FIPS 140-2 Security Policy for Cisco Aironet LWAPP AP1131AG and AP1242AG Wireless LAN Access Points

October 30, 2008
Version 1.4

Contents

This security policy contains these sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco Aironet Lightweight AP1131AG and AP1242AG (herein collectively called *the modules*) are wireless access points that support the IEEE 802.11a/b/g Wi-Fi standards for wireless LAN communications, and the IEEE 802.11i standard for wireless LAN security. They are multiple-chip standalone cryptographic modules, compliant with all requirements of FIPS 140-2 Level 2.

In the FIPS mode of operations, the modules support the Lightweight Access Point Protocol (LWAPP) and Management Frame Protection (MFP). LWAPP, together with X.509 certificates, authenticates the module as a trusted node on the wired network. All wired network communications for control and bridging traffic are protected with AES encryption. The modules secure all wireless communications with Wi-Fi Protected Access 2 (WPA2). WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. The modules use the following cryptographic algorithm implementations:

- AES
- AES-CCM
- AES-CMAC
- SHA-1
- HMAC SHA-1
- X9.31 Random Number Generator
- RSA

This document details the security policy for the lightweight AP1131AG and AP1242AG cryptographic modules. This document is non proprietary and may be freely distributed.

The evaluated platforms are summarized in Table 1.

Table 1 Evaluated Platforms

Model	Firmware Version	Hardware Revision
AP1131AG	4.1.171.0 and 4.1.185.10	C0
AP1242AG	4.1.171.0 and 4.1.185.10	A0

Physical Security Policy

For the AP1131AG, place tamper evident labels over the bottom panel and over the top cover as shown in Figures 1 through 6 below.

