Crossbeam Systems, Inc.

X60 and X80-S Platforms

Hardware Version: APM-9600, CPM-9600, NPM-9610, and NPM-9650
Firmware Version: XOS v9.9.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.14

Prepared for:

Crossbeam Systems, Inc.
80 Central Street
Boxborough, MA 01719
United States of America

Phone: +1 (978) 318-7500

http://www.crossbeam.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the X60 and X80-S Platforms from Crossbeam Systems, Inc., hereafter referred to as Crossbeam. This Security Policy describes how the X60 and X80-S Platforms meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The X60 and X80-S Platforms are referred to in this document as the X-Series module or the module.

1.2 References

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

- The Crossbeam website (http://www.crossbeam.com) contains information on the full line of products from Crossbeam.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. The Submission Package contains:

- Non-proprietary Security Policy document
- Vendor Evidence document
- Finite State Model document
- Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Crossbeam Systems, Inc. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Crossbeam and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Crossbeam.

2 X60 and X80-S Platforms

2.1 Overview

The X60 and X80-S Platforms belong to Crossbeam's family of security application platforms. There are three possible chassis: the X60, X80-S-AC, and X80-S-DC. The platforms consolidate multiple security applications onto a single multifunction device. The applications that can be installed on the Crossbeam platform include antivirus applications, firewall applications, spam filtering applications, Intrusion Prevention Systems (IPS), proxies, and web content gateways. A full list of supported applications can be found on Crossbeam's website (http://www.crossbeam.com) by clicking on the "Applications" tab, although not all of these have been FIPS 140-2 validated.

The platforms are composed of a combination of hot-swappable blades seated on a common backplane. The blades provide processing and storage that is used to implement module functionality. The blades can be one of the following three types:

- Control Processor Modules (CPMs) – provide all generic system-wide functions, including a switched Ethernet control network for all slots in the chassis, all management ports, management of the system boot process, management of alarms, system health monitoring, and statistical reporting.
- Network Processor Modules (NPMs) – provide network connectivity, handle traffic flows into and out of the system, and make load-balancing decisions.
- Application Processor Modules (APMs) – host security applications and provide application-level processing of traffic flows. Incoming traffic is received from the NPMs, and outgoing traffic is returned to the NPMs. Applications are loaded during the APM boot process from storage on the CPM; these applications are referred to as Virtual Application Processors, or VAPs. A VAP contains a base kernel and usually a security application installed on top of that kernel.

Only the CPM blades implement cryptographic functionality.

The CPM communicates to the other blades via a dual, redundant, private, switched control plane. The CPM contains the switching elements with all point-to-point connections from each of the other blades connecting through the backplane connector. The cryptographic libraries run on independent CPM blades that are inserted into the chassis backplane.

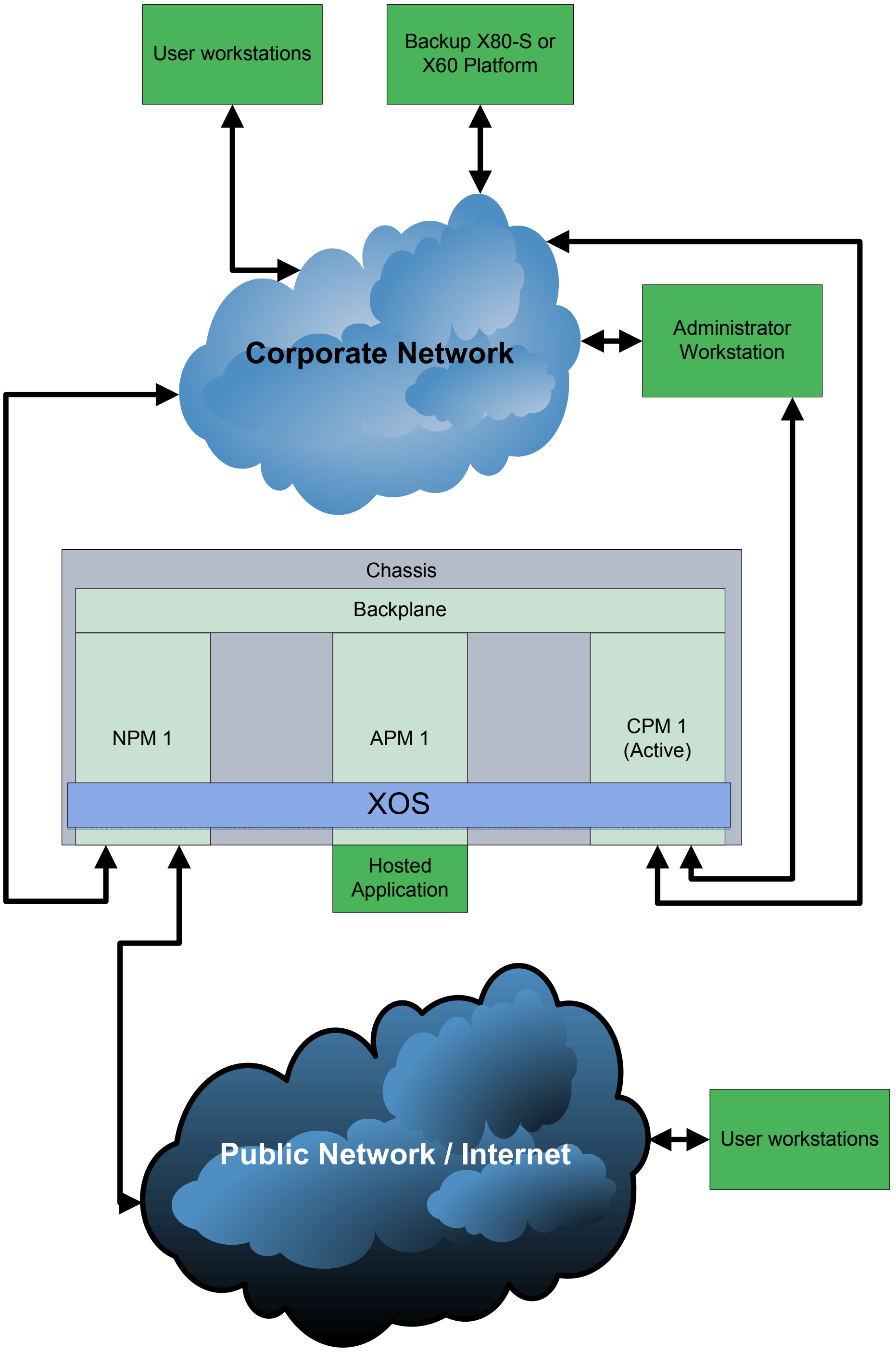

Figure 1 - X-Series Typical Deployment Configuration

The X-Series module is validated at the FIPS 140-2 Section levels listed in Table 1 below. The overall security level of the module is 2.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section 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[1]
7	Cryptographic Key Management	2
8	EMI/EMC[2]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Specification

The X-Series is a Multi-Chip Standalone hardware module. The cryptographic boundary of the X-Series is defined by the chassis of the platform. The testing configuration for the module includes one of each blade type (CPM, APM, and NPM) loaded into the chassis. The CPM runs the CPM kernel, the APM runs either the xsve kernel or xslinux_v5_64 kernel, and the NPM runs a network-specific operating system. This results in a total of 12 different testing configurations, as shown in Table 2 below. Please note that the CPM is present in all of the below configurations running the CPM kernel.

