



## **Cisco Catalyst 3560-C, 3560-X and 3750-X Switches**

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

**Version 0.1**

**February, 14**

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	PURPOSE.....	4
1.2	MODULE VALIDATION LEVEL .....	5
1.3	REFERENCES.....	5
1.4	TERMINOLOGY .....	6
1.5	DOCUMENT ORGANIZATION .....	6
<b>2</b>	<b>CISCO CATALYST 3560-C, 3560-X AND 3750-X SERIES SWITCHES.....</b>	<b>7</b>
2.1	CRYPTOGRAPHIC MODULE PHYSICAL CHARACTERISTICS .....	8
2.2	MODULE INTERFACES.....	8
<b>3</b>	<b>ROLES, SERVICES, AND AUTHENTICATION .....</b>	<b>12</b>
3.1	USER ROLE .....	12
3.2	CO ROLE .....	13
3.3	SERVICES.....	13
<b>4</b>	<b>PHYSICAL SECURITY.....</b>	<b>14</b>
4.1	MODULE OPACITY .....	14
4.2	TAMPER EVIDENCE.....	16
<b>5</b>	<b>CRYPTOGRAPHIC ALGORITHMS .....</b>	<b>22</b>
5.1.1	<i>Approved Cryptographic Algorithms.....</i>	<i>22</i>
5.1.2	<i>Non-Approved Algorithms .....</i>	<i>22</i>
5.1.3	<i>Self-Tests .....</i>	<i>23</i>
<b>6</b>	<b>CRYPTOGRAPHIC KEY/CSP MANAGEMENT.....</b>	<b>24</b>
<b>7</b>	<b>SECURE OPERATION OF THE 3560C/3560X/3750X SERIES SWITCHES .....</b>	<b>28</b>
7.1	INITIAL SETUP .....	28
7.2	SYSTEM INITIALIZATION AND CONFIGURATION.....	28
7.3	REMOTE ACCESS .....	29
<b>8</b>	<b>RELATED DOCUMENTATION.....</b>	<b>30</b>
<b>9</b>	<b>OBTAINING DOCUMENTATION.....</b>	<b>30</b>
9.1	CISCO.COM .....	30
9.2	PRODUCT DOCUMENTATION DVD .....	30
9.3	ORDERING DOCUMENTATION .....	30
<b>10</b>	<b>DOCUMENTATION FEEDBACK.....</b>	<b>31</b>
<b>11</b>	<b>CISCO PRODUCT SECURITY OVERVIEW .....</b>	<b>31</b>
11.1	REPORTING SECURITY PROBLEMS IN CISCO PRODUCTS.....	31
<b>12</b>	<b>OBTAINING TECHNICAL ASSISTANCE .....</b>	<b>32</b>

12.1	CISCO TECHNICAL SUPPORT & DOCUMENTATION WEBSITE .....	32
12.2	SUBMITTING A SERVICE REQUEST .....	33
12.3	DEFINITIONS OF SERVICE REQUEST SEVERITY .....	33
<b>13</b>	<b>OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION.....</b>	<b>33</b>
<b>14</b>	<b>DEFINITION LIST.....</b>	<b>35</b>

# 1 Introduction

## 1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 3560-C, 3560-X and 3750-X series switches. This security policy describes how the modules listed below meet the security requirements of FIPS 140-2, and how to operate the router with on-board crypto enabled in a secure FIPS 140-2 mode. Modules covered in this document are listed below:

- 3560-C switches
  - 3560CG-8PC-S
  - 3560CG-8TC-S
  - 3560CPD-8PT-S
- 3560-X switches
  - WS-C3560X-24P-L
  - WS-C3560X-48T-L
- 3750-X switches
  - WS-C3750X-12S
  - WS-C3750X-24S
  - WS-C3750X-24T
  - WS-C3750X-48P
  - WS-C3750X-48T
- Service module
  - C3KX-SM-10G
- Network Field Replaceable Uplink (FRU<sup>1</sup>) module
  - C3KX-NM-1G
  - C3KX-NM-10G
  - C3KX-NM-BLANK
  - C3KX-NM-10GT
- IOS Software Version - 15.0(2)SE3
- C3KX-FIPS-KIT 700-34443-01
- C3KX-FIPS-KIT 47-25129-01

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Catalyst 3560-C, 3560-X and 3750-X series switches.

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>.

---

<sup>1</sup> The FRUlink modules implement no FIPS 140-2 security functions and are considered equivalent for the purposes of this security policy with the exception of physical security opacity requirements.

## 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	2
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 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 routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco products.

Please refer to the following websites for:

Catalyst 3560-C series switches -

<http://www.cisco.com/en/US/products/ps11290/index.html>

Catalyst 3560-X series switches –

<http://www.cisco.com/en/US/products/ps10744/index.html>

Catalyst 3750-X series switches –

<http://www.cisco.com/en/US/products/ps10745/index.html>

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at [www.cisco.com](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 Catalyst 3560-C, 3560-X and 3750-X switches are referred to as the switch.

