Brocade® X6-8 and X6-4 Directors

FIPS 140-2
Non-Proprietary
Security Policy

Document Version 1.0

Brocade Communications Systems, Inc.

February 2, 2018

Document History

Version	Publication Date	Summary of Changes
1.0	February 2, 2018	Initial Release

Table of Contents:

Table of Tables

Table of Figures

1 Module Overview

The Brocade X6-8 and X6-4 are multiple-chip standalone cryptographic modules, as defined by FIPS 140-2. The cryptographic boundary for X6-8 and X6-4 Directors are the outer perimeter of the metal chassis including the removable cover, control processor blades, core switch blades, and port blades or filler panels. The module is a Fiber Channel and/or Gigabit Ethernet routing switch that provides secure network services and network management.

A validated module configuration is comprised of Fabric OS v8.1.0 (P/N: 63-1001736-01) installed on, a switch or backbone and a set of installed blades. The below platforms may be used in a validated module configuration:

Table 1 – Firmware Version

Firmware
Fabric OS v8.1.0

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.1 X6 and X4 Directors

Brocade X6-4 and X6-8 refer to two distinct 32 Gbps core Fiber Channel switch configurations. These configurations are based on two chassis, a common Control Processor blade, two different (32Gbps) Core blades; one 32Gbps FC port blade, and two FC extender blades.

1.1.1 Overview of X6 product and validated configurations

Table below shows the exact validated configuration of Chassis, Control Processor blade, Core blades, Fiber Channel (FC) Port blades, and extender blades for Brocade X6 family Directors

Table 2 – Validated X6-4 and X6-8 configurations

Configuration Name (see, Note 1, 5)	Chassis (see, Note 1)	Core blade(s) (Core) (see, Note 2)	Control Processor (CP) blade (see, Note 3)	Fiber Channel (FC) Port blade(s) (see, Note 4)	Fiber Channel (FC) Extender blade {Data Processor (DP)} (see, Note 3)
X6-4	BR-X64-0001 (80-1009190-01) - An 8 slot chassis with 4 slots for FC related blades. - Quantity 1	XBR-X64-0106 (80-1009341-01) - 32G Core blade for X6-4 chassis - Quantity 2	XBR-CPX6-0103 (80-1009332-01) - Control Processor blade - Quantity 2	BR-X6-2148 (80-1009225-01) - 48 ports bundled with 48 32G SFP+ optics blade - Quantity 1	BR-SX6-0001 (80-1009227-01) FC Extender blade - Quantity 2
X6-8	BR-X68-0001 (80-1009230-01) - A 12 slot chassis with 8 slots for FC related blades. - Quantity 1	XBR-X68-0106 (80-1009342-01) - 32G Core blade for X6-8 chassis - Quantity 2	XBR-CPX6-0103 (80-1009332-01) - Control Processor blade - Quantity 2	BR-X6-2148 (80-1009225-01) - 48 ports bundled with 48 32G SFP+ optics blade - Quantity 1	BR-SX6-0001 (80-1009227-01) FC Extender blade - Quantity 2

Notes for tables above:

1) There are two different chassis sizes:
    i) Four (4) slot chassis refers to as **X6-4** chassis.
        (1) After CP and Core blades are added to this chassis, four (4) slots will be left available for FC Port blades or FC Extender blades as specified in Table 2 above.
    ii) Eight (8) slot chassis refers to as **X6-8** chassis.
        (1) After CP and Core blades are added to this chassis, eight (8) slots will be left available for FC Port blades or FC Extender blades as specified in Table 2 above.
    iii) One chassis is required to assemble a validated configuration.
2) There are two (2) possible variations of core blades. Depending on the configuration being assembled (4 slot or 8 slot chassis) an appropriate Core blade is to be selected. This blade is required.
3) There is only one type of Control Processor (CP) blade for any one of the two possible X6 family of directors. This blade is required. This blade and the Data Processor (DP) extender blades are the only blades in these configurations which perform cryptographic processing.
4) One Fiber Channel port blade (48 ports with 32 Gbps SFP+ optics) was used as part of the configuration assembled.

5) Appropriate filler panel is to be used in each empty FC blade slot.

Table below lists power supply, fan assemblies, and filler panels supported on Brocade X6 Directors:

Table 3 – Brocade X6 Director Supported Power Supplies, Fan Assemblies, Filler Panels

SKU	Part Number	Description
BR-X6-RACNPIPSU-0104	80-1009326-01	Power supply - X6 power supplies with NPI (Non-port side Intake/ Port side exhaust) supporting both 4-slot and 8-slot; Regular AC Input Type with standard IEC Receptacle (100V-120V AC, 200V – 240V AC)
BR-X6-FANNPI-0122	80-1009441-01	X6, Fan assembly for non-port side intake (NPI)
XBR-X6-0130	80-1009349-01	Power Supply Filler Panel
XBR-X6-0128	80-1009348-01	Fan Filler Panel
XBR-X6-0128	80-1009348-01	Filler Panel

Figure 1 illustrates representative configuration of the X6-4 cryptographic module.

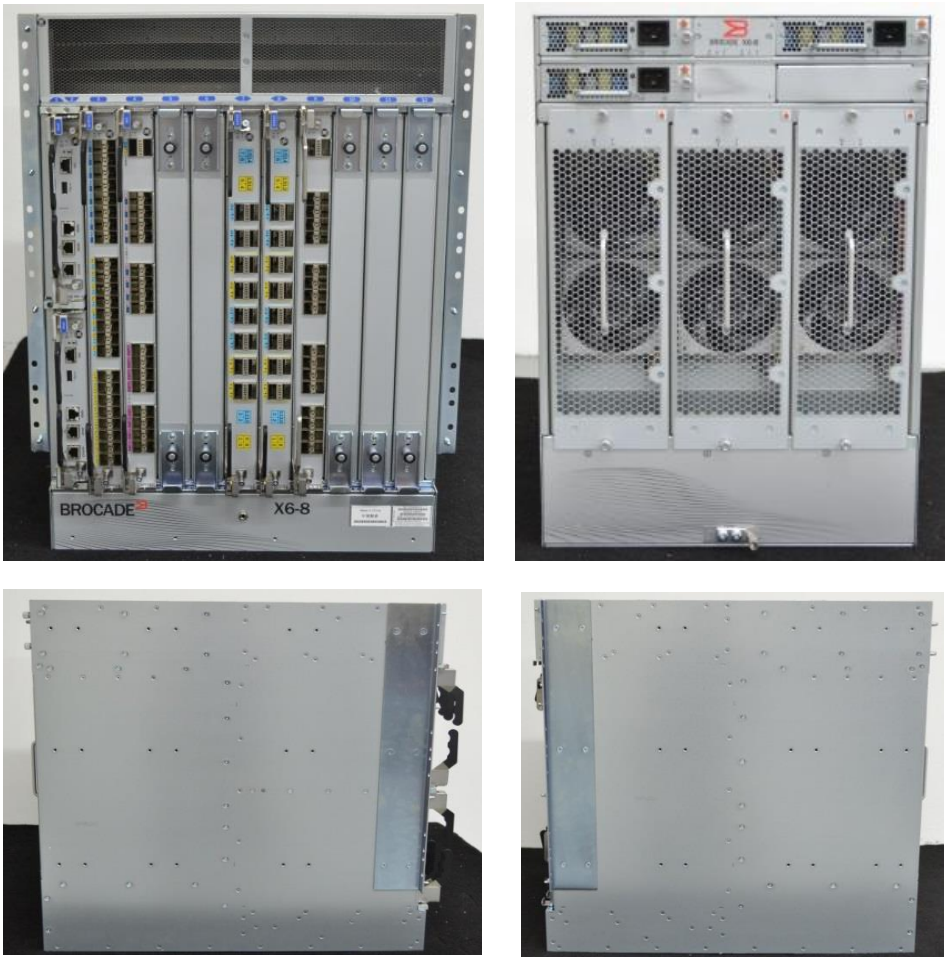
Figure 1 – Brocade X6-4 (clockwise from top left pictures refer to front, rear, left and right sides)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 2 illustrates representative configuration of the X6-8 cryptographic module.

Figure 2 – Brocade X6-8 (clockwise from top left pictures refer to front, rear, left and right sides)



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 4 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

3 Modes of Operation

Module State: Non-compliant FIPS state:

An uninitialized module provides an operational environment which is not a FIPS compliant state (it is a non-compliant FIPS state). A Crypto-officer must follow the instructions in section 3.1.2 to configure the module in order to place the module in a FIPS compliant state.

Module State: Compliant FIPS state:

A module must be configured to provide a compliant FIPS state. Section 3.1.2 provides the required detailed instructions on how to configure the module into a compliant FIPS state.

The Crypto-Officer must use the admin user-account to login to the module and configure the module into FIPS compliant state (see section 3.1.2.) These configuration steps, also, configure the module to use FIPS Approved cryptographic algorithms (see Table 5, Table 6, Table 7 and Table 8).

Term Crypto-Officer in this document refers to the Crypto-Officer who has logged in using the admin user-account.

Mode of Operation: FIPS Approved mode

After module is configured to enter FIPS compliant state it must operate adhering to use only the FIPS approved cryptographic algorithms (see Table 5, Table 6, Table 7 and Table 8), the FIPS approved services and follow the security rules defined in this Security Policy.

NOTE: Operating the module with Non-Approved FIPS cryptographic algorithms (see Table 9) or FIPS Non-Approved services (see Table 10) is in explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.

Mode of Operation: FIPS Non-Approved mode

NOTE: A module configured to operate in FIPS compliant state can be re-configured by the Crypto-Officer to use FIPS Non-Approved cryptographic algorithms (see Table 9) and/or FIPS Non-Approved services (see Table 10). Operating the module with Non-Approved FIPS cryptographic algorithms or FIPS Non-Approved services is in explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.

3.1 FIPS Compliant State and Approved Mode of Operation

This section provides information on how to configure the module to create a FIPS compliant state. It also describes the requirements for providing a FIPS Approved operational environment.

This section provides the following information:

A. Reference to approved algorithms and their CAVP granted certificates (section 3.1.1),

B. The initialization steps (section 3.1.2) to configure the module to operate in Approved mode of operation (FIPS enabled), and

C. Steps and procedures (section 3.1.3) on how to examine that the module is operating in Approved mode of operation (FIPS enabled).

Note that special attention must be paid to section, 3.2, Non-Approved FIPS cryptographic algorithms and services (post following steps to enable FIPS mode), to understand additional requirements for operating in Approved mode of operation.

3.1.1 FIPS Approved Cryptographic Algorithms

3.1.1.1 Brocade X6-4 and X6-8 Control Processor (CP) Cryptographic Algorithms Certificates

Table 5 – Brocade X6-4 and X6-8 Directors, Control Processor (CP), Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4243	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR	128, 192, and 256	Data Encryption/Decryption ([1])
4243	AES	FIPS 197, SP 800-38A	CFB	128	Data Encryption/Decryption
991	CVL, SSHv2, TLSv1.0/v1.1, TLSv1.2, SNMPv3	SP 800-135rev1			Key Derivation
992	CVL, Partial ECDH	SP 800-56Arev2	ECC CDH Primitive	P-256, P-384	Shared Secret Computation ([2])
990	CVL, Partial DH	SP 800-56Arev2	FFC	(2048, 256)	Shared Secret Computation
990	CVL, Partial ECDH	SP 800-56Arev2	ECC	P-256, P-384	Shared Secret Computation ([3])
1322	DRBG	SP 800-90Arev1	CTR_DRBG	256	Deterministic Random Bit Generation
1133	DSA	FIPS 186-4	PQG(gen), PQG(ver), KeyPairGen	2048	Key Pair Generation, PQG(Gen) and PQG(Ver) ([4])
983	ECDSA	FIPS 186-4	PKG. PKV, SigGen, SigVer	P-256, P-384	Digital Signature Generation and Verification ([5])
2781	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication ([6])
2289	RSA	FIPS 186-4	186-4KEY (gen), PGM (ProbPrimeCondition), ALG [RSASSA-PKCS1_V1_5]	2048	Digital Signature Generation and Verification ([7])
3480	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest

[1] AES (Cert. #4243) supports the ECB mode only as a pre-requisite for other implementations in the module. AES ECB mode is not invoked independently by any approved service in the FIPS Approved mode.
[2] CVL (Cert. #992): P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[3] CVL (Cert. #990): P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[4] DSA (Cert. #1133) is only used as a prerequisite for CVL (Cert. #990)
[5] ECDSA (Cert. #983): P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[6] HMAC (Cert. #2781): HMAC-SHA-224 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[7] RSA (Cert. #2289): The only mode utilized by the module is RSA 2048 with SHA-256. All other modes and key sizes are latent functionality.

