



**Cisco Network Convergence System 2000 Series  
Cryptographic Module**

**FIPS 140-2 Non Proprietary Security Policy  
Level 2 Validation**

**Version 2.8**

**August 22, 2019**

# Table of Contents

<b>CISCO NETWORK CONVERGENCE SYSTEM 2000 SERIES CRYPTOGRAPHIC MODULE .....</b>	<b>1</b>
<b>1 INTRODUCTION .....</b>	<b>3</b>
1.1 PURPOSE .....	3
1.2 MODULE VALIDATION LEVEL .....	3
1.3 REFERENCES .....	3
1.4 TERMINOLOGY .....	4
1.5 DOCUMENT ORGANIZATION .....	4
<b>2 CISCO NETWORK CONVERGENCE SYSTEM 2000 SERIES APPLIANCES .....</b>	<b>5</b>
2.1 VALIDATED CONFIGURATION .....	5
2.2 CRYPTOGRAPHIC BOUNDARY .....	7
2.3 MODULE INTERFACES .....	7
2.4 NCS2K APPLIANCES .....	9
2015 Front .....	9
2006 Front .....	10
2002 Front .....	11
2.5 CONTROLLER CARDS .....	11
2.6 ENCRYPTION CARDS .....	12
2.7 ROLES AND SERVICES .....	12
2.8 USER SERVICES .....	13
2.9 CRYPTO OFFICER SERVICES .....	13
2.10 NON-FIPS MODE SERVICES .....	14
2.11 UNAUTHENTICATED SERVICES .....	15
2.12 CRYPTOGRAPHIC KEY/CSP MANAGEMENT .....	15
2.13 CRYPTOGRAPHIC ALGORITHMS .....	18
Approved Cryptographic Algorithms .....	18
Non-FIPS Approved Algorithms Allowed in FIPS Mode .....	19
Non-Approved Cryptographic Algorithms .....	19
2.14 SELF-TESTS .....	20
2.15 PHYSICAL SECURITY .....	21
2.16 SECURE OPERATION .....	30
2.16.1 Initial Setup .....	30
2.16.2 System Initialization and Configuration .....	30
2.16.3 HTTPS/TLSv1.2 Management Requirements and Cryptographic Algorithms .....	30
2.16.4 SSHv2 Management Requirements and Cryptographic Algorithms .....	30

# 1 Introduction

## 1.1 Purpose

This is the non-proprietary cryptographic module security policy for the Cisco Network Convergence System 2000 Series Cryptographic Module running with firmware version 11.0. This security policy describes how this module meets the security requirements of FIPS 140-2 Level 2 and how to run the module in a FIPS 140-2 mode of operation. This Security Policy 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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	<b>Overall module validation level</b>	<b>2</b>

**Table 1 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 Network Convergence System 2000 Series Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2 IG and additional rules imposed by Cisco Systems, Inc. More information is available on the module from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following website:

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

<http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html>

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at [www.cisco.com](http://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 Network Convergence System 2000 Series Cryptographic Module is referred to as NCS2K, Cryptographic Module, Module or Appliance.

## 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 Network Convergence System 2000 Series Cryptographic Module identified above and explains the secure layout, 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 Network Convergence System 2000 Series Appliances

The Cisco Network Convergence System 2000 Series delivers an Evolved Programmable Network (EPN) that lets you simplify network operations, reduce network costs, and make your network more dynamic and profitable. The NCS2K Series delivers agility, programmability, and massive scale across ultra-long-haul, metro, and enterprise optical networks. These appliances sets the industry benchmark for dense wavelength-division multiplexing (DWDM) solutions. It delivers the touchless programmability, massive scale, and ultra-long-haul performance necessary for tomorrow's converged network architectures. The system's Wavelength Switched Optical Network (WSON) control plane architecture enhances Generalized Multiprotocol Label Switching (GMPLS) capabilities with awareness of wavelength properties and optical impairments

The Cisco NCS2K Series offers three chassis variants to meet varying scale and space requirements. The Cisco NCS 2015 has 17 slots for the various service cards listed below and is a 14 rack unit (14RU), allowing three chassis to fit into one standard rack. The Cisco NCS 2006 chassis is 6 rack unit (6RU) and has 8 slots for the various service cards listed below. The NCS 2002 is a 2 rack unit (2RU) and has 3 slots for the various service cards listed below.



Image 1: NCS 2015, 2006 and 2002

### 2.1 Validated configuration

The validated platforms consist of the following components:

- Chassis:
  - NCS2002
  - NCS2006
  - NCS2015
- Service Cards:
  - Controller Cards:
    - NCS2K-TNCS-O-K9
    - NCS2K-TNCS-K9

- NCS2K-TNCS-2-K9
- NCS2K-TNCS-2O-K9
- Encryption Cards:
  - 15454-M-WSE-K9
  - NCS2K-MR-MXP-LIC
  - NCS2K-400G-XP
- Line Cards:
  - 15454-M-10X10G-LC
  - NCS2K-200G-CK-LIC
  - NCS2K-16-AD-CCOFS
  - NCS2K-20-SMRFS-CV
- Blanks:
  - 15454-Blank=
  - 15454E-Blank=
  - 15454-M-Filler=
  - 15454-M-T-Filler=
- FIPS Kit:
  - AIR-AP-FIPSKIT=

The switches can be configured as follows while in the FIPS mode:

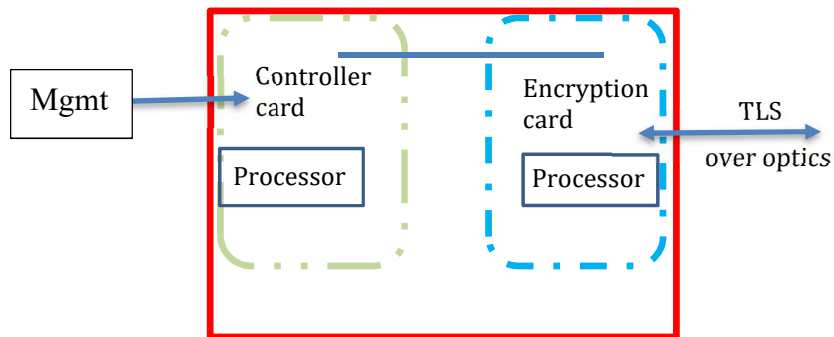
Chassis	Controller Card(s)	Encryption Card(s)	Line Cards and Blanks Cards
NCS2002 (3 slots)	<b>Single</b> NCS2K-TNCS-O-K9 NCS2K-TNCS-K9 NCS2K-TNCS-2-K9 NCS2K-TNCS-2O-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC	15454-M-10X10G-LC NCS2K-200G-CK-LIC NCS2K-16-AD-CCOFS NCS2K-20-SMRFS-CV 15454-Blank= 15454E-Blank= 15454-M-Filler= 15454-M-T-Filler=
NCS2006 (8 slots)	<b>Single or Dual</b> NCS2K-TNCS-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	15454-M-10X10G-LC NCS2K-200G-CK-LIC NCS2K-16-AD-CCOFS NCS2K-20-SMRFS-CV 15454-Blank= 15454E-Blank= 15454-M-Filler= 15454-M-T-Filler=
	<b>Single or Dual</b> NCS2K-TNCS-O-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	
	<b>Single or Dual</b> NCS2K-TNCS-2-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	
	<b>Single or Dual</b> NCS2K-TNCS-2O-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	