## ***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 Catalyst 3560-X, 3560-C and 3750-X series switches and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

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

## **2 Cisco Catalyst 3560-C, 3560-X and 3750-X series switches**

The 3560-C series – Cisco® Catalyst® compact switches easily extend an intelligent, fully managed Cisco Catalyst wired switching infrastructure, including end-to-end IP and Borderless Network services, with a single Ethernet cable or fiber from the wiring closet. These attractive, small form-factor Gigabit and Fast Ethernet switches are ideal for connecting multiple devices on the retail sales floor and for extending wireless LAN networks: wherever space is at a premium and multiple cable runs could be challenging. These switches deliver advanced Layer 2 switching with intelligent Layer 2 through 4 services for the network edge, such as voice, video, and wireless LAN services, including support for routed access, Cisco TrustSec®, Media Access Control Security (MACsec), and other Cisco Borderless Network services. These models also include Power over Ethernet (PoE) pass-through that enables the compact switch to draw power from the wiring closet and pass it to end devices. The Cisco® Catalyst® 3750-X and 3560-X Series Switches are enterprise-class stackable switches that provide high availability, scalability, security, energy efficiency, and ease of operation with innovative features such as Cisco StackPower, Power over Ethernet Plus (PoE+), optional network modules, redundant power supplies, and MAC security. The Catalyst 3750-X 3560-X and 3560-C Series Switches meet FIPS 140-2 overall Level 2 requirements as multi-chip standalone modules.

The 3560-C, 3560-X and 3750-X series switches include cryptographic algorithms implemented in IOS software as well as hardware ASICs. The module provides 802.1X-rev with MACSec and MACSec Key Agreement (MKA), Cisco TrustSec (CTS), RADIUS, TACACS+, HTTPS, SNMPv3 and SSHv2. The module implements Layer 2 MACsec / IEEE 802.1AE on the downlink ports using a hardware cryptographic implementation (MACSec PHY) of AES-GCM. The module's IOS software implements 128 bit AES-CBC, CTR-DRBG, SHA-1, HMAC-SHA-1 and RSA. Media Access Control Security (MACsec), defined in 802.1AE, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful key establishment using the 802.1x Extensible Authentication Protocol (EAP) framework.

## 2.1 *Cryptographic Module Physical Characteristics*



**Figure 1- Cisco 3560-C series switch**



**Figure 2 - Cisco 3560-X and 3750-X series switch**

The 3560-C series switches are a line of small form factor, fixed chassis switches. Of the configurations considered in this security policy, three models have 8 Gigabit Ethernet ports, one has 8 Fast Ethernet ports and one has 12 Fast Ethernet ports. With the exception of two models, all switches possess at least 8 PoE+ ports. More details on the interfaces are provided in the table in the following section.

## 2.2 *Cryptographic Boundary*

The cryptographic boundary is defined as being the physical enclosure of the chassis. All of the functionality described in this publication is provided by components within this cryptographic boundary.



## 2.3 Module 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 module also supports a power interface.

The following table identifies the differences between the models of switches covered by this Security Policy:

Model	Ethernet Ports	PoE Output Ports	Available PoE Power	Uplinks	MACsec
3560CG-8TC-S	8 x 10/100/1000 Gigabit Ethernet	N/A		2 x 1G copper or 1G SFP	Yes
3560CG-8PC-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE+	124W	2 x 1G copper or 1G SFP	Yes
3560CPD-8PT-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE	Up to 15.4W	2 x 1G (PoE+ input)	Yes

**Table 2 - 3560-C Interface information**

Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power	MACSec
WS-C3560X-48T-L	48	350W	-	Yes
WS-C3560X-24P-L	24 PoE+	715W	435W	Yes

**Table 3 - 3560-X Interface information**

Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
WS-C3750X-24T	24	350W	-
WS-C3750X-48T	48		
WS-C3750X-48P	48 PoE+		

WS-C3750X-12S	12 GE SFP	350W+	-
WS-C3750X-24S	24 GE SFP	350W	-

**Table 4 - 3750-X Interface information**

Model	1G SFP Ports	10G SFP+ Ports
C3KX-NM-1G	4	0
C3KX-NM-10G	0	2
C3KX-NM-10GT	0	2
C3KX-NM-BLANK	N/A	N/A
C3KX-SM-10G	0	2

**Table 5 - Network/Service Modules Interface information**

**Note:** Please notice that the Network/Service modules listed in table 5 above are only available on each of Cisco Catalyst 3750-X and 3560-X switches to provide up to 2 x 10 Gigabit uplinks. Each configuration used in 3750-X and 3560-X must use one of each Network/Service modules listed in table 5 above. There is no network/service slot on each of Cisco Catalyst 3560-C switches.

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

Physical Interface	Logical Interface
MACsec 1G Ethernet Ports,  Type A USB port Console Port (RJ45 and USB Type B) Mgmt Port	Data Input Interface
MACsec 1G Ethernet Ports,	Data Output Interface

Type A USB port Console Port (RJ45 and USB Type B) Mgmt Port	
Console Port (RJ45 and USB Type B), Mgmt Port MACsec 1G Ethernet Ports, Reset Button	Control Input Interface
Console Port (RJ45 and USB Type B) Mgmt Port LEDs	Status Output Interface
Power Plug, PoE+ Ethernet Ports	Power Interface