3.1.1.2 Brocade X6-4 and X6-8 – Data Processor (DP) Algorithms Certificates

Table 6 – Brocade X6-4 and X6-8 Directors, Data Processor (DP), Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4116	AES	FIPS 197, SP 800-38A	CBC	256	Data Encryption/Decryption
4116	AES	FIPS 197, SP 800-38D	GCM	256	Data Encryption/Decryption
924	CVL, IKEv2	SP 800-135rev1			Key Derivation
923	CVL, Partial ECDH	SP 800-56Arev2	ECC	P-384	Shared Secret Computation
1239	DRBG	SP 800-90Arev1	CTR_DRBG	256	Deterministic Random Bit Generation
934	ECDSA	FIPS 186-4	PKG	P-384	Key Pair Generation
2688	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication
3386	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest

3.1.1.3 Brocade X6-4 and X6-8 – Blitzer FPGA Algorithms

Table 7 – Brocade X6-4 and X6-8 Directors, Blitzer FPGA, Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4145	AES	FIPS 197, SP 800-38A	ECB	256	Data Encryption
4145	AES	FIPS 197, SP 800-38D	GCM	256	Data Encryption/Decryption

For additional information on transitions associated with the use of cryptography refer to NIST Special Publication SP800-131Ar1. This document can be located on the CMVP website at:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

FIPS Approved mode enables:

- HTTPS TLS v1.0/1.1 and TLS v1.2
- SSHv2
- IKEv2
- SNMPv3

Next page →

The following Non-Approved algorithms and protocols are allowed within the Approved mode of operation:

Table 8 – Non Approved Algorithms Allowed in FIPS Mode

Algorithm	Caveat	Use
Diffie-Hellman (CVL Certs. #990 and #991)	Key agreement; key establishment methodology provides 112 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Certs. #990 and #991) Supported curves: P-256, P-384([8])	Key agreement; key establishment methodology provides 128 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Certs. #992 and #991) Supported curves: P-256, P-384([8])	Key agreement; key establishment methodology provides 128 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Certs. #923 and #924) Supported curve: P-384	Key agreement; key establishment methodology provides 192 bits of encryption strength.	Key establishment within IKEv2 protocol
HMAC-MD5	Used in RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)	RADIUS authentication
HMAC-SHA-1-96 ([9])	Used in SNMPv3 (HMAC-SHA-1-96 is not exposed to the operator)	SNMPv3
HMAC-SHA-384-192 Note: See HMAC certificate #2688 in Table 6, above	Used in IKEv2 for message integrity (HMAC-SHA-384-192 is not exposed to the operator)	IKEv2
MD5	Used in storage of passwords (MD5 is not exposed to the operator)	Used in store password hash
NDRNG – entropy data		Seeding for the Approved DRBG. The minimum number of bits of entropy generated by the module for use in key generation is 112-bits.
RSA Key Wrapping	Provides 112 bits of encryption strength.	Key establishment within TLS v1.0/1.1 and TLS v1.2

Next page →

[8] P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[9] Key size for HMAC-SHA-1-96 is 20 bytes as per CSP #33 – "SNMPv3 Auth and Priv Secrets" (see, section 15)

3.1.2 Creating FIPS Compliant State and Entering FIPS Approved mode

Physical Security:

Follow instructions provided in section 9 (Physical Security Policy) to apply the required tampered seals. Validate that the tamper evident seals are applied and the module is untampered.

Module Configuration:

The cryptographic module IS NOT operating in the Approved mode of operation until the required configurations steps in this section are followed to initialize the module. When the module is yet to be initialized and configured to enter the FIPS compliant State, the module is known to be in a non-compliant FIPS state.

In such non-compliant FIPS state the module provides access to three different user accounts: root user-account, admin user-account, and user user-account. The Crypto-Officer must use the admin user-account to login to the module and configure the module as per instructions provided below to enter the Approved mode of operation (to enable FIPS mode.)

After this configuration is complete, root user-account is permanently disabled and only admin and user user-accounts are left available to login to the module.

Term Crypto-Officer in this document refers to the Crypto-Officer who has logged in using the admin user-account.

3.1.2.1 Notes and Guidance to Crypto-Officer

A. Guidance for module being upgraded to FOS 8.1.0:
    1. Only a module running FOS 7.4.0 can be upgraded to FOS 8.1.0.

B. Following features and capabilities are not supported FIPS mode. Instructions listed below must be followed by the Crypto-Officer when configuring a device to operate in FIPS mode:

    1. Do not enable FC port authentication. This level of authentication is considered as plain text and not supported in Approved mode of operation (FIPS mode). The security it provides does not meet FIPS security requirements. This includes use of Common-Certs which are not supported in FIPS Mode.

    2. The client authentication feature for TLS clients is not supported in Approved mode of operation. The Crypto-Officer must not configure client authentications for TLS connections as it is not supported in Approved mode of operation (FIPS mode).

    3. Do not configure access-time feature for any users in the FIPS mode.
    The Crypto-Officer must not configure access-time feature. Access-time feature is not supported in Approved mode of operation.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

3.1.2.2 Cryptographic module initialization

The following is the procedure to enable FIPS mode on CP and DP. Unless explicitly mentioned all commands should be executed on the Active CP. Ensure that notes and guidance mentioned in Section 3.1.2.1 are reviewed and adhered to.

1. Login to the switch (to active CP in case of chassis) as an authorized user

2. Verify the firmware version using *firmwareshow* command
   a. *firmwareshow*

3. User Defined roles:
   User Defined role is not supported in FIPS mode. The Crypto-Officer must not use this feature. The Crypto-Officer must delete any User Defined roles which may exist prior to placing the module in FIPS mode.
   a. Examine existing User Defined roles by issuing the following CLI command:

      roleconfig --show -all

      If no User Defined roles is present then the above CLI command will report the following message:

      "There are no user-defined roles on the switch."

   b. If User Defined roles have been configured, then '*roleconfig --show -all*' command will display a list of defined roles. In this case, use the following CLI command to delete all existing User Defined roles.

      roleconfig --delete <role_name>

4. Configure the extension *blades in FCIP mode.*
   a. Execute extncfg –slot <slotno> --appmode fcip

   NOTE: Extension blades shall not be configured for Hybrid mode or the cryptographic module would not be deemed as FIPS 140-2 validated.

5. Zeroize the switch
   a. Execute zeroization to zeroize all the CSP on the Switch and DP
      i. If DP exists
         fipscfg --zeroize –dp
      ii. If DP does not exist
         fipscfg --zeroize
   b. Reboot the switch
      1. On both CP's explicitly execute *"reboot".*

6. Enable the self-tests mode using the command *'fipscfg --enable selftests'*
      i. If DP exists
         fipscfg --enable selftests –dp
      ii. If DP does not exist
         fipscfg --enable selftests

NOTE: Once this step occurs the cryptographic module will perform power-up self-tests during all subsequent power-ups regardless of whether the cryptographic module is in FIPS mode or non-FIPS mode. There is no service, method, or mechanism to disable such power-up self-tests thereafter.

7. Disable the non-secure ports using *ipfilter* CLI. Follow the procedure outlined below for disabling a given port. Use the same approach to disable port 80, 23 and 897 for both IPv4 and IPv6 rules

   For e.g.: For IPv4
   ipfilter --clone fips_ipv4 -from default_ipv4
   ipfilter --delrule fips_ipv4 -rule 2
   ipfilter --addrule fips_ipv4 -rule 2 -sip any -dp 23 -proto tcp -act deny -type INPUT -dip any
   ipfilter --delrule fips_ipv4 -rule 3
   ipfilter --addrule fips_ipv4 -rule 3 -sip any -dp 80 -proto tcp -act deny -type INPUT -dip any
   ipfilter --addrule fips_ipv4 -rule 7 -sip any -dp 897 -proto tcp -act deny -type INPUT -dip any
   ipfilter --addrule fips_ipv4 -rule 7 -sip any -dp 897 -proto udp -act deny -type INPUT -dip any
   ipfilter --delrule fips_ipv4 -rule 10
   ipfilter --delrule fips_ipv4 -rule 9
   ipfilter --addrule fips_ipv4 -rule 9 -sip any -dp "600-896" -proto tcp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv4 -rule 10 -sip any -dp "898-1023" -proto tcp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv4 -rule 11 -sip any -dp "600-896" -proto udp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv4 -rule 12 -sip any -dp "898-1023" -proto udp -act permit -type INPUT -dip any
   ipfilter --activate fips_ipv4

   For IPv6
   ipfilter --clone fips_ipv6 -from default_ipv6
   ipfilter --delrule fips_ipv6 -rule 2
   ipfilter --addrule fips_ipv6 -rule 2 -sip any -dp 23 -proto tcp -act deny -type INPUT -dip any
   ipfilter --delrule fips_ipv6 -rule 3
   ipfilter --addrule fips_ipv6 -rule 3 -sip any -dp 80 -proto tcp -act deny -type INPUT -dip any
   ipfilter --addrule fips_ipv6 -rule 7 -sip any -dp 897 -proto tcp -act deny -type INPUT -dip any
   ipfilter --addrule fips_ipv6 -rule 7 -sip any -dp 897 -proto udp -act deny -type INPUT -dip any
   ipfilter --delrule fips_ipv6 -rule 10
   ipfilter --delrule fips_ipv6 -rule 9
   ipfilter --addrule fips_ipv6 -rule 9 -sip any -dp "600-896" -proto tcp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv6 -rule 10 -sip any -dp "898-1023" -proto tcp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv6 -rule 11 -sip any -dp "600-896" -proto udp -act permit -type INPUT -dip any
   ipfilter --addrule fips_ipv6 -rule 12 -sip any -dp "898-1023" -proto udp -act permit -type INPUT -dip any
   ipfilter --activate fips_ipv6

8. Configure supported host keys for use for SSH:
   Delete the unsupported host key for SSH i.e. DSA and RSA using *sshutil delknownhost*

   ```
   sshutil delhostkey -rsa

   sshutil delhostkey -dsa
   ```

   NOTE: this action ensures that only ecdsa-sha2-nistp256 based SSHv2 host key are available for use in Approved mode of operation

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9. Configuring AAA authentication:

   NOTE: TACACS+ is not supported in FIPS mode and should not be enabled.

   If AAA authentication is to be used in FIPS mode, configure the preferred and supported AAA server (LDAP/RADIUS) using *aaaconfig* CLI command.

   a. Set the initial state
      i. Set the authentication to the local database
         aaaconfig --authspec "local"

         NOTE: By default, authentication is set using the local database.

   b. Requirements for CA certificate

      i. Existence of CA certificate is mandatory for RADIUS and/or LDAP services.

         1. Ensure that the CA certificate is imported using *seccertmgmt* CLI
            a. Ex: For radius:
               seccertmgmt import -ca -server radius

            b. Ex: For ldap:
               seccertmgmt import -ca -server ldap

      ii. CA certificate also must meet the requirement listed below:

         1. All certificates must be of RSA 2048 key pair signed with SHA256 hash

   c. Add the server
      i. If RADIUS server is used, then issue the following CLI command and ensure only '*peap-mschapv2*' is configured.

         aaaconfig --add <radius-serverip> -conf radius -a peap-mschapv2

      ii. If LDAP server is used, then issue the following CLI command,

         aaaconfig --add <ldap-serverip> -conf ldap -d <domain>

   d. Set the final authentication setting
      i. If setting up a RADIUS server, then issue the following CLI command:
         aaaconfig --authspec "radius;local"

      ii. If setting up a LDAP server, then issue the following CLI command:
         aaaconfig --authspec "ldap;local"

10. If in-flight encryption feature is enabled, disable it using *portcfgencrypt --disable <portnum>*

11. If management IP Sec feature is enabled, disable it using *ipsecconfig* CLI

12. If Inband Management feature is enabled, disable it using
    portcfg mgmtif <port num> disable.

13. In FIPS mode http is blocked and only https is allowed. For using https in FIPS mode, configure HTTPS using the seccertmgmt CLI with a third-party certificate

```
seccertmgmt import –ca –server https
seccertmgmt import –cert https
```

14. ***** CIPHER CONFIGURATION SETUP STEP *****
    Configure cipher using *seccryptocfg* CLI to configure ciphers for SSH, TLS, RADIUS and LDAP

    a. Export *default_strong* template from the switch.
       seccryptocfg ––export default_strong -server <server-ip> -name <username> -proto scp -file <filename>
    b. Edit the template to include only the ciphers as mentioned in section, 3.1.1 (FIPS Approved Cryptographic Algorithms.)
    c. Download the template and enable it

       seccryptocfg ––import <custom template name> -server <serverip> -name <username> -proto scp -file <filename>

       seccryptocfg ––apply <custom template name>

15. Enable secure protocols using *configurechassis* command

    configurechassis

    Configure…

    cfgload attributes (yes, y, no, n): [no] y

    Enforce secure config Upload/Download (yes, y, no, n): [no] y

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16. SNMP configurations

    a. Disable SNMPv1 using *snmpconfig –disable snmpv1* CLI command
    b. If SNMPv3 is to be used in FIPS mode,
        i. enable SNMPv3 and sec level to auth and Priv
        ii. Passwords for all users should be of minimum length 8
        iii. Auth protocol shall be SHA1
        iv. Priv protocol shall be AES128
        NOTE: DES must not be configured for SNMPv3

    E.g.: snmpconfig ––set snmpv3

    SNMP Informs Enabled (true, t, false, f): [false]

    SNMPV3 Password Encryption Enabled (true, t, false, f): [false] true
    Warning: The encrypted password cannot be decrypted. Do you want to continue? (yes, y, no, n): [no] y

    SNMPv3 user configuration(snmp user not configured in FOS user database will have default VF context and admin role as the default):
    User (rw): [snmpadmin1]
    Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 2
    New Auth Passwd:
    Verify Auth Passwd:
    Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (1..4) [2] 3
    New Priv Passwd:
    Verify Priv Passwd:

17. Passwords for default accounts (admin and user) must be changed after every zeroization to maintain FIPS 140-2 compliance. Change the default password for “admin” and “user” by pressing “Enter” instead of “Ctrl-C” after logging in as “admin”.