Chassis	Controller Card(s)	Encryption Card(s)	Line Cards and Blanks Cards
NCS2015 (17 slots)	Single or Dual NCS2K-TNCS-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	15454-M-10X10G-LC NCS2K-200G-CK-LIC NCS2K-16-AD-CCOFS NCS2K-20-SMRFS-CV 15454-Blank= 15454E-Blank= 15454-M-Filler= 15454-M-T-Filler=
	Single or Dual NCS2K-TNCS-O-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	
	Single or Dual NCS2K-TNCS-2-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	
	Single or Dual NCS2K-TNCS-2O-K9	15454-M-WSE-K9 and/or NCS2K-MR-MXP-LIC and/or NCS2K-400G-XP	

Table 1: Chassis configuration

## 2.2 Cryptographic Boundary

The module is a hardware, multi-chip standalone crypto module. The cryptographic boundary is defined as the physical enclosure of the chassis (red box).



All of the functionality described in this publication is provided by components (Controller (light green) and Encryption (light blue) cards) within this cryptographic boundary (red color). The module can incorporate up to one or two controller cards (depending on chassis used), and up to six (6) encryption cards (depending on the chassis used) and up to four (4) line cards in a single configuration (depending on the chassis used).

## 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 provides 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 Interfaces	FIPS 140-2 Logical Interfaces
Encryption Card: <ul style="list-style-type: none"> <li>• SFP+ ports<sup>1</sup> (NCS2K-MR-MXP-LIC, 15454-M-WSE-K9)</li> <li>• QSFP+ ports<sup>2</sup> (NCS2K-MR-MXP-LIC and NCS2K-400G-XP)</li> <li>• CPAK port<sup>3</sup> (NCS2K-MR-MXP-LIC)</li> <li>• CFP2 port<sup>4</sup>(NCS2K-400G-XP)</li> </ul> Controller Card: <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• SFP ports<sup>5</sup></li> </ul> Line Card: <ul style="list-style-type: none"> <li>• SFP+ ports</li> <li>• Cisco CPAK port</li> </ul>	Data Input Interface
Encryption Card: <ul style="list-style-type: none"> <li>• SFP+ ports (NCS2K-MR-MXP-LIC, 15454-M-WSE-K9)</li> <li>• QSFP+ ports (NCS2K-MR-MXP-LIC and NCS2K-400G-XP)</li> <li>• Cisco CPAK port (NCS2K-MR-MXP-LIC)</li> <li>• CFP2 port (NCS2K-400G-XP)</li> </ul> Controller Card: <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• SFP ports</li> </ul> Line Card: <ul style="list-style-type: none"> <li>• SFP+ ports</li> <li>• Cisco CPAK port</li> </ul>	Data Output Interface
Controller Card: <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• Up to four SFP ports</li> </ul> External Connection Unit (part of NCS chassis): <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• SFP ports</li> </ul>	Control Input Interface
Encryption Card: <ul style="list-style-type: none"> <li>• SFP+ ports (NCS2K-MR-MXP-LIC, 15454-M-WSE-K9)</li> <li>• QSFP+ ports (NCS2K-MR-MXP-LIC and NCS2K-400G-XP)</li> <li>• Cisco CPAK port (NCS2K-MR-MXP-LIC)</li> <li>• CFP2 port (NCS2K-400G-XP)</li> <li>• LED</li> </ul> Controller Card: <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• Up to four SFP ports</li> <li>• LED</li> </ul> External Connection Unit (part of NCS Chassis) <ul style="list-style-type: none"> <li>• RJ-45 Ethernet Port</li> <li>• SFP ports</li> <li>• USB ports</li> <li>• LCD</li> </ul>	Status Output Interface

**Table 2 Hardware/Physical Boundary Interfaces**

**Note:**

1. The RS232 port (on each Controller Card) that was protected by the front cover of each chassis shall not be used while in FIPS mode.

<sup>1</sup> SFP+: Enhanced Small Factor Pluggable

<sup>2</sup> QSFP+: Enhanced Quad Small Factor Pluggable

<sup>3</sup> CPAK: Cisco CPAK (Cisco developed)

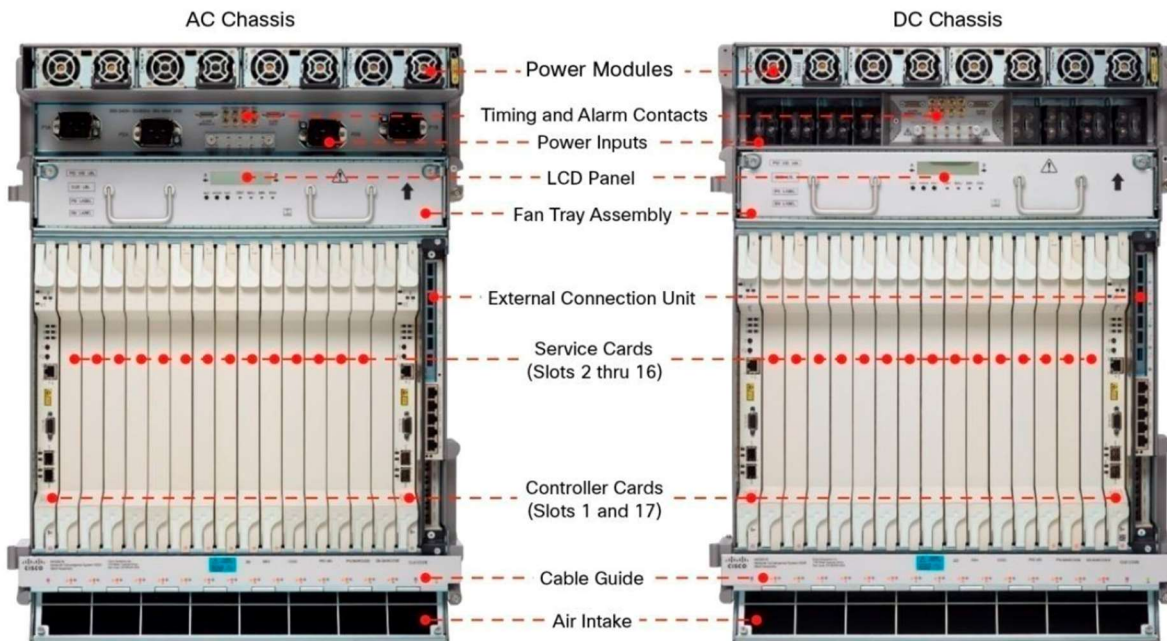
<sup>4</sup> CFP2: C Form-Factor Pluggable 2