**Table 6 – FIPS 140-2 Logical Interfaces 3560-C Switches**

Physical Interface	Logical Interface
MACsec 1G Ethernet Ports, FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports Service Module 10G SFP+ Ports Stackwise+ ports (only on 3750-x models) Type A USB port Console Port (RJ45 and USB Type B) Mgmt Port	Data Input Interface
MACsec 1G Ethernet Ports, FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports Service Module 10G SFP+ Ports Stackwise+ ports (only on 3750-x models) Type A USB port Console Port (RJ45 and USB Type B) Mgmt Port	Data Output Interface
Console Port (RJ45 and USB Type B), Mgmt Port MACsec 1G Ethernet Ports, FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports	Control Input Interface

Service Module 10G SFP+ Ports Stackwise+ ports (only on 3750-x models), Reset Button	
Console Port (RJ45 and USB Type B) Mgmt Port Type A USB port MACsec 1G Ethernet Ports, FRUlink 1G SFP Ports, FRUlink 10G SFP+ Ports, Service Module 10G SFP+ Ports LEDs Stackwise+ ports (only on 3750-x models),	Status Output Interface
Power Plug, PoE+ Ethernet Ports Stackwise+ ports (only on 3750-x models)	Power Interface

**Table 7 – FIPS 140-2 Logical Interfaces 3560-X/3750-X**

### **3 Roles, Services, and Authentication**

Authentication is role-based. Each user is authenticated upon initial access to the module. There are two roles in the Switch that may be assumed the Crypto Officer (CO) role and the User role. The administrator of the Switch assumes the CO role in order to configure and maintain the Switch using CO services, while the Users exercise security services over the network.

#### **3.1 User Role**

The role assumed by users obtaining general security services. From a logical view, user activity exists in the data-plane. Users are authenticated using EAP methods and 802.1X-REV, and their data is protected with 802.1AE protocols.

EAP and 802.1X-REV can use password based credentials for User role authentication – in such a case the user passwords must be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). 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. The calculation should be  $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251,596,800$ ). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

EAP and 802.1X-REV can also authenticate User role via certificate credentials by using 2048 bit RSA keys – in such a case the security strength is 112 bits, so the associated probability of a successful random attempt is 1 in  $2^{112}$ , which is less than 1 in 1,000,000 required by FIPS 140-2.

### 3.2 CO Role

This role is assumed by an authorized CO connecting to the switch via CLI through the console port and performing management functions and module configuration. Additionally the stack master (in stacking scenario for 3750-X switches) is considered CO for stack members. From a logical view, CO activity exists only in the control plane. IOS prompts the CO for their username and password, if the password is validated against the CO's password in IOS memory, the user is allowed entry to the IOS executive program. A CO can assign permission to access the CO role to additional accounts, thereby creating additional COs. The module supports RADIUS and TACACS+ for authentication of COs.

CO passwords must be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). 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. The calculation should be  $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251,596,800$ ). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

Additionally on a stack, the CO is authenticated via possession of SESA Authorization key that is 128 bits long. So an attacker would have a 1 in  $2^{128}$  chance of a successful authentication which is much stronger than the one in a million chance required by FIPS 140-2.

### 3.3 Services

Role	Authentication Method	Services
User	EAP and 802.1X-REV Authentication, Local database, TACACS+ or RADIUS	MACsec Network Functions: authentication, access control, confidentiality and data integrity services provided by the MACsec protocol.
Cryptographic Officer	Local database, TACACS+ or RADIUS, SESA	Configure the switch: define network interfaces and settings, create command aliases, set the protocols the switch will support, enable interfaces and network services, set system date and time, and load authentication information.  Management protocols: remote access to the switch via SSHv2, TLS or SNMPv3.  Status functions: view the switch configuration, routing tables,

		and active sessions; view health, temperature, memory status, voltage, and packet statistics; review accounting logs, and view physical interface status.  Set Encryption/Bypass: Place module into Encryption or Bypass state.  Perform Self Tests: Perform the FIPS 140 start-up tests on demand
<b>Unauthenticated</b>	<b>N/A</b>	Show status (viewing LEDs), passing traffic through the device, power-cycling the device.  Perform Self Tests: occurs upon system startup

**Table 8 - Services**

## 4 Physical Security

This module is a multi-chip standalone cryptographic module.

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front and side panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence. The following sections illustrate the physical security provided by the module.

The following table shows the number of tamper evident labels and opacity shields that shall be installed for the module to operate in a FIPS approved mode of operation. The CO is responsible for securing and having control at all times of any unused tamper evident labels.