Figure 1 Front view of tamper labels on AP1131AG

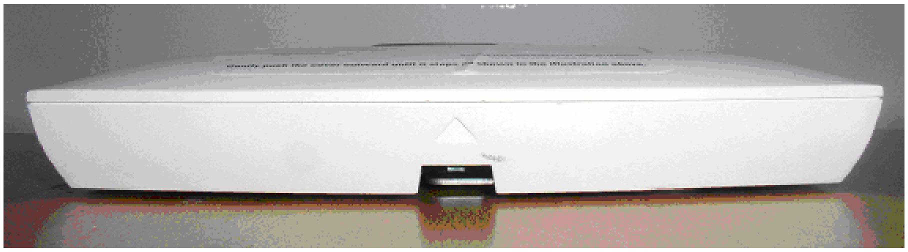


Figure 2 *Back view of tamper labels on AP1131AG*

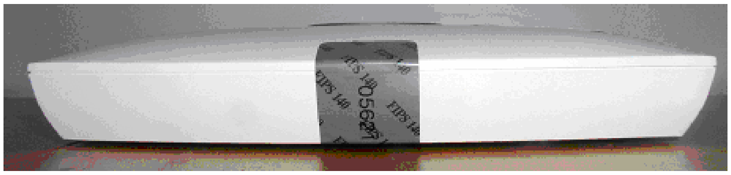


Figure 3 *Left side view of tamper labels on AP1131AG*

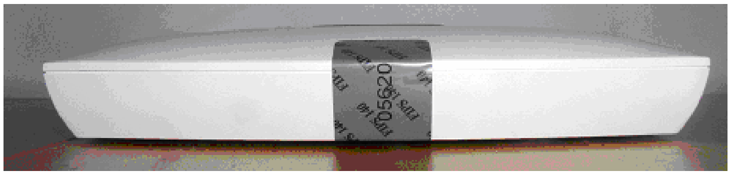


Figure 4 *Right side view of tamper labels on AP1131AG*

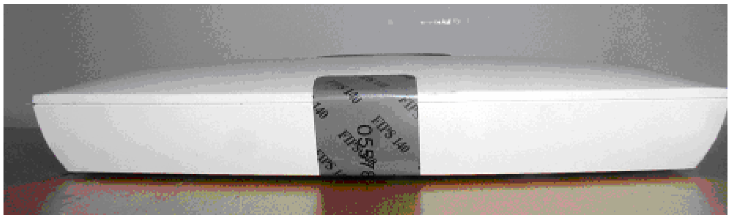


Figure 5 *Top view of tamper labels on AP1131AG*

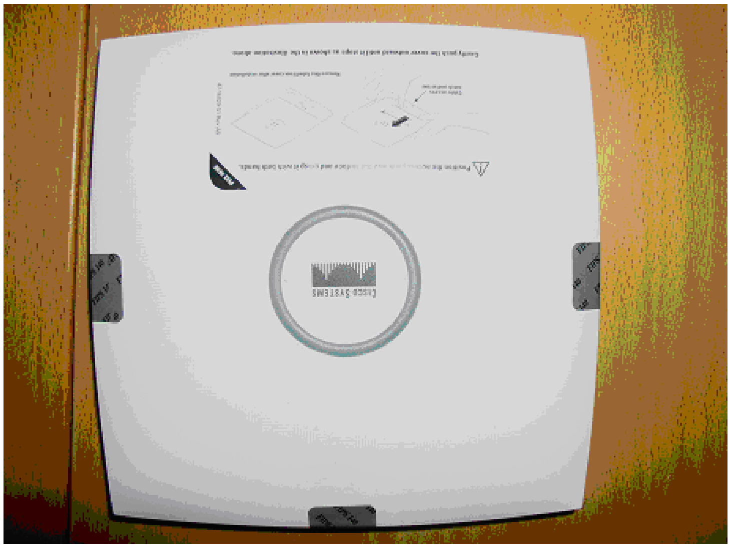
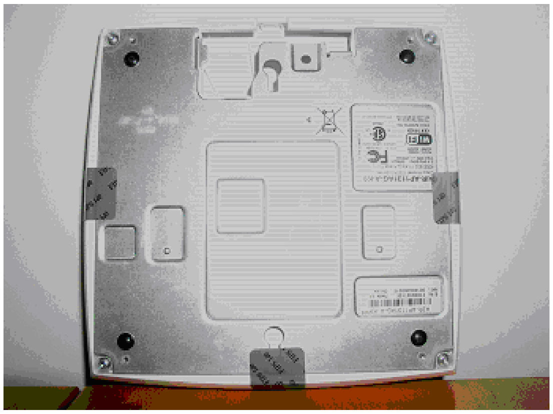


Figure 6 Bottom view of tamper labels on AP1131AG



For the AP1242AG, put tamper evident labels over the removable top cover, over the cap of the mode button, and over the console port as shown in Figures 7 through 12 below:

