BROCADE

Brocade® DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 FC Switch, 6520 FC Switch, 7800 and 7840 Extension Switch

FIPS 140-2

Non-Proprietary

Security Policy

Document Version 1.0

Brocade Communications

December 17, 2015

Document History

Version	Summary of Changes	Publication Date
1.0	Initial Release	November 25, 2015
1.01	Provided updates	December 17, 2015

1 Module Overview

The Brocade DCX, DCX 8510-8, DCX-4S and DCX 8510-4, 6510, 6520, 7800 and 7840, are multiple-chip standalone cryptographic modules, as defined by FIPS 140-2. The cryptographic boundary for DCX, DCX 8510-8, DCX-4S and DCX 8510-4 backbone is the outer perimeter of the metal chassis including the removable cover, control processor blades, core switch blades, and port blades or filler panels. The cryptographic boundary of the 6510 FC Switch, 6520 FC Switch, 7800 and 7840 Extension Switch is the outer perimeter of the metal chassis including the removable cover. The power supply units are not included in the cryptographic boundary. The module is a Fibre Channel and/or Gigabit Ethernet routing switch that provides secure network services and network management.

For each module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in FIPS Kit P/N Brocade XBR-000195 must be installed as defined in Appendix A.

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.

A validated module configuration is comprised of Fabric OS v7.3.0 (P/N: 63-1001447-01) installed on, a switch or backbone and a set of installed blades. The below platforms may be used in a validated module configuration:

Firmware
Fabric OS v7.3.0

Table 1 Firmware Version

Switch	SKU	Part Number	Brief Description
6510	BR-6510-24-16G-F	80-1005232-03[1]	6510,24P,16GB SFP,NON-PORT[2] SIDE AIR FLOW
	BR-6510-24-16G-R	80-1005267-03[1]	6510,24P,16GB SFP,PORT SIDE[2] AIR FLOW
	BR-6510-24-8G-F	80-1005268-03[1]	6510,24P,8GB SFP,NON-PORT SIDE AIR FLOW
	BR-6510-24-8G-R	80-1005269-03[1]	6510,24P,8GB SFP,PORT SIDE AIR FLOW
	BR-6510-48-16G-F	80-1005271-03	6510,48P,16GB SFP,NON-PORT SIDE AIR FLOW, 24-PORT POD LICENSE
	BR-6510-48-16G-R	80-1005272-03	6510,48P,16GB SFP, PORT SIDE AIR FLOW, 24-Port POD LICENSE
6520	BR-6520-48-8G-F	80-1007245-03	6520, 48 port 8G, SWL SFP, non-port side exhaust. Includes three fan FRUs and two 1100W AC power supplies
	BR-6520-48-8G-R	80-1007246-03	6520, 48 port 8G, SWL SFP, port side exhaust. Includes three fan FRUs and two 1100W AC power supplies
	BR-6520-48-16G-F	80-1007242-03	6520, 48 port 16G, SWL SFP, non-port side exhaust. Includes three fan FRUs and two 1100W AC power supplies
	BR-6520-48-16G-R	80-1007244-03	6520, 48 port 16G, SWL SFP, port side exhaust. Includes three fan FRUs and two 1100W AC power supplies
	BR-6520-96-16G-R	80-1007257-03	6520, 96 port, 16G, SWL SFP, port side exhaust. Includes three fan FRUs and two 1100W AC power supplies
7800	BR-7800F-0001	80-1002607-07[3] 80-1006977-02[4]	7800,UPG LIC,22P,16 8 SWL
	BR-7800F-0002	80-1002608-07[3] 80-1006980-02[4]	7800,UPG LIC,22P,16 8 LWL
	BR-7800-0001	80-1002609-07[3] 80-1006979-02[4]	7800,6P,8GB SWL SFP
7840	BR-7840-0002	80-1008000-01	7840, 42P, 24 16G LW SFPS, 0 1/10/40GBE SFP

Table 2 Switch Platforms

Table 2 Notes

1. Ports 25 – 48 are physically present but disabled. A POD license is required to enable ports 25 – 48.
2. Port side and non-port side air flow indicates whether the fan direction causes air to be draw into the port side air vents or exhausted from the port side air vents.
3. Serviceable assembly.
4. Production assembly.
5. Serviceable and production assemblies are functionally equivalent. The part number assigned to each production assembly was created to support the release of new agency labels with new CCC mark, humidity and altitude marks.

Backbone	SKU	Part Number	Brief Description
DCX	BR-DCX-0001	80-1001064-10[1] 80-1006751-01[2]	DCX,2PS,0P,2CP,2 CORE,0SFP
	BR-DCX-0002	80-1004920-04[1] 80-1006752-01[2]	DCX,2PS,0P,2CP,2 CORE,0 SFP,ENT BUN[4],2 WWN
DCX-4S	BR-DCX4S-0001	80-1002071-10[1] 80-1006773-01[2]	DCX-4S,2PS,0P,2CP,2 CORE,0SFP
	BR-DCX4S-0002	80-1002066-10[1] 80-1006772-01[2]	DCX-4S,2PS,0P,2CP,2 CORE,0SFP,BR,ENT BUN[4]
DCX 8510-4	BR-DCX8514-0001	80-1004697-04[1,] 80-1006963-01[2]	DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP
	BR-DCX8514-0002	80-1005158-04[1] 80-1006964-01[2]	DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP,ENT BUN[4]
DCX 8510-8	BR-DCX8518-0001	80-1004917-04[1] 80-1007025-01[2]	DCX8510-8,2PS,0P,2CP,2 16GB,0SFP,ENT BUN[4]

Table 3 Backbone Models

Table 3 Notes

1. Serviceable assembly.
2. Production assembly.
3. Serviceable and production assemblies are functionally equivalent. The part number assigned to each production assembly was created to support the release of new agency labels with new CCC mark, humidity and altitude marks.
4. Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized.

The blades listed below may be used in backbone-based validated module configurations:

Blade	Acronym[4]	Part Number	Brief Description
CP8 Control Processor Blade	CP8	80-1001070-07[1] 80-1006794-01[2]	FRU,CP BLADE,DCX
CR16-4 Core Switch Blade	CR16-4	80-1004897-01	FRU, CORE BLADE, DCX8510-4
CR16-8 Core Switch Blade	CR16-8	80-1004898-01	FRU, CORE BLADE, DCX8510-8
CR4S-8 Core Switch Blade	CR4S-8	80-1002000-02[1] 80-1006771-01[2]	FRU, CORE BLADE, DCX-4S
CR8 Core Switch Blade	CR8	80-1001071-02[1] 80-1006750-01[2]	FRU, CORE BLADE, DCX
FC16-32 Port Blade	FC16-32	80-1005166-02	FRU, PORT BLADE,32P,DCX8510,16G SFP
FC16-48 Port Blade	FC16-48	80-1005187-02	FRU,PORT BLADE,48P,DCX8510,16G SFP
FC8-16 Port Blade	FC8-16	80-1001066-01[1] 80-1006936-01[2]	FRU, PORT BLADE, 16P, DCX, 8G SFP
FC8-32 Port Blade	FC8-32	80-1001067-01[1] 80-1006779-01[2]	FRU, PORT BLADE, 8P, DCX, 8G SFP
FC8-48 Port Blade	FC8-48	80-1001453-01[1] 80-1006823-01[2]	FRU, PORT BLADE, 48P, DCX, 8G SFP
FC8-64 Port Blade	FC8-64	80-1003887-01[1] 80-1007000-01[2]	FRU, PORT BLADE, 48P, DCX, 8G SFP
FX8-24 Port Blade	FX8-24	80-1002839-03[1] 80-1007017-01[2]	FRU, EXT BLADE, 8G X 12P, 10x1GBE, 2X10GBE
DCX/DCX 8510-8 Filler Panel	DCX/DCX 8510-8 Filler Panel	49-1000016-04	FILLER PANEL
DCX-4S Backbone Filler Panel	DCX-4S Backbone Filler Panel	49-1000064-02	FILLER PANEL
DCX-4S/DCX 8510-4 Filler Panel	DCX-4S/DCX 8510-4 Filler Panel	49-1000294-05	FILLER PANEL

Table 4 Supported Blades

Table 4 Notes

1. Serviceable assembly.
2. Production assembly.
3. Serviceable and production assemblies are functionally equivalent. The part number assigned to each production assembly was created to support the release of new agency labels with new CCC mark, humidity and altitude marks.
4. Acronym referenced in **Table 5 Backbone Blade Support Matrix.**

Each backbone model supports a selected set of blades:

Backbone Model	Blades (max count)
DCX (12 slots) [1]	CP8 (2), CR8 (2), FC8-16 (8), FC8-32 (8), FC8-48 (8), FC8-64 (8), FX8-24 (1), DCX/DCX 8510-8 Filler Panel (10)
DCX 8510-8 (12 slots) [1]	CP8 (2) [1], CR16-8 (2), FC8-64 (8), FC16-32 (8), FC16-48 (8), FX8-24 (1), DCX/DCX 8510-8 Filler Panel (10)
DCX-4S (8 slots) [1]	CP8 (2) , CR4S-8 (2), FC8-16 (4), FC8-32 (4), FC8-48 (4), FC8-64 (4), FX8-24(1), DCX-4S Backbone Filler Panel (6), DCX-4S/DCX 8510-4 Filler Panel (6)
DCX 8510-4 (8 slots) [1]	CP8 (2) , CR16-4 (2), FC8-64 (4), FC16-32 (4), FC16-48 (4), FX8-24 (1), DCX-4S/DCX 8510-4 Filler Panel (6)

Table 5 Backbone Blade Support Matrix

Table 5 Notes

1. Each Backbone Model shall be fully populated with a minimum of two CP8 Control Processor Blades (Part Number: 80-1001070-06 or 80-1006794-01), with every remaining slot populated with a blade as per Table 5 above.