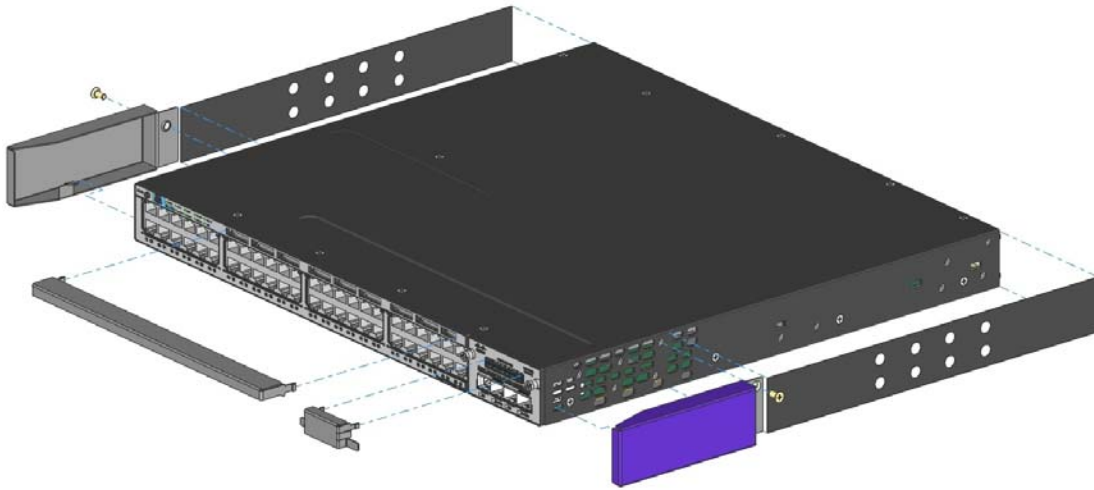
Face	3750x/3560x		3560c	
	Tamper Evident Labels	Opacity Shields	Tamper Evident Labels	Opacity Shields
Front	5	2	N/A	N/A
Left	6	2	1	N/A
Right	6	2	N/A	N/A
Back	8	N/A	N/A	N/A
Top	N/A	N/A	1	1
Bottom	N/A	N/A	4	N/A
<b>Total</b>	<b>25</b>	<b>6</b>	<b>6</b>	<b>1</b>

**Table 9 - Tamper Evident Labels and Opacity Shields – All Models**

### 4.1 Module Opacity

To install an opacity shield, follow these steps:

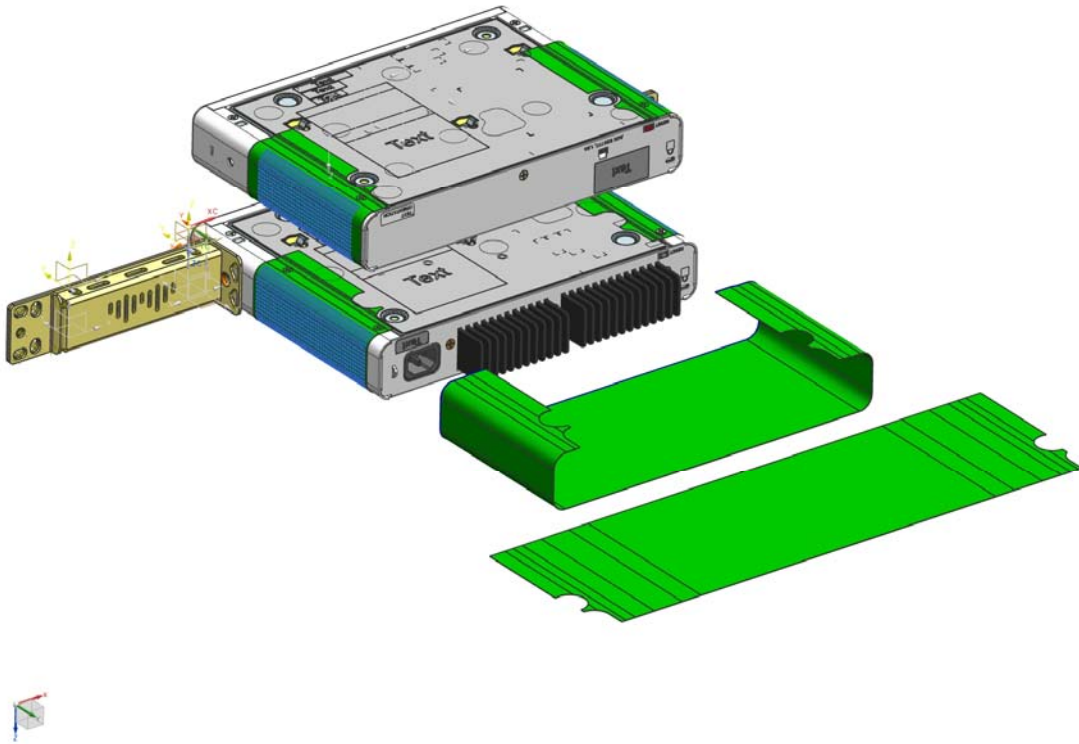
- Open the FIPS kit (part numbers: C3KX-FIPS-KIT 700-34443-01 for 3560X and 3750X or C3KX-FIPS-KIT 47-25129-01 for 3560C). The kit contains:
  - a. Opacity shields for front and sides
  - b. Tamper evident labels
- 2. Apply the opacity shields as per the diagram below



**Figure 3a) - Opacity Shields<sup>2</sup> for 3750x/3560x**

---

<sup>2</sup> WS-C3750X-12S and WS-C3750X-24S modules do not need opacity shields on the front face.