Table 2 – Module Test Configurations

Testing Configuration	X80-S-AC	X80-S-DC	X60	APM running xsve	APM running xslinux_v5_64	NPM-9610	NPM-9650
1	✓			✓		✓	
2	✓			✓			✓
3	✓				✓	✓	
4	✓				✓		✓
5		✓		✓		✓	
6		✓		✓			✓
7		✓			✓	✓	
8		✓			✓		✓
9			✓	✓		✓	
10			✓	✓			✓
11			✓		✓	✓	
12			✓		✓		✓

[1] N/A – Not Applicable
[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

The NPM blades, APM blades, power supplies, fan trays, and Air Flow Panels (AFPs) do not provide any cryptographic functionality. They provide network connections and contribute to the integrity of the module physical enclosure. Blades can occupy the slots of each chassis as defined in Table 3 below.

Table 3 – X60 and X80-S Blade Types by Slot

Slot Number	X60 Blade Type	X80-S Blade Type
1	NPM	NPM
2	NPM or APM	NPM
3	APM	NPM or APM
4	APM	NPM or APM
5	APM	APM
6	APM or CPM	APM
7	CPM	APM
8	N/A	APM
9	N/A	APM
10	N/A	APM
11	N/A	APM
12	N/A	APM
13	N/A	CPM
14	N/A	CPM

The cryptographic module was tested and found compliant on the platforms listed in Table 4 below.

Table 4 – Cryptographic Module Platforms

Blade	VAP OS	Linux Kernel(s)	Architecture
CPM	n/a	2.6.18-164.2.1	x86_64
APM	xsve	2.6.18-164.2.1	x86_64
APM	xslinux_v5_64	2.6.18-164.2.1	x86_64

2.3 Module Interfaces

The X60 and X80-S Platforms consist of Ethernet ports, Small Form Pluggable (SFP) ports, a console port, a Universal Serial Bus (USB) port, and status Light-Emitting Diodes (LEDs). All empty blade slots on the chassis backplane are covered with plastic AFPs. The AFPs and blade front panels are affixed with tamper-evident labels to prevent unauthorized access.

The physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Data input/output is categorized as the packets entering and leaving the module through the network ports (Ethernet ports) on the NPM blades. Control input consists of configuration or administration data entered into the module via the Command Line Interface (CLI) management interface (accessed via the CPM blades). Any User can be given administrative permissions by the Crypto Officer (CO). Status output consists of the status provided via the LEDs, CLI command output, and log information.

The APM-9600, CPM-9600, and NPM-96x0[3] blades are shown in Figure 2, Figure 3, and Figure 4. The front and rear of the X60 are shown in Figure 5 and Figure 6.

Acronyms shown in the diagrams below:

- AC – Alternating Current
- ESD – Electrostatic Discharge

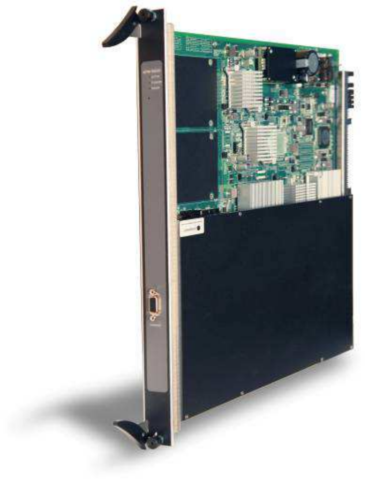

Figure 2 – APM-9600 Blade

[3] NPM-96x0 refers to either the NPM-9610 or NPM-9650 blade, or both.

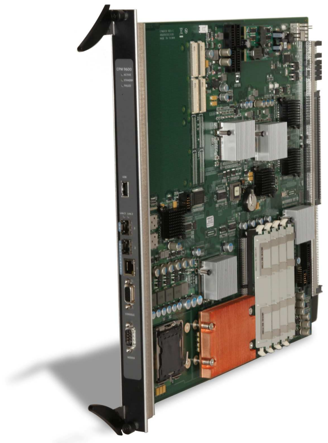

Figure 3 – CPM-9600 Blade

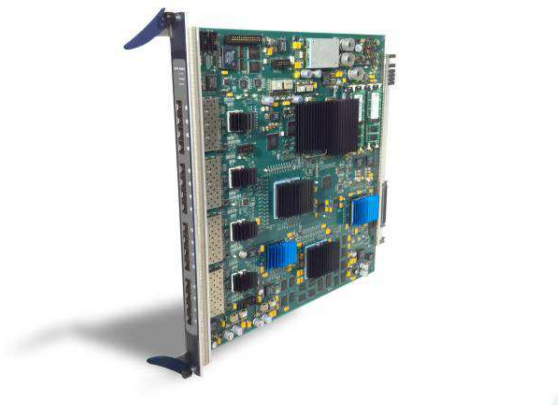

Figure 4 – NPM-96x0 Blade

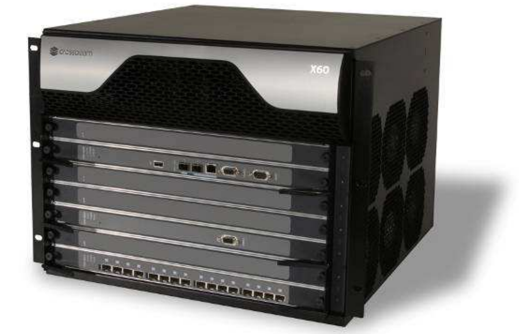

Figure 5 – X60 Front View

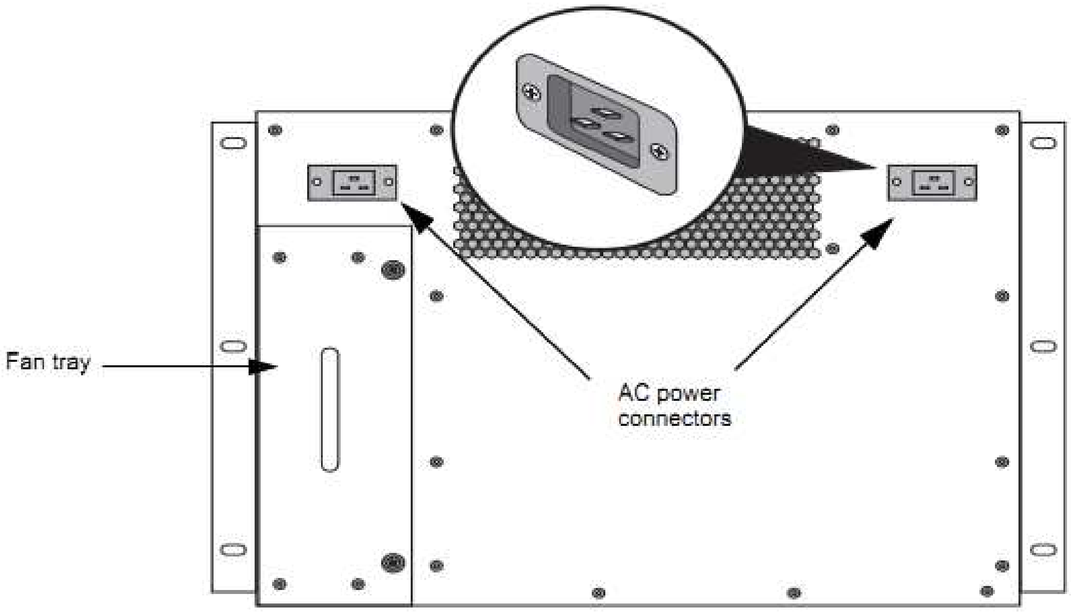

Figure 6 – X60 Back View

The front and rear of the X80-S are shown in Figure 7 and Figure 8.