   The name of a backbone-based validated module configuration is formed by a concatenation of part numbers of the specific set of blades installed in the backbone.

   For the DCX and DCX 8510-8 platforms:

   <Backbone PN><Slot 1 PN><Slot 2 PN>….<Slot 12 PN>

   For the DCX-4S and DCX 8510-4 platforms:

   <Backbone PN><Slot 1 PN><Slot 2 PN>….<Slot 8 PN>

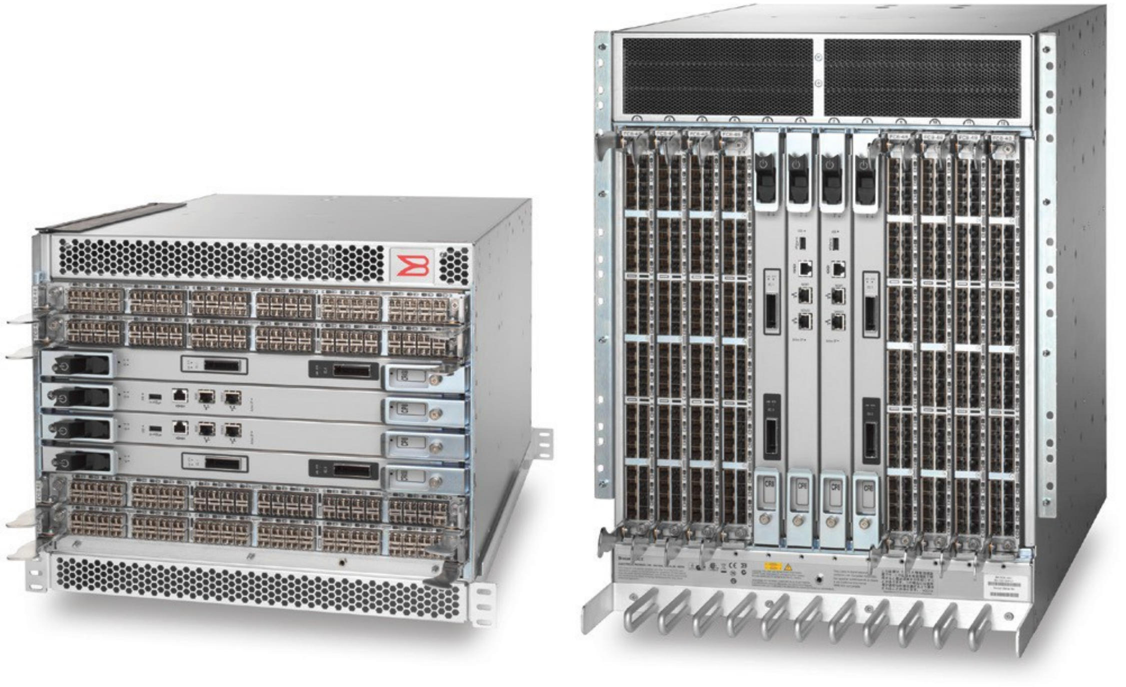

Figure 1 DCX-4S and DCX

Figure 1 illustrates representative configurations of the DCX-4S (left image) and DCX (right image) cryptographic modules. These are not the only possible configurations. Other possible configurations can be created by utilizing the blade and support matrix information in Table 4 and Table 5.

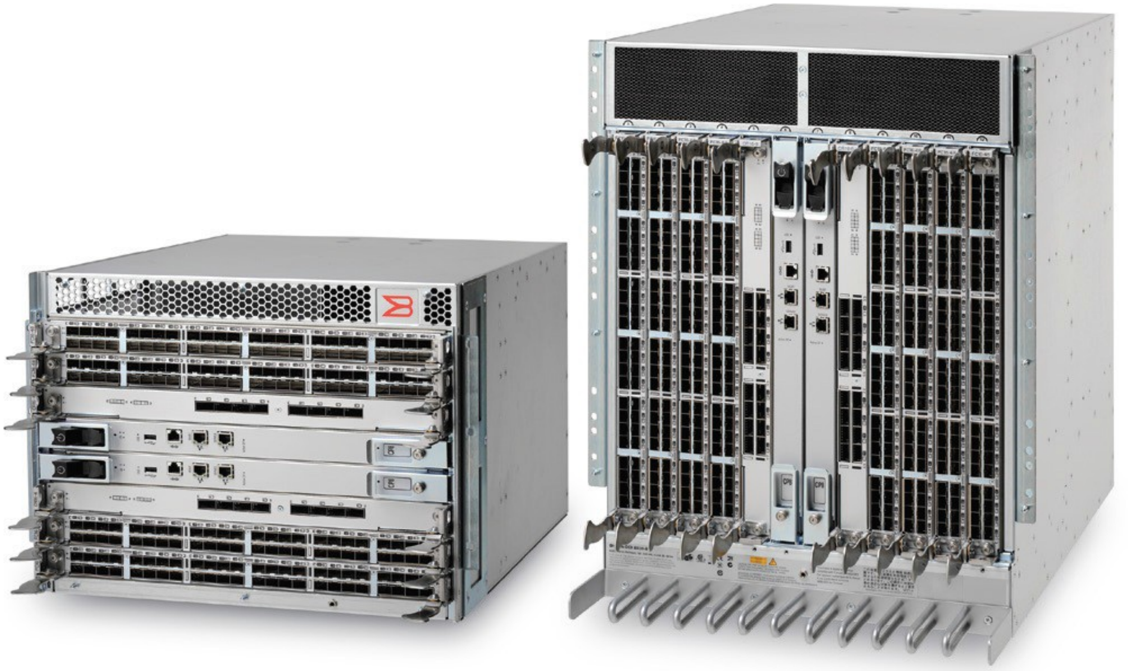

Figure 2 DCX 8510-4 and DCX 8510-8

Figure 2 illustrates representative configurations of the DCX 8510-4 (left image) and DCX 8510-8 (right image) cryptographic modules. These are not the only possible configurations. Other possible configurations can be created by utilizing the blade and support matrix information in Table 4 and Table 5.

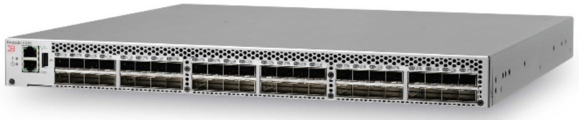

Figure 3 Brocade 6510

Figure 3 illustrates the Brocade 6510 cryptographic module.

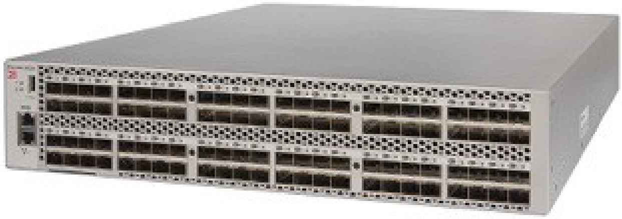

Figure 4 Brocade 6520

Figure 4 illustrates the Brocade 6520 cryptographic module.

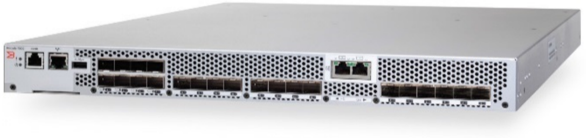

Figure 5 Brocade 7800

Figure 5 illustrates the Brocade 7800 cryptographic module.

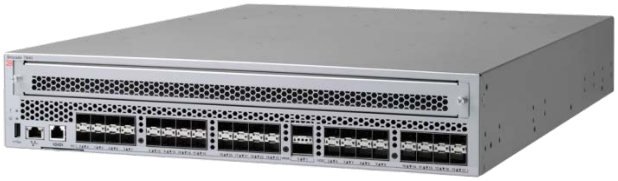

Figure 6 Brocade 7840

Figure 6 illustrates the Brocade 7840 cryptographic module.

2 Security Level

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

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	NA
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	NA

Table 6 Module Security Level Specification

3 Modes of Operation

Module supports an Approved mode of operation and a non-Approved mode of operation. The initial state of the cryptographic module is the non-Approved mode of operation. The Crypto-Officer shall follow the procedures in section 3.1, Approved mode of operation, to initialize the module into the Approved mode of operation. The module cannot be configured into the non-Approved mode once the initialization procedures have been completed by the Crypto-Officer.