<sup>5</sup> SFP: Small Factor Pluggable

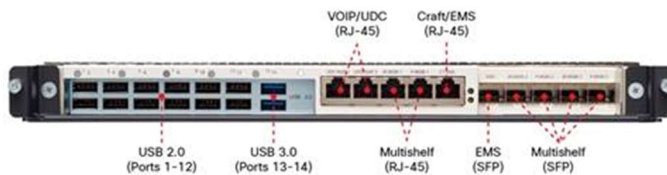


## 2.4 NCS2K Appliances

### 2015 Front

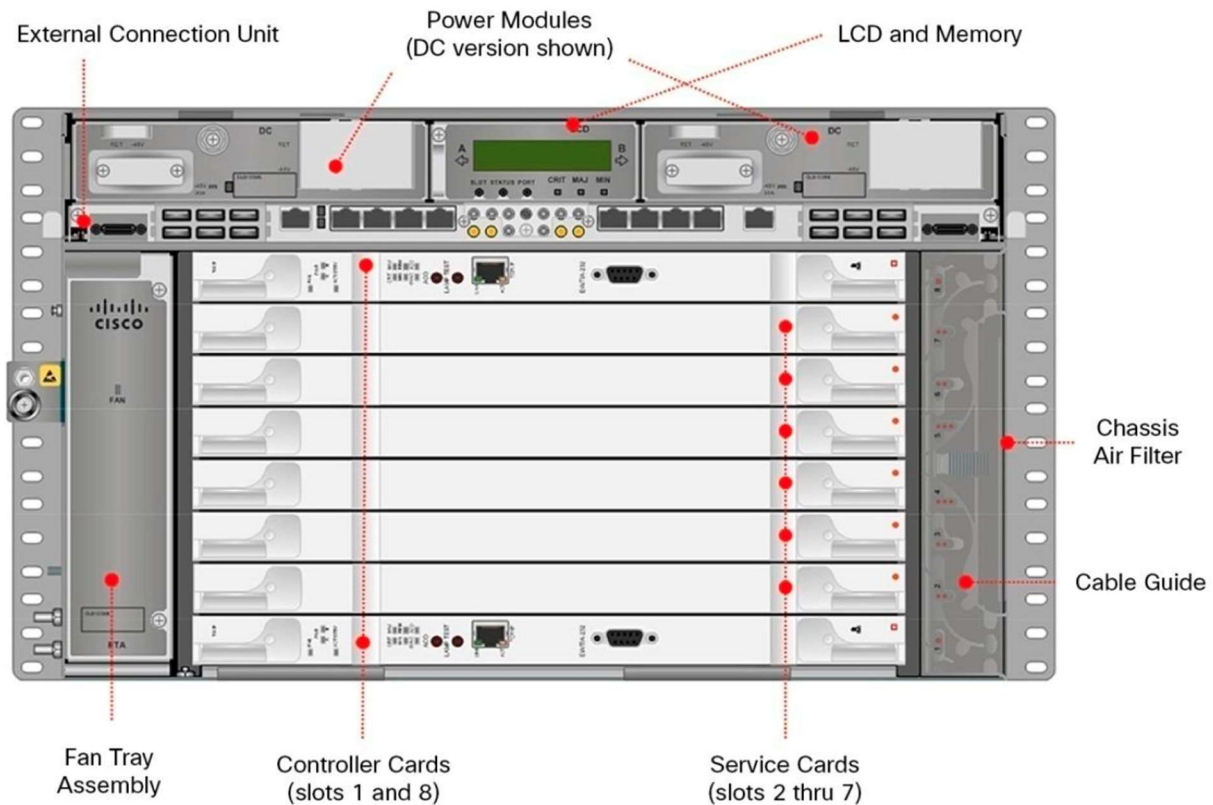


### External Connection Unit



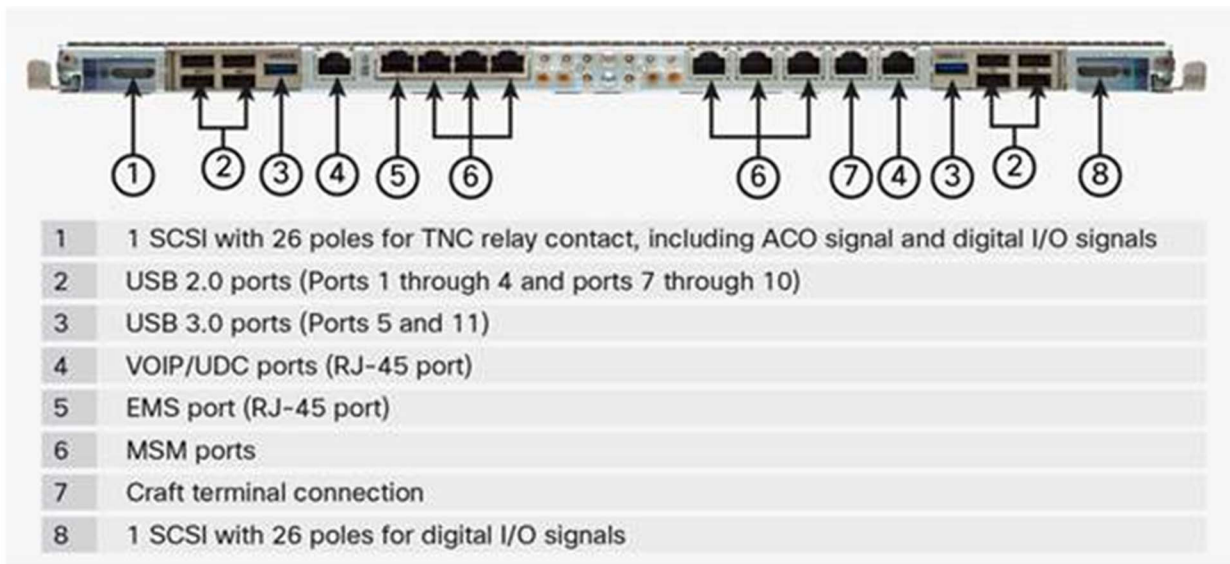
Note: External connection unit is a part of the chassis that provides interfaces for passive device inventory and management, multishelf management, and element management. Both RJ-45 and SFP interfaces are provided for multi-shelf and element management, allowing the convenience of copper as well as the distance flexibility of optical connections.