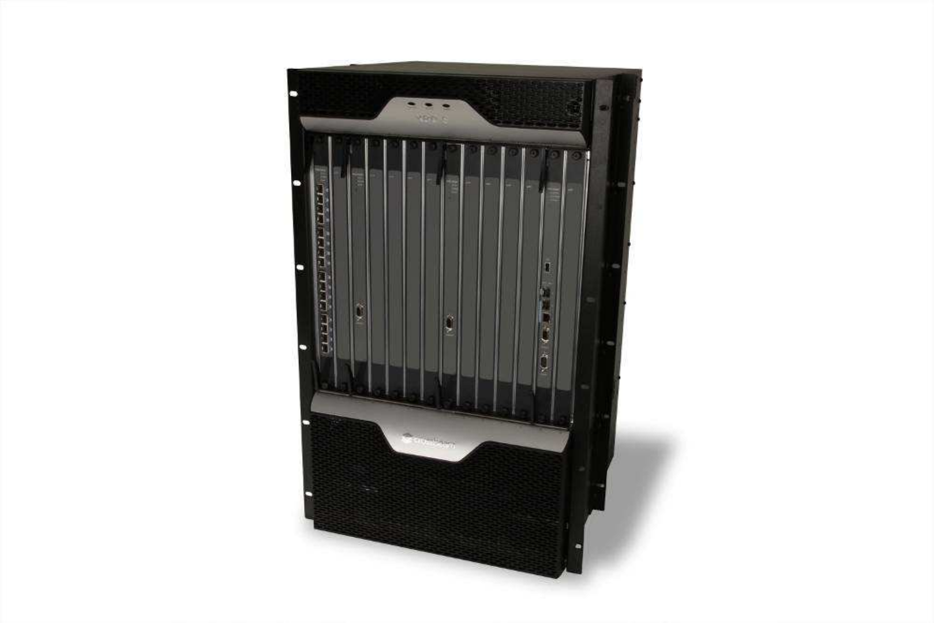

Figure 7 – X80-S Front View

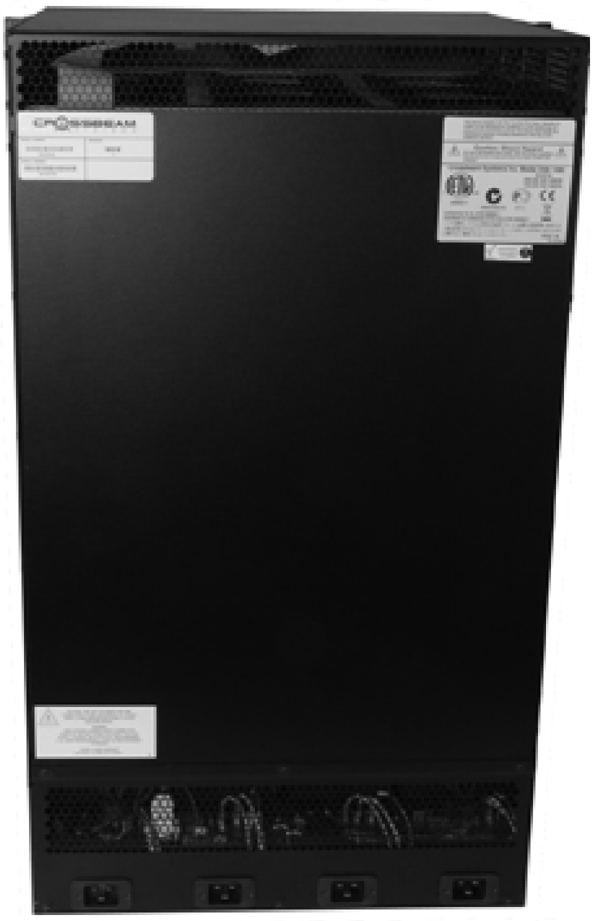

Figure 8 – X80-S Back View

All of the physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 5 below.

Table 5 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
Ethernet	1 (CPM-9600) 16 (NPM-96x0)	• Control Input (CPM) • Status Output (CPM) • Data Input (NPM) • Data Output (NPM)
SFP	2 (CPM-9600)	• Control Input • Status Output

Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
Serial	2 (CPM-9600)	• Control Input • Status Output
LED	3 (APM-9600) 7 (CPM-9600) 35 (NPM-96x0) 3 on the X80-S chassis, controlled by CPM	• Status Output
Power	2 (X60) 4 (X80-S)	• Power Input

2.4 Roles and Services

The module supports identity-based authentication for two roles: CO and User (as required by FIPS 140-2).

The CO role is the administrator for the system and can perform the setup, maintenance, and User management tasks. The User role can have a permission level from 0-15 and is allowed to perform configuration and monitoring tasks commensurate with the assigned permission level.

Descriptions of the services available to the CO and User roles are provided in Table 6 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

- Read: The CSP is read.
- Write: The CSP is established, generated, modified, or zeroized.
- Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 6 – Operator Services

Service	Description	Operator	CSP and Type of Access
configure no fips-mode	Disables FIPS-mode	CO	None
shutdown	Shuts down the module and all crypto services	CO	None
reload	Restarts the module and reloads crypto services	CO	None
clear fips-error	After an error occurs, checks to see if all self-tests passed, and if so re-enables module functionality. If self-tests have not passed, indicates the failed self-tests. The administrator should re-run any failed self-tests.	CO	None
show fips-mode	Displays whether the module is running in FIPS mode or not	CO User	None

Service	Description	Operator	CSP and Type of Access
show running-config	Shows the currently-loaded configuration, including version number for the module	CO	CO Password – Read (encrypted) User Password – Read (encrypted)
show startup-config	Shows the startup configuration, including version number for the module (option for displaying encrypted CO and user passwords)	CO	CO Password – Read (encrypted) User Password – Read (encrypted)
copy running-config	Copies the running configuration to a file	CO	CO Password – Read (encrypted) User Password – Read (encrypted)
copy startup-config	Copies the startup configuration to a file	CO	CO Password – Read (encrypted) User Password – Read (encrypted)
show tech-support	Shows many system properties including module version, startup config, and running config	CO	None
show tech-crash	Shows information on the latest module crash, including version information	CO	None
lock-config	Prevents other operators from modifying the configuration	CO	None
clear alarms	Clears all clearable notifications from the active alarms table	CO	None
show ip ssh	Shows SSH settings, including inactivity timeout settings	CO	None
configure ip ssh	Enables, disables, or changes options for the Secure Shell (SSH) server on the module	CO	None
disconnect ssh	Terminates an existing SSH session with the specified session identifier	CO	None
configure password-policy	Sets the password policy for the module	CO	None
remove-ssh-keys	Zeroizes the keys used by SSH on the module	CO	RSA[4] public key – Write RSA private key – Write DSA[5] public key – Write DSA private key – Write
configure password	Changes the password for the current user	CO User	CO Password – Write (only for self) User Password – Write (only for self)

[4] RSA – Rivest, Shamir, and Adelman

[5] DSA – Digital Signature Algorithm

Service	Description	Operator	CSP and Type of Access
configure username	Creates a new operator account or configures/deletes the specified existing user account	CO	User password – Write
configure fips-mode crypto-officer-role	Promotes the specified User with privilege level 15 to the CO role, or demotes the CO to a User with privilege level 15	CO	None
Commands for configuring X-Series platform management interfaces	Commands that allow the CO or User to configure the interfaces available for remote management of the module	CO User	None
Commands for configuring user accounts and managing user access to the X-Series platform	Commands that allow the CO to manage users and access levels.	CO	None
Commands for displaying XOS configuration settings	Commands that allow the CO or User to view non-sensitive configuration elements.	CO User	None

The module authenticates the Crypto Officer and User operator's account before providing any services. Once the operator authenticates, the operator assumes the role associated with the operator's account.