3.1 Approved mode of operation

The cryptographic module supports the following Approved algorithms:

Approved Algorithm	Description	Certificate Number
AES	128, 192, and 256-bit keys (ECB, CBC)	2876, 2892, 2893
ECDSA	P-256	518, 522, 523
HMAC	HMAC-SHA1, 224, 256, 384, 512	1814, 1828, 1829
RNG	ANSI X9.31	1284, 1288, 1289
RSA NOTICE: 3072-bit keys are latent functionality and are not available within any service.	2048-bit keys	1514, 1522, 1523
SHS	SHA-1, 224, 256, 256, 384, 512	2417, 2435, 2436
Triple-DES	KO 1, 2 CBC mode	1719, 1723, 1724
CVL	ECC CDH Primitive	311, 318, 320
CVL	TLS v1.0/1.1 and v1.2 NOTE: SSL “is not” supported in FIPS mode.	312, 319, 321
CVL	SSHv2	312, 319, 321

Table 7 Approved Algorithms available in firmware

Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

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

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)

- HMAC-MD5 to support RADIUS authentication
- NDRNG – used for seeding Approved RNG (Note: The module generates cryptographic keys whose strengths are modified by available entropy. The module NDRNG provides approximately 383 bits of equivalent encryption strength.)
- MD5 (used for password hash)

The following non-Approved and not allowed cryptographic methods are not allowed within limited scope in the FIPS Approved mode of operation.

1. DES

The initial state of the cryptographic module is not in a FIPS-compliant state. The cryptographic module contains four default accounts: root, factory, admin, and user. Each default account has a public, default password.

The cryptographic module may be configured for FIPS mode via execution of the following procedure:

1) Login as Root
2) Perform zeroization operation.
3) Power cycle the module.
4) Change passwords for all existing user accounts.
5) Disable Telnet, HTTP
6) Enable HTTPS
7) Do not use FTP
    a) Config Upload
    b) Config Download
    c) Support Save
    d) FW Download
8) Do not use MD5 and SHA-1 hash and 0-3 within Authentication Protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
9) Configure to use SHA256 as the signature algorithm for FCAP authentication with group 4.
10) Do not define FCIP IKEv2 or IPSec policies.
11) Disable Management Interface IPSec/IKEv2
12) Disable In-Band Management Interface
13) Disable In-Flight Encryption
14) Disable TACACS+ authspec mode
15) LDAP CA certificate should be of RSA 2048 bits signed with SHA256.
16) Do not enable SNMP Access List.
17) Enable Self-Tests
18) Within Radius, only use PEAP MS-CHAP V2. Configure RADIUS Server to only use PEAP MS-CHAP V2 (Note: This is a protocol that relies on the strength of TLSv1.0, which is utilizing RSA 2048 with SHA-256 and FIPS Approved cipher suites (AES, HMAC-SHA-1)).

19) Enable Signed FW Download

20) Install removable front cover (as applicable) and apply tamper labels

21) Disable Boot PROM Access

22) Disable Factory role Access

23) Disable Root Access

24) Login as Admin

25) Enable FIPS mode via the "`fipscfg –-enable fips`" command

26) Power-cycle the module.

27) Externally generated RSA key pairs shall only be imported if they are RSA 2048.

28) After certificate operations (e.g. importing) view "`fipscfg --verify fips`" to validate FIPS.

29) The operator can use either ECDSA or RSA. If RSA is used for SSHv2 sessions, execute "`fipscfg –-enable SHA256`" for SSHv2 sessions signed/verified with SHA 256.

30) Execute "`fipscfg --verify fips`" and ensure that all verifications are passed.

31) SSHv2 clients and server should support diffie-hellman-group-exchange-256 and the ability to sign/verify with SHA256 to connect to the switch.

The operator can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the CLI command, "`fipscfg --show`" service. The module will return the following as an indicator for the FIPS Mode of Operation: "`FIPS mode is: Enabled`". When operating in the Non-Approved mode of operation the following will be displayed "`FIPS mode is: Disabled`".

3.2 Non-Approved mode of operation

In non-Approved mode, an operator will have no access to CSPs used within the Approved mode. When switching from the non-Approved mode of operation to the Approved-mode, the operator is required to perform zeroization of the module's plaintext CSPs as indicated in the procedure in section 3.1, above.

Please refer to Table 13b for Service/Functions in non-Approved mode.

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
- 1 GbE & 10 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
    - Brocade USB flash device, XBR-DCX-0131
- Power Supply Connectors: Power Input, Data Output, Status Input
- LEDs: Status Output (1)

4.1 LED Indicators

1) Blades:
    a) Blade Power LED
    b) Blade Status LED
    c) Fibre Channel port status LED
    d) Fibre Channel port speed LED
    e) USB port Status LED
    f) Active CP LED
    g) Ethernet port (SERVICE) Link LED
    h) Ethernet port (SERVICE) Activity LED
    i) Ethernet port (MGMT) Link LED
    j) Ethernet port (MGMT) Activity LED
    k) ICL port LINK LED
    l) ICL port ATTN LED
2) Backbone:
    a) WWN Status Interface LED
    b) FAN power LED
    c) FAN status LED
3) Switches:
    a) Switch Power LED
    b) Switch Status LED
    c) Ethernet port Link LED
    d) Ethernet port Activity LED
    e) Gigabit Ethernet (GE) port status LED
    f) Gigabit Ethernet (GE) port activity LED
    g) Fiber Channel port status LED

Model	Port/Interface Type						
	Fibre Channel Ports	1 GbE & 10 GbE	Ethernet	Serial Port	USB	Power Supply Connectors	LED
DCX-4S	256	24	4	2	2	2	4
DCX	512	24	4	2	2	4	30
DCX 8510-4	192	12	4	2	2	2	4
DCX 8510-8	384	12	4	2	2	4	30
6510	48	0	1	1	1	2	54
6520	96	0	1	1	1	2	107
7800	16	8	1	1	1	2	32
7840	24	16	2	1	1	2	32

Table 8 Port/Interface Quantities

Blade	LED		Blade	LED
CP8 Control Processor	8		FC8-16 Port Blade	18
CR16-4 Core Switch Blade	4		FC8-32 Port Blade	34
CR16-8 Core Switch Blade	4		FC8-48 Port Blade	50
CR4S-8 Core Switch Blade	6		FC8-64 Port Blade	66
CR8 Core Switch Blade	4			
FC16-32 Port Blade	34		FX8-24 Port Blade	26
FC16-48 Port Blade	50			

Table 9 DCX-4S, DCX, DCX 8510-4, and DCX 8510-8 blade LED counts

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports the operator roles. The cryptographic module shall enforce 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 randomly chosen from the 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:

Role	Type of Authentication	Authentication Data	FOS RBAC Role
Admin(Crypto-Officer)	Role-based operator authentication	Username and Password	Admin
User (User role)	Role-based operator authentication	Username and Password	User, BasicSwitchAdmin, SwitchAdmin, Operator
Security Admin	Role-based operator authentication	Username and Password	SecurityAdmin
Fabric Admin	Role-based operator authentication	Username and Password	FabricAdmin
Maximum Permissions (for a user-defined role)	Role -based operator authentication	Username and Password	N/A
LDAP Server	Role -based operator authentication	LDAP Root CA certificate	N/A
RADIUS Server	Role -based operator authentication	RADIUS Shared Secret	N/A
Host/Server/Peer Switch	Role -based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)	N/A

Table 10 Roles and Required Identification and Authentication continued

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 1/2^80 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 10/2^80 which is less than 1/100,000.
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 is 16 attempts. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Table 11 Strengths of Authentication Mechanisms

Service Name	Description	FOS Interface
Fabric Element Authentication	Fabric element authentication, including selection of authentication protocols, protocol configuration selection and setting authentication secrets.	authutil secauthsecret
FIPSCfg	Control FIPS mode operation and related functions.	fipscfg
Zeroize	Zeroize all CSPs.	fipscfg --zeroize
FirmwareManagement	Control firmware management.	firmwarecommit firmwaredownload firmwaredownloadstatus
PKI	PKI configuration functions, including FOS switch certificates and SSL certificates.	seccertutil
RADIUS	RADIUS configuration functions.	aaaconfig
LDAP	LDAP configuration functions.	aaaconfig
UserManagement	User and password management.	passwd passwdconfig userconfig

Table 12 Service Descriptions

6 Access Control Policy

6.1 Roles and Services

	User	Admin	FabricAdmin	SecurityAdmin	Maximum Permissions	LDAP Server	RADIUS Server	Host Server/Peer Switch
Fabric Element Authentication		X		X	X			X
FIPSCfg		X		X	X			
Zeroize		X		X	X			
FirmwareManagement	X	X	X	X	X			
PKI	X	X	X	X	X			
RADIUS		X		X	X		X	
LDAP		X		X	X	X		
UserManagement		X		X	X			