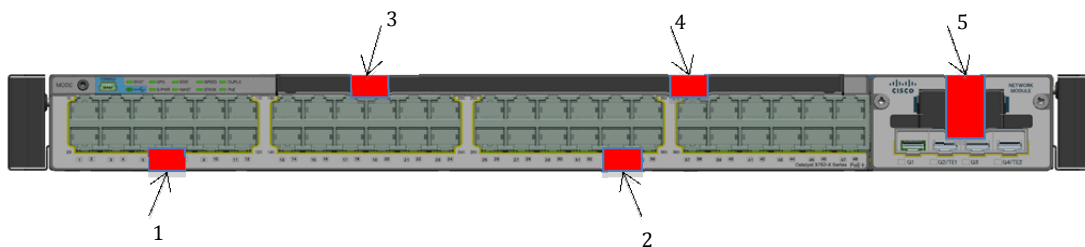


**Figure 3b) - Opacity Shields for 3560c**

## 4.2 Tamper Evidence

Once the module has been configured to meet overall FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. The CO shall inspect for signs of tampering periodically.

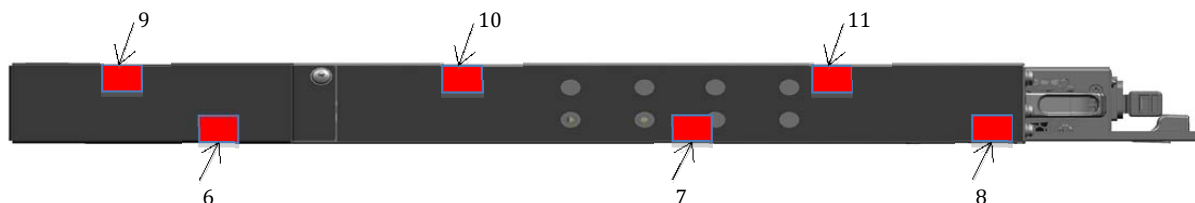
To seal the system, apply serialized tamper-evidence labels as depicted in the figures below. This label placement is applicable to the C3560-X and the C3750-X models included in this validation.



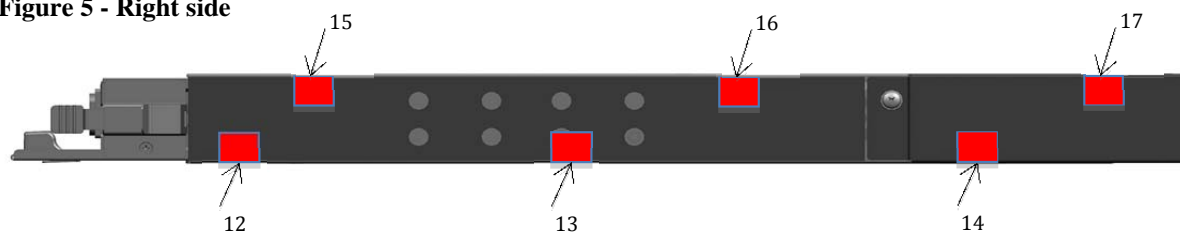
**Figure 4 - Front face**

© Copyright 2010 Cisco Systems, Inc.

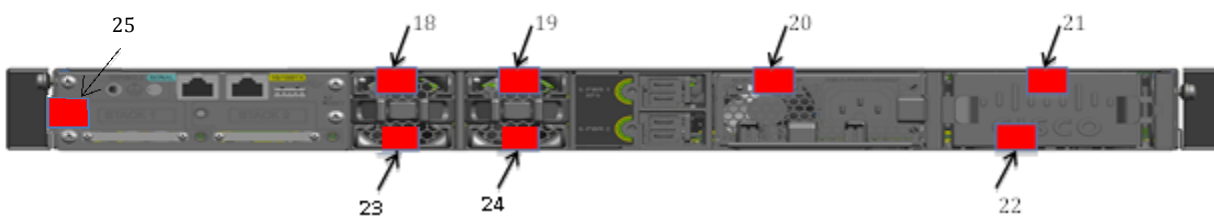




**Figure 5 - Right side**



**Figure 6 - Left side**



**Figure 7 - Rear face<sup>3</sup>**

Note: No extra TELs are required to be put on the top or bottom side of each C3560-X or C3750-X model while in the FIPS mode.

<sup>3</sup> TEL #20 is used to protect the power supply unit

The 3560C tamper evident labels are detailed in the following photographs.