Figure 7 Front view of tamper labels on AP1242AG

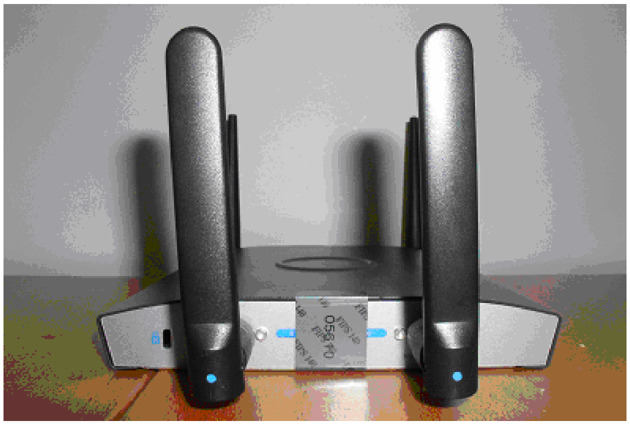


Figure 8 Back view of tamper labels on AP1242AG

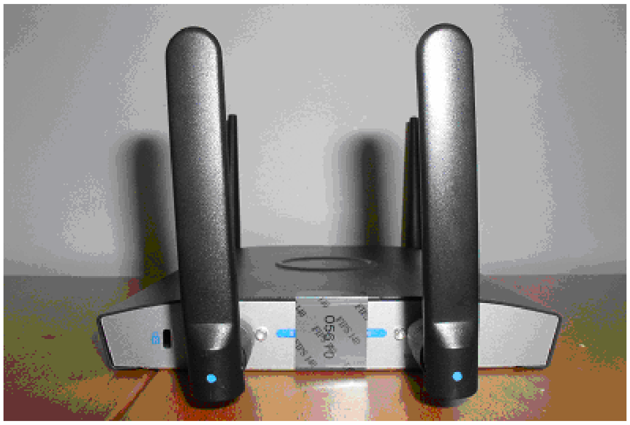


Figure 9 Left view of tamper labels on AP1242AG

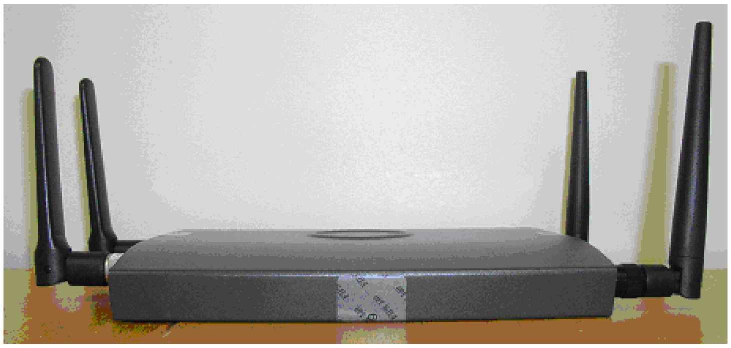


Figure 10 Right view of tamper labels on AP1242AG

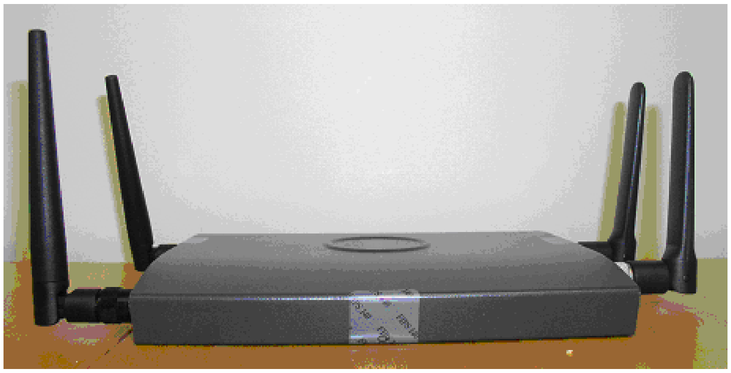


Figure 11 Top view of tamper labels on AP1242AG

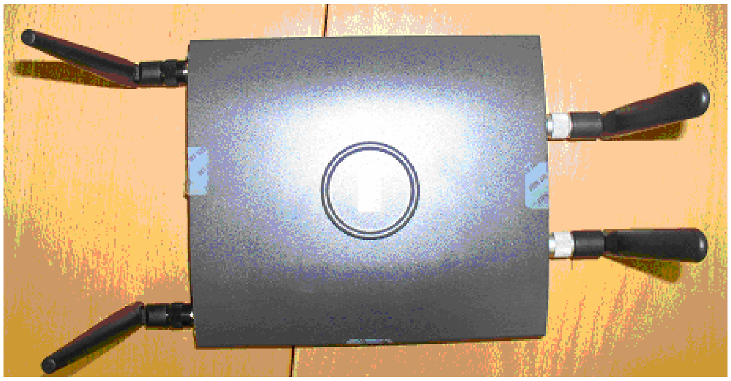
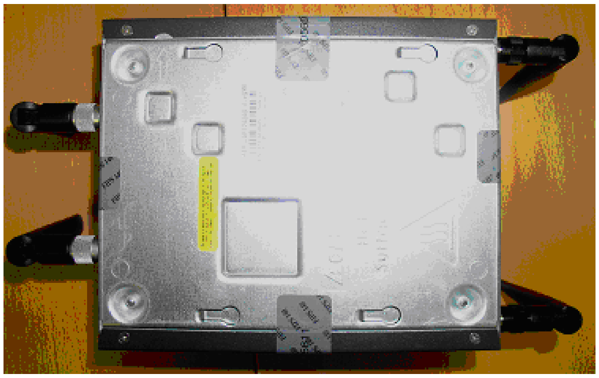


Figure 12 Bottom view of tamper labels on AP1242AG



Secure Configuration

This section details the steps used to securely configure the modules to operate in FIPS 140-2 mode of operations. The administrator configures the modules from the wireless LAN controller with which the access point is associated. The wireless LAN controller shall be placed in FIPS 140-2 mode of operations prior to secure configuration of the access points.

