES	CTR (128, 256) ECB (128, 256) GCM (128, 256) XPN	AES 4369

Table 12: FIPS-Approved Algorithms for use in FIPS Mode

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

The NCS-5500 series router cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Diffie-Hellman – provides between 112 and 150-bits of encryption strength. Diffie-Hellman with less than 112-bit of security strength is non-compliant and may not be used.

- EC Diffie-Hellman – shared secret computation providing 128, 192, and 256-bits of encryption strength.

- RSA Key Wrapping – provides 112 and 128-bits of encryption strength. RSA with less than 112-bit of security strength is non-compliant and may not be used.

7.3 Non-Approved Algorithms

The cryptographic module, in addition to the above listed FIPS approved algorithms, 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, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

The NCS 5500 cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations:

RSA:

- Key Generation: MOD: 1024-bit keys and 1536-bit keys
- Signature Generation: 1024-bit keys and 1536-bit keys

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:

- Known Answer Tests:
    - AES (both software and hardware implementations)
    - AES-GCM (both software and hardware implementations)
    - DRBG
    - EC Diffie-Hellman
    - HMAC SHA-1, SHA-256, SHA-384 and SHA-512
    - RSA
    - SHA-1, SHA-256, SHA-384 and SHA-512
    - Triple-DES
- Firmware Integrity Test
    - RSA 2048 with SHA-256

Conditional Tests Performed:

- Continuous Random Number Generator Test for the FIPS-approved DRBG
- Firmware load test
- RSA pairwise consistency test

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.

8 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

9 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Upon initial boot from the factory, the NCS5500 is in a non-FIPS mode of operation. To transition from a non-FIPS mode of operation to a FIPS mode of operation, the Cryptographic Officer must follow all steps detailed in section 9.1 of this security policy.

9.1 System Initialization and Configuration

Step 1 - Initially the router does not have any user configuration. The system prompts you to specify the username of the root user as well as a secret (password).

```
- Enter root-system username: [USERNAME]
- Enter secret: [PASSWORD]
- Enter secret again:[PASSWORD]
```

Enter the root-system username and password.

```
- Username:[USERNAME]
- Password:[PASSWORD]
```

Step 2- CO assigns passwords to users for Identification and Authentication.

```
- Configure Terminal
- line con 0
- password [PASSWORD]
- Login Local
```

Step 3 - Configure Management port

```
- configure terminal
- interface MgmtEth [rack/slot/port]
- ipv4 address [ipv4-address subnet-mask]
- no shutdown
- exit
- router static address-family ipv4 unicast
  [0.0.0.0/0 default-gateway]
- commit
```

Step 4 - Configure SSH

```
- configure terminal
- hostname [hostname]
- domain-name [domain-name]
- commit
```

```
- exit
- crypto key generate rsa [keypair-label]
- configure terminal
- ssh server v2
- commit
```

Step 5 - Enable FIPS 1402- logging

```
- configure Terminal
- logging buffered debugging
- commit
```

Step 6 - Enable FIPS mode.

```
- configure terminal
- crypto fips-mode
- commit
- reload location all
```

On either reboot or reload the device will be in the FIPS Approved Mode of Operation.

NOTE: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

To transition from a FIPS mode of operation to a non-FIPS mode of operation, the Cryptographic Officer shall zeroize all keys and CSP's that were generated and remove the FIPS mode command from the configuration. For key zeroization, please refer to the "Zeroization" column in table 10 of this security policy. To remove the FIPS mode command from the configuration, follow the steps below:

To disable FIPS mode

```
- configure terminal
- no crypto fips-mode
- commit
- reload location all
```

On reboot/reload device will be in the non-FIPS Approved Mode of Operation.

Secure DNS, RADIUS, and TACACS+ shall not be used in a FIPS mode of operation. TLS and IPsec shall not be used in the FIPS mode of operation. If they are used then all data transmitted is considered plaintext.

9.2 Remote Access

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

SNMPv3 communications with the module are allowed in FIPS approved mode.

9.3 Key Strength

Key sizes with security strength of less than 112-bits shall not be used in FIPS mode of operation.

10 Related Documentation

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

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.

For LED related information, please review the following document:

- Hardware Installation Guide for NCS 5500 Series Modular Routers. Chapter: LEDs (https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/hardware-install/b-ncs5500-hardware-installation-guide/b-ncs5500-hardware-installation-guide_appendix_0111.html)

Software configuration guides for the NCS 5500 platform can be found using the following source:

- https://www.cisco.com/c/en/us/support/routers/network-convergence-system-5500-series/products-installation-and-configuration-guides-list.html

11 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

11.1 Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

11.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

11.3 Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

12 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

13 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://tools.cisco.com/security/center/rss.x?i=44

13.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- Non-emergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with

PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

14 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

14.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

14.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: +1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

14.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) – Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

15 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

16 Definitions List

ACL	Access Control List
AES	Advanced Encryption Standard
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DRAM	Dynamic RAM
DRBG	Deterministic Random Bit Generator
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GigE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ISSU	In-service software upgrade
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
PIN	Personal Identification Number
RAM	Random Access Memory
RNG	Random Number Generator
RP	Route Processor
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VPN	Virtual Private Network