The module performs identity-based authentication. All CO and User services provided by the module require the operator to authenticate with a username and password. Operators signing into a CO account assume a permission level that grants access to all commands. Operators signing into a User account assume permissions at a level from 0-15 (as designated by a CO). This allows the CO to permit different User accounts to have multiple access levels to CLI commands.

The module uses password-based authentication mechanisms. Password requirements can be modified by a CO, but must meet the following minimum criteria:

- 96-character password space (upper- and lower- case letters, numbers, and special characters)
- Passwords must be at least 8 characters in length
- Passwords must include at least 1 upper- and lower-case letter, 1 number, and 1 special character
- Passwords have a default lifetime of 1 month
- New passwords must have a minimum of 4 character changes from the previous password

The chance of a random brute-force attempt succeeding at guessing an operator's password is $1:96^8$, or 1: 7,213,895,789,838,336. The fastest network connection supported by the module is 1 Gbps[6]. Hence, at most ($10^9 \times 60 = 6 \times 10^{10}$ = 60,000,000,000 bits, or 7,500,000,000 bytes) of data can be transmitted in one minute. Given a minimum password length of 8 characters only 937,500,000 passwords can be guessed in a minute. Therefore, the probability that a random attempt will succeed or false acceptance will occur in a one-minute period is less than $937{,}500{,}000:96^8$ or 1: 7,694,822.

[6] Gbps – Gigabits Per Second

2.4.1 Non-Approved Services

When the module is operating in the non-Approved mode of operation (described in Section 3.2.3), the following additional services are available to the operator of the module:

- Non-Approved HTTPS (RSA, AES, and TDES),
- Blowfish
- CAST[7]-128
- RC4[8]
- Use of LibGCrypt for RSA (key gen) and RNG

2.5 Physical Security

The X-Series is a multi-chip standalone cryptographic module. It is enclosed in a hard and opaque painted-metal case that completely encloses all internal components. There are only a limited set of ventilation holes provided by the case, and the view of internal components of the module is obscured by:

- Baffles on the left side of the X60 chassis,
- Fan trays on the right side of the X60 chassis,
- Baffles provided by the power supply units (X60 and X80-S),
- Baffles provided by the APM, CPM, and NPM blades and AFPs (X60 and X80-S),
- An internal metal enclosure that surrounds the internal components of the X80-S chassis, and
- Baffles provided by the backplane of the X80-S chassis.

Tamper-evident labels are applied to the case to provide physical evidence of attempts to gain access to the module’s internal components. All of the module’s components are production grade. The placement of the tamper-evident labels can be found in Section 3.1.1.

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.6 Operational Environment

The operational environment requirements do not apply to the module, because the module does not provide a general-purpose Operating System (OS) for operators. The X60 and X80-S Platforms employ one of three kernels listed in Table 4 above. Each kernel is a non-modifiable OS that provides only a limited operational environment, and only the module’s custom-written images can be run on the system.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 7 below.

[7] CAST – Carlisle Adams Stafford Tavares

[8] RC4 – Ron’s Code 4

Table 7 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Numbers	
	OpenSSL	LibGCrypt
Advanced Encryption Standard (AES) – CBC[9], ECB[10], OFB[11], and CFB-128[12] modes (128-bit, 192-bit, and 256-bit keys)	Cert. # 1877	Cert. # 1878
AES – CTR[13] mode (128-bit, 192-bit, and 256-bit keys)	N/A	Cert #1878
Triple Data Encryption Standard (TDES) – CBC, ECB, OFB, and CFB-64 with 3-key	Cert. # 1220	Cert. # 1221
TDES – CTR mode with 3-key	N/A	Cert #1221
RSA ANSI X9.31 Key gen, Public Key Cryptography Standard #1 (PKCS#1) v1.5 (sign/verify) – 1024-, 1536- , 2048- , 3072- , and 4096-bit	Cert. # 958	N/A
RSA ANSI X9.31 (sign/verify) Probabilistic Signature Scheme (PSS) (sign/verify) – 1024-, 1536-, 2048-, 3072-, and 4096-bit	Cert. # 958	N/A
DSA PQG(gen), sign/verify 1024-bit	Cert. #587	N/A
DSA key generation – 1024-bit	Cert #587	N/A
Secure Hash Algorithm (SHA)-1, SHA-224, SHA-256, SHA-384, and SHA-512	Cert. # 1650	Cert. # 1651
ANSI X9.31 Appendix A.4.2 Pseudo Random Number Generator (PRNG)	Cert. # 983	N/A

***NOTE**: As of December 31, 2010, the following algorithms listed in the table above are considered "deprecated". For details regarding algorithm deprecation, please refer to NIST Special Publication 800-131A.*

- *SHA-1 for digital signature generation and verification*
- *Random number generation using ANSI X9.31-1998*
- *Digital signature generation using 1024-bit DSA*

The RNG in LibGCrypt does not conform to all of the requirements of the FIPS standard. The RSA key generation algorithm in LibGCrypt relies on random bits provided by the RNG, and thus, it is likewise deemed non-conformant due to the dependency on the RNG. The Crossbeam module does not rely on the RNG or key generation capabilities of LibGCrypt, and the non-conformance does not impact the security profile or posture of the module.

The module also supports the following non-FIPS-Approved algorithms:

- RSA (encrypt, decrypt) (key wrapping, key establishment methodology provides between 80 and 150 bits of encryption strength),
- RSA (key gen) using LibGCrypt
- DSA PQG(gen) and sign/verify using libgcrypt
- RNG using LibGCrypt
- Diffie-Hellman (key agreement, key establishment methodology provides between 80 and 219 bits of encryption strength).

[9] CBC – Cipher Block Chaining
[10] ECB – Electronic Codebook
[11] OFB – Output Feedback
[12] CFB – Cipher Feedback
[13] CTR – Counter

The module supports the CSPs listed below in Table 8.

Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
OpenSSL RSA private key	2048-bit RSA private key	Internally generated	Never exits the module	Hard disk in plaintext	By command	Key exchange for SSH sessions
OpenSSL RSA public key	1024-, 1536-, 2048-, 3072-, or 4096-bit RSA public key	Internally generated	Exits in plaintext form during SSH session establishment	Hard disk in plaintext	By command	Key exchange for SSH sessions
OpenSSL DSA public key	1024-bit DSA public key	Internally generated	Exits in plaintext form during SSH session establishment	Hard disk in plaintext	By command	Key exchange for SSH sessions
OpenSSL DSA private key	1024-bit DSA private key	Internally generated	Never exits the module	Hard disk in plaintext	By command	Key exchange for SSH sessions
OpenSSL Session key	• 128-bit AES CBC • 192-bit AES CBC • 256-bit AES CBC • 192-bit TDES CBC	Internally generated	Exits in encrypted form during SSH key establishment	Resides in volatile memory only in plaintext	By power cycle or session termination	Data encryption and decryption for SSH sessions
Diffie-Hellman Session key	• 128-bit AES CBC • 192-bit AES CBC • 256-bit AES CBC • 192-bit TDES CBC	Generated internally during Diffie-Hellman key negotiation	Never exits the module	Resides in volatile memory only in plaintext	By power cycle or session termination	Data encryption and decryption for SSH sessions.
Crypto Officer password	8-character minimum password	Enters the module in encrypted form via the Ethernet port on the CPM	Never exits the modules	Hard disk in hashed format	Overwritten by another password	Authenticates the CO
User password	8-character minimum password	Enters the modules in encrypted form via the Ethernet port on the CPM	Never exits the modules	Hard disk in hashed format	Overwritten by another password	Authenticates the User