Follow these steps to prepare the secure configuration for the wireless LAN controller:

Enable FIPS Mode of Operations

The following controller CLI command places the controller in FIPS mode of operations, enabling all necessary self tests and algorithm restrictions:

```
>config switchconfig fips-prerequisite enable
```

Disable Boot Break

The following controller CLI command prevents breaking out of the boot process. It must be executed after enabling FIPS mode of operations:

```
>config switchconfig boot-break disable
```

Configure RADIUS KeyWrap KEK and MACK Keys

The following controller CLI commands configure the RADIUS secret and AES-key wrap KEK and MACK:

```
>config radius auth add index ip-address port hex secret
>config radius auth keywrap add hex kek mack index
>config radius auth keywrap enable
```

Note The AES key wrap operation does not take place on the AP but rather at the RADIUS server and the controller; it is listed here for the sake of completeness.

Configure Pre-shared Keys for 802.11i

WPA2 Pre-shared key (WPA2-PSK) is an optional mode permitted for the Controller. Generation of pre-shared keys is outside the scope of this security policy, but they should be entered as 64 hexadecimal values (256 bits) by the following controller CLI commands:

```
> config wlan security wpa akm psk set-key hex key index
> config wlan security wpa akm psk enable index
```

Refer to the *Cisco Wireless LAN Controller Configuration Guide* for additional instructions.

Configure Ciphersuites for 802.11i

The following controller CLI commands create a wireless LAN, configure it to use WPA2, associate it with a RADIUS server, and enable it:

```
> config wlan create index profile_name ssid
> config wlan radius_server auth add index radius-server-index
> config wlan enable index
```

Configure MFP (Management Frame Protection)

Infrastructure MFP enables one Access Point to validate a neighboring Access Point's management frames. Configuring the module to use MFP is optional. The following controller CLI command is used to enable infrastructure MFP:

```
> config wps mfp infrastructure enable
```

Client MFP is used to encrypt and sign management frames between the AP and the wireless client. The following controller CLI command is used to enable client MFP:

```
> config wlan mfp client enable index required
```

Refer to the *Cisco Wireless LAN Controller Configuration Guide* for additional instructions.

Configure CCKM (Cisco Centralized Key Management)

CCKM is Cisco's wireless key management and is an optional mode permitted by this security policy. CCKM uses the same cipher suite as 802.11i; however, it has a slightly different key management scheme to support wireless client fast roaming between access points. Wireless client must comply with the updated CCKM specification described in CCXv5 in the FIPS mode of operation. The following controller CLI command configures CCKM on a given WLAN:

```
> config wlan security wpa akm cckm enable index
```

Refer to the *Cisco Wireless LAN Controller Configuration Guide* for additional instructions.

Note The module does not participate in the CCKM key establishment but rather assists in passing data between the client and the RADIUS server.

Set Primary Controller

Enter the following controller CLI command from a wireless LAN controller with which the access point is associated to configure the access point to communicate with trusted wireless LAN controllers operating in FIPS mode:

```
> config ap primary-base controller-name access-point
```

Enter this command once for each trusted controller. Enter **show ap summary** to find the access point name. Enter **show sysinfo** to find the name of a controller.

Save and Reboot

After executing the above commands, you must save the configuration and reboot the system:

```
> save config
> reset system
```

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

The module supports the roles of Crypto Officer and User. The CO role is fulfilled by the wireless LAN controllers on the network that the module communicates with, and performs routine management and configuration services, including loading session keys and zeroization of the module. The User role is fulfilled by wireless clients. The module does not support a maintenance role.