### Group 1: 3560CG-8PC-S



Figure 8 - Front of 3560CG-8PC-S



Figure 9- Right side of 3560CG-8PC-S



Figure 10- Left side of 3560CG-8PC-S



Figure 11- Back of 3560CG-8PC-S



Figure 12- Top of 3560CG-8PC-S



Figure 13- Bottom of 3560CG-8PC-S

## Group 2: C3560CG-8TC-S

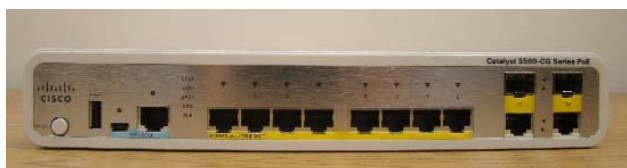


Figure 14- Front of C3560CG-8TC-S



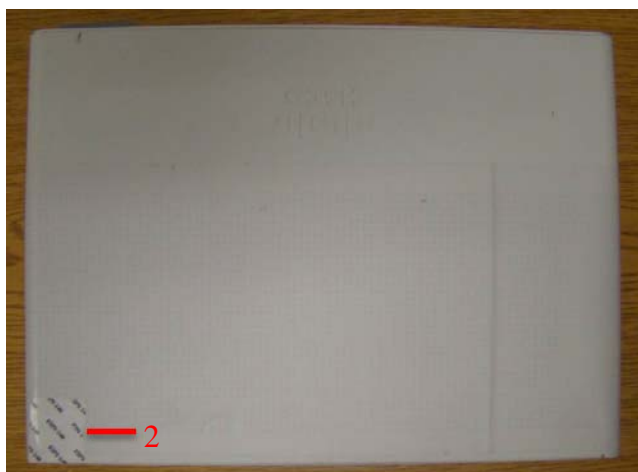
Figure 15- Right side of C3560CG-8TC-S



Figure 16- Left side of C3560CG-8TC-S



Figure 17- Rear of C3560CG-8TC-S

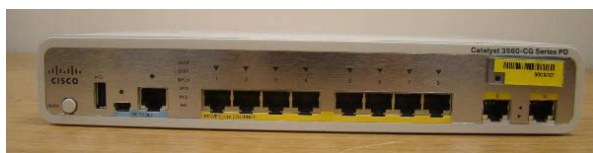


**Figure 18- Top of C3560CG-8TC-S**



**Figure 19- Bottom of 3560CG-8PT-S**

### **Group 3: 3560CPD-8PT-S**



**Figure 20- Front of 3560CPD-8PT-S**



**Figure 21- Right side of 3560CPD-8PT-S**



Figure 22- Left side of 3560CPD-8PT-S



Figure 23- Rear of 3560CPD-8PT-S

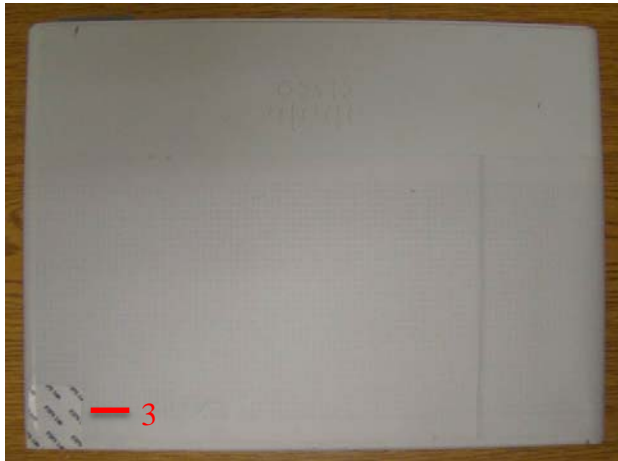


Figure 24- Top of 3560CPD-8PT-S



Figure 25- Bottom of 3560CPD-8PT-S

## 5 Cryptographic Algorithms

### 5.1.1 Approved Cryptographic Algorithms

The Cisco Switches 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 Switches for use in the FIPS mode of operation.

Algorithm	Implementation	CAVP Certificate
AES	<i>CBC – IOS Common Crypto Module</i>	<i>2134</i>
	<i>ECB – MACsec PHY</i>	<i>1024</i>
	<i>GCM – MACsec PHY</i>	<i>1275</i>
	<i>GCM – MACsec PHY (Service Module)</i>	<i>1269</i>
HMAC	<i>IOS Common Crypto Module</i>	<i>1304</i>
DRBG	<i>IOS Common Crypto Module</i>	<i>237</i>
RSA	<i>IOS Common Crypto Module</i>	<i>1100</i>
SHS	<i>IOS Common Crypto Module</i>	<i>1858</i>
Triple-DES	<i>IOS Common Crypto Module</i>	<i>1358</i>

**Table 10 - FIPS-Approved Algorithms for use in FIPS Mode**

### 5.1.2 Non-Approved Algorithms

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

- DES
- HMAC-MD5
- MD5
- RC4

In addition, the modules support the following key establishment schemes allowed in FIPS mode:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- AES (Cert. #2134, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)

### 5.1.3 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 ensure all components are functioning correctly. The modules implement the following power-on self-tests:

- IOS Known Answer Tests:
  - AES KAT
  - AES-CMAC KAT
  - AES-GCM KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-512 KAT
  - DRBG KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SHA-512 KAT
  - RSA KAT
  - Triple-DES KAT
- MAC PHY (Service Module PHY included) crypto Known Answer Tests:
  - AES-GCM KAT
- Firmware Integrity Test
  - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior any other operations; this prevents the module from passing any data during a power-on self-test failure.

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

- Continuous Random Number Generator Test for the FIPS-approved RNG
- Continuous Random Number Generator Test for the non-approved RNG
- Pairwise Consistency Test for RSA
- Conditional IPSec Bypass Test
- Conditional MACSec Bypass Test

## 6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the CO role login, and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Note that the command **fips zeroize all** will zeroize a large majority of the listed CSPs. The CTS specific CSPs will require the **cts key zeroize** CLI.