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
OpenSSL PRNG seed key	32 bytes of random value	Internally generated	Never exits the module	Resides in volatile memory only in plaintext	By power cycle or session termination	Seeds the FIPS-Approved PRNG
OpenSSL PRNG seed	16 bytes of random value	Internally generated	Never exits the module	Resides in volatile memory only in plaintext	By power cycle or session termination	Seeds the FIPS-Approved PRNG

2.8 Self-Tests

The module implements cryptographic algorithms using firmware. The module performs various Self-Tests (Power-Up Self-Tests and Conditional Self-Tests) to verify the functionality and correctness of the algorithms. If any of the power-up or conditional self-tests fail, the module immediately enters a critical error state. While in the critical error state, the module inhibits any data output services by terminating the process providing cryptographic services at the time of the self-test failure. Additionally, the module disables all data output interfaces on the NPM and all interfaces on the CPM except for the serial interface. These interfaces remain disabled until the error state is cleared, or until the module is taken out of FIPS mode. The Crypto Officer can clear the error state by rebooting the module with the `reload` command, which causes the self-tests to be reinvoked. If all self-tests pass, then the module leaves the error state, but interfaces remain disabled until the CO runs the `clear fips-error` command.

2.8.1 Power-Up Self-Tests

The X-Series module performs the following self-tests at power-up to verify the integrity of the firmware binaries and the correct operation of the FIPS-Approved algorithm implementations employed by the module for the OpenSSL library:

- Firmware integrity check using a Digital Authentication Code (SHA-256)
- Cryptographic algorithm tests:
  - AES-ECB-128 Known Answer Test (KAT)
  - TDES KAT
  - RSA sign/verify test
  - DSA sign/verify test
  - RSA (key generation) pair-wise consistency test
  - DSA (key generation) pair-wise consistency test
  - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
  - ANSI X9.31 PRNG KAT

The X-Series module performs the following self-tests at power-up to verify the integrity of the firmware binaries and the correct operation of the FIPS-Approved algorithm implementations employed by the module for the LibGCrypt library:

- Firmware integrity check using a Digital Authentication Code (SHA-256)
- Cryptographic algorithm tests:
  - AES-ECB-128 Known Answer Test (KAT)
  - TDES KAT
  - RSA sign/verify test
  - DSA sign/verify test
  - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs

The CO can perform the power-up self-tests at any time by power-cycling the module or issuing a reload command from the module’s CLI.

2.8.2 Conditional Self-Tests

The X60 and X80-S Platforms perform the following conditional self-tests for the OpenSSL library:

- Continuous Random Number Generator (RNG) test for ANSI X9.31 implementation
- RSA pairwise consistency tests
- DSA pairwise consistency tests

2.9 Mitigation of Other Attacks

This section is not applicable.

3 Secure Operation

The X60 and X80-S Platforms meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-approved mode of operation.

3.1 Initial Setup

The following sections provide the necessary step-by-step instructions for the secure installation and configuration of the X60 and X80-S Platforms, including the steps necessary to place the module into a FIPS-Approved mode of operation. When the module arrives it is not considered to be in any FIPS or non-FIPS mode of operation until it has been provisioned by a CO.

3.1.1 X60 and X80-S Setup

The CO is responsible for installing the platform and powering it up. Before powering up the platform, the CO must ensure that the required tamper-evident labels (included in the FIPS kit) are correctly applied to the platform enclosures following the instructions below.

Prior to applying the tamper evident labels, the CO must ensure that all blade slots are populated with a blade (APM-9600, CPM-9600, NPM-9610, or NPM-9650) or an AFP. The chassis must be loaded with at least one CPM-9600, one APM-9600 and one NPM-9610 or NPM-9650. Failure to populate every slot with a blade or AFP would expose the internal circuitry to a potential attacker, compromising the physical security of the module.

The *Crossbeam X60 Platform Hardware Installation Guide* gives detailed instructions on how to install the X60 chassis in a server room environment and how to install blades into the chassis. The *Crossbeam X80-S Platform Hardware Installation Guide* gives detailed instructions on how to install the X80-S chassis into a server room environment and how to install blades into the chassis. These guides also contain step-by-step instructions on how to configure basic host information required for the platform. The *Crossbeam FIPS Level 2 Label Installation Guide* gives detailed steps for caring for and applying the tamper-evident seals to the module. To order more labels, the CO should contact Crossbeam sales and request Stock Keeping Unit XS-FIPS-LABEL-KIT.

Tamper-evident seals (hereafter referred to as labels) must be applied to the X60 and X80-S chassis to ensure the physical security of the module. Below are instructions for applying the labels.

3.1.1.1 Recording the FIPS Label Numbers

Each FIPS label is numbered. The CO may choose to record in a log the serial number of each label that is used along with its associated location on the chassis.

3.1.1.2 Cleaning the Chassis Surfaces

Ensure that all surfaces are cleaned with 99% isopropyl alcohol and dried with a clean cloth and that the surface temperature is a minimum of 10°C (50°F) before applying the labels.

3.1.1.3 Label Curing Time

Labels should be applied 30 minutes before the module is placed into operation.

3.1.1.4 Applying FIPS Labels to an X60 Chassis

It is the responsibility of the CO to apply the tamper-evident labels to the module. Apply 10 FIPS labels to an X60 chassis as shown in Figure 9 and Figure 10. Each label position (numbered 1 through 10 in the two pictures) is explained in Table 9.