## 2006 Front

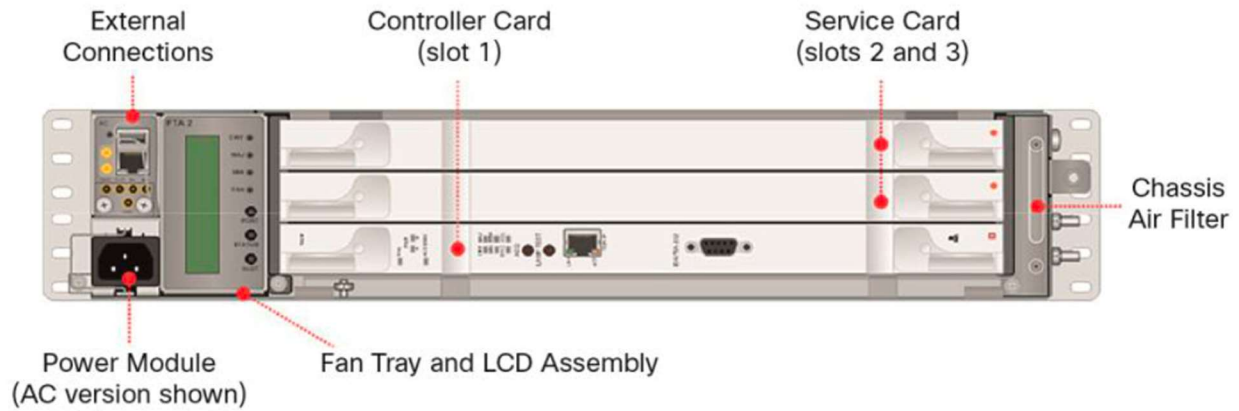


### External Connection Unit

Note: External connection unit is a part of the chassis that provides interfaces for passive device inventory and management, multishelf management, and element management. Both RJ-45 and SFP interfaces are provided for multishelf and element management, allowing the convenience of copper as well as the distance flexibility of optical connections.



## 2002 Front



Note: External Connection provides status output, management connectivity and passive device connectivity with integrated RJ-45 and USB ports.

## 2.5 Controller Cards

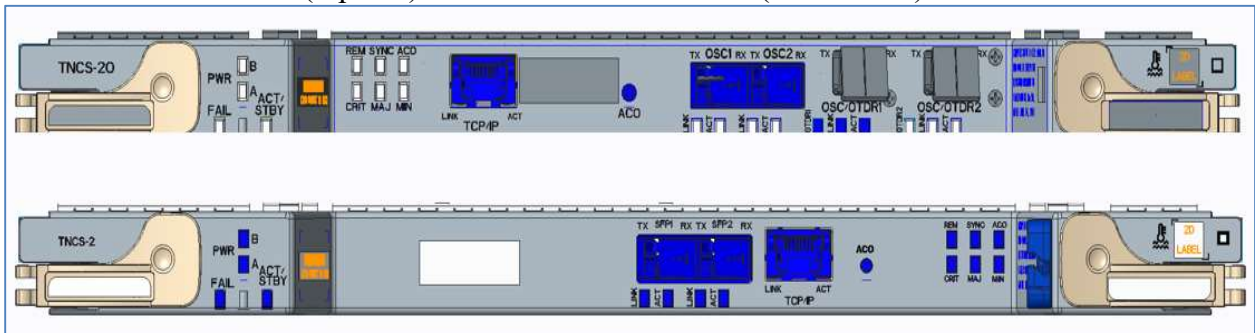
### NCS2K-TNCS-K9



### NCS2K-TNCS-O-K9



### NCS2K-TNCS-2O-K9 (top one) and NCS2K-TNCS-2-K9 (bottom one)



## 2.6 Encryption Cards

### NCS2K-MR-MXP-LIC



### 15454-M-WSE-K9



### NCS2K-400G-XP



## 2.7 Roles and Services

The module can be accessed in one of the following ways:

- SSHv2
- HTTPS/TLSv1.2

The cryptographic module supports identify-based authentication. There are two roles in the Switch that may be assumed the Crypto Officer (CO) role and the User role. The administrator of the module assumes the Crypto Officer role and associated services in order to configure and maintain ONS, while the Users exercise only the basic User services.

All Crypto Officer (CO) role and the User role passwords and all 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  $94 \times 93 \times 92 \times 91 \times 90 \times 89 \times 32 \times 10$ . 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, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. 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  $8.6 \times 10^{31}$  ( $5.2 \times 10^{33} / 60 = 8.6 \times 10^{31}$ ) attempts per second, which far exceeds the operational capabilities of the module to support.

## 2.8 User Services

A User enters the system by accessing the Serial Console port, SSHv2, or HTTPS/TLSv1.2. The User role can be authenticated via either User Name/Password or RSA based authentication method. 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 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 the module configuration, routing tables, active sessions health, and view physical interface status.	User password (r, w, d)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	User password (r, w, d)
Network Functions	Connect to other nodes and initiate diagnostic network services (i.e., ping, mtrace).	User password (r, w, d)
Self-Tests	Perform the FIPS 140 start-up tests by cycling the power.	N/A
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2.	User password, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 integrity key and SSHv2 session key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
HTTPS Functions (TLSv1.2)	Negotiation and encrypted data transport via HTTPS/TLSv1.2.	User password, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)
Optical TLS (TLSv1.2)	Negotiation and encrypted data via TLSv1.2	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, ECDH private ECDH public key, ECDH shared secret, Optical TLS server private key, Optical TLS server public key, Optical TLS pre-master secret, Optical TLS expansion master secret, Optical TLS session key, and Optical TLS integrity key (r, w, d)

**Table 3 User Services**

## 2.9 Crypto Officer Services

During initial configuration of the module, the Crypto Officer 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 module. A Crypto Officer enters the system by accessing the Serial Console port, SSHv2, or HTTPS/TLSv1.2. The CO role can be authenticated via either User Name/Password or RSA based authentication method. 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	Description	Keys and CSPs Access
Configure the Security	Define network interfaces and settings, enable interfaces and network services, set system date and time, and load authentication information.	DRBG seed, DRBG entropy input, DRBG V and DRBG key, DH private DH public key, DH shared secret, ECDH private ECDH public key, ECDH shared secret, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 session key, SSHv2 integrity key, Optical TLS server private key, Optical TLS server public key, Optical TLS pre-master key, Optical TLS expansion master key, Optical TLS client key, Optical TLS session key, and Optical TLS integrity key , (r, w, d)
Define Rules and Filters	Create packet Filters that are applied to User data streams for each node.	User password, Crypto Officer password (r, w, d)
View Status Functions	View the appliance configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	User password, Crypto Officer password (r, w, d)
HTTPS/TLS (TLSv1.2)	Configure HTTPS/TLSv1.2 parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys and TLS integrity key (r, w, d)
Optical TLS (TLSv1.2)	Configure TLS encryption parameters. Over Optical channel	ECDH private ECDH public key, ECDH shared secret, Optical TLS server private key, Optical TLS server public key, Optical TLS pre-master secret, Optical TLS expansion master secret, Optical TLS session key, and Optical TLS integrity key (r, w, d)
SSHv2 Function	Configure SSHv2 parameter, provide entry and output of CSPs.	DRBG entropy input, DRBG seed, DRBG V and DRBG key, 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 integrity key and SSHv2 session 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.	User password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

**Table 4 Crypto Officer Services**

The module doesn't support maintenance service.