18. Modify the authutil policy in every VF present, to use hash sha256 and DH group 4 (setcontext to each VF and execute below commands):
    authutil ––set -h sha256
    authutil ––set -g 4

19. Disable bootprom using the CLI *fipscfg –disable bootprom.*

    a. Bootprom account can be disabled only as root.
    b. Enable root account using following CLI
        userconfig ––change root –e yes
    c. Login as “root” and disable the bootprom using
        fipscfg ––disable bootprom
    d. Login as “admin” again and disable “root” using
        userconfig ––change root –e no

Next page →

20. Verify if the switch is configured to be FIPS compliant
    a. Execute *'fipscfg --verify fips'*
    b. Execute *'fipscfg --verify fips -dp '* if DP exists
    c. Ensure that all conditions are met and the message is displayed that FIPS mode can be enabled.

    Ex: (Indicates of both failure and pass example)
    fipscfg --verify fips
    Standby firmware supports FIPS - PASS
    SELF tests check has passed - PASS
    Root account check has passed - PASS
    Radius check has passed - PASS
    Authentication check has passed - PASS
    Inflight Encryption check has passed - PASS
    IPSec check has passed - PASS
    IPv6 policies FIPS compliant - PASS
    IPv6 policies FIPS compliant - PASS
    SNMP is in read only mode. - PASS
    SNMP User password length check - PASS
    SNMP Users have no MD5 auth protocol check - PASS
    Bootprom access is disabled. - PASS
    Secure config upload/download is enabled. - PASS
    SSH DSA Keys check passed - PASS
    Inband Management interface is disabled - PASS
    Ipsecconfig is disabled. – PASS
    FCIP validations - PASS
    Certificates validation has passed - PASS
    SSH host key (RSA) validation has passed - PASS

21. If all the tests are PASS in above step, then proceed to enable FIPS mode.

22. Enable FIPS Mode
- Execute *'fipscfg --enable fips'*
    sw0:test> fipscfg --enable fips
    FIPS mode has been set to : Enabled

- Verify that the FIPS mode has been set to 'Enabled'' using *'fipscfg --show'*
    sw0:test> fipscfg --show
    FIPS mode is : Enabled
    FIPS Selftests mode/status is : Enabled/None

- Execute *'fipscfg --enable fips -dp'* to enter DP FIPS mode

    sw0:test> fipscfg --enable fips -dp
    FIPS mode has been set to : Enabled
    DP FIPS mode has been set to : Enabled

- Power-cycle the chassis. Alternatively, reboot the active node. On a dual CP system, reboot the standby as well.

- Login to the Active node as an authorized user, and verify that the self-tests mode is set to ' Enabled/Pass'

- On a dual CP system, ensure that the standby has booted up properly.

  Sw0sar068:test> fipscfg --show
  FIPS mode is : Enabled
  FIPS Selftests mode/status is : Enabled/Pass

- If you are entering DP FIPS mode

  sw0:FID128:admin> fipscfg --show
  FIPS mode is : Enabled
  FIPS Selftests mode/status is : Enabled/Pass
  diffie-hellman-group-exchange-sha256 is : Enabled
  Slot: 4
  DP FIPS mode is : Enabled
  DP FIPS Selftests mode/status is : Enabled/Pass
  Slot: 8
  DP FIPS mode is :Enabled
  DP FIPS Selftests mode/status is : Enabled/Pass
  sw0:FID128:admin>

23. Enable the DH key size configuration using *'fipscfg --enable dh'*

24. The tamper evident seals supplied in FIPS Kit Brocade XBR-000195 (P/N: 80-1002006-02) must be installed as defined in section 13 (Appendix A: Tamper Label Application).

25. After successful completion of step 24, your switch is now in FIPS Approved mode

26. **WARNING: At this point, the algorithms in Section 3.2, Table 10 are disabled. Any use of these algorithms, or an attempt by the operator to revert the configuration specified in Section 3.1.2.2, is an explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.**

    NOTICE: Upon successful completion of all configuration steps in Section 3.1.2.2, self-tests will forevermore be enabled, even if the operator violates this Security Policy which implicitly toggles the module out of FIPS mode after configuration.

3.1.3 How to determine that an Approved mode of operation is selected

After all steps specified in section 3.1.2.2 (Cryptographic module initialization) are performed, the operator shall perform the following instructions to examine the mode of operation:

1. Check for successful status of the powerup Self-Tests. For details, see section 8, Security Rules.
2. Confirm the firmware version using `firmwareshow` command
   a. `firmwareshow`
3. Check status of FIPS mode
   a. `fipscfg –show`
4. Validate that the tamper evident seals are applied and the module is untampered (see section 9.2 for details).
5. Do not configure the device to use any of the algorithms listed in section 3.2, Non-Approved FIPS cryptographic algorithms and services.

3.2 Non-Approved FIPS cryptographic algorithms and services

This section lists all Non-Approved FIPS cryptographic algorithms and all Non-Approved FIPS services which MUST NOT be used. The use of any such algorithms or services, is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy.

The module supports a Non-Approved mode of operation. This mode of operation exists when:

1. After the module has been initialized and configured as per Section 3.1, the Crypto-Officer reverts **any** of the configuration procedures and executes the Non-Approved services in Table 10 using the Non-Approved Algorithms in Table 9.

The algorithms marked "non-compliant" are not compliant simply because they are invoked in the Non-Approved mode of operation, by a Non-Approved mode service.

Table 9 – Non-Approved Algorithms – post invoking Approved mode (FIPS enabled)

Algorithm	Use
AES 128, 192 and 256 (non-compliant)	Encryption / Decryption
CAMELLIA 128 and 256	Encryption / Decryption
DES	Encryption / Decryption
Diffie-Hellman (non-compliant)	Key Establishment
DSA (non-compliant)	Digital Signature
EC-DH (non-compliant)	Key Establishment
ECDSA (FIPS 186-4; non-compliant)	Digital Signature
HMAC-MD5	Message Authentication
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 (non-compliant)	Message Authentication
KDF (SSHv2, IKEv2, SNMPv3, TLS) (non-compliant)	Key Derivation
MD5	Message Digest
PSK	Key Establishment
RC-4	Encryption / Decryption
SEED	Encryption/ Decryption
SHA-1, SHA-256, SHA-384 (non-compliant)	Message Digest
Triple-DES (non-compliant)	Encryption / Decryption

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

These functions and services are non-compliant and disallowed in Approved mode of operation.

Table 10 – Functions/Services, Roles in Non-Approved Mode Services

Crypto Function/Service	User Role Change Access	Additional Details
Ciphers, Message Authentication Codes, Key Exchange, Digital Signature, and KDF algorithms for TLS	Crypto-Officer	Cipher: - aes128-cbc (non-compliant), aes256-cbc (non-compliant), aes128-gcm (non-compliant), aes256-gcm (non-compliant) - camellia-128, camellia-256 - des - seed - rc-4 - triple-des (non-compliant) Message Authentication Code: - hmac-sha-1, hmac-sha-256 (non-compliant), hmac-sha-384 (non-compliant) Key Exchange: - dh-dss, dh-rsa (non-compliant) - dhe-dss, dhe-rsa (non-compliant) - ecdh (non-compliant) - ecdhe (non-compliant) - psk Digital Signature: - ecdsa (non-compliant) - rsa (non-compliant) KDF: - TLSv1.0/1.1 (non-compliant), TLSv1.2(non-compliant)
Ciphers, Message Authentication Codes, Key Exchange, and KDF algorithms for SSHv2	Crypto-Officer	Cipher: - aes128-ctr (non-compliant), aes192-ctr (non-compliant), aes256-ctr (non-compliant), aes128-cbc (non-compliant), aes192-cbc (non-compliant), aes256-cbc (non-compliant) - 3des-cbc (non-compliant) Message Authentication Code: - hmac-md5 - hmac-sha1 (non-compliant), hmac-sha2-256 (non-compliant), hmac-sha2-512 (non-compliant) Key Exchange: - ecdh-sha2-nistp256 (non-compliant), ecdh-sha2-nistp384 (non-compliant), ecdh-sha2-nistp521 (non-compliant) - diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256 (non-compliant) - diffie-hellman-group1-sha1, diffie-hellman-group14-sha1 KDF: - SSHv2 (non-compliant)
Common Certificates for FCAP and HTTPS	Crypto-Officer	FCAP and HTTPS are supported with certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)

Crypto Function/Service	User Role Change Access	Additional Details
SNMP	Crypto-Officer	SNMPv1 (plaintext) and SNMPv3 KDF (non-compliant); Algorithms: AES128 (non-compliant), SHA-1 (non-compliant) and MD5
RADIUS or LDAP	Crypto-Officer	PAP and CHAP authentication method for RADIUS (all considered as plaintext) LDAP and RADIUS is supported with CA certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant) LDAP uses TLS connections in non-FIPS mode without certificates
Telnet	Crypto-Officer	N/A – No algorithms (plaintext)
HTTP	Crypto-Officer	N/A – No algorithms (plaintext)
FTP	Crypto-Officer	Config Upload, Config Download, Support Save, FW Download, autoftp
Management IPSec	Crypto-Officer	Management Interface IPSec/IKEv2 (disabled for management interface)
In-Band Management Interface	Crypto-Officer	N/A – No algorithms (plaintext)
RSA	Crypto-Officer	RSA key size < 2048 bits for SSHv2 and TLS
Diffie-Hellman	Crypto-Officer	DH key size < 2048 bits for SSHv2
In-Flight Encryption	Crypto-Officer	DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm FCAP: Certificates with any key size signed by MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
TACACS+ authspec mode	Crypto-Officer	PAP or CHAP authspec is supported
FC-SP Authentication	Crypto-Officer	DH-CHAP and FCAP for FC-SP Authentication DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm FCAP supported with certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

4 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- Fiber Channel: Data Input, Data Output, Control Input, Status Output
- Management port: Control Input, Status Output
- Service port: Control Input, Status Output
- 1 GbE, 10 GbE & 40 GbE: Data Input, Data Output, Control Input, Status Output
- Ethernet Ports: Control Input, Status Output
- Serial port: Control Input, Status Output
- USB: Data Input, Data Output, Status Output
- Power Supply Connectors: Power Input
- LEDs: Status Output

4.1 LED Indicators

1. Chassis (1 each):
    a. WWN Status Interface LED
    b. POWER status LED
    c. FAN status LED
2. Blades:
    a. BR-X6-2148, Port blade (1 each)
        i. Green blade power LED
        ii. Amber blade status LED
        iii. Bicolor green/amber FC port status LEDs

    b. BR-SX6-001, Extension blade (2 each):
        i. Green blade power LED
        ii. Amber blade status LED
        iii. Bicolor green/amber 40 GbE and 10 or 1 GbE port status LEDs
        iv. Bicolor green/amber FC port status LEDs

    c. XBR-X64-0106, XBR-X68-0106, Core blade (2 each)
        i. Green blade power LED
        ii. Amber blade status LED
        iii. Bicolor green/amber QSFP port status LEDs

    d. XBR-CPX6-0103, Control Processor blade (2 each)
        i. Blade status LED
        ii. Blade power LED
        iii. Chassis beacon LED
        iv. Active (blue) CP LED
        v. 10/100/1000 Mb/s Ethernet port (MGMT) link status LED
        vi. 10/100/1000 Mb/s Ethernet port (MGMT) link activity LED
        vii. 10/100/1000 Mb/s Ethernet port (SERVICE) link status LED
        viii. 10/100/1000 Mb/s Ethernet port (SERVICE) link activity LED

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Table 11 – Port/Interface Quantities

Model	Port/Interface Type each						
	Fiber Channel Ports	1 GbE & 10 GbE	Ethernet	Serial Port	USB	Power Supply Connectors	LED
X6-4 Chassis Inc Fan/Power	n/a	n/a	n/a	n/a	n/a	2	6
X6-8 Chassis Inc Fan/Power	n/a	n/a	n/a	n/a	n/a	4	12
BR-X6-2148 Port blade	48	0	0	0	0	n/a	98
BR-X6-2148 Extension blade	16	16, 2 40GbE	0	0	0	n/a	36
XBR-X64-0106 Core blade X6-4	16	0	0	0	0	n/a	42
XBR-X68-0106 Core blade X6-8	32	0	0	0	0	n/a	80
XBR-CPX6-0103 Control Processor blade	0	1	2	1	1	n/a	8

4.2 LED Descriptions

Descriptions are same for both X6-4 and X6-8 Chassis.

Table 12 – Port blade LED descriptions

LED purpose	Color	Status
Power	Steady green	Blade is on.
	No light (LED is off)	Blade is not powered on.
Status	No light (LED is off)	Blade is either healthy or does not have power.
	Steady amber	Blade is faulty.
	Slow-flashing amber (on 2 seconds, then off 2 seconds)	Blade is not seated correctly or is faulty.
	Fast-flashing amber (on 1/2 second, then off 1/2 second)	Environmental range exceeded.
FC port Status	No light (LED is off)	Port has no incoming power, or there is no light or signal carrier detected.
		Polling is in progress.
		Connected device is configured in an offline state.
	Steady green	Port is online (connected to an external device) but has no traffic.
	Slow-flashing green (on 1 second, then off 1 second)	Port is online but segmented, indicating a loopback plug or cable or an incompatible switch.
	Fast-flashing green (on 1/4 second, then off 1/4 second)	Port is in internal loopback (diagnostic).
	Flickering green	Port is online, with traffic flowing through port.
	Steady amber	Port is receiving light or signal carrier, but it is not online yet.
	Slow-flashing amber (on 2 seconds, then off 2 seconds)	Port is disabled due to diagnostic tests or portDisable or portCfgPersistentEnable command.
	Fast-flashing amber (on 1/2 second, then off 1/2 second)	Transceiver or port is faulty.
	Alternating green/amber	Port is beaconing.