The module supports the following secret and private keys and critical security parameters (CSPs):

ID	Algorithm	Size	Description	Storage	Zeroization Method
<b>General Keys/CSPs</b>					
User Password	Password	Variable (8+ characters)	Used to authenticate local users	NVRAM (plaintext)	Zeroized by overwriting with new password
Enable Secret	Password	Variable (8+ characters)	Used to authenticate local users at a higher privilege level	NVRAM (plaintext)	Zeroized by overwriting with new password
RADIUS secret	Shared Secret	Variable (8+ characters)	The RADIUS Shared Secret	NVRAM (plaintext)	# no radius-server key
RADIUS Key wrap key	AES	128/256 bits	Used to protect SAK	DRAM (plaintext)	Zeroized when data structure is freed
TACACS+ secret	Shared Secret	Variable (8+ characters)	The TACACS+ shared secret	NVRAM (plaintext)	# no tacacs-server key
DRBG entropy input	SP 800-90 CTR_DRBG	256-bits	HW based entropy source output used to construct seed	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG seed	SP 800-90 CTR_DRBG	384-bits	Input to the DRBG that determines the internal state of the DRBG	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG V	SP 800-90 CTR_DRBG	128-bits	Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Automatically when the switch is power cycled



DRBG Key	SP 800-90 CTR_DRBG	256-bits	This is the 256-bit DRBG key used for SP 800-90 CTR_DRBG	DRAM (plaintext)	Automatically when the switch is power cycled
Diffie-Hellman private key	DH	2048-4096 bits	The private exponent used in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Automatically after shared secret generated.
Diffie-Hellman Shared Secret	DH	2048-4096 bits	This is the shared secret agreed upon as part of DH exchange	DRAM (plaintext0)	Zeroized upon deletion
<b>SSH</b>					
SSH RSA private key	RSA	2048 bits	SSH key	NVRAM (plaintext)	# fips zeroize all
SSH session key	Triple-DES/AES	168-bits/256-bits	This is the SSH session symmetric key.	DRAM (plaintext)	Automatically when SSH session terminated
SSH session authentication key	HMAC SHA-1	160-bits	This is the SSH session authentication key	DRAM (plaintext)	Automatically when SSH session terminated
<b>TLS</b>					
TLS Server RSA private key	RSA	2048 bits	Identity certificates for module itself and also used in TLS negotiations.	NVRAM (plaintext)	# fips zeroize all
TLS pre-master secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated.
TLS session keys	Triple-DES/AES	168-bits/256-bits	This is the TLS session key	DRAM (plaintext)	Automatically when session terminated.
<b>MacSec</b>					
MACsec Security Association Key (SAK)	AES-GCM	128 bits	Used for creating Security Associations (SA) for encrypting/decrypting the MACSec traffic in the MACSec hardware.	MACsec PHY (plaintext)	Automatically when session expires
MACsec Connectivity Association	AES-GCM	128 bits	A secret key possessed by members of a MACSec connectivity	MACsec PHY (plaintext)	Automatically when session expires

Key (CAK)			association.		
MACsec KEK	AES-GCM	128 bits	Used to transmit SAKs to other members of a MACSec connectivity association	MACsec PHY (plaintext)	Automatically when session expires
MACsec ICK	secret	128 bits	Used to verify the integrity and authenticity of MPDUs	MACsec PHY (plaintext)	Automatically when session expires
<b>SESA</b>					
SESA Authorization Key	AES	128 bits	Used to authorize members of a single stack on Incredible Units. Used as input to SP800-108 derivation methods to derive four additional 128 fields to transfer the Master Session Key and additional aggressive exchange material	NVRAM (plaintext)	"no fips authorization-key"
SESA Master Session Key	AES	128 bits	Used to derive SESA session key	DRAM (plaintext)	Upon completion of key exchange
SESA Derived Session Keys	AES and HMAC-SHA-1	128 bits and 192 bits	Used to protect traffic over stacking ports	DRAM (plaintext)	Upon bringing down the stack
<b>CTS</b>					
Pairwise Master Key (PMK)	SAP/AES-GCM	256 bits	The PMK is used to derive the PTK (Pairwise Transient Key) which in turn is used in the session encryption (symmetric) key generation process.	NVRAM (plaintext)	"cts key zeroize" CLI
Protected Access Credential (PAC) Key	AES-CBC	256 bits	The PAC (Protected Access Credential) is dynamically provisioned in EAP-FAST phase 0 The PAC-key is a shared secret that is used to secure further communications.	NVRAM (plaintext)	"clear cts pacs" CLI

Pairwise Transient Key (PTK)	SAP/AES-GCM	256 bits	Used to encrypt SAP payloads during SAP protocol implementations.	DRAM (plaintext)	Zeroized automatically when SAP implementation is terminated
Key Confirmation Key (KCK)	SAP/AES-GCM	160 bits	Used to protect SAP payloads integrity during SAP protocol implementations	DRAM (plaintext)	Zeroized automatically when SAP implementation is terminated
<b>IPSec</b>					
skeyid	Shared Secret	160 bits	Used for key agreement in IKE. This key was derived in the module	DRAM (plaintext)	Automatically when session expires
skeyid_d	Shared Secret	160 bits	Used for key agreement in IKE	DRAM (plaintext)	Automatically when session expires
IKE session encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Derived in the module used for IKE payload integrity verification	DRAM (plaintext)	Automatically when session expires
IKE session authentication key	HMAC-SHA1	160 bits	HMAC-SHA1 key	DRAM (plaintext)	Automatically when session expires
ISAKMP preshared	pre-shared key	8 characters	This key was configured by CO and used for User role authentication using IKE Pre-shared key based authentication mechanism	DRAM (plaintext)	Automatically when session expires
IKE RSA Authentication private Key	RSA	2048 bits	private key used for IKE protocol during the handshake	NVRAM	# fips zeroize all
IPSec Authentication key	HMAC-SHA1	160 bits	used to authenticate the IPSec peer	DRAM (plaintext)	Automatically when session expires
IPSec encryption key	TRIPLE-DES/AES	168-bit TRIPLE-DES or a 256-bit AES	Used to Secure IPSec traffic	DRAM (plaintext)	Automatically when session expires

**Table 11 – Secret and private keys and CSPs**

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below.