## 2.10 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 2.10, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Services <sup>6</sup>	Non-Approved Algorithms
SSH	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

**Table 5 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.

## 2.11 Unauthenticated Services

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

## 2.12 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.

The Crypto Officer needs to be authenticated to store keys and CSPs. Only an authenticated Crypto Officer can view the CSPs. All Diffie-Hellman (DH)/ECDH keys agreed upon for individual tunnels are directly associated with that specific tunnel. All other keys are associated with the user role that entered them. The entropy source (NDRNG) within the module provides at least 384 bits of entropy to seed SP800-90a DRBG for use in key generation. The NCS2K module uses Cisco ACT2Lite Cryptographic Module for providing the sufficient entropy to seed the DRBG.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256)	384-bits	This is the entropy for SP 800-90A CTR_DRBG. Used to construct the seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256)	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 the entropy source.	DRAM (plaintext)	Power cycle the device

<sup>6</sup> These approved services become non-approved when using any non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG V	SP800-90A CTR_DRBG (AES-256)	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 CTR_DRBG (AES-256)	256-bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman shared secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-384 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 – 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman shared Secret	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an Optical TLS session. 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
EC Diffie-Hellman private key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an Optical TLS session. The private 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 public key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an Optical TLS 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
SSHv2 RSA private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 RSA public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command



Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SSHv2 session key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	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 (SSHv2).	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 integrity key	HMAC-SHA-1/256/512	160-512 bits	Used for SSH connections integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when SSH session is terminated
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	At least eight characters	Keying material used to derive TLS master key during the TLS session establishment. This key entered into the module encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS master secret	keying material	48 Bytes	Keying material used to derive other HTTPS/TLSv1.2 keys. This key was derived from TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when TLS session is terminated
TLS session keys	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLSv1.2 connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA 256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
Optical TLS server private key	RSA	2048 bits	2048 bits RSA private key used for Optical TLS (TLS over Optics) server. This key is generated by calling SP	NVRAM (plaintext)	Deleted via the GUI interface
Optical TLS server public key	RSA	2048 bits	2048 bits RSA public key used for Optical TLS server. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Automatically when TLS session terminates

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
Optical TLS pre-master secret	Keying material	48 bytes	keying material created from ECDH key establishment scheme. It is used to derive Optical TLS expansion master secret.	DRAM (plaintext)	Automatically when TLS session terminates
Optical TLS expansion master secret	Keying material	48 bytes	Optical TLS keying material was derived from Optical TLS pre-master secret during the TLS session establishment. Used to derive Optical TLS session keys.	DRAM (plaintext)	Automatically when TLS session terminates
Optical TLS session keys	AES-GCM	AES 256 bits	Used in Optical TLS to protect the session traffic. This key was derived via SP800-135KDF in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
Optical TLS integrity key	HMAC-SHA 256/384	256-384 bits	Used for Optical TLS integrity to assure the traffic integrity. This key was derived via SP800-135KDF in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
User password	Password	8-25 characters	The password of the User role, including at least one letter and at least one number character.	NVRAM (plaintext)	Overwrite with new password
Crypto Officer password	Password	8-25 characters	The password of the Crypto Officer role, including at least one letter and at least one number character.	NVRAM (plaintext)	Overwrite with new password

**Table 6 Cryptographic Keys and CSPs**

## 2.13 Cryptographic Algorithms

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

### Approved Cryptographic Algorithms

	NCS2K FOM Implementation	NCS2K FPGA
<b>AES (AES-CBC, AES-CTR, AES-GCM); Key Length: 128, 192, 256</b>	Cert. #C426	
<b>AES (AES-ECB, AES-GCM); Key Length 256</b>		2769/2770
<b>Triple-DES (CTR and ECB, 3-key); Key Length: 192</b>	Cert. #C426	
<b>SHS (SHA-1, SHA-256, SHA-384, SHA-512)</b>	Cert. #C426	
<b>HMAC (HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512)</b>	Cert. #C426	
<b>RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)</b>	Cert. #C426	
<b>DRBG (AES-CTR_DRBG)</b>	Cert. #C426	
<b>CVL Components (TLSv1.2 and SSHv2)</b>	Cert. #C426	

**Table 7 Approved Cryptographic Algorithms and Associated Certificate Number**

## 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 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- No parts of the SSH and TLS protocols, other than the KDF, have been tested by the CAVP and CMVP.
- Each of TLSv1.2 (HTTPS/TLS) and SSHv2 protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS) and RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to  $2^{20}$ .
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

**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:

- Diffie-Hellman (Cert. #C426, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (Cert. #C426, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (non-deterministic random number generator)

**Non-Approved Cryptographic Algorithms**

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

- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- DES
- HMAC MD5
- MD5
- RC4
- HMAC-SHA1 is not allowed with key size under 112-bits

## 2.14 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.

### *Power On Self-tests*

- NCS2K FOM Algorithm Implementation POSTs
  - AES (encrypt/decrypt) KATs
  - AES-GCM KAT
  - Triple-DES Encrypt/Decrypt KATs
  - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA KAT (separate KAT for signing; separate KAT for verification)
- Hardware (FPGA) POSTs
  - AES-GCM KAT
- Firmware Integrity Test (32-bit CRC)

### *Conditional Tests*

- NCS2K FOM Algorithm Implementation Conditional Tests
  - CRNGT for approved DRBG
  - CRNGT for NDRNG
  - Pair-Wise Consistency Test for RSA

The module performs all power-on self-tests automatically 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 network interfaces; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a security appliance reboot.