Table 13 – Extension blade LED description

LED purpose	Color	Status
Power	Steady green	Blade is operational.
	No light (LED is off)	Blade is not powered on.
Status	No light (LED is off)	Blade is either healthy or does not have power.
	Steady amber	Blade is faulty or initializing.
	Blinking amber and green.	Attention. Blade is not seated correctly or is faulty.
	Green	Blade is operational.
GbE port status	No light (LED is off)	Port has no incoming power, or is offline.
	Steady green	Port is online but has no traffic.
	Blinking green	Port is online, with traffic flowing through port.
	Steady amber	Transceiver or port has error or is faulty.
FC port status	No light (LED off)	Port has no incoming power, or there is no light or signal carrier detected.
		Polling is in progress.
		Connected device is configured in an offline state.
	Steady green	Port is online (connected to an external device) but has no traffic.
	Slow-flashing green (on 1 second, then off 1 second)	Port is online but segmented, indicating a loopback plug or cable or an incompatible switch.
	Fast-flashing green (on 1/4 second, then off 1/4 second)	Port is in internal loopback (diagnostic).
	Flickering green	Port is online, with traffic flowing through port.
	Steady amber	Port is receiving light or signal carrier, but it is not online yet.
	Slow-flashing amber (on 2 seconds, then off 2 seconds)	Port is disabled due to diagnostic tests or portDisable or portCfgPersistentEnable command.
	Fast-flashing amber (on 1/2 second, then off 1/2 second)	Transceiver or port has error or is faulty.
	Alternating green and amber	Port is bypassed.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Table 14 – CP blade LED descriptions

LED purpose	Color	Status
Power	Steady green	CP blade is on.
	No light (LED is off)	CP blade is not on.
Attention	No light (LED is off)	CP blade is either healthy or does not have power.
	Steady amber	If on for more than 5 seconds, the CP blade is faulty.
	Slow-flashing amber (on 2 seconds, then off 2 seconds)	CP blade is not seated correctly or is faulty.
	Fast-flashing amber (on 1/2 second, then off 1/2 second)	Environmental range exceeded.
Beacon	Steady white	LED illuminates white on both CP blades when chassisbeacon 1 is issued from management interface to locate chassis in equipment racks. To turn off beaconing, issue the chassisbeacon 0.
Ethernet link status (10 Gb/s port)	No light (LED is off)	Either an Ethernet link is not detected, or the blade does not have incoming power.
	Blinking green	Activity is present on link.
Ethernet link activity (10 Gb/s port)	No light (LED is off)	No activity on link.
	Blinking green	Activity is present on link.
Active CP	Steady blue	Active CP blade.
	No light (LED is off)	CP blade is either booting, negotiating to be active, or is the standby CP blade.
Ethernet link status (10/100/1000 Mb/s port)	No light (LED is off)	Ethernet link speed is 10 Mb/s or link is not established.
	LED is on	Ethernet link speed is 100/1000 Mb/s.
		Ethernet link is healthy and traffic is flowing through port.
Ethernet link activity (10/100/1000 Mb/s port)	No light (LED is off)	No activity on link.
	Blinking green	Activity is present on link.

Table 15 – Core routing blade LED descriptions

LED purpose	Color	Status
Power	Steady green	Blade is on.
	No light (LED is off)	Blade is not on.
Status	No light (LED is off)	Blade is either healthy or does not have power.
	Steady amber	Blade is faulty or the switch is still booting.
	Slow-flashing amber (on 2 seconds, then off 2 seconds)	Blade is not seated correctly or is faulty.
	Fast-flashing amber (on 1/2 second, then off 1/2 second)	Environmental range exceeded.
QSFP port status LED	No light (LED is off)	No QSFP module, all four QSFP ports are disabled
	Steady amber	QSFP module is in, all four ports have no signal/no sync.
	Blinking amber	Port is disabled or faulted, FC link activity, segmented, loopback mode, also during transition between cable plug in and all four ports online.
	Steady green	QSFP module is in and all ports are online.

Table 16 – Fan Card LED Descriptions

LED purpose	Color	Status
Power	No light (LED is off)	Card is not receiving power.
	Steady green	Card is receiving power.
Status	No light (LED is off)	Card is either healthy or does not have power.
	Steady amber	Card is faulty

Table 17 – Power supply LED descriptions

LED purpose	Color	Status
Power	No light (LED is off)	Power supply does not have incoming power and is not providing power to the device.
	Steady green	Power supply has incoming power and is providing power to the device.
	Flashing on once, and then off 5 seconds.	AC power disconnected.
	Flashing on two times, and then off 5 seconds.	48V is out of range.
Status	Flashing on three times, and then off 5 seconds.	12V is out of range.
	Flashing on four times, and then off 5 seconds.	AC input is under voltage.
	Flashing on five times, and then off 5 seconds.	Power supply assembly fan is faulty.
	Flashing on six times, and then off 5 seconds.	Over temperature protection.
	Flashing on seven times, and then off 5 seconds.	Power supply is disabled.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports the following operator roles listed in the table below. The cryptographic module enforces the separation of roles using role-based operator authentication. An operator must enter a username and its password to log in. The username is an alphanumeric string of maximum 40 characters. The password is an alphanumeric string of 8 to 40 characters chosen from 96 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the context of the module. At the end of a session, the operator must log-out. The module supports a maximum of 256 operators, five Radius servers and five LDAP servers that may be allocated the following roles:

Table 18 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer)	Role-based operator authentication	Username and Password
User (User role)	Role-based operator authentication	Username and Password
Security Admin	Role-based operator authentication	Username and Password
Fabric Admin	Role-based operator authentication	Username and Password
LDAP Server	Certificate based server authentication	LDAP Root CA certificate
RADIUS Server	Certificate based server authentication	RADIUS Shared Secret and RADIUS Root CA Certificate
Host/Server/Peer Switch	Role-based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)
IKEv2 Peer	Role-based operator authentication	IKEv2 Authentication Key or PKI (ECDSA P-384 signing (private) key)
SNMP	Role-based operator authentication	"Auth" and "Priv" passwords

5.2 Strength of Authentication Mechanism

Table 19 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum attempts possible within one minute is 20. The probability of successfully authenticating to the module within one minute is 20/96^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112 which is less than 1/1,000,000. The module will restrict the number of consecutive failed authentication attempts to 10. The probability of successfully authenticating to the module within one minute is 10/2^112 which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
Knowledge of a Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The maximum possible authentication attempts within a minute are 16 attempts. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.
Knowledge of IKEv2 Authentication Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^512, which is less than 1/1,000,000. The maximum attempts allowed in a one minute period are equal to one attempt. If an authentication error is detected, the session goes into a fault state, and no new attempts are allowed. Therefore, the probability of a random success in a one minute period is 1/2^512, which is less than 1/100,000.
Knowledge of IKEv2 ECDSA P-384 Private Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^192, which is less than 1/1,000,000. The maximum attempts allowed in a one minute period are equal to one attempt. If an authentication error is detected, the session goes into a fault state, and no new attempts are allowed. Therefore, the probability of a random success in a one minute period is 1/2^192, which is less than 1/100,000.

5.3 Command association and Service Descriptions

Table 20 – Service Descriptions

Service Name	Description	FOS Interface
FIPSCfg	Control FIPS mode operation and related functions.	Fipscfg
Zeroize	Zeroize all CSPs.	fipgscfg--zeroize
FirmwareManagement	Control firmware management.	firmwarecommit firmwaredownload firmwaredownloadstatus, firmwareshow
IKEv2 Negotiation - IPsec Traffic	Negotiate IKEv2 sessions, key security associations for IPsec	portcfg ipsec-policy portcfg fciptunnel
PKI	PKI configuration functions, including FOS switch certificates, SSL certificates and IKEv2 ECDSA P-384 certificates.	seccertmgmt
RADIUS	RADIUS configuration functions.	aaaconfig
LDAP	LDAP configuration functions.	aaaconfig
UserManagement	User and password management.	passwd passwdconfig userconfig
SSHv2 and TLS	Crypto configuration	seccryptocfg
SNMPv3	SNMPv3 configuration	snmpconfig

6 Access Control Policy

6.1 Roles and Services

Table 21 – Services Authorized for Roles

Services \ Roles	User	Admin (Crypto-Officer)	FabricAdmin	SecurityAdmin	LDAP Server	RADIUS Server	Host Server / Peer Switch	IKEv2 Peer	SNMP
FIPSCfg		X		X			X		
Zeroize		X		X					
FirmwareManagement	X	X	X	X					
PKI	X	X	X	X					
RADIUS		X		X		X			
LDAP		X		X	X				
UserManagement	X	X		X					
IKEv2 Negotiation-IPsec Traffic		X		X			X	X	
SSHv2 and TLS	x	X		X					
SNMPv3		X	X	X					X

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6.3 Definition of Critical Security Parameters (CSPs)

DH Private Key:

- DH Private Keys for use with 2048-bit modulus

SSHv2/SCP/SFTP CSPs:

- SSHv2/SCP/SFTP Encryption Keys
- SSHv2/SCP/SFTP Authentication Key
- SSHv2 KDF Internal State
- SSHv2 DH Shared Secret Key (2048 bit)
- SSHv2 ECDH Shared Secret Key (P-256)
- SSHv2 ECDH Private Key (P-256)
- SSHv2 ECDSA Private Key (P-256)
- Value of K during SSHv2 P-256 ECDSA session

TLS CSPs:

- TLS Private Key (RSA 2048)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS KDF Internal State
- TLS Session Keys - 128, 256 bit AES CBC
- TLS Authentication Key for HMAC-SHA-1 (160 bits) and HMAC-SHA-256

CP DRBG CSPs:

- CP DRBG Seed Material
- CP DRBG Internal State (V and Key)

Passwords:

- Passwords

RADIUS Secret:

- RADIUS Secret

IKEv2 and IPsec CSPs:

- DH Private Key (256 bits) (Used in IKEv2)
- DH Shared Secret (2048 bits) (Used in IKEv2)
- IKEv2 AES-256 Encrypt/Decrypt Keys
- ESP AES-256-GCM Encrypt/Decrypt Keys
- IKEv2 KDF State
- IKEv2 Authentication Key (PSK)
- IKEv2 ECDH P-384 Private Key
- IKEv2 ECDSA P-384 Private Key
- IKEv2 Integrity Key (HMAC-SHA-384)

DRBG Internal State and Entropy Data
(On Cavium)

- DRBG Internal State (V and Key) (On Cavium)
- Entropy Data (on Cavium)

SNMPv3 CSPs:

- SNMPv3 Auth and Priv password
- SNMPv3 KDF Internal State
- SNMPv3 Auth and Priv Secrets

6.4 Definition of Public Keys

DH Public Keys:

- DH Public Key (2048-bit modulus)
- DH Peer Public Key (2048 bit modulus)

TLS Public Keys:

- TLS Public Key (RSA 2048)
- TLS Peer Public Key (RSA 2048)

FW Download Public Key:

- FW Download Public Key (RSA 2048)

SSHv2 Public Keys:

- SSHv2 ECDSA Public Key (P-256)
- SSHv2 ECDSA Peer Public Key (P-256)
- SSHv2 ECDH Public Key (P-256)
- SSHv2 ECDH Peer Public Key (P-256)
- DH Public Key (2048-bit) (Used in IKEv2)
- DH Peer Public Key (2048-bit) (Used in IKEv2)

LDAP ROOT CA Public Key:

- LDAP ROOT CA certificate (RSA 2048)

RADIUS ROOT CA Public Key:

- RADIUS ROOT CA certificate (RSA 2048)

IKEv2 and IPsec Public Keys:

- IKEv2 ECDH P-384 Public Key
- IKEv2 ECDH P-384 Peer Public Key
- IKEv2 ECDSA P-384 Public Key
- IKEv2 ECDSA P-384 Peer Public Key

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6.5 Definition of CSPs Modes of Access

Table below defines the relationship between access to CSPs and the different module services. Please see Section 6.3 and Section 6.4 for explicit designation of CSPs and Public Keys. The modes of access shown in the table are defined as follows:

- R: Read
- W: Write
- N: No Access
- Z: Zeroize (Session Termination and "fipscfg –zeroize" command)

Table 22 – CSP Access Rights within Roles & Services

Services \ CSPs	SSHv2/SCP/SFTP CSPs	DH Private Keys	TLS CSPs	CP DRBG Seed Material / Internal State	DRBG Internal State and Entropy Data (On Cavium)	Passwords	RADIUS Secret	IKEv2 and IPsec CSPs	SNMPv3 CSPs
FIPSCfg	N	N	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	R	N	N	N	N	N	N	N
PKI	RW	RW	N	RW	N	N	N	N	N
RADIUS	N	N	N	N	N	RW	RW	N	N
LDAP	N	N	N	N	N	N	N	N	N
UserManagement	N	N	RW	RW	N	RW	N	N	N
IKEv2 Negotiation – IPsec Traffic	N	N	N	N	RW	N	N	RW	N
SSHv2 and TLS	RW	RW	RW	N	N	RW	N	N	N
SNMPv3	N	N	N	N	N	RW	N	N	RW

Next page →

Table 23 – Public Key Access Rights within Roles & Services

Services \ Public Keys	DH Public Keys	TLS Public Keys	Firmware Download Public Key	SSHv2 Public Keys	LDAP Root CA Certificate	RADIUS Root CA Certificate	IKEv2 and IPSEC Public Keys
FIPSCfg	N	N	N	N	N	N	N
Zeroize	N	N	N	N	N	N	N
FirmwareManagement	N	N	RW	N	N	N	N
PKI	N	RW	N	RW	N	N	N
RADIUS	N	N	N	N	N	RW	N
LDAP	N	N	N	N	RW	N	N
UserManagement	N	N	N	N	N	N	N
IKEv2 Negotiation – IPsec Traffic	RW	N	RW	N	N	N	RW
SSHv2 and TLS	RW	RW	N	RW	R	R	N
SNMPv3	N	N	N	N	N	N	N

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code RSA signed may be executed.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

8 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS140-2 Level 2 module.