Table 13 Services Authorized for Roles

Crypto Function/Service	***User Role Change***	***Additional Details***
Cipher suites for SSL and TLS	Crypto-Officer*	AES-128-CBC (non-compliant), AES-128-ECB (non-compliant), AES-192-CBC (non-compliant), AES-192-ECB (non-compliant), AES-256-CBC (non-compliant), AES-256-ECB (non-compliant), BF, BF-CBC, BF-CFB, BF-ECB, BF-OFB, CAST, CAST-CBC, CAST5-CBC, CAST5-CFB, CAST5-ECB, CAST5-OFB, DES, DES-CBC, DES-CFB, DES-ECB, DES-EDE, DES-EDE-CBC, DES-EDE-CFB, DES-EDE-OFB, DES-EDE3, DES-EDE3-CBC, DES-EDE3-CFB, DES-EDE3-OFB, DES-OFB, DES3, DESX, RC2, RC2-40-CBC, RC2-64-CBC, RC2-CBC, RC2-CFB, RC2-ECB, RC2-OFB, RC4, RC4-40
Message Digests for SSL and TLS	Crypto-Officer*	MD2, MD4, RMD160

Crypto Function/Service	*User Role Change*	*Additional Details*
Ciphers and Message Authentication Codes for configuring SSH	Crypto-Officer	Ciphers: AES-128-CTR (non-compliant), AES-192-CTR (non-compliant), AES-256-CTR (non-compliant), ARCFOUR256, ARCFOUR128, AES-128-CBC (non-compliant), 3DES-CBC (non-compliant), BLOWFISH-CBC, CAST128-CBC, AES-192-CBC (non-compliant), AES-256-CBC (non-compliant), ARCFOUR Message Authentication Codes: HMAC-MD5, HMAC-SHA-1 (non-compliant), UMAC-64, HMAC-RIPEMD160, HMAC SHA-1-96 (non-compliant), HMAC-MD5-96
Common Certificates for FCAP and HTTPS	Crypto-Officer	FCAP and HTTPS are supported with certificates of any size (512 to 2048) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
SNMP	Crypto-Officer	SNMPv1 (plaintext) and SNMPv3 KDF (non-compliant); Algorithms: SHA-1 (non-compliant) and MD5
RADIUS or LDAP	Crypto-Officer	PAP and CHAP authentication method for RADIUS (all considered as plaintext) RADIUS and LDAP are supported with CA certificates of any size (512 to 2048) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant) LDAP uses TLS connections in non-FIPS mode without certificates
Telnet	N/A	N/A (plaintext)
HTTP	N/A	N/A (plaintext)
FTP	Crypto-Officer	Config Upload, Config Download, Support Save, FW Download, autoftp
FCIP IKE or IPSec	N/A	Management Interface IPSec/IKE (disabled for management interface)
In-Band Management Interface	N/A	N/A (plaintext)
RSA	Crypto-Officer	RSA key size < 2048 bits for SSH and TLS
Diffie-Hellman	Crypto-Officer	DH public key size for SSH can be 1024 bits to 2048 bits DH private key size for SSH can only be 256 bits
In-Flight Encryption	Crypto-Officer	IKE: DH 2048 keys with SHA-1 (non-compliant) for key exchange and HMAC SHA-512 (non-compliant) for IKE protocol 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)

***No longer available after FIPS mode is set**

Table 13b Services/Functions in non-Approved mode

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.

6.3 Definition of Critical Security Parameters (CSPs)

DH Private Keys:

- DH Private Keys (256 bits) for use with 2048 bit modulus

FCSP CHAP Secret:

- Fibre-Channel Security Protocol (FCSP) CHAP Secret

FCAP Private Key:

- Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 2048)

SSHv2/SCP/SFTP CSPs:

- SSHv2/SCP/SFTP Session Keys - 128, 192, and 256 bit AES CBC or Triple-DES 3 key CBC
- SSHv2/SCP/SFTP Authentication Key (HMAC-SHA-1)
- SSHv2 KDF Internal State
- SSHv2 DH Shared Secret Key (2048 bits)
- SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- SSHv2 2048 RSA Private Key
- Value of K during SSHv2 256 ECDSA Session
- SSHv2 ECDSA Private Key (P-256)

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, Triple-DES 3 key CBC
- TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256

RNG Seed CSPs

- Approved RNG Seed Material
- ANSI X9.31 DRNG Internal State

Operator Authentication/Passwords

- Passwords
- RADIUS Secret

6.4 Definition of Public Keys

- DH Public Key (2048 bit modulus)
- DH Peer Public Key (2048 bit modulus)
- FCAP Public Key (RSA 2048)
- FCAP Peer Public Key (RSA 2048)
- TLS Public Key (RSA 2048)
- TLS Peer Public Key (RSA 2048)
- FW Download Public Key (RSA 2048)
- SSHv2 RSA 2048 bit Public Key
- LDAP ROOT CA certificate (RSA 2048)
- SSHv2 ECDSA Public Key (P-256)
- SSHv2 ECDH Public Key (P-256, P-384 and P-521)

6.5 Definition of CSPs Modes of Access

Table 14 CSP Access Rights within Roles & Services defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

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

	SSHv2/SCP/SFTP CSPs	DH Private Keys	TLS CSPs	RNG Seed Material/Internal State	Passwords	RADIUS Secret	FCAP Private Key	FCSP CHAP Secret
Fabric Element Authentication	N	N	N	RW	N	N	RW	RW
FIPSCfg	N	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	R	N	N	N	N	N	N
PKI	RW	RW	N	RW	N	N	N	N
RADIUS	N	N	N	N	RW	RW	N	N
UserManagement	N	N	RW	RW	RW	N	N	N

Table 14 CSP Access Rights within Roles & Services

.

	DH Public Key	FCAP Public Key	TLS Public Key	Firmware Download Public Key	SSHv2 RSA 2048 Public Key	LDAP Root CA Certificate
Fabric Element Authentication	RW	RW	N	N	N	N
FIPSCfg	N	N	N	N	N	N
Zeroize	N	N	N	N	N	N
FirmwareManagement	N	N	N	RW	N	N
PKI	N	N	RW	N	RW	N

Table 15 Public Key Access Rights within Roles & Services

	DH Public Key	FCAP Public Key	TLS Public Key	Firmware Download Public Key	SSHv2 RSA 2048 Public Key	LDAP Root CA Certificate
LDAP	N	N	N	N	N	RW
User Management	N	N	N	N	N	N

Table 15 Public Key Access Rights within Roles & Services continued

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.

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:
        i) Cryptographic algorithm tests:
            (1) Three Key Triple-DES CBC KAT (Encrypt/Decrypt)
            (2) AES (128, 192, 256) CBC KAT (Encrypt/Decrypt)
            (3) HMAC SHA-1 KAT
            (4) HMAC SHA-256 KAT
            (5) HMAC SHA-384 KAT
            (6) HMAC SHA-512 KAT
            (7) ANSI X9.31 DRNG KAT
            (8) SHA-1 KAT
            (9) SHA-256 KAT
            (10) SHA-384 KAT
            (11) SHA-512 KAT
            (12) RSA 2048 SHA-256 Sign/Verify KAT
            (13) SP800-135 SSHv2 KDF KAT
            (14) SP800-135 TLS v1.0 KDF KAT
            (15) SP800-135 TLS v1.2 KDF KAT
        ii) Firmware Integrity Test (128-bit EDC)
        iii) Critical Functions Tests:
            (1) RSA 2048 Encrypt/Decrypt

b) Conditional Self-Tests:

   i) Continuous Random Number Generator (RNG) test – performed on non-approved RNG.

   ii) Continuous Random Number Generator test – performed on ANSI X9.31 DRNG.

   iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

   iv) RSA 2048 Pairwise Consistency Test (Encrypt/Decrypt)

   v) ECDSA Pairwise Consistency Test (Sign/Verify)

   vi) Firmware Load Test (RSA 2048 with SHA-256 Signature Verification)

   vii) Bypass Test: N/A

   viii) Manual Key Entry Test: N/A

4) 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.

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

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

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

8) 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.

9) NOTE: As per FIPS 140-2 Implementation Guidance D.11, Brocade hereby states that the following protocols have not been reviewed or tested by the CAVP or CMVP:

   a) TLS v1.0/1.1

   b) TLS v1.2

   c) SSHv2

10) As per FIPS 140-2 Implementation Guidance 7.9, the authorized operator performing the zeroization service shall be physically present at the cryptographic boundary and in full control of the module for the duration of the zeroization to observe that the zeroization was completed successfully.
The operator shall follow this procedure to zeroize and validated the successful completion:

   a) Issue the zeroize command, "`fipscfg --zeroize`"

   b) Confirm the status by examining the following status on the console:

      i) "`Event: zeroize, Status: success`"

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.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	12 months	Reference Appendix A for a description of tamper label application for all evaluated platforms.

Table 16 Inspection/Testing of Physical Security Mechanisms

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.