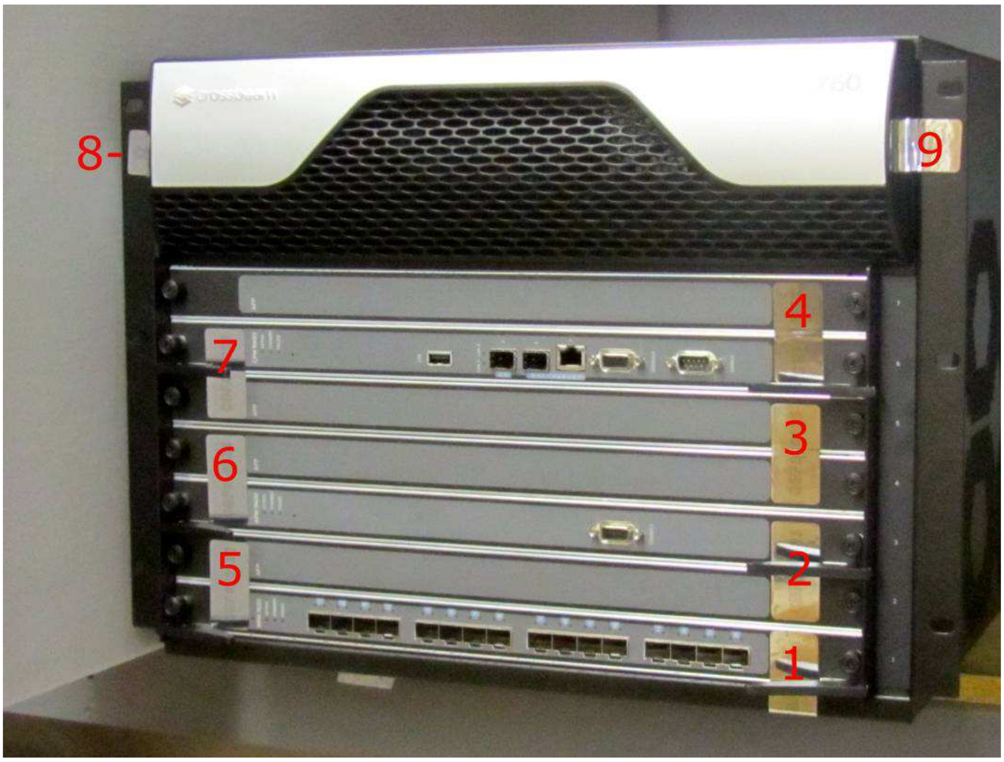

Figure 9 – X60 Tamper Evident Label Placement – Front

Table 9 – Label Application Instructions for the X60 Chassis

Label Number	Location	Description
1	Blade in bottom slot	1. Attach the first label (1) to the right side of the blade in the bottom chassis slot, starting at the top edge of the blade. 2. After applying the label from the top to the bottom of the blade, wrap the remainder of the label around the edge of the chassis. 3. Finish by applying the end of the label to the bottom of the chassis.
2 through 7	Blades and Air Flow Panels	Attach one label across each adjacent pair of blades as shown in Figure 9 above.
8 and 9	Bezel	Attach a label between the left and right sides of the bezel and the chassis, ensuring that the label fits snugly into the corner between the bezel and the chassis.
10	Fan Tray	At the rear of the chassis, attach a label to the fan tray and the chassis as shown in Figure 10.

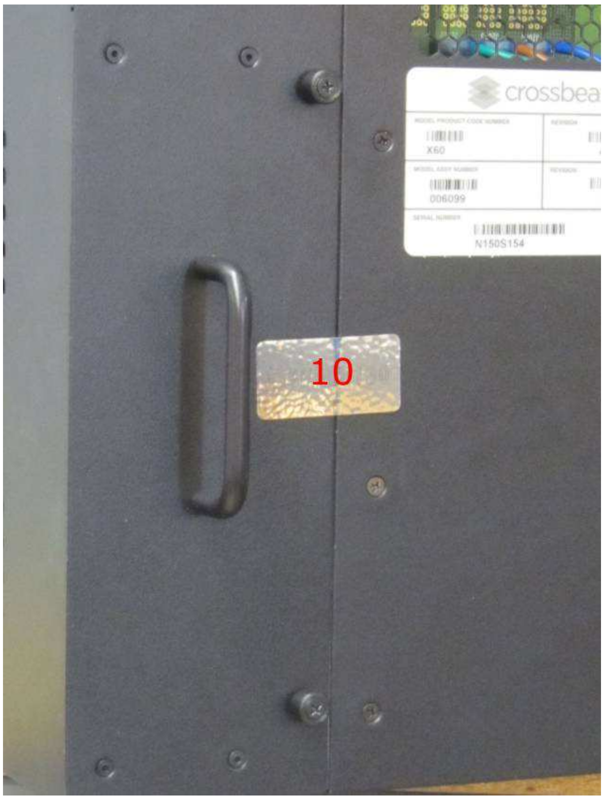

Figure 10 – X60 Tamper Evident Label Placement – Back

3.1.1.5 Applying FIPS Labels to an X80-S Chassis

Apply 19 FIPS labels to an X80-S-AC chassis as shown in Figure 11 and Figure 12 and as described in Table 10 below.

Apply 17 FIPS tamper-evident labels to an X80-S-DC chassis as described in Table 11 below.