1) The cryptographic module shall provide role-based authentication.
2) When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3) The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      - AES (128,192 and 256) CBC Encrypt KAT
      - AES (128,192 and 256) CBC Decrypt KAT
      - AES (256) GCM KAT Encrypt
      - AES (256) GCM KAT Decrypt
      - HMAC SHA-1 KAT
      - HMAC-SHA-224 KAT
      - HMAC SHA-256 KAT
      - HMAC SHA-384 KAT
      - HMAC SHA-512 KAT
      - SP800-90A DRBG KAT
      - SHA-1 KAT
      - SHA-256 KAT
      - SHA-384 KAT
      - SHA-512 KAT
      - RSA 2048 SHA-256 Sign KAT
      - RSA 2048 SHA-256 Verify KAT
      - SP800-135 SSHv2 KDF KAT
      - SP800-135 TLS 1.0 KDF KAT
      - SP800-135 TLS 1.2 KDF KAT
      - SP800-135 IKEv2 KDF KAT
      - ECDSA KAT
      - ECDH KAT (Primitive "Z" Computation KAT)
      - SP800-135 SNMPv3 KDF KAT

   B. Critical Functions Tests:

      - RSA 2048 Encrypt/Decrypt

C. Message reporting for Status of Power-Up Self-Tests

- On Success, CP will display the status as below,

  <Algorithm Detail>.....successful

- On Failure, CP will display the Power-Up Self-Tests status as shown below,

  <Algorithm Detail>.....FAILED!

- On Failure in the DP, CP will display the error message as shown below,

  POST failure detected on DP<DP#>

D. Firmware Integrity Tests (128-bit EDC)

- On Failure, the following message is displayed:

  Firmware integrity check failed

- On Success, the following message is displayed:

  Firmware integrity test passed

E. Conditional Self-Tests

- Continuous Random Number Generator NDRNG test – Performed on non-Approved RNG.
- Continuous Random Number Generator test – performed on DRBG (CTR_DRBG, AES-256).
- RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)
- RSA 2048 Pairwise Consistency Test (Encrypt/Decrypt)
- ECDSA P-256 Pairwise Consistency Test (Sign/Verify)
- ECDSA P-384 Pairwise Consistency Test (Sign/Verify)
- Firmware Load Test (RSA 2048 with SHA-256 Signature Verification)
- Bypass Test: N/A
- Manual Key Entry Test: N/A

F. Message reporting for Status of Conditional Self-Tests

- On failure in Continuous Random Number Generator related tests
  - On CP

    NDRNG continuous test failed!
    or
    ERROR: DRBG Critical Failure! FIPS Drbg Health Check Failed
    or
    ERROR: DRBG Critical Failure! FIPS DRBG Init Failed

  - On DP

    Continuous health check failed on DP<DP#>

- On Failure in RSA 2048 Pairwise Consistency related Tests

  Conditional tests failed at Sign/Verify
  or
  Conditional tests failed Encrypt/Decrypt

- On Failure in CP for ECDSA pairwise Consistency Test,

  ECDSA pair wise consistency test failed

- On Failure in Firmware Load Test
  - On Failure, the following message is displayed:

    Firmware download failed - Failed to download RPM package

    or

    Firmwaredownload failed because the signature for the firmware could not be validated.

G. At any time, the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.

4) Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

5) Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

6) The module does not support a maintenance role or maintenance interface.

7) The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.

8) The following protocols have not been reviewed or tested by the CAVP nor CMVP

   i) TLS v1.0/v1.1

   ii) SSHv2

   iii) TLS v1.2

   iv) IKEv2

   v) SNMPv3

9) The module complies with FIPS 140-2 Implementation Guidance, Section A.5, Key/IV Pair Uniqueness Requirements from SP 800-38D

   The AES GCM session key is established via the IKEv2 KDF (internally). The 96-bit IV is also constructed internally (deterministically) as per FIPS 140-2 IG A.5 Scenario 3. The fixed field (64-bits) is randomly generated bits from the SP 800-90A DRBG; this is an acceptable construction of the fixed field as per SP 800-38D Section 8.2.1 which states “the entire fixed field may consist of arbitrary bits when there is only one context to identify, such as when a fresh key is limited to a single session of a communications protocol”.

   Furthermore, this is satisfactory because as per the implementation guidance “just the fact that the modules can possibly have at least 2^32 different names will be sufficient to meet this requirement.” The invocation field is a separate 32-bit deterministic non-repetitive counter which increments by one. The implementation of the deterministic non-repetitive counter management logic inside the module ensures that after 2^31 operations, a new AES GCM session key and IV must be created (i.e. IKE V2 renegotiation is automatically enforced which results in new GCM Key and new IV). The IV restoration conditions are satisfied for the deterministic non-repetitive counter as per the IG A.5 bullet 3: The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new IKE session and thus a new GCM key and IV will be created.

10) This module complies with FIPS 140-2 Implementation Guidance, Section A.8 Use of HMAC-SHA-1-96 and Truncated HMAC

    If IKEv2 is configured to use HMAC-SHA-384-192 as specified in RFC 6379 Suite B Cryptographic Suites for IPsec Section 3.2. The HMAC-SHA-384-192 integrity algorithm is specified in RFC 4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. In RFC 4868 Section 2.3 the truncation of HMAC output when used as an integrity verification algorithm for IKEv2 is described. The

bits used as the integrity value shall be one-half the length of the algorithm output. In this case, the message is MAC'ed using the HMAC-384 algorithm, and the digest is shortened to 192 bits by truncating the least-significant 192 bits of the digest. This use of the HMAC-SHA-384-192 as an integrity algorithm is summarized in RFC 4868 Section 2.6.

The HMAC standard is FIPS 198-1 -The Keyed-Hash Message Authentication Code (HMAC). Section 5 of that standard specifies that applications of that standard may truncate the output of the HMAC function. Per FIPS 198-1, the leftmost bits of the HMAC output shall be used as the MAC. There is no conflict in this case between FIPS 198-1 and RFC 4868. FIPS 198-1 references SP800-107 Recommendation for Applications Using Approved Hash Algorithms.

In SP800-107 Section 5.3.3, the use of truncated HMAC output for integrity tags is described. This section requires that n leftmost bits are used as the tag, and that n is no less than 32 bits. This implementation adheres to RFC 4868, so the leftmost 192 bits of the 384-bit output of the HMAC are used as the MAC tag, and the requirements of SP800-107 are met.

11) When the extension platform is configured for FIPS mode, and a PSK IPSec policy is used, the operator must ensure the IKEv2 Authentication Key (PSK) is configured using a full 64 byte (512 bits) value.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals.

9.2 Operator Required Actions

The operator is required to inspect the tamper evident seals, periodically, per the guidance provided in the user documentation.

Table 24 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Tamper Evident Seals	12 months	Confirm that there is no visible evidence of tampering. Reference Appendix A for a description of tamper label application for all evaluated platforms.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Table 25 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Next page →

11 Definitions and Acronyms

Table 26 – Acronyms and Definitions

Acronym	Definition
10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
Blade	Any functional assembly that can be installed in a chassis, excluding power and fan FRUs
CBC	Cipher Block Chaining
CLI	Command Line interface
CP	Control Processor
CSP	Critical Security Parameter
DH	Diffie-Hellman
DP	Data Processor
FIPS	Federal Information Processing Standard
FOS	Fabric Operating System
FRU	Field Replaceable Unit
GbE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
NOS	Network Operating System
NTP	Network Time Protocol
PKI	Public Key Infrastructure
POD	Ports on Demand licensing
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SHA	Secure Hash Algorithm
SSHv2	Secure Shell Protocol
Triple-DES	Triple Data Encryption Standard
TLS	Transport Layer Security Protocol
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve Digital Signature Algorithm

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

12 Brocade Abbreviations

Table 27 – Abbreviations

Abbreviation	Description
0 1/10/40GBE SFP	Zero SFP devices provided
16GB	16 Gigabit
2 CORE	Two core switch blades
42P	42 Ports
8GB	8 Gigabit
BR	Brocade
FC	Fiber Channel
FCIP	Fiber Channel over Internet Protocol
FX8-24	8G, 24 port, Extension blade
GBE	Gigabit Ethernet
GE	Gigabit Ethernet
ICL	Inter-Chassis Link
LIC	License
LWL	Long Wave Length
MGMT	Management
POD	Ports on Demand, Defines the size of an upgrade license. For example, a 24-Port POD License allows the user to enable twenty-four additional ports
SFP	Small form-factor pluggable
SWL	Short wave length
UPG	Upgrade
WWN	World Wide Name card

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13 Appendix A: Tamper Label Application

For each module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in FIPS Kit Brocade XBR-000195 (P/N: 80-1002006-02).

The Crypto-Officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The Crypto-Officer shall maintain a serial number inventory of all used and unused tamper evident seals. The Crypto-Officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The Crypto-Officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The Crypto-Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

Use ethyl alcohol to clean the surface area at each tamper evident seal placement location. Prior to applying a new seal to an area that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use ethyl alcohol to clean off any residual adhesive remover before applying a new seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1 Applying Tamper-Evident Seals on the Brocade X6-4

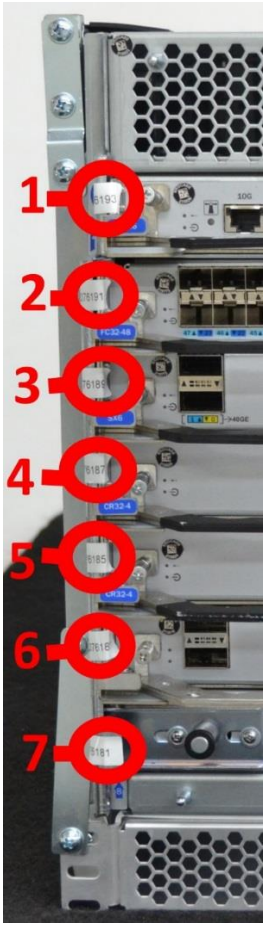
The Brocade X6-4 requires a total of thirty (30) seals. See Figure 3 through Figure 10 for details on how to position each seal. It is recommended that you perform the steps in the order described.

NOTE: DO NOT PUT A SECOND SEAL AT THE SAME LOCATION.

Step 1. **Front Left:** Seven (7) tamper evident seals are required to complete this step of the procedure.

Affix a seal each at locations 1 through 7 from the left side of the module onto the edge of the inserted card. These labels secure the inserted card to the chassis. See Figure 3 for correct seal orientation and positioning.

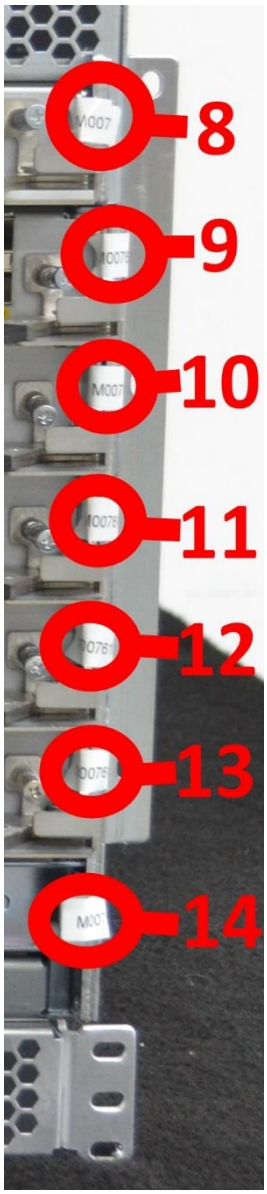
Figure 3 – Brocade X6-4 – Front left side view with tamper evident seals



Step 2. **Front Right:** Seven (7) tamper evident seals are required to complete this step of the procedure.

Affix a seal each at locations 8 through 14 from the right side of the module onto the edge of the inserted card. These labels secure the inserted cards to the chassis. See Figure 4 for correct seal orientation and positioning.

Figure 4 – Brocade X6-4 – Front right side view with tamper evident seals



Next page →

Figure 5 shows the front of the Brocade X6-4 device with the seals placed at their correct locations.