11 Definitions and Acronyms

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
CSP	Critical Security Parameter
DH	Diffie-Hellman
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
KDF	Key Derivation Function
KAT	Known Answer Test
LED	Light Emitting Diode
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NTP	Network Time Protocol
NOS	Network Operating System
PKI	Public Key Infrastructure
PROM	Programmable read-only memory
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
TLS	Transport Layer Security Protocol

12 Brocade Abbreviations

24P	24 ports
48P	48 ports
16GB	16 Gigabit
8GB	8 Gigabit
SFP	Small form-factor pluggable
LWL	long wave length
SWL	Short wave length
LIC	License
UPG	Upgrade
2PS	Two power supply modules
0P	No port blades
0SFP	Zero SFP devices provided
2CP	Two Control processor blades (see Table 4)
2 CORE	Two core switch blades (see Table 4)
ENT BUN	Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized (see table note for Table 3)
BR	Brocade
WWN	World Wide Name card
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
FC	Fibre Channel
FCIP	Fiber Channel over Internet Protocol
GE	Gigabit Ethernet
GBE	Gigabit Ethernet
CP8	8G Control Processor blade
CR8	8G Core Switch Blade for DCX backbone
CR4S-8	8G Core Switch Blade for DCX -4S backbone
CR16-8	16G core switch blade for DCX 8510-8 backbone
CR16-4	16G core switch blade for DCX 8510-4 backbone
FC8-16	8G, 16-port, Fibre Channel port blade
FX8-24	8G, 24 port, Extension blade
ICL	Inter-Chassis Link
MGMT	Management

Appendix A: Tamper Label Application

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.

Brocade DCX and DCX 8510-8 Backbone

Twenty-two (22) tamper evident seals are required to complete the physical security requirements total. See Figure 7 to Figure 12 for directions.

- Apply three (3) seals to the right side of the chassis.

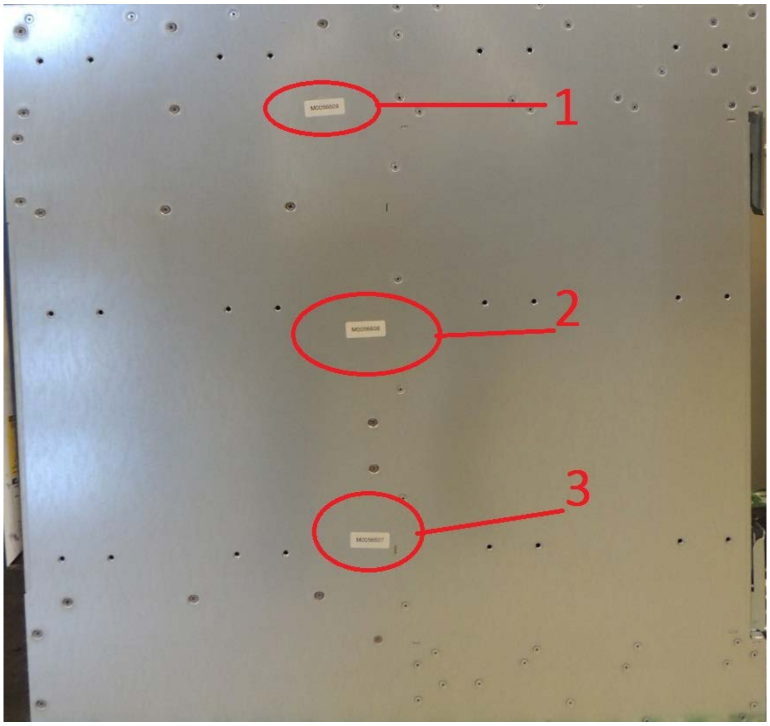

Figure 7 Brocade DCX and DCX 8510-8 Backbone chassis right side seal location

- Apply twelve (12) seals to the front side of the chassis.

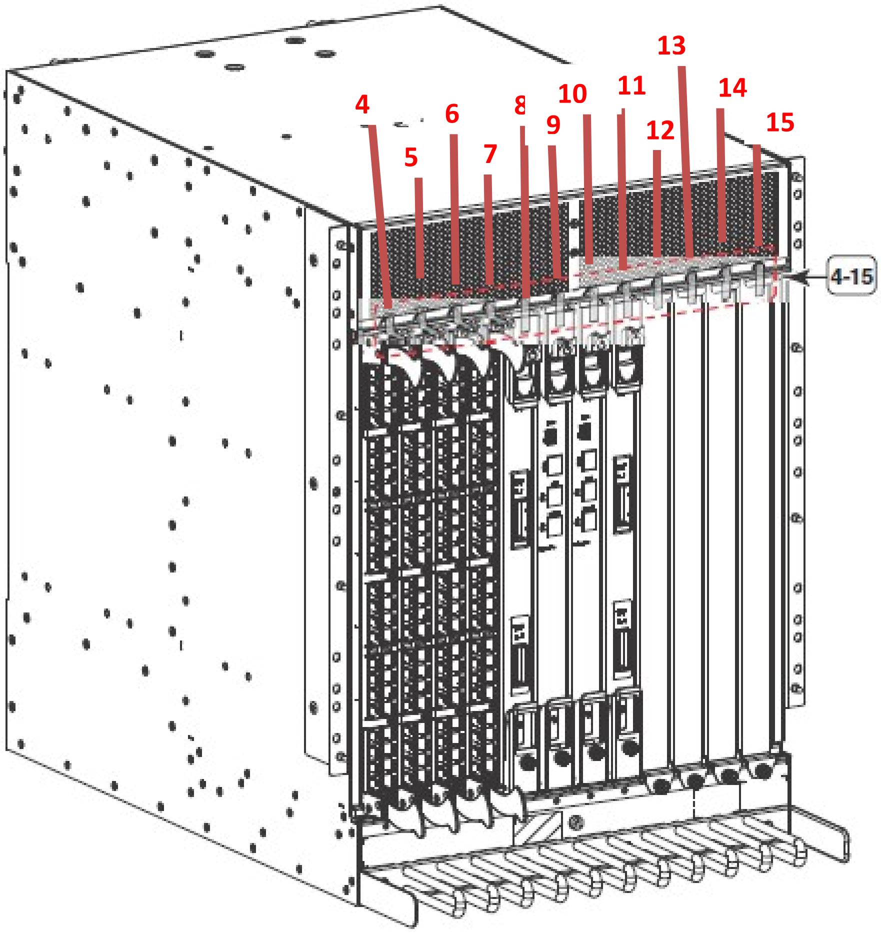

Figure 8 Brocade DCX and DCX 8510-8 Backbone front side seal locations (QTY 12)

- Apply seven (7) seals to the back side of the chassis

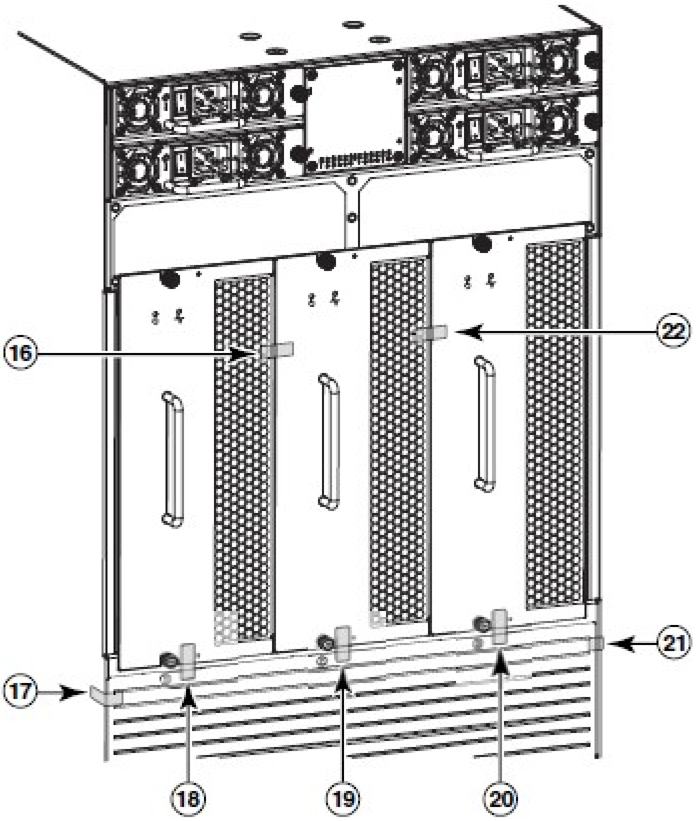

Figure 9 Brocade DCX and DCX 8510-8 Backbone back side seal locations

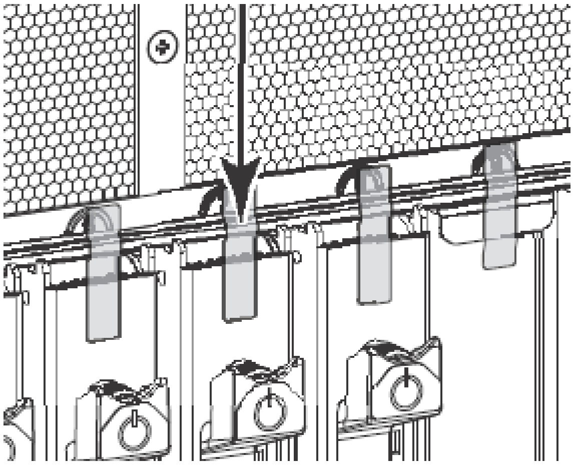

Figure 10 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application on the port side