Services

All services can be viewed by typing **?** from within the appropriate roles. This command will show all the services available to the role currently logged in.

The services provided are summarized in Table 2.

Table 2 Module Services

Service	Role	Purpose
Self Test and Initialization	CO	Cryptographic algorithm tests, software integrity tests, module initialization. **Note** Module initialization can be obtained either by the CO resetting the access point remotely or by someone with physical access to the module manually cycling the power.
System Status	User, CO	The LEDs show the network activity and overall operational status.
Key Management	CO	Key and parameter entry, key output, key zeroization.
Module Configuration	CO	Selection of non-cryptographic configuration settings.
LWAPP	CO	Establishment and subsequent data transfer of an LWAPP session for use between the module and the CO.
802.11i	User, CO	Establishment and subsequent data transfer of an 802.11i session for use between the wireless client and the AP.
CCKM	User, CO	Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP
MFP	User, CO	• Validating one AP with a neighboring AP's management frames using infrastructure MFP • Encrypt and sign management frames between AP and wireless client using client MFP

The module does not support a bypass capability in the approved mode of operations.

The meaning of the LED indicators on the AP1131AG are summarized in Table 3 below:

Table 3 LED Status Indicators on the AP1131AG

Sequence	Color pattern	Status
Power up	Off	DRAM test in progress
	Green	DRAM test OK
	Off	Board init in progress
	Light blue	Init flash file system
	Pink	Flash test OK
	White	Init Ethernet
	Blue	Ethernet OK
	Green	Boot software
	Off	Init OK
Power up error indicators	Yellow	Ethernet link down, Ethernet failure, Configuration recovery
	Pink	Image recovery
	Blink pink/Off	Image recovery in progress
Ongoing status	Pale green	Normal with no clients associated
	Blue	Normal with client(s) associated
	Deep blue	Software upgrade in progress
	Orange	Software failure or error condition
	Blink green/Off	User set location

The AP1242AG module has three LEDs that indicate the Ethernet status, radio status and system operational status. Any LEDs blinking yellow or red indicate a warning or error condition.

Crypto Officer Authentication

The modules authenticate to a wireless LAN controller through the LWAPP protocol, using an RSA key pair with 1536 bit modulus. NIST SP 800-57 defines this modulus size as having effective symmetric key strength of 96 bits, therefore an attacker would have a 1 in 296 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 7.9x1023 attempts per minute, which far exceeds the operational capabilities of the modules to support.

User Authentication

Users are authenticated by means of possession of 802.11i Pairwise Transient Key (PTK) which is a shared secret between the AP and the wireless client (User role). This key is set-up as a result of a successful IEEE 802.1X authentication session between a wireless client and a backend authentication server, followed by a successful IEEE 802.11i 4-way handshake between the wireless client and the attaching wireless controller. Acting as a conduit, the AP relays both IEEE 802.1X authentication messages and IEEE 802.11i 4-way handshake messages between the wireless client and the wireless controller. Any EAP methods such as EAP-TLS, EAP-FAST or PEAP may be used. An optional user authentication mode using 802.11i Pre-shared-key (PSK) is also supported.

The Key Confirmation Key portion of the PTK is 128 bits. An attacker would have a 1 in 2^{128} change 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 $3.4x10^{33}$ attempts per minute, which far exceeds the operational capability of the module to support.

Cryptographic Key Management

Cryptographic keys are stored in flash and in SDRAM for active keys.

No keys are generated in the module. All keys are input into the module from the controller over an LWAPP session. During an LWAPP session, the APs first authenticate to the Wireless LAN controller using an RSA key pair. After a successful authentication, the LWAPP session key generated in the controller is transported from the controller to the module wrapped with AP's RSA key. The 802.11i GTK and TK and CCKM PTK and GTK are input into the module encrypted with the LWAPP session key over an LWAPP session. These keys are the 802.11i and CCKM session keys and are used by the module to encrypt 802.11i and CCKM traffic. The module does not output any plain text cryptographic keys.