## 2.15 Physical Security

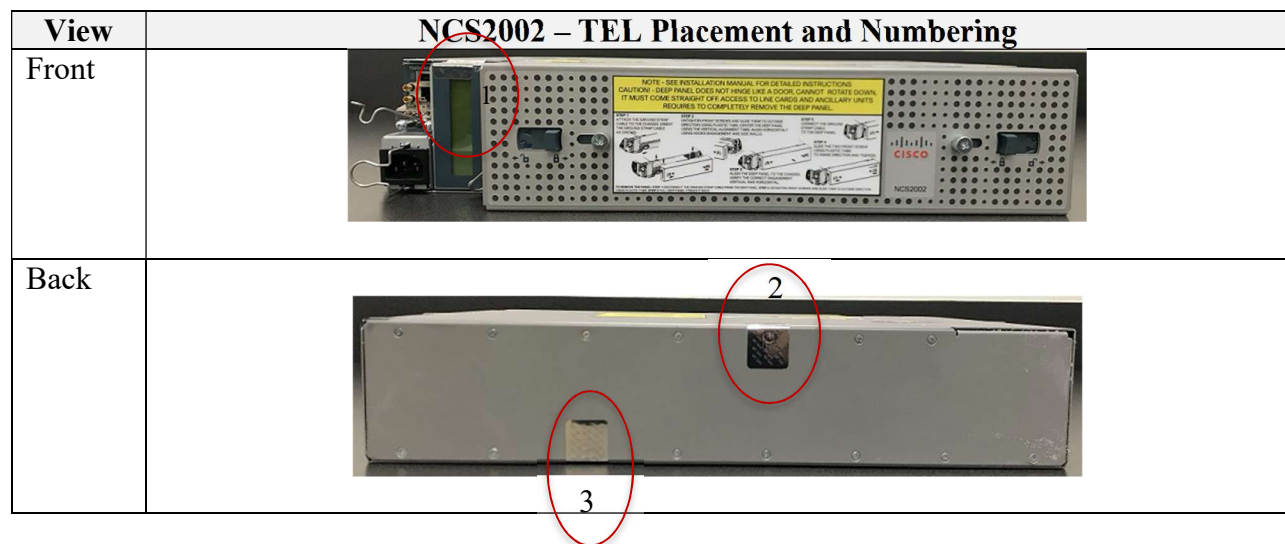
The module is entirely encased by a metal, opaque case. The module natively meets the FIPS 140-2 opacity requirements. However, tamper evident labels are required to meeting the FIPS 140-2 tamper evidence requirements.

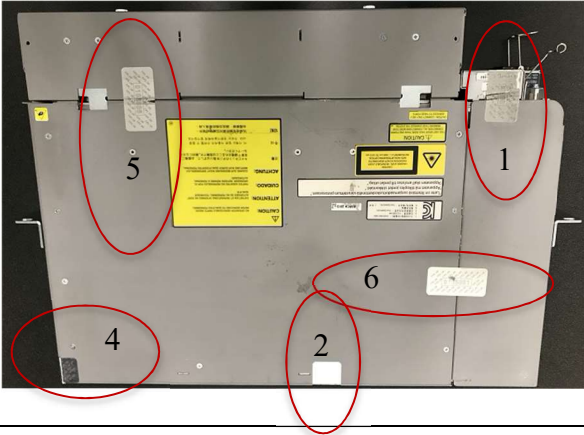
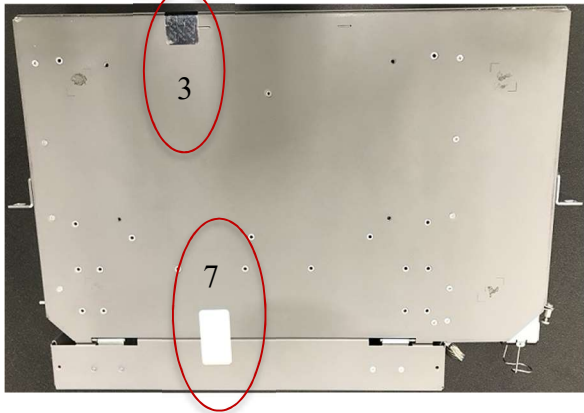
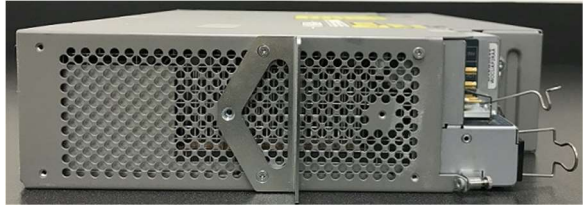
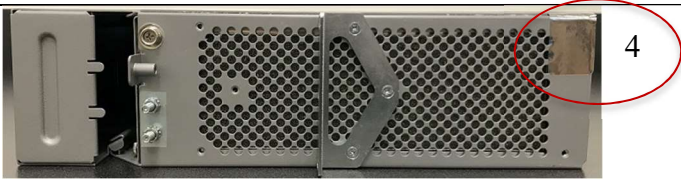
### Tamper Evidence Label (TEL) placement

The tamper evident labels (TELs) shall be installed on the module prior to operating in FIPS mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location. Once the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be physically accessed without signs of tampering. Any attempt to open the NCS2K units will damage the tamper evidence seals or the material of the module cover. Tamper evidence seals can be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices.

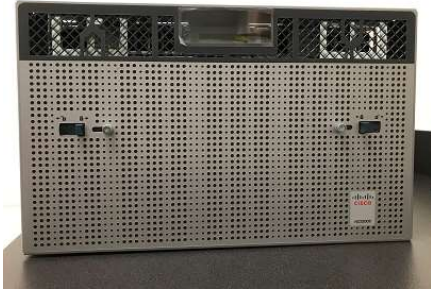
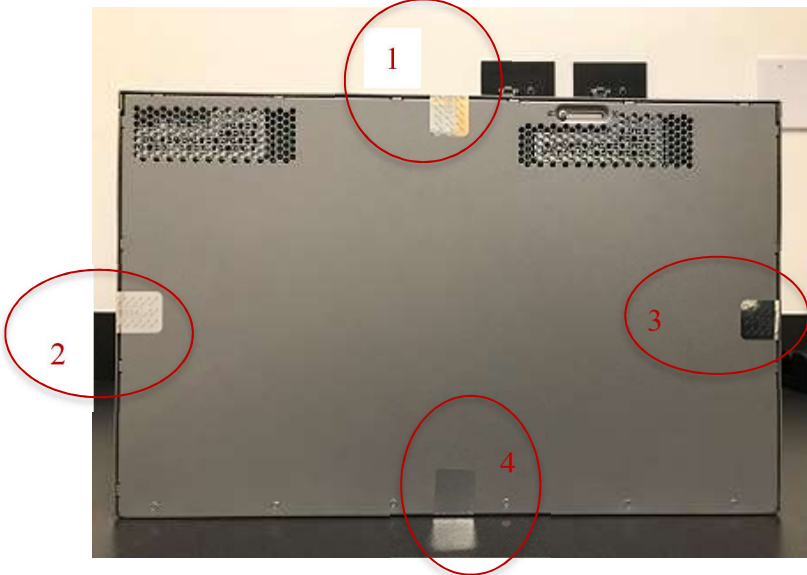
Should the CO have to remove, change or replace TELs for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth. Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in FIPS mode of operation. Returning the system back to FIPS mode of operation requires the replacement of the TELs as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy. To seal the system, apply tamper-evidence labels as depicted in the figures below.