Figure 5 – Brocade X6-4 - Front view with tamper evident seals

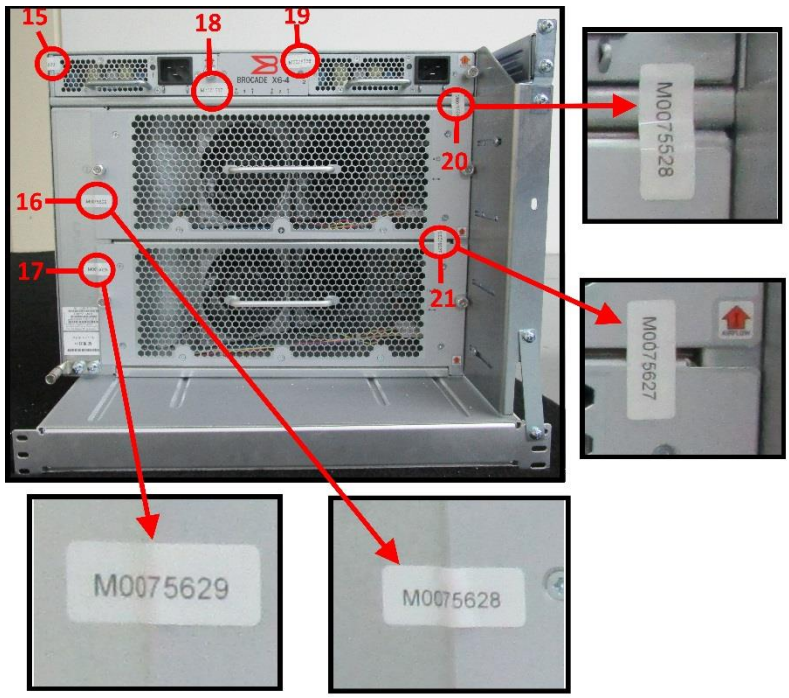
Next page →

Step 3. **Rear:** Seven (7) tamper evident seals are required to complete this step of the procedure.

See Figure 6 for correct seal orientation and positioning for the following.

1. Affix a seal at location 15 which wraps from the rear to the side of the module. The purpose of this seal is to secure the removable fan and power supply assembly in place.
2. Affix a seal each at locations 16 and 17 across the fan module and onto the chassis. The purpose of these seals is to secure the removable fan modules in place.
3. Affix a seal at location 18 across the fan and power supply assembly and onto the upper center of the rear of the chassis. The purpose of this seal is to secure the removable fan and power supply assembly in place.
4. Affix a seal at location 19 from the upper center of the chassis onto the fan and power supply assembly. The purpose of this seal is to secure the removable fan and power supply assembly in place.
5. Affix a seal at location 20 from the removable fan and power supply assembly across and onto the fan assembly. The purpose of this seal is to secure the removable fan assembly in place.
6. Affix a seal at location 21 from the upper fan assembly across the lower fan assembly. The purpose of this seal is to secure both fan assemblies in place.

Figure 6 – Brocade X6-4 - Rear view with tamper evident seals



Next page →

Step 4. **Left side:** Six (6) tamper evident seals are required to complete this step of the procedure.

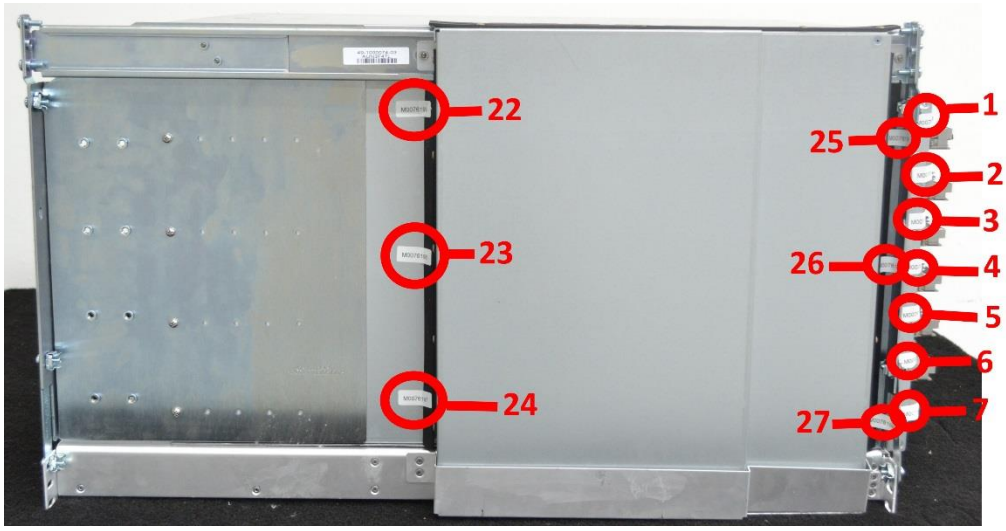
See Figure 7 for correct seal orientation and positioning for the following.

1. Affix a seal each at locations 22, 23, and 24 from the chassis onto the rubber siding for the opaque cover. These labels secure the rubber siding to the chassis.
2. Affix a seal each at locations 25, 26, and 27 from the rubber siding for the opaque cover onto the chassis. These labels secure the rubber siding for the opaque cover onto the chassis.

Figure 7 – Brocade X6-4 – Left side view with tamper evident seal

Figure 8 shows all the labels for the left side view.

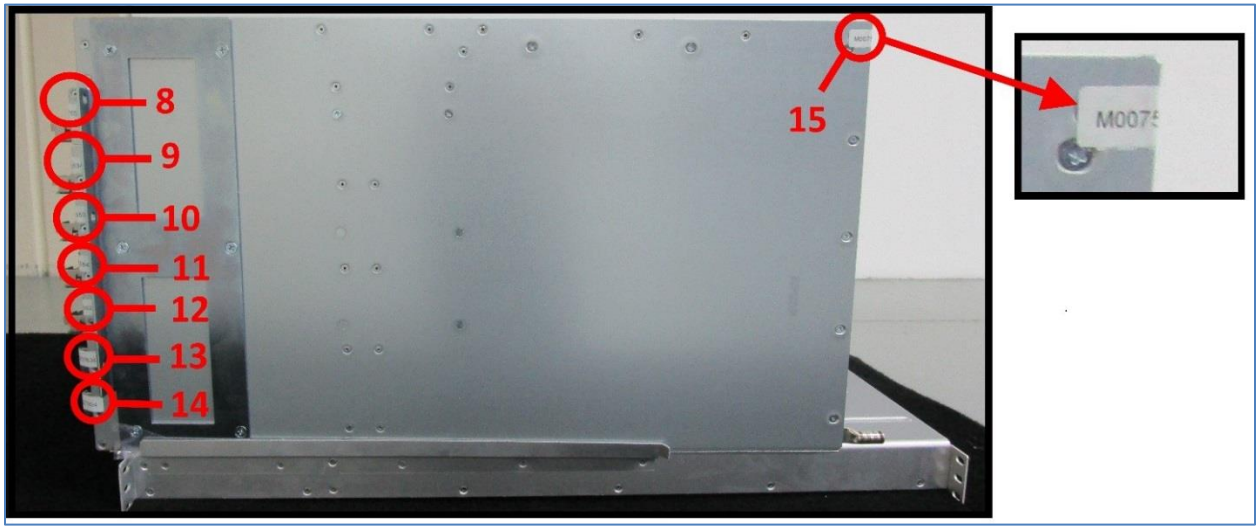
Figure 8 – Brocade X6-4 – Left side view with tamper evident seals



Step 5. **Right side:** Zero (0) tamper evident seal is required to complete this step of the procedure.

Figure 9 shows seals which are placed in one or more of the steps described earlier.

Figure 9 – Brocade X6-4 – Right side view with tamper evident seals placed earlier

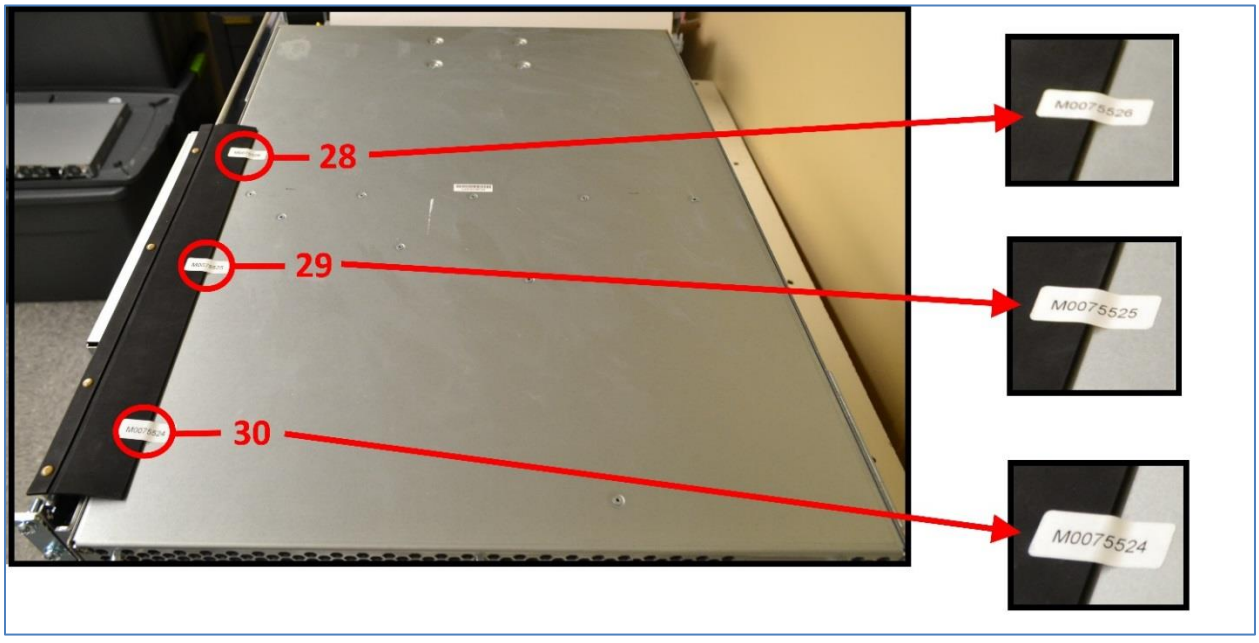


Step 6. Top: Three (3) tamper evident seals are required to complete this step of the procedure.

See Figure 10 for correct seal orientation and positioning for the following.

Affix a seal each at locations 28, 29, and 30 from the rubber siding of the opaque cover to the top side of the module. These labels secure the rubber siding of the opaque cover to the top side of the module.

Figure 10 – Brocade X6-4 - Top view with tamper evident seals and zoomed sections



13.2 Applying Tamper-Evident Seals on the Brocade X6-8

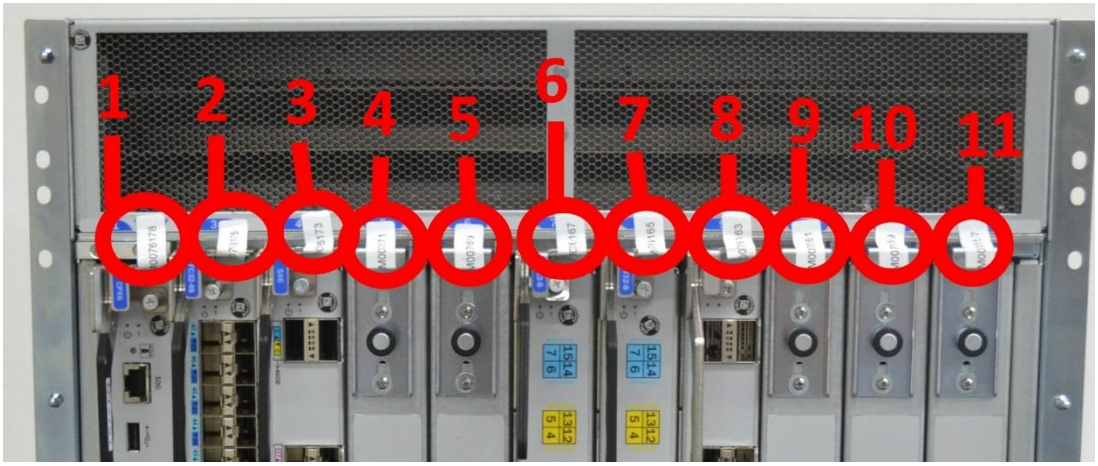
The Brocade X6-8 requires a total of thirty-five (35) seals. See Figure 11 through Figure 17 for details on how to position each seal. It is recommended that you perform the steps in the order described.

NOTE: DO NOT PUT A SECOND SEAL AT THE SAME LOCATION.

Step 1. Front Top Edge: Eleven (11) tamper evident seals are required to complete this step of the procedure.

Affix a seal each at locations 1 through 11 from the top side of the module underneath the ventilation onto the edge of the inserted card. These labels secure the inserted card to the chassis. See Figure 11 for correct seal orientation and positioning.