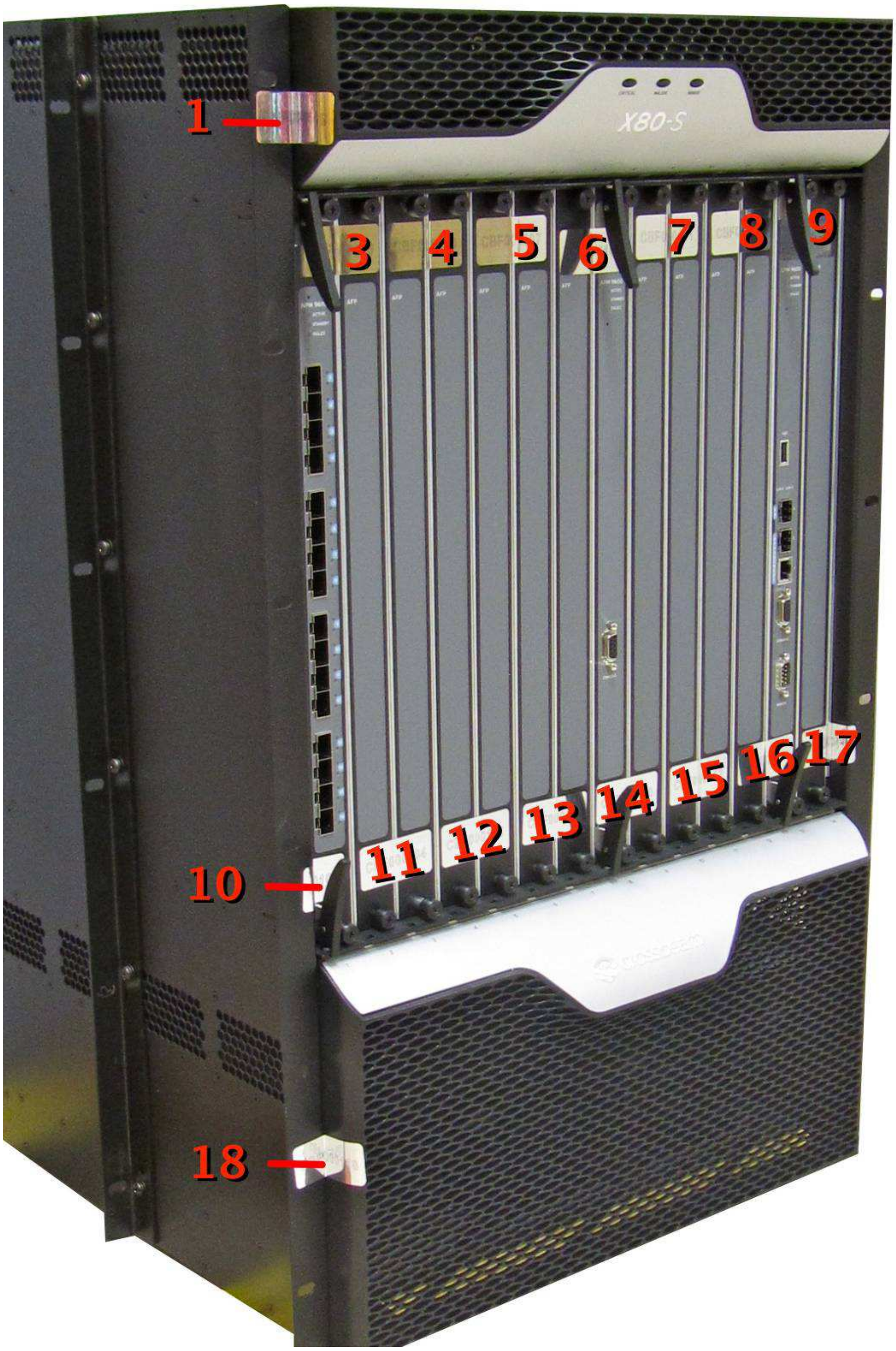

Figure 11 – X80-S Tamper Evident Label Placement – Left

Table 10 – Label Application Instructions for the X80-S-AC Chassis

Label Number	Location	Description
1 and 2	Upper Bezel	Attach a label between the left and right sides of the upper bezel and the chassis, ensuring that the label fits snugly into the corner between the chassis and the bezel.
3 through 9 and 11 through 16	Blades and Air Flow Panels	Attach one label across each adjacent pair of blades as shown in Figure 11, above.
10 and 17	Blades and Air Flow Panels	1. Attach label 10 to the bottom of the blade in the leftmost chassis slot, starting at the right edge of the blade. 2. After applying the label from the right to the left of the blade, apply the remainder of the label to the adjacent part of the chassis. 3. Finish by applying the end of the label to the front of the chassis. **NOTE:** For label 17, use a similar approach, but start on the left side of the rightmost blade.
18 and 19	Lower Bezel	Apply a label to the left and right sides of the lower bezel so that the label is attached to the bezel and the chassis, as shown in Figure 11 and Figure 12. Ensure that the label fits snugly into the corner between the chassis and the bezel.

Table 11 – Label Application Instructions for the X80-S-DC Chassis

Label Number	Location	Description
1 and 2	Upper Bezel	Attach a label between the left and right sides of the upper bezel and the chassis, ensuring that the label fits snugly into the corner between the chassis and the bezel.
3 through 9 and 11 through 16	Blades and Air Flow Panels	Attach one label across each adjacent pair of blades as shown in Figure 11, above.
10 and 17	Blades and Air Flow Panels	1. Attach label 10 to the bottom of the blade in the leftmost chassis slot, starting at the right edge of the blade. 2. After applying the label from the right to the left of the blade, apply the remainder of the label to the adjacent part of the chassis. 3. Finish by applying the end of the label to the front of the chassis. **NOTE:** For label 17, use a similar approach, but start on the left side of the rightmost blade.
NOTE: The X80-S-DC chassis has no lower bezel. As a result, there is no need to apply labels 18 and 19 when dealing with this chassis type.		

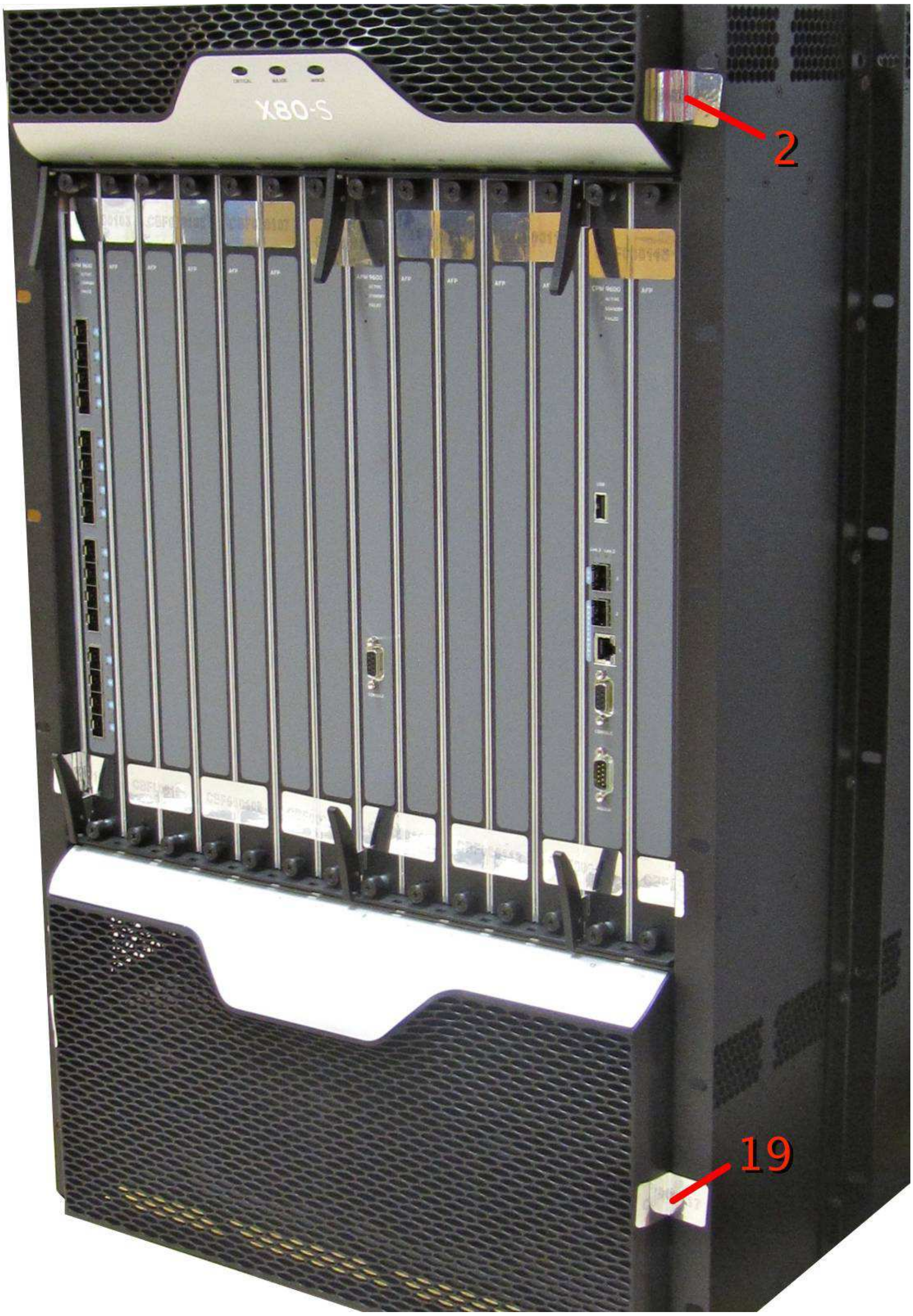

Figure 12 – X80-S Tamper Evident Label Placement – Right

3.1.1.6 Replacing a Label

The CO is responsible for the direct control and observation of any changes to the equipment, such as reconfigurations where the tamper evident labels or security appliances are removed or installed to ensure that the security of the equipment is maintained during such changes and that the module is returned to a FIPS-Approved state.

If any label has been compromised, either deliberately or by accident, it must be replaced immediately using the procedures in this document.

If a label must be compromised as part of the maintenance or replacement procedure, replace it using the procedures in this document.

3.1.1.7 Label Storage

The CO is responsible for securing and having control at all times of any unused labels. The recommended storage conditions are:

- Temperature: 20°C – 25°C (68°F – 77°F)
- Relative Humidity Less than 50%

When stored under these conditions, the shelf life of labels is 1 year.

3.1.2 X60 and X80-S FIPS Mode Configuration

Once all necessary setup procedures have been performed as described in the preceding section, the module needs to be configured to comply with FIPS 140-2 requirements. Once configured as described in this section, the module will be considered to be in the FIPS-Approved mode, which can be verified at any time by executing the show fips-mode command via the CLI.