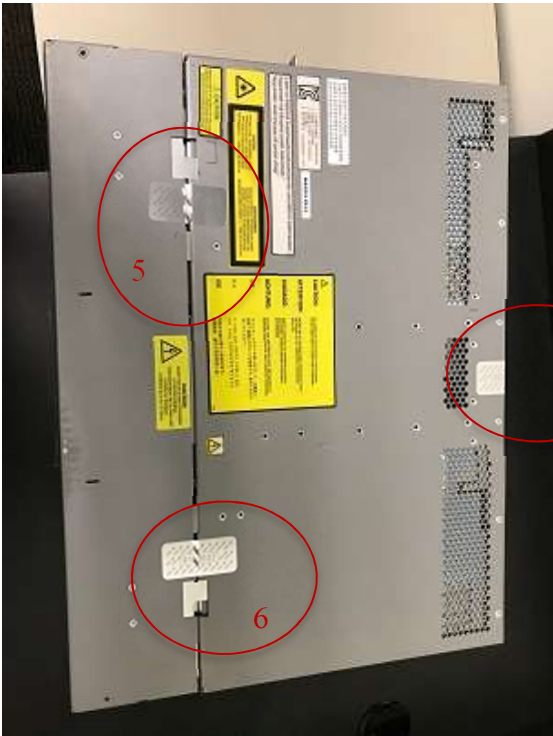
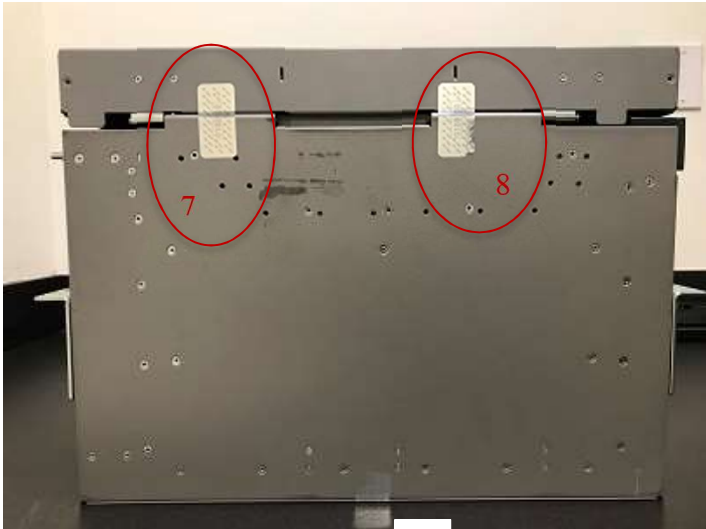
Models	Number Tamper labels	Tamper Evident Labels
Cisco NCS2002	7	AIR-AP-FIPSKIT=
Cisco NCS2006	8	AIR-AP-FIPSKIT=
Cisco NCS2015	8	AIR-AP-FIPSKIT=



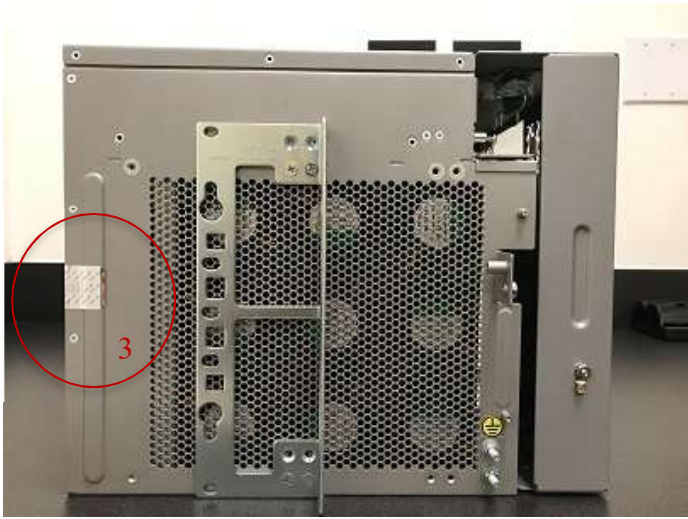
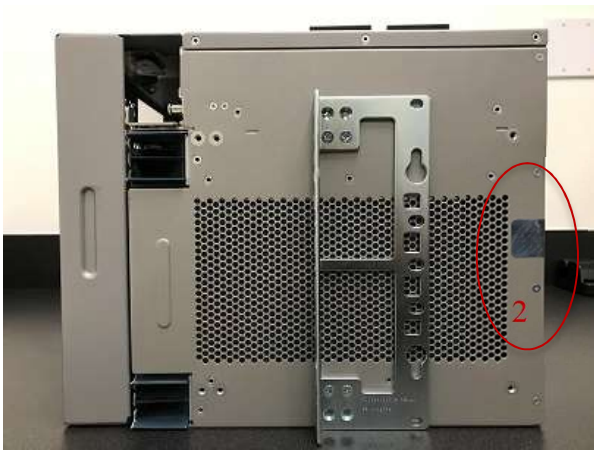
View	NCS2002 – TEL Placement and Numbering
Top	
Bottom	
Left	
Right	