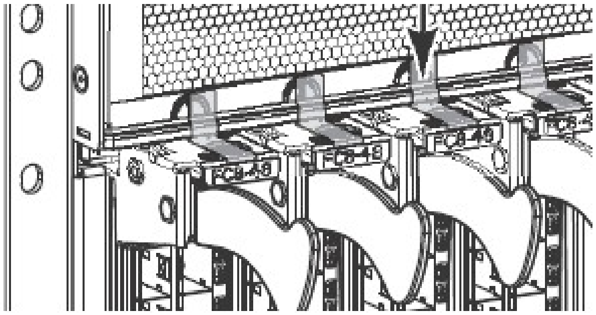

Figure 11 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application on the port side

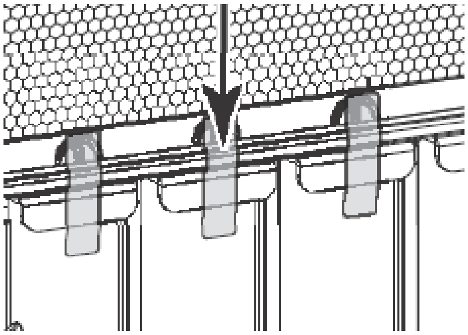

Figure 12 Brocade DCX and DCX 8510-8 Backbone filler panel seal application on the port side

Brocade DCX-4S and DCX 8510-4 Backbone

Nineteen (19) tamper evident seals are required to complete the physical security requirements total. See Figure 13- Figure 18 for directions.

- Apply fourteen (14) seals to the backbone front side of the chassis.

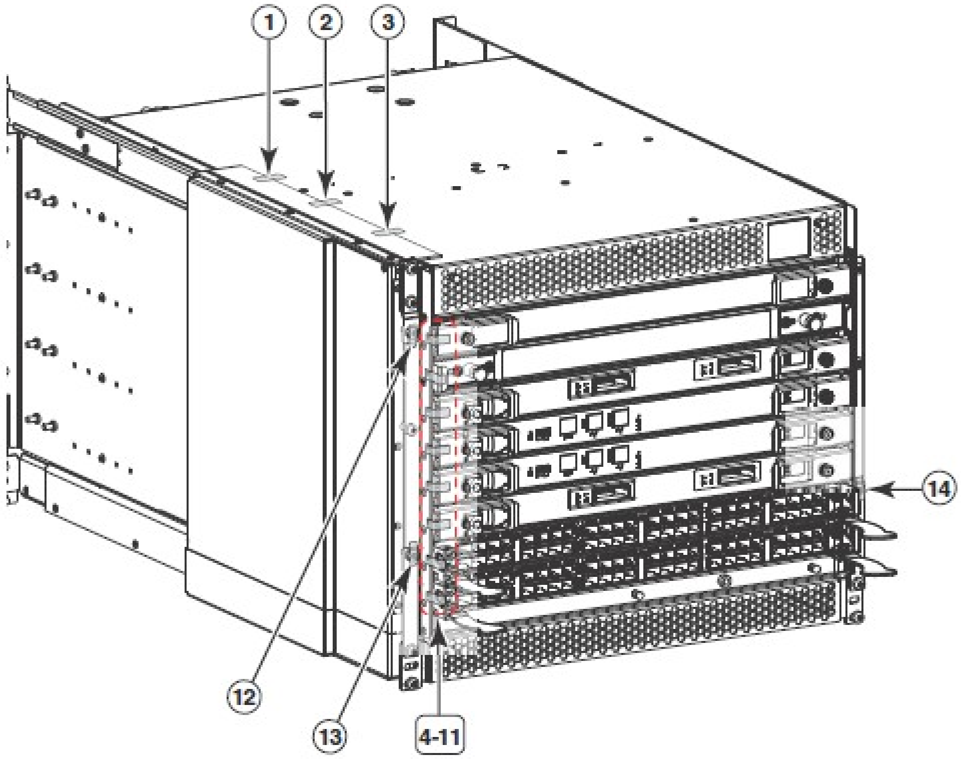

Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone front side seal locations

- Apply five (5) seals to the back side of the chassis

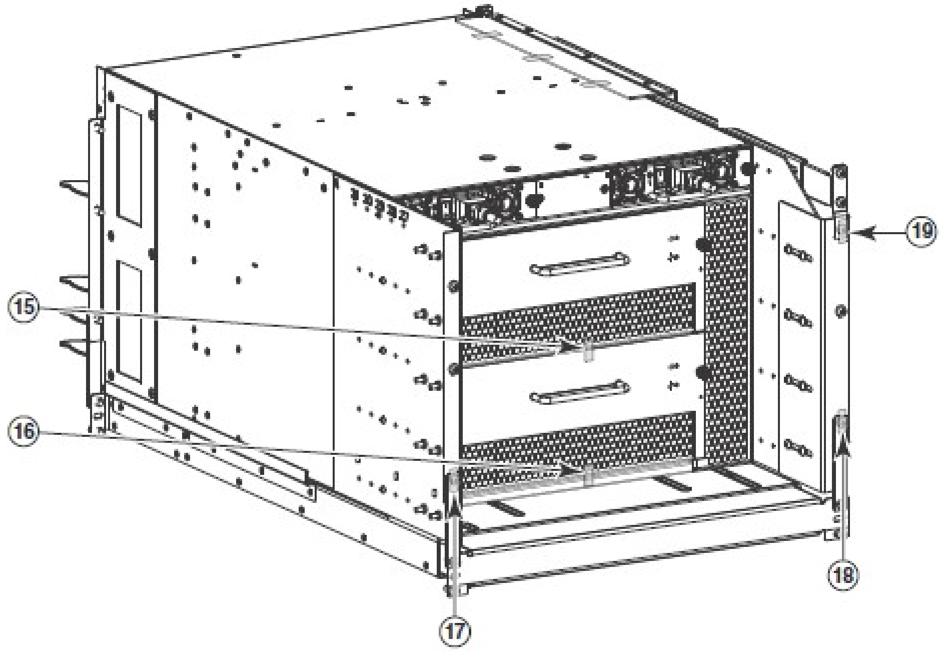

Figure 14 Brocade DCX-4S and DCX 8510-4 Backbone back side seal locations

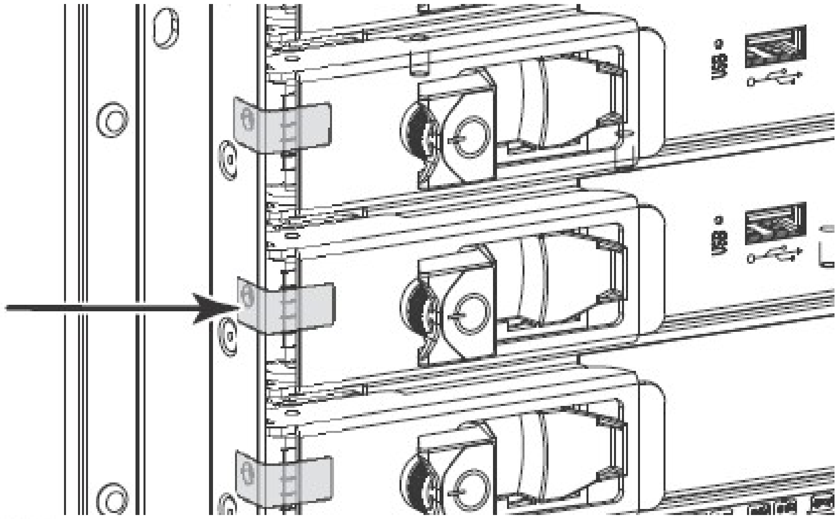

Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application

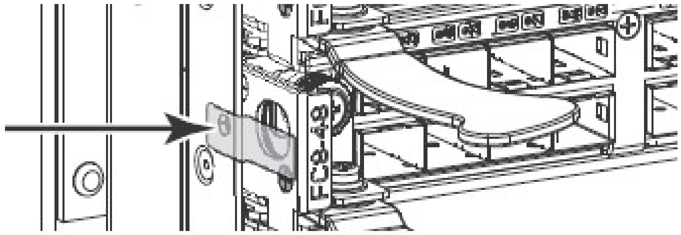

Figure 16 Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application

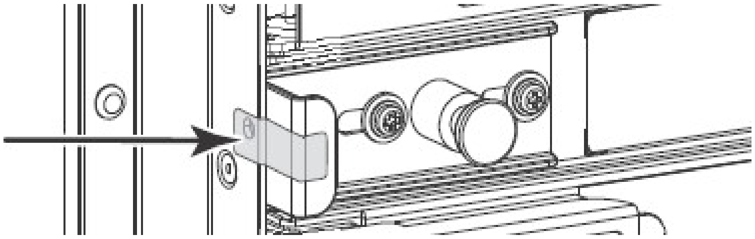

Figure 17 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application

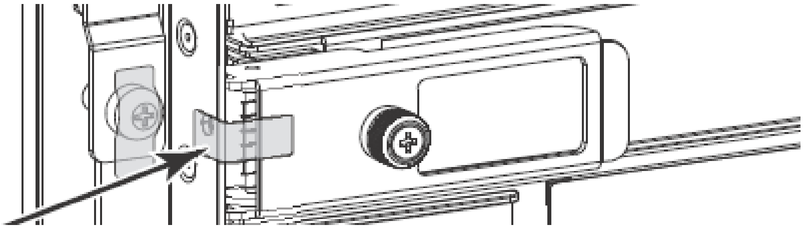

Figure 18 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application

Brocade 6510

Two tamper evident seals are required to complete the physical security requirements. See Figure 19 to Figure 21 for directions.