To configure the module for FIPS mode, log into the CLI and run the “configure fips-mode” command. This command initiates a series of scripts that automatically check for running insecure services and configuration settings. If the check finds any insecure services running, the administrator is notified and must manually disable the insecure services and re-run the “configure fips-mode” command. Once the configuration is complete, the system prompts to change the administrator’s password. The administrator who ran the command is now the CO for the system. Once this step is complete, the module is considered to exist in a well-defined state for the first time and is operating in FIPS mode.

Only the FIPS-Approved VAPs found in Table 4 can be run on the APM-9600 while in FIPS mode. The CO may get into the vap-group context only for limited configuration tasks.

3.1.3 Firmware Version Verification

To ensure that the module is running the validated version of the module firmware, operators should compare the running versions to those documented in this Security Policy. To display the running version of the firmware, an operator must type the “show current-release” command via the CLI.

3.1.4 FIPS Mode Compliance

When setup, installed, and configured per the guidance provided in Section 3.1 of this document, the module is considered to be in a well-defined FIPS-Approved mode of operation. Deviation from this guidance will result in non-compliance.

Additionally, the guidance provided below must be followed to ensure that the module remains in a FIPS-Approved mode of operation. Failure to do so will result in non-compliance.

- Never install a non-FIPS-validated version of the module.

- Although a `configure no fips-mode` command is available, the CO should never use this command.

The CO must periodically ensure that the labels or blade slots do not show any signs of tampering. Evidence of tampering can be indicated by any of the following:

- Deformation of the label or “dot” pattern visible
- Label appearing broken or torn
- Missing label (in parts or full) from its expected position
- Warped or bent metal covers
- Scratches in the paint of the module

In case of any evidence indicating that the physical security has been violated, it is up to the CO to ensure that the module is secured in terms of its functionality and re-apply the tamper evident labels, following the procedure as described in Section 3.1.1. If required, the CO should perform a reboot or follow the Zeroization process as described in Section 3.2.2. Additionally, the CO should keep all unused labels in a secure location at all times.

3.2 Crypto-Officer Guidance

The CO can initiate the execution of self-tests and can access the module’s status reporting capability. Self-tests can be initiated at any time by re-loading the module or rebooting the module.

3.2.1 Management

It is the responsibility of the CO to ensure that the module is set up to run securely. Please refer to Section 3.1.4 above for guidance that the CO must follow for the module to remain in a FIPS-Approved mode of operation. Additionally, the CO should be careful to protect any secret or private keys in his possession.

For details regarding the management of the modules, please refer to the *Crossbeam XOS Configuration Guide*.

3.2.2 Zeroization

The module stores an RSA keypair as plaintext in disk memory.

There are many CSPs within the module’s cryptographic boundary, including private keys, operator passwords, and configuration files. All ephemeral keys used by the module are zeroized when the module is rebooted, power is removed, or upon session termination. CSPs reside in disk memory and Random Access Memory (RAM). CSPs in RAM are zeroized when the module is rebooted, power is removed, or the process using the CSP is terminated or completed. CSPs in disk memory are zeroized when overwritten by another CSP.

3.2.3 Non-Approved Mode of Operation

The X60 and X80-S Platforms contain both an Approved and Non-Approved mode of operation. Instructions on how to place the module into an Approved mode of operation are available in Section 3.1. To take the module out of an Approved mode of operation, the CO can call “configure no fips-mode”.

When operating in a Non-Approved mode, the module provides all cryptographic algorithms listed in Table 7 in a non-compliant form, with the addition of the following services:

Table 12 – Non-FIPS mode Services

Service	Non-Approved Algorithms

Telnet is enabled
`configure ip telnet`
`show ip telnet`
	None

Installation and use of non-FIPS OS and VAP OS Kernels
`configure vap-group vap-count`
`configure vap-group max-load-count`
`configure vap-group ap-list`
`rebuild-vap-group`
	None

Can configure non-FIPS OS and VAP OS Kernels
`application`
`application-update`
`application-upgrade`
	None

Automated workflow system commands are available:
`automated-workflow-menu`
`automated-workflows`
`show automated-workflow-progress`
	None

SNMP[14] support is enabled
`show snmp`
`configure snmp-user`
`show snmp-user`
	None

RMON[15] support is enabled
`configure rmon`
`show rmon`
`show traplog`
	None

LDAP[16] support is enabled
`configure ldap-parameter`
`show ldap-parameters`
`configure ldap-server`
	None

RADIUS[17] support is enabled
`configure radius-server`
`show radius-server`
	None

Remote syslog support is enabled
`configure logging server`
`show logging server`
	None

FTP[18] support is enabled
`configure ip ftp`
`show ip ftp`
`validate-fips-configuration`
	None

[14] SNMP – Simple Network Management Protocol

[15] RMON – Remote Monitoring

[16] LDAP – Lightweight Directory Access Protocol

[17] RADIUS – Remote Access Dial-In User Service

[18] FTP – File Transfer Protocol

Service	Non-Approved Algorithms

GUI[19] is enabled (informational displays only, no access to configure the system)
`configure web-server`
`show web-server`
	Uses non-approved cryptography for HTTPS connections (non-validated RSA, AES, and TDES).

Unix shell access is allowed
`unix`
`exec`
`cd`
`pwd`
`dir`
	None

Root shell is enabled
`cd`
`pwd`
`dir`
	None

CPM configuration options are available
`configure cp-redundancy`
`configure module`
`configure cp-action`
`configure cp-action disk-error`
`show cp-disk-error`
`cp-disk-scheme`
`cp-next-boot`
`reset-cp-serial`
`reset-configuration`
`configure reset-password`
	None

Routing protocol configuration options are available
`configure routing-protocol`
`configure routing-protocol-services`
`routing-protocol`
`routing-protocol-services`
	None

Admin can upgrade firmware `upgrade`	None
Debug command is available `debug`	None

Archiving tools are available
`archive`
`archive-vap-group`
	None

Additional SSH options `ssh`	Blowfish, CAST-128, RC4
RSA Keygen using libgcrypt	RSA keygen 1024-, 1536- , 2048- , 3072- , and 4096-bit via non-approved PRNG.
DSA PQG(gen) and sign/verify using libgcrypt	DSA PQG(gen), sign/verify 1024-bit

Additionally, the services listed in Table 6 are available to the user of the module and can be run in a non-Approved form. While operating in a non-Approved mode, all module services are available to all operators with access to the module.

[19] GUI – Graphical User Interface

3.3 User Guidance

Users do not have the ability to configure sensitive information on the modules, with the exception of their own passwords. Users must be diligent to pick strong passwords and must not reveal their passwords to anyone. Users should not increase the password duration interval beyond 1 month.

4 Acronyms

This section describes the acronyms.

Table 13 – Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
AFP	Air Flow Panel
ANSI	American National Standards Institute
APM	Application Processor Module
CAST	Carlisle Adams Stafford Tavares
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPM	Control Processor Module
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
Gbps	Gigabits Per Second
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
IPS	Intrusion Prevention System
KAT	Known Answer Test
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
N/A	Not Applicable
NIST	National Institute of Standards and Technology

Acronym	Definition
NPM	Network Processor Module
OFB	Output Feedback
OS	Operating System
PKCS#1	Public Key Cryptography Standard #1
PRNG	Pseudo-Random Number Generator
PSS	Probabilistic Signature Scheme
RADIUS	Remote Access Dial-In User Service
RAM	Random Access Memory
RC4	Ron's Code 4
RMON	Remote Monitoring
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SFP	Small Form Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VAP	Virtual Application Processor

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com