**Table 10: NCS2002 TEL Placement**

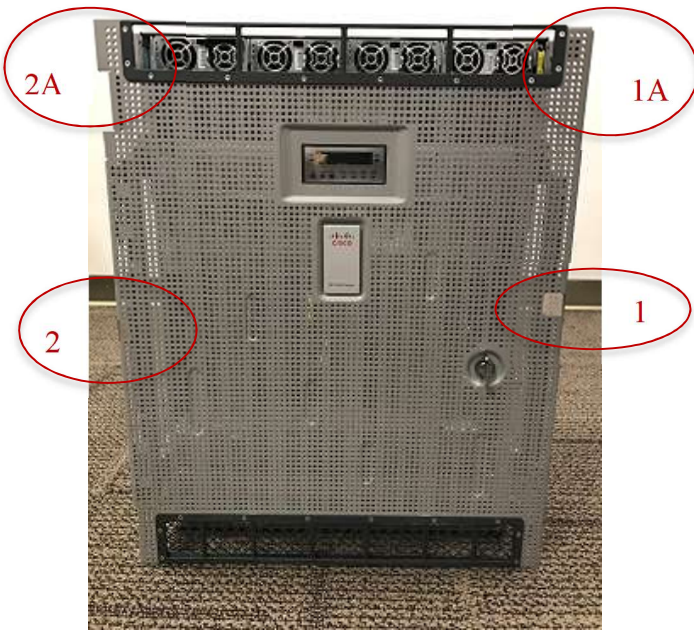
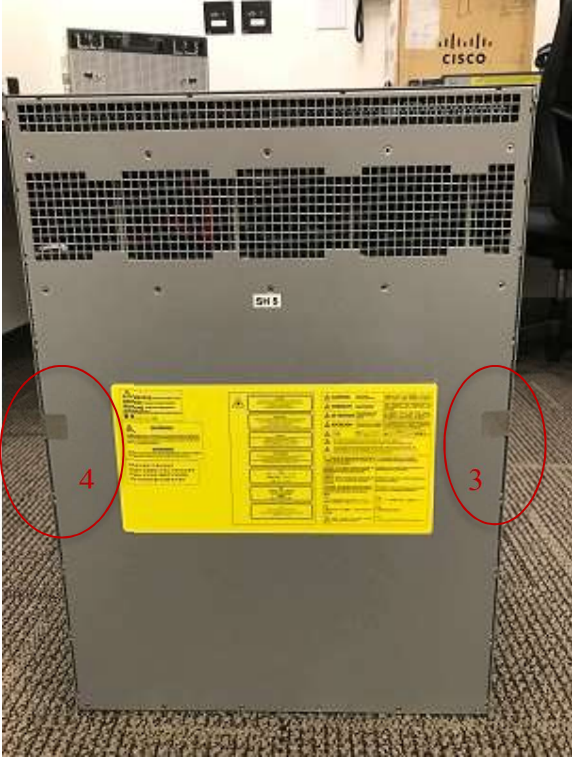
View	NCS2006 – TEL Placement and Numbering
Front	
Back	



View	NCS2006 – TEL Placement and Numbering
Top	 <p>The top view of the NCS2006 chassis shows three TEL placement locations circled in red and numbered: '1' is on the right side panel, '5' is on the top edge near the left door hinge, and '6' is on the bottom edge near the left door hinge. Yellow warning labels are visible on the top edge.</p>
Bottom	 <p>The bottom view of the NCS2006 chassis shows three TEL placement locations circled in red and numbered: '7' and '8' are on the top edge of the front panel, and '4' is on the bottom edge of the front panel.</p>



View	NCS2006 – TEL Placement and Numbering
Left	 <p>The image shows the left side of the NCS2006 chassis. A red circle highlights a small white rectangular label on the left vertical panel, with the number '3' written in red next to it. The chassis features a central vertical slot with a perforated metal mesh and various ports and connectors.</p>
Right	 <p>The image shows the right side of the NCS2006 chassis. A red circle highlights a small blue rectangular label on the right vertical panel, with the number '2' written in red next to it. The chassis features a central vertical slot with a perforated metal mesh and various ports and connectors.</p>

**Table 11: NCS2006 TEL Placement**

View	NCS2015 – TEL Placement and Numbering
Front	 <p data-bbox="365 945 1380 1018">Note: The placement/use of either 2 or 2A and 1 or 1A is dependent on if door handles are installed on unit. See below</p>
Back	

View	NCS2015 – TEL Placement and Numbering
Left (with door handles)	 <p>A photograph showing the left side of a grey NCS2015 TEL unit with its door handles. Four red circles are overlaid on the image, labeled with the numbers 2, 3, 5, and 7. Location 2 is on the right side of the unit, location 3 is on the left side near a yellow warning label, location 5 is at the top center, and location 7 is at the bottom center.</p>
Left (without door handles)	 <p>A photograph showing the left side of a grey NCS2015 TEL unit without its door handles. Four red circles are overlaid on the image, labeled with the numbers 2A, 3, 5, and 7. Location 2A is on the right side of the unit, location 3 is on the left side near a yellow warning label, location 5 is at the top center, and location 7 is at the bottom center.</p>



**Table 12: NCS2015 TEL Placement**

Right  
(with door  
handles)



Right  
(without  
door  
handles)



View	NCS2015 – TEL Placement and Numbering
Top	 <p>The image shows the top view of a white NCS2015 chassis. Two tamper evidence labels are circled in red and numbered: label 5 is on the left side, and label 6 is on the right side. A yellow warning label is visible in the bottom right corner of the chassis.</p>
Bottom	 <p>The image shows the bottom view of the NCS2015 chassis. Two tamper evidence labels are circled in red and numbered: label 7 is on the left side, and label 8 is on the right side. The chassis is resting on a carpeted floor.</p>

### Applying Tamper Evidence Labels

**Step 1:** Turn off and unplug the module before cleaning the chassis and applying labels.

**Step 2:** Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

**Step 3:** Apply a label to cover the module as shown in the figures above.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “FIPS” or “OPEN” may appear if the label was peeled back.

Inspection of the tamper seals should be incorporated into facility security to include how often to inspect and any recording of the inspection. It is recommended inspection of TELs occur at least every 30 days but this is the facilities Security Manager decision.

## 2.16 Secure Operation

The Cisco Network Convergence System 2000 Series Cryptographic Module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are 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.

The module's firmware is installed in the NCS2K by Cisco and cannot be externally loaded so no firmware load test is supported.

### 2.16.1 Initial Setup

- 1 The Crypto Officer must apply tamper evidence labels as described in of this document. Please be aware that the RS232 port (on each Controller Card) that was protected by the front cover of each chassis shall not be used while in FIPS mode.
- 2 On the GUI make the following changes:
  - a. Provisioning/Access
    - i. TL1 – Access: Secure
    - ii. Shell – Access: Secure
    - iii. EMS - Access: Secure
    - iv. Psuedo IOS – Access: Secure
  - b. Provisioning/FIPS
    - i. FIPS: Enabled

### 2.16.2 System Initialization and Configuration

- 1 The Crypto Officer must perform the initial configuration.

### 2.16.3 HTTPS/TLSv1.2 Management Requirements and Cryptographic Algorithms

- 1 When negotiating TLS cipher suites, only FIPS approved algorithms may be specified.
- 2 HTTPS over TLSv1.2 must be used in FIPS mode of operation.
- 3 The following algorithms are not FIPS approved and should not be used in the FIPS-approved mode:
  - a. MD5
  - b. HMAC-MD5
  - c. RC4
  - d. DES

### 2.16.4 SSHv2 Management Requirements and Cryptographic Algorithms

- 1 SSH v2 access to the module is only allowed if SSH v2 is configured to use a FIPS-approved algorithm.

2 Note: All users must still authenticate after remote access is granted.

Remote access is permitted via SSHv2 and HTTPS/TLSv1.2. While in FIPS 140-2 Mode of Operations the modules will enforce use of Approved algorithms for the management protocols.