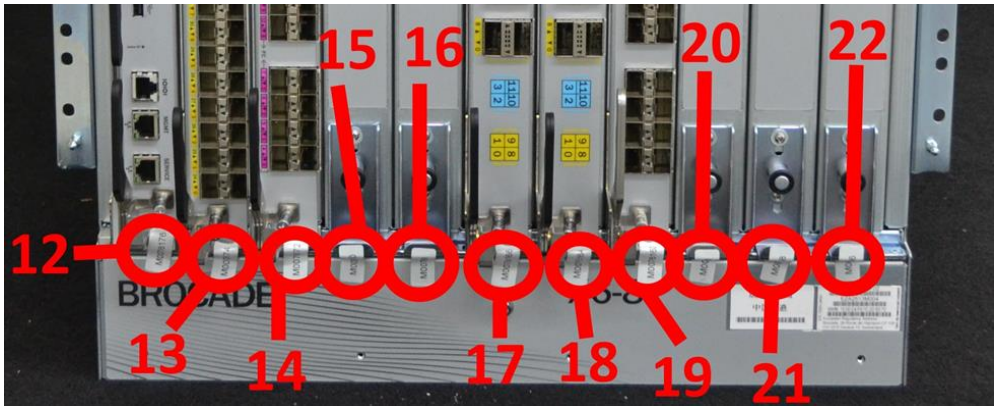
Figure 11 – Brocade X6-8 – Front top edge view with tamper evident seals



Step 2. Front Bottom Edge: Eleven (11) tamper evident seals are required to complete this step of the procedure.

Affix a seal each at locations 12 through 22 from the bottom half of the module onto the edge of the inserted card. These labels secure the inserted cards to the chassis. See Figure 12 Front bottom edge view with tamper evident seals for correct seal orientation and positioning.

Figure 12 – Brocade X6-8 – Front bottom edge view with tamper evident seals



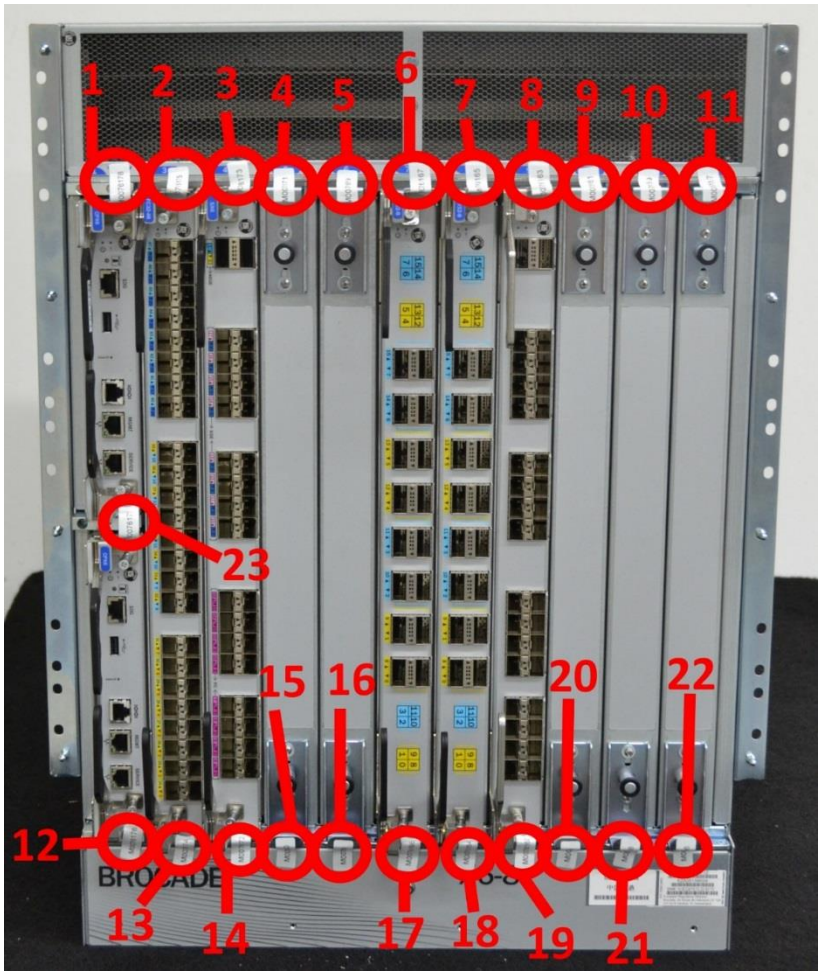
Step 3. **Front Middle:** One (1) tamper evident seal is required to complete this step of the procedure.

Affix a seal at location 23 across the center of the two management modules. This label secures both management modules in place. See Figure 13 for correct seal orientation and positioning.

Figure 13 – Brocade X6-8 – Front middle view with tamper evident seals

Figure 14 shows the front of the Brocade X6-8 device with the seals placed at their correct locations.

Figure 14 – Brocade X6-8 - Front view with tamper evident seals

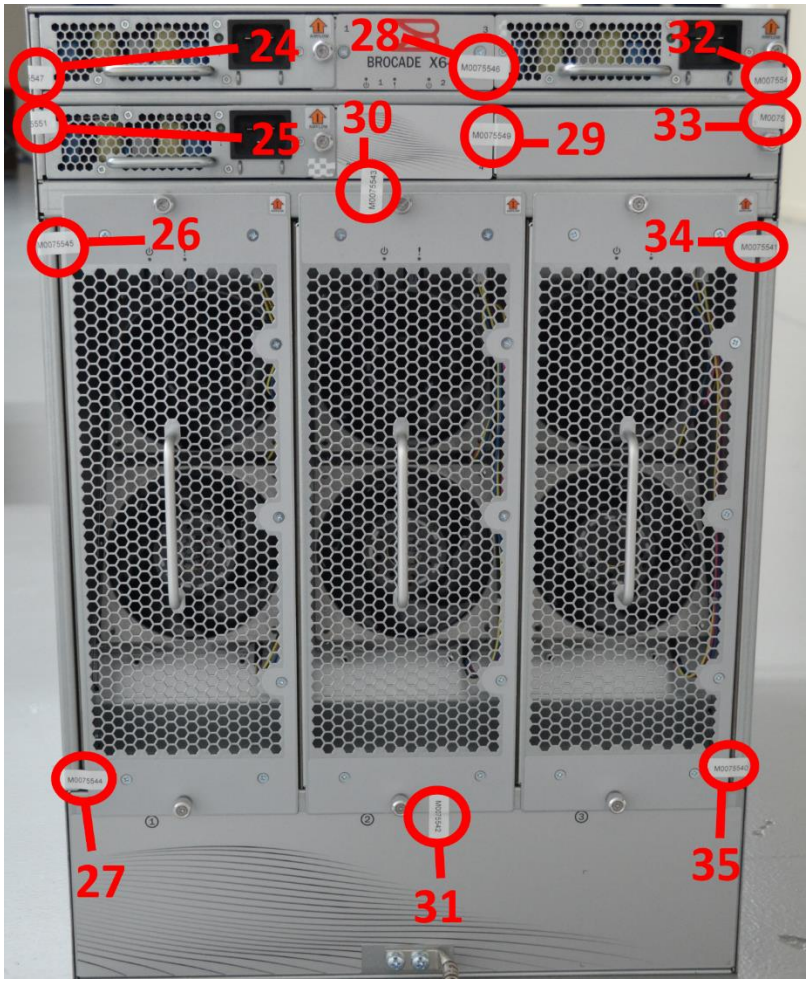


Step 4. Rear: Twelve (12) tamper evident seals are required to complete this step of the procedure.

See Figure 15 for correct seal orientation and positioning for the following.

1. Affix a seal each at locations 24, 25, 32, and 33 from the left and right sides of the chassis respectively and onto the removable fan and power supply assemblies. The purpose of these seals is to secure the removable fan and power supply assemblies in place.
2. Affix a seal each at locations 28 and 29 from the top center of the chassis onto the fan and power supply assemblies. These labels secure the removable fan and power supply assemblies.
3. Affix a seal each at locations 30 and 31 from the top center and bottom of the chassis respectively onto the removable fan assemblies. These labels secure the fan assemblies to the chassis.
4. Affix a seal each at locations 26, 27, 34, and 35 from the left and right sides of the chassis respectively and onto the removable fan assemblies. The purpose of these seals is to secure the removable fan assemblies in place.

Figure 15 – Brocade X6-8 - Rear view with tamper evident seals

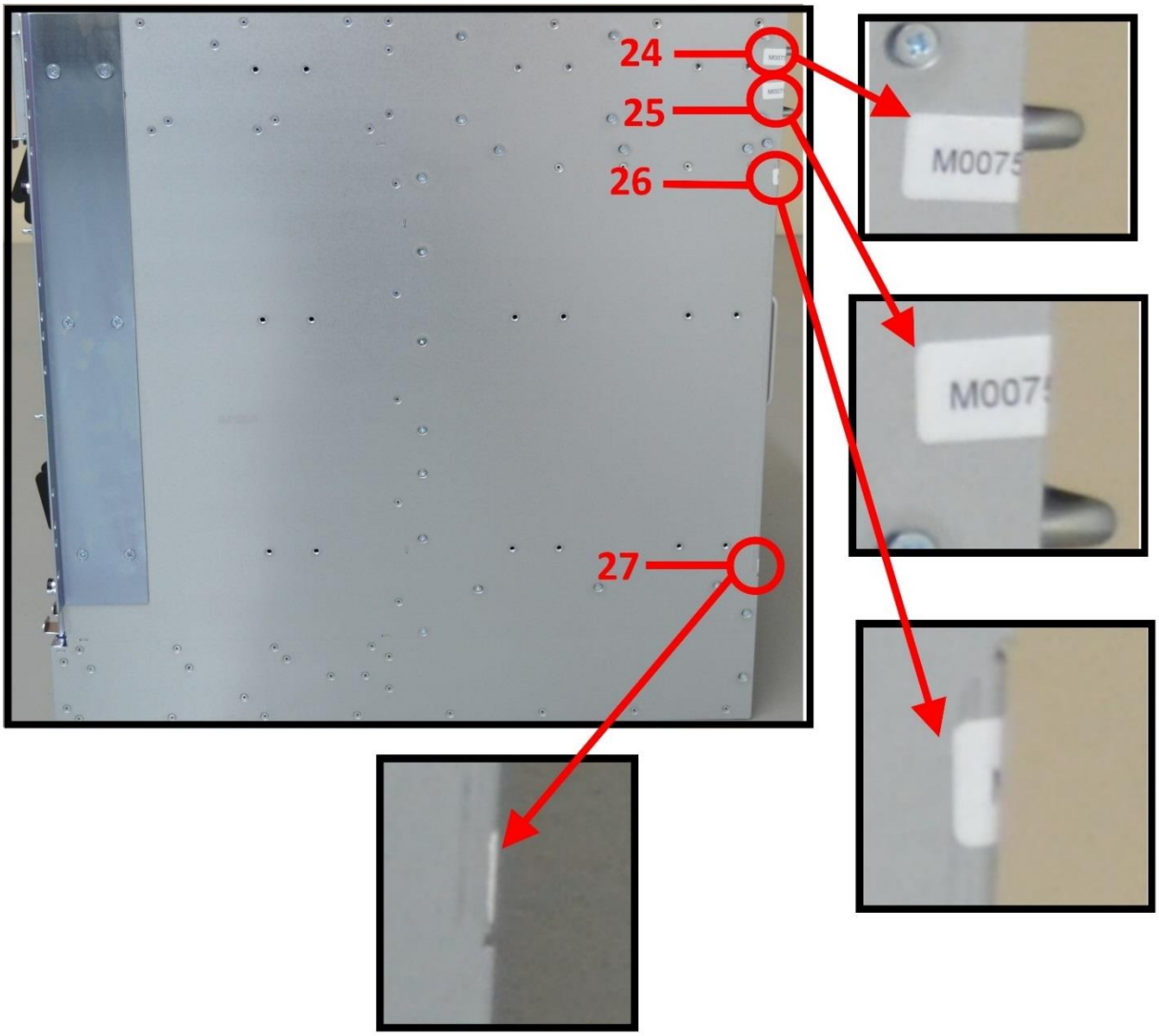


If you have performed the above steps, all seals are now in place.

Following information is provided for your reference only.

Figure 7 (Brocade X6-4 left side) shows the correct seal orientation and positioning for locations 24 through 27 from the right side of the chassis.