Role	Service	Critical Security Parameters
User Role	MACsec Network Functions	RNG Seed, RNG Seed key, DH private exponent, DH Shared Secret MACsec Security Association Key, MACsec Connectivity Association Key, MACsec KEK, MACsec ICK <b>(X)</b>
Crypto-Officer Role	Manage the Switch	TLS Server RSA private key, SSH RSA private key, RADIUS secret, TACACS+ secret, RADIUS key wrap key, User Password, Enable Password, SESA Authorization Key <b>(R/W/D)</b>
Crypto-Officer Role	Management Protocols	TLS Server RSA private key, TLS pre-master secret, TLS session key, SSH RSA private key, SSH session key, RADIUS secret, TACACS+ secret, SESA Master Session Key, SESA Derived Session key <b>(X)</b>

R=Read, W=Write, D=Zeroize, X=Execute

**Table 12 - Role CSP Access**

## 7 Secure Operation of the 3560c/3560x/3750x series switches

The switches meet all the overall Level 2 requirements for FIPS 140-2. Follow the setup instructions provided below to place the module in FIPS-approved mode. Operating this Switch without maintaining the following settings will remove the module from the FIPS approved mode of operation.

### 7.1 Initial Setup

1. The CO must apply opacity shield and tamper evidence labels as described above.

### 7.2 System Initialization and Configuration

1. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the “configure terminal” command line, the CO enters the following syntax:

**config-register 0x0F**

2. The CO must create the “enable” password for the CO role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the CO first engages the “enable” command. The CO enters the following syntax at the “#” prompt:

**Switch(config)# enable secret [PASSWORD]**

3. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the “configure terminal” command line, the CO enters the following syntax:

**Switch(config)# line con 0**  
**Switch(config)# password [PASSWORD]**  
**Switch(config)# login local**

4. To ensure all FIPS 140-2 logging is received, set the log level:

**Switch(config)# logging console errors**

5. The CO enables secure stacking (SESA) but configuring the Authorization key:

**Switch(config)# fips authorization-key <128 bit, i.e, 16 hex byte key>**

6. The CO may configure the module to use RADIUS or TACACS+ for authentication. If the module is configured to use RADIUS, the Crypto-Officer must define RADIUS or shared secret keys that are at least 8 characters long, including at least one letter and at least one number.

7. To enable MACsec:

- a. First configure the MKA Protocol:

**Switch(config)# mka policy *policy-name***

**Switch(config-mka-policy)# replay-protection window-size 300**

**Switch(config-mka-policy)# end**

- b. Then configure MACsec on the desired interfaces:

**Switch(config-if)# macsec**

**Switch(config-if)# authentication host-mode multi-domain**

**Switch(config-if)# authentication linksec policy must-secure**

**Switch(config-if)# authentication port-control auto**

**Switch(config-if)# authentication violation protect**

**Switch(config-if)# mka policy *policy-name***

**Switch(config-if)# dot1x pae authenticator**

**Switch(config-if)# end**

8. The CO shall only assign users to a privilege level 1 (the default).
9. The CO shall not assign a command to any privilege level other than its default.

### **7.3 Remote Access**

1. Remote access is permitted via SSHv2, TLS and SNMPv3. While in FIPS 140-2 Mode of Operations the switches will enforce use of Approved algorithms for the management protocols. Please be aware that, as per NIST Implementation Guidance (IG) D.8, scenario 4, those protocols and associated Key Derivation Functions (KDFs) are allowed to be used in FIPS mode but are non-compliant.

## 8 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.

## 9 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.

### 9.1 *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](http://www.cisco.com/public/countries_languages.shtml)

### 9.2 *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/>

### 9.3 *Ordering Documentation*

Beginning June 30, 2005, 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](mailto: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.

## 10 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](mailto: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.

## 11 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](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://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

### 11.1 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 a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — [security-alert@cisco.com](mailto: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 nonemergencies.

- Nonemergencies — [psirt@cisco.com](mailto: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](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.

## 12 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.

### 12.1 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.

## ***12.2 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>

## ***12.3 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.

## **13 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>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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>

## **14 Definition List**

AES – Advanced Encryption Standard

CMVP – Cryptographic Module Validation Program

CSEC – Communications Security Establishment Canada

CSP – Critical Security Parameter

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

HTTP – Hyper Text Transfer Protocol

KAT – Known Answer Test

LED – Light Emitting Diode

MAC – Message Authentication Code

MACsec – IEEE MAC Security protocol 802.1AE

NIST – National Institute of Standards and Technology

NVRAM – Non-Volatile Random Access Memory

PoE+ – Power over Ethernet Plus

RAM – Random Access Memory

RNG – Random Number Generator

SHA – Secure Hash Algorithm

Triple-DES – Triple Data Encryption Standard