Table 4 lists the secret and private cryptographic keys and CSPs used by the module. Table 5 lists the public keys used by the module. Table 6 lists the access to the keys by service.

Table 4 Secret and Private Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description and Zeroization
PRNG seed key	X9.31	SDRAM	This is the seed key for the PRNG. It is statically stored in the code and is zeroized when the controller image is erased during zeroization procedure.
PRNG seed	X9.31	SDRAM	This is the seed for the PRNG. It is generated using the reg_add_fresh_entropy function. It is zeroized during the zeroization procedure.
cscoIdCert key	RSA	Flash	This is the AP's RSA private key. It is zeroized during the zeroization procedure.
LWAPP Session Key	AES-CCM	SDRAM	The session key used to authenticate and encrypt LWAPP traffic. It is zeroized during the zeroization procedure.[1]
Infrastructure MFP MIC Key	AES-CMAC	SDRAM	The 128 bit AES Key which is used to sign management frames when infrastructure MFP is enabled. It is zeroized during the zeroization procedure.

Table 4 Secret and Private Cryptographic Keys and CSPs (continued)

Name	Algorithm	Storage	Description and Zeroization
802.11i Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The PTK, also known as the CCMP key, is the 802.11i session key for unicast communications. This key also used to encrypt and sign management frames between AP and the wireless client. It is zeroized during the zeroization procedure.
802.11i Temporal Key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. It is zeroized during the zeroization procedure.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications. It is zeroized during the zeroization procedure.
CCKM Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The CCKM PTK is the CCKM session key for unicast communications. It is zeroized during the zeroization procedure.
CCKM Group Temporal Key (GTK)	AES-CCM	SDRAM	The CCKM GTK is the CCKM session key for broadcast communications. It is zeroized during the zeroization procedure.
WPA2 PSK	AES-CCM	SDRAM	The PSK is a pre shared key used to derive the TK and GTK. It is zeroized during the zeroization procedure.

[1] RSA key wrapping provides 96 bits of effective symmetric key strength.

Table 5 Public Keys

Name	Algorithm	Storage	Description and Zeroization
bsnOldDefaultCaCert	RSA	Flash	Verification certificate, used with LWAPP to authenticate the controller. It is zeroized during the zeroization procedure.
bsnDefaultRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
bsnDefaultCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.

Table 5 Public Keys (continued)

Name	Algorithm	Storage	Description and Zeroization
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, not used in FIPS mode of operations. It is zeroized during the zeroization procedure.
cscoIdCert	RSA	Flash	This is the AP's RSA public key.

Table 6 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG Seed
System Status	• None
Key Management	• Zeroize cscoIdCert
Module Configuration	• None
LWAPP	• Authenticate to controller using cscoIdCert Private Key • Authenticate controller using bsnOldDefaultCaCert • LWAPP session key entry and then encrypt/decrypt LWAPP traffic with the Session Key • Encrypted GTK and TK entry from the controller for 802.11i service • Encrypted MFP MIC key entry from the controller for use in MFP
802.11i	• Encrypt/decrypt using TK, GTK
CCKM	• Encrypt/decrypt using CCKM PTK and GTK
MFP	• Sign AP management frames using Infrastructure MIC key • Encrypt and sign AP management frames using 802.11i PTK

Key Zeroization

All keys in the module may be zeroized by entering this command on the controller to which the access point is associated:

```
> config switchconfig key-zeroize ap ap-name
```

Disallowed Security Functions

These cryptographic algorithms are not approved, and may not be used in FIPS mode of operations:

- RC4
- MD5
- HMAC MD5

Self Tests

These self tests are performed by the module:

- Firmware integrity test
- AES KAT (Software and Hardware)
- AES-CCM KAT (Software and Hardware)
- AES-CMAC KAT (Software and Software/hardware Combination)
- SHA-1 KAT (Software)
- HMAC SHA-1 KAT (Software)
- RNG KAT (Software)
- RSA KAT (Software)
- Continuous random number generator test for Approved and non-Approved RNGs

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html