- Apply one (1) seal to the left side. See Figure 19.

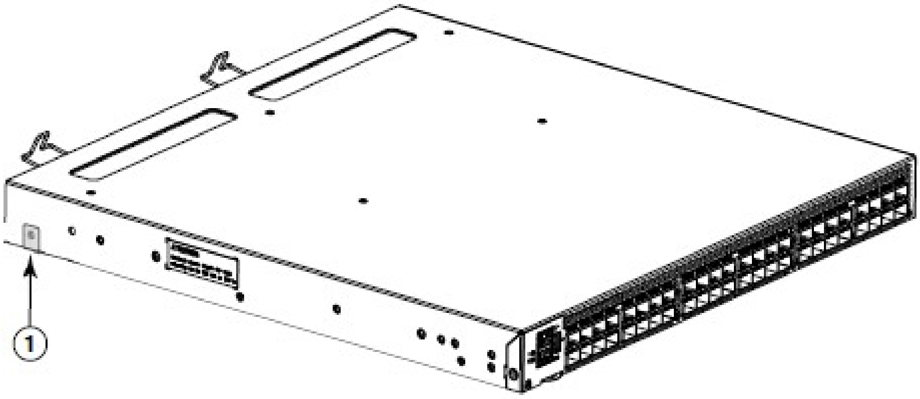

Figure 19 Brocade 6510 left side seal application

- Apply one (1) seal to the right side. See Figure 20.

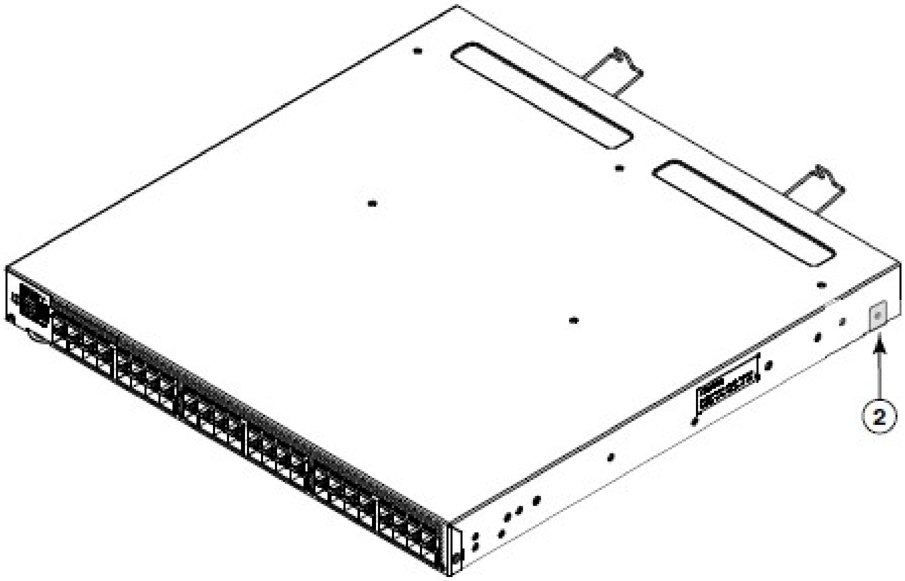

Figure 20 Brocade 6510 right side seal application

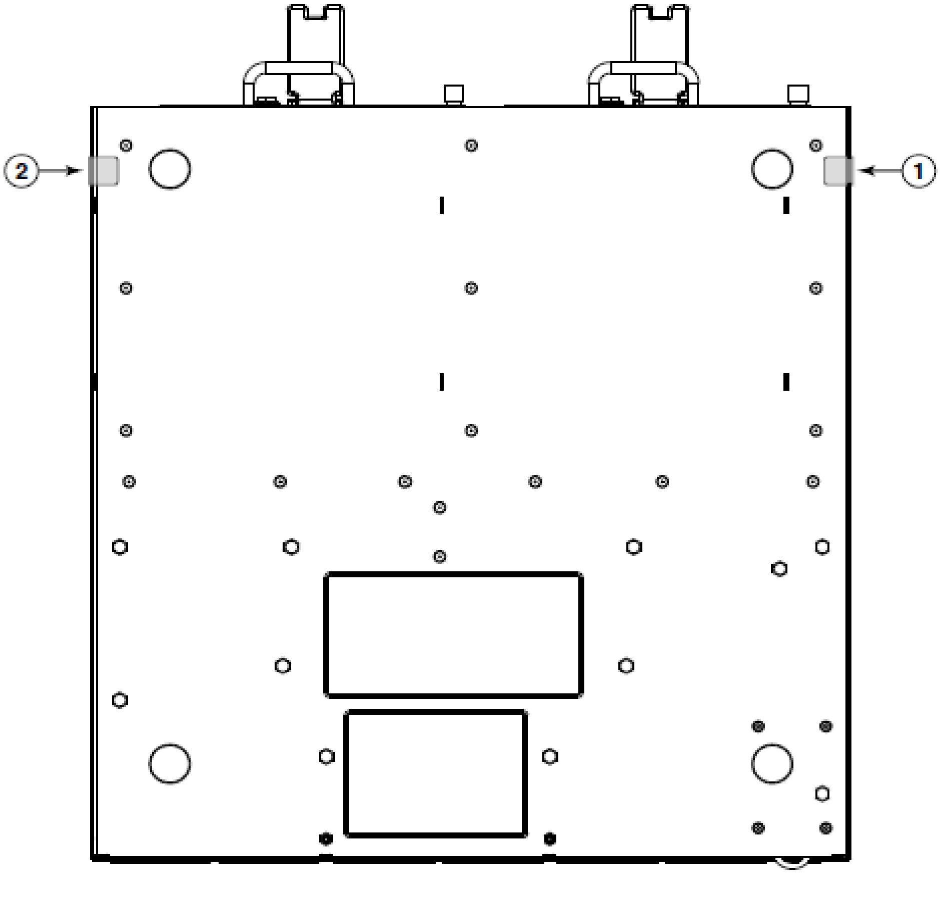

Figure 21 Brocade 6510 bottom seal locations

Brocade 6520

Twenty-six (26) tamper evident seals are required to complete the physical security requirements. See Figure 22 to Figure 25 for seal placement directions.

1. Relative to the left side of the Brocade 6520, apply four (4) seals along the left bottom side of the chassis. Make a 90 degree bend from the left side to the bottom side of the chassis. See Figure 22 for details on how to position each seal.
2. Relative to the left side of the Brocade 6520, apply one (1) seal vertically, on the left side of the switch, over the seam between the top cover and the front panel of the switch. Do not allow the seal to cover either of the rack mount screw holes on the left side of the switch. See Figure 22 for details on how to position each seal.

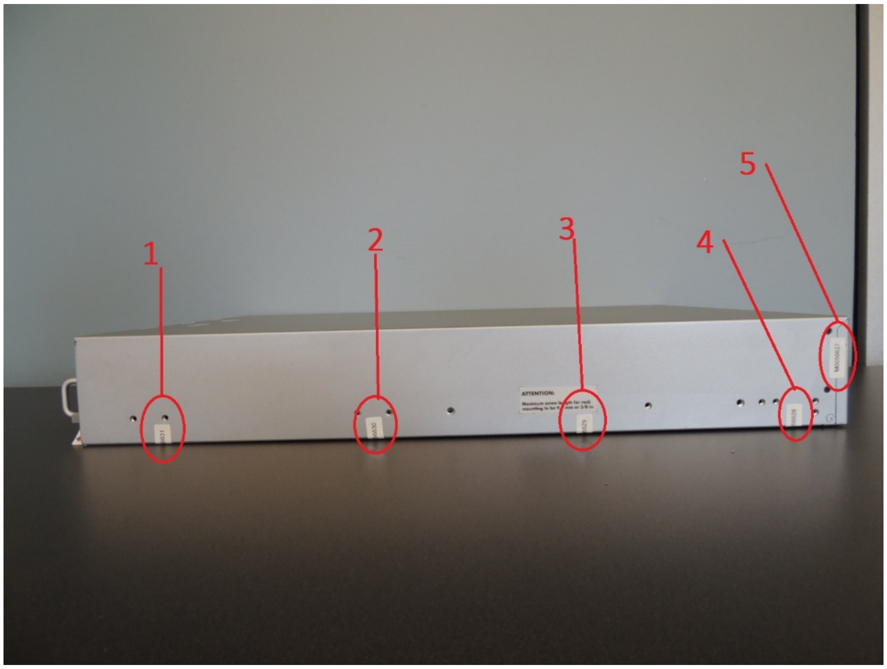

Figure 22 Brocade 6520 left side seal locations (QTY 5)

3. Relative to the right side of the Brocade 6520, apply four (4) seals along the right bottom side of the chassis. Make a 90 degree bend from the right side to the bottom side of the chassis. See Figure 23 for details on how to position each seal.
4. Relative to the right side of the Brocade 6520, apply one (1) seal vertically, on the right side of the switch, over the seam between the top cover and the front panel of the switch. Do not allow the seal to cover either of the rack mount screw holes on the left side of the switch. See Figure 23 for details on how to position each seal.