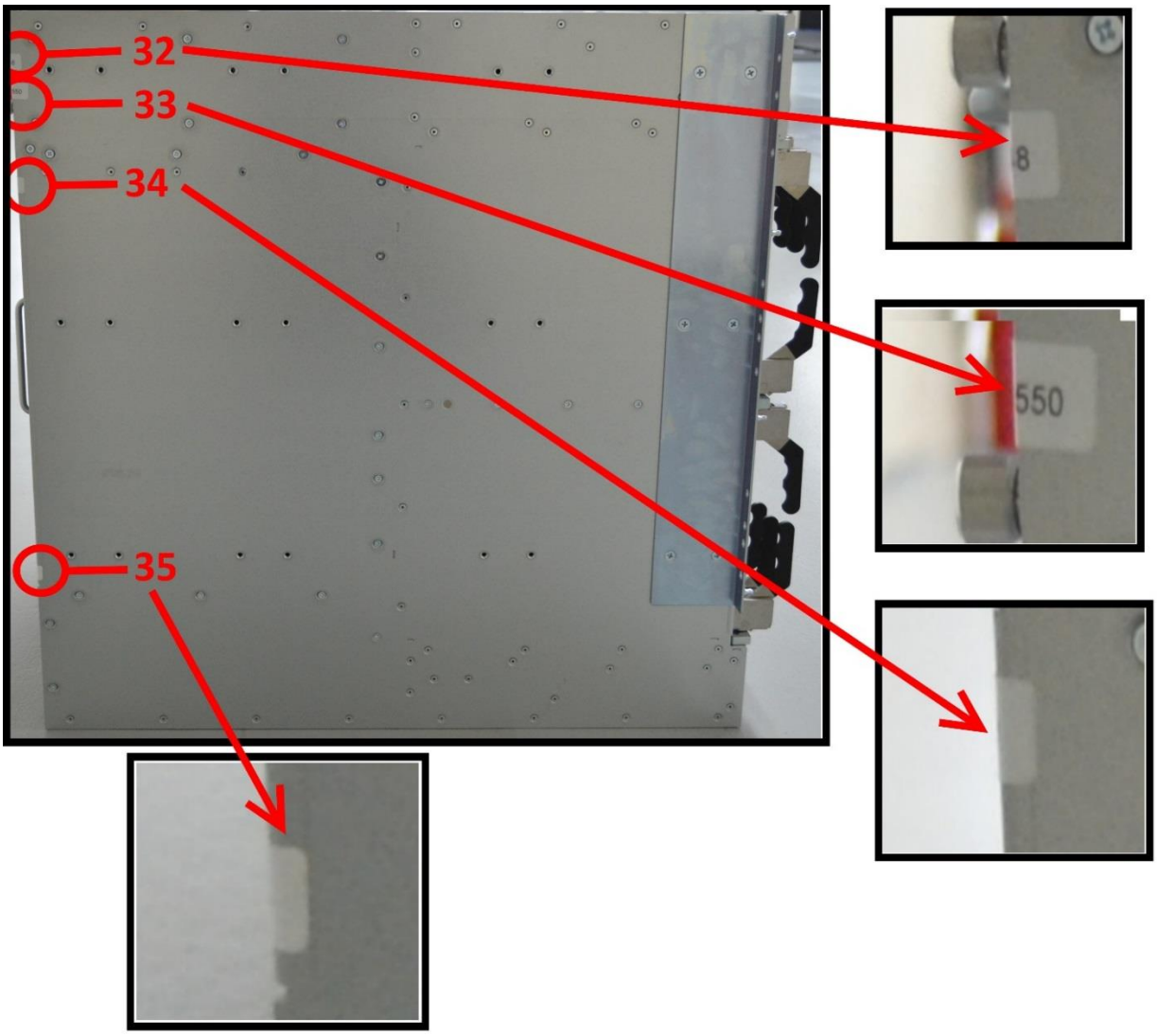
Figure 16 – Brocade X6-8 – Right side view with tamper evident seal



Next page →

Figure 17 (Brocade X6-8 left side) shows the correct seal orientation and positioning for locations 32 through 35 from the left side of the chassis.

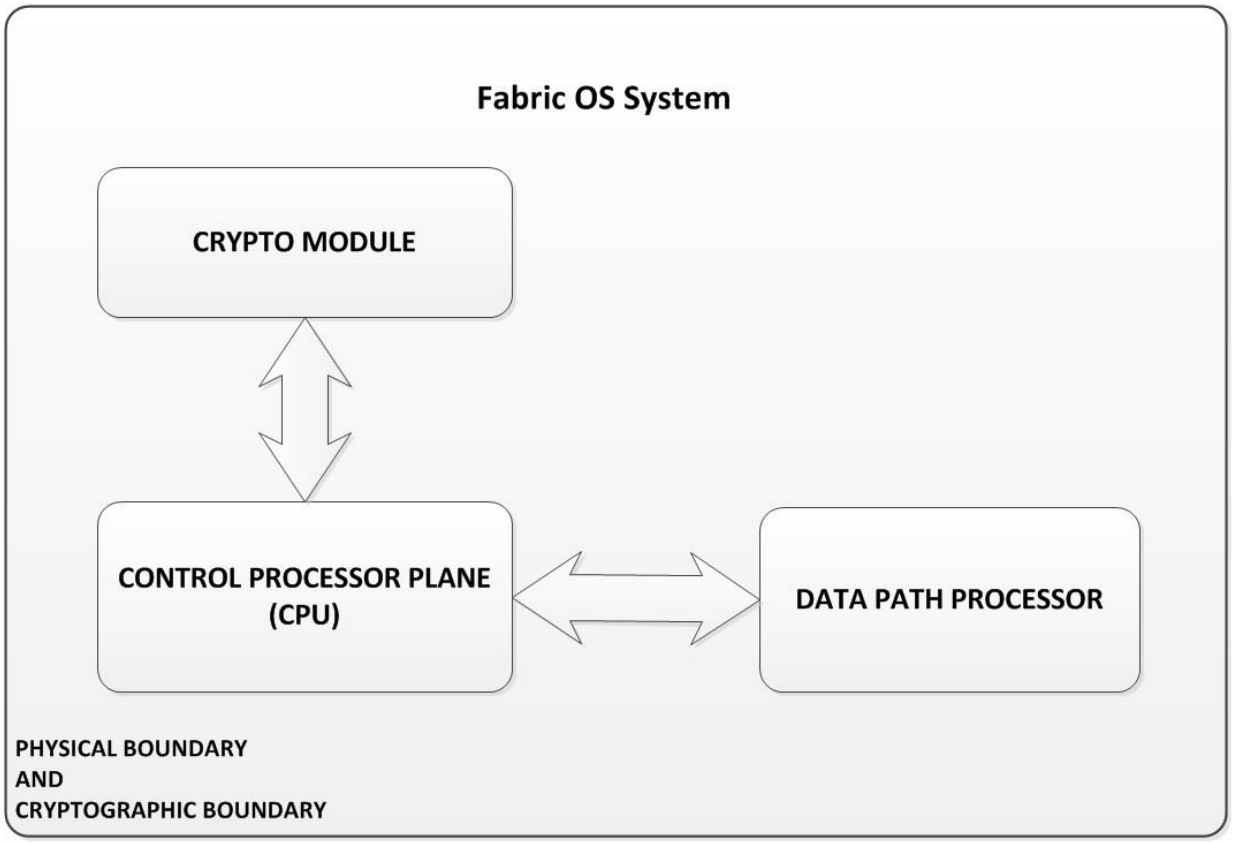
Figure 17 – Brocade X6-8 – Left side view with tamper evident seal



Next page →

14 Appendix B: Block Diagram

Figure 18 – Block Diagram



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

15 Appendix C: Critical Security Parameters and Public Keys

The module supports the following CSPs and Public Keys:

1. DH Private Keys for use with 2048 bit modulus
- Description: Used in SSHv2 to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination and "fipscfg --zeroize" command

2. SSHv2/SCP/SFTP Encryption Keys
- Description: AES (CBC or CTR mode) supporting 128, 192, and 256 Key sizes.
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg --zeroize" command

3. SSHv2/SCP/SFTP Authentication Key
- Description: HMAC-SHA-1 (160 bits), HMAC-SHA-256 and HMAC-SHA-512 Session authentication keys used to authenticate and provide integrity of SSHv2 session
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

4. SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

5. SSHv2 DH Shared Secret Key (2048 bit)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process

- Destruction: Session termination or "fipscfg -zeroize" command

6. SSHv2 ECDH Shared Secret Key (P-256)
- Description: Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys
- Generation: N/A
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

7. SSHv2 ECDH Private Key (P-256)
- Description: ECDH private key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or performing the "fipscfg -zeroize" command

8. SSHv2 ECDSA Private Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

9. Value of K during SSHv2 P-256 ECDSA session
- Description: Used to generate keys that sign and verify
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

10. TLS Private Key (RSA 2048)
- Description: RSA key used to establish TLS sessions (decrypt padded TLS Pre-Master secret key block)
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

11. TLS Pre-Master Secret
- Description: 48-byte secret value used to establish the Session and Authentication key
- Generation: Approved SP800-90A DRBG

- Establishment: RSA key wrapped over TLS session; allowed as per FIPS 140-2 IG D.9
- Storage: Plaintext in RAM
- Entry: RSA key wrapped (after padding to block size) during TLS handshake
- Output: RSA key wrapped (after padding to block size) during TLS handshake
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

12. TLS Master Secret
- Description: 48 bytes secret value used to establish the Session and Authentication key
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

13. TLS KDF Internal State
- Description: Values of the KDF internal state.
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

14. TLS Session Keys - 128, 256 bit AES CBC
- Description: AES key used to secure TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination and "fipscfg -zeroize" command

15. TLS Authentication Key for HMAC-SHA-1 (160 bits) and HMAC-SHA-256
- Description: HMAC-SHA-1 or HMAC-SHA-256 key used to provide data authentication for TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination and "fipscfg -zeroize" command

16. CP DRBG Seed Material
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: Internally generated; raw random data from NDRNG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

17. CP DRBG Internal State (V and Key)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

18. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A
- Establishment: N/A
- Storage: MD5, SHA-256 or SHA-512 digest in Compact Flash (Plaintext)
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

19. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: Encrypted/Authenticated over SSHv2 session
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

20. DH Private Key (256 bits) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: IKEv2 KDF completion or session termination

21. DH Shared Secret (2048 bits) (Used in IKEv2)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H) used in in IKEv2.
- Generation: N/A
- Establishment: IKEv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: Session termination

22. IKEv2 AES-256 Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256-CBC or AES-256-GCM encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section 4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in Cavium key memory
- Entry: N/A
- Output: N/A

- Key-To-Entity: IKEv2 SA Number
- Destruction: Session termination

23. ESP AES-256-GCM Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256-GCM encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section 4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in Blitzer FPGA key memory
- Entry: N/A
- Output: N/A
- Key-To-Entity: ESP SA Number
- Destruction: Session termination

24. IKEv2 KDF State
- Description: Values of the IKEv2 KDF (HMAC-SHA-384 or HMAC-SHA-512) internal state
- Generation: N/A
- Establishment: IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: N/A
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

25. IKEv2 Authentication Key (PSK)
- Description: Pre-shared secret key used for IKEv2 session authentication (512 bits)
- Generation: N/A
- Establishment: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Storage: Plaintext in RAM
- Entry: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

26. IKEv2 ECDH P-384 Private Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for elliptic curve is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: IKEv2 KDF completion or session termination

27. IKEv2 ECDSA P-384 Private Key
- Description: Used to authenticate IKEv2 Peer
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command or certificate/CSR deletion

28. IKEv2 Integrity Key (HMAC-SHA-384)
- Description: HMAC-SHA-384 key used to provide data integrity for IKEv2
- Generation: N/A
- Establishment: IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA Number
- Destruction: Session termination

29. DRBG Internal State (V and Key) (On Cavium)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: OpenSSL context per core
- Destruction: Session termination

30. Entropy Data (on Cavium)
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: internally generated; raw random data from NDRNG
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: Cavium Random Number Memory
- Destruction: DRBG Instantiation

31. SNMPv3 Auth and Priv password
- Description: Auth and Priv Password (8-32 bytes)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM; Plaintext in Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

32. SNMPv3 KDF Internal State
- Description: SHA-1 Key Localization Function
- Generation: N/A
- Establishment: SNMPv3 KDF (SP800-135 Section 5.4); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

33. SNMPv3 Auth and Priv Secrets
- Description: Auth Secret 20-bytes (input to HMAC-SHA-1-96 function); Priv secret AES-128-CFB 128-bit key
- Generation: N/A
- Establishment: SNMPv3 KDF (SP800-135 Section 5.4); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM and Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

- - - - - - - - - - - - PUBLIC KEYS - - - - - - - - - - - -

34. DH Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2)

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User

35. DH Peer Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

36. TLS Public Key (RSA 2048)
- Description: Used by client to encrypt TLS Pre-Master Secret
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: User

37. TLS Peer Public Key (RSA 2048)
- Description: Used to authenticate the client
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

38. FW Download Public Key (RSA 2048)
- Description: Used to update the FW of the module.
- Generation: N/A; Generated outside the module
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

39. SSHv2 ECDSA Public Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: User

40. SSHv2 ECDSA Peer Public Key (P-256)
- Description: Used to authenticate SSHv2 client to server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash

- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

41. LDAP ROOT CA certificate (RSA 2048)
- Description: Used to authenticate LDAP server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: Process

42. RADIUS ROOT CA certificate (RSA 2048)
- Description: Used to authenticate RADIUS server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: Process

43. DH Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: IKEv2 SPI

44. DH Peer Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: IKEv2 SPI

45. IKEv2 ECDH P-384 Public Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for elliptic curve is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: IKEv2 SPI

46. IKEv2 ECDH P-384 Peer Public Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: IKEv2 SPI

47. IKEv2 ECDSA P-384 Public Key
- Description: Used for IKEv2 Authentication
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

48. IKEv2 ECDSA P-384 Peer Public Key
- Description: Used for IKEv2 Authentication
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

49. SSHv2 ECDH Public Key (P-256)
- Description: ECDH public key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM
- Key-To-Entity: Process

50. SSHv2 ECDH Peer Public Key (P-256)
- Description: ECDH public key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: Plaintext
- Output: N/A
- Storage: Plaintext in RAM
- Key-To-Entity: Process

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16 Appendix D: CKG as per SP800-133

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated seed, for asymmetric key generation, is the unmodified output from SP800-90A DRBG. Please see section 15 - Appendix C: Critical Security Parameters and Public Keys for further details.