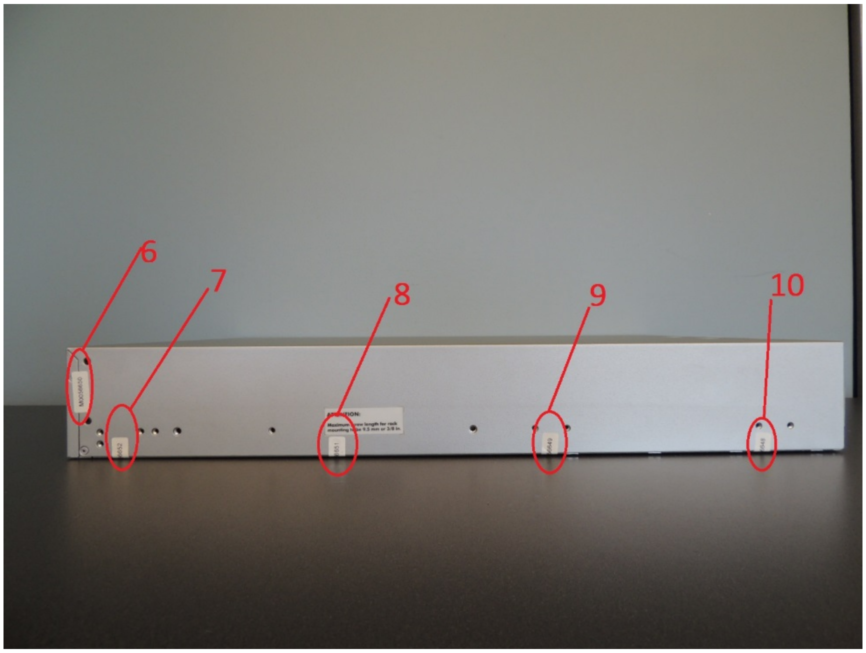

Figure 23 Brocade 6520 right side seal locations (QTY 5)

5. Relative to the non-port side of the Brocade 6520, apply one (1) seal over the seam between the top cover and the grill of the each of the three (3) FAN FRUs. Each seal makes a 90 bend from the top of the switch and the grill of each FAN FRU. See Figure 24 for details on how to position each seal. Apply two (2) seals over the flathead screws on the top cover near the FAN FRUs. See Figure 24 for details on how to position each seal. Five (5) seals are required to complete this step.
6. Relative to the non-port side of the Brocade 6520, apply two (2) seals over the seam between the chassis and the AC power module on the left non-port side of the chassis. See Figure 24 for details on how to position each seal.

7. Relative to the non-port side of the Brocade 6520, apply two (2) seals over the seam between the chassis and the AC power module on the right non-port side of the chassis. See Figure 24 for details on how to position each seal.
8. Relative to the non-port side of the Brocade 6520, apply one (1) seal to the flange of each of the three (3) FAN FRUs and the bottom of the switch. Each seal makes a 90 bend from the bottom of the switch to the flange of each FAN FRU. See Figure 24 for details on how to position each seal. Three (3) seals are required to complete this step.

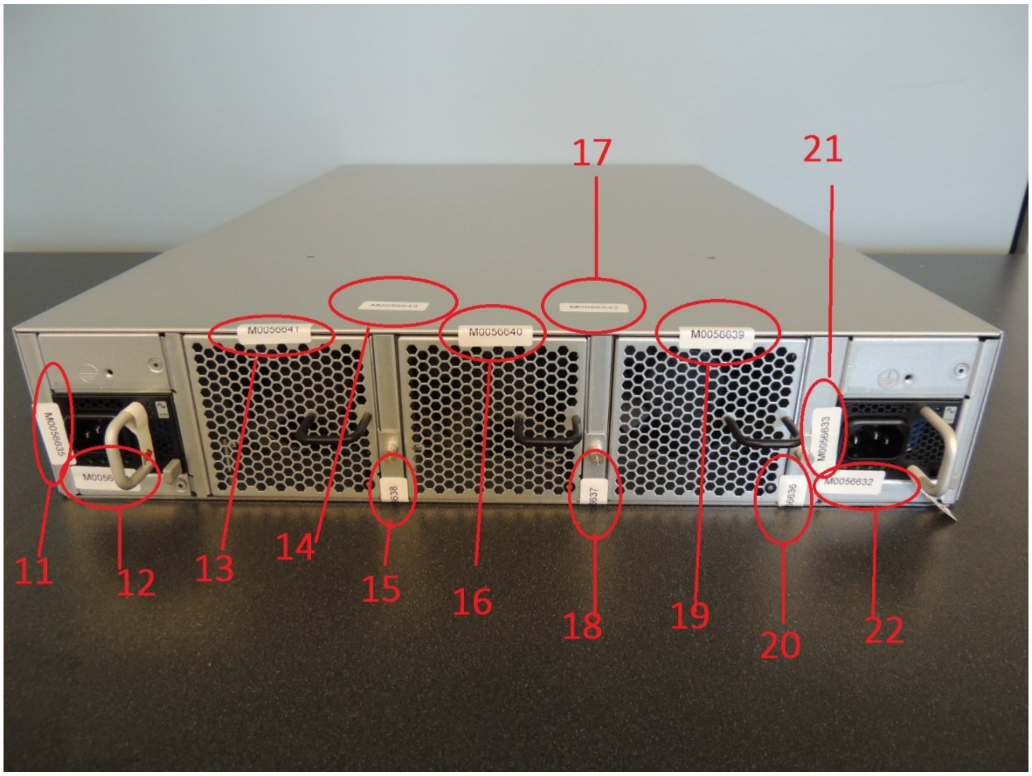

Figure 24 Brocade 6520 top and non-port side seal locations (QTY 11)

9. Relative to the bottom side of the Brocade 6520, apply four (4) seals diagonally, on the bottom side of the switch, over the seam between the front panel and the bottom panel of the switch. See Figure 25 for details on how to position each seal.

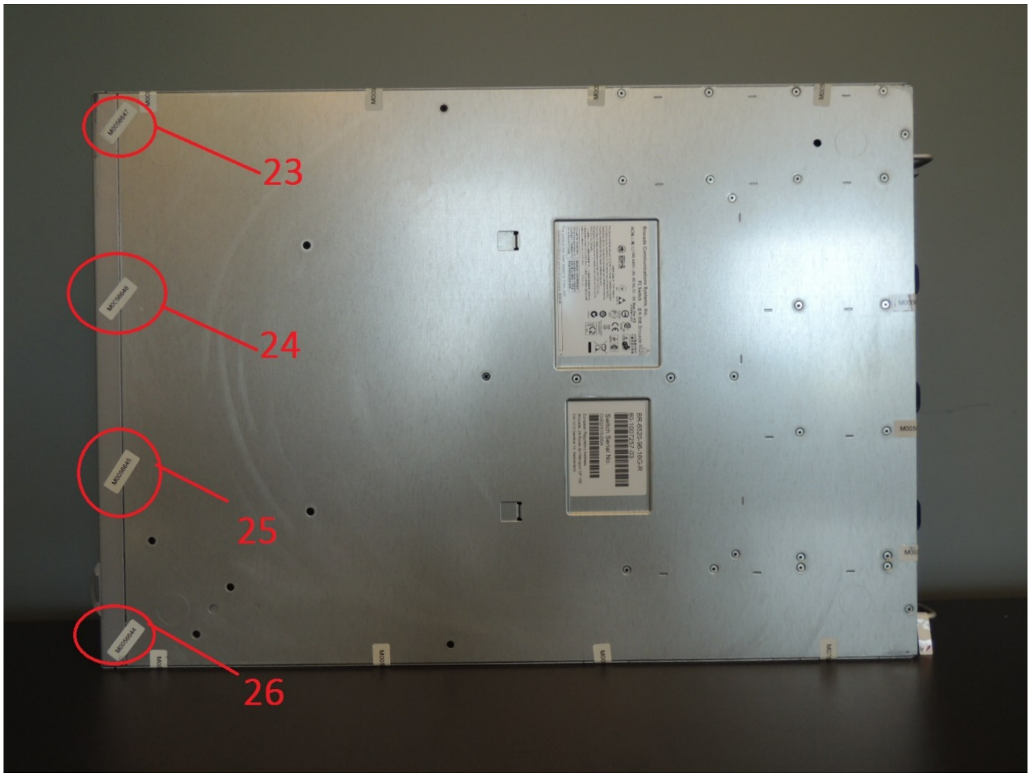

Figure 25 Brocade 6520 bottom side seal locations (QTY 4)

Brocade 7800

Two (2) tamper evident seals are required to complete the physical security requirements. See Figure 26 to Figure 28 for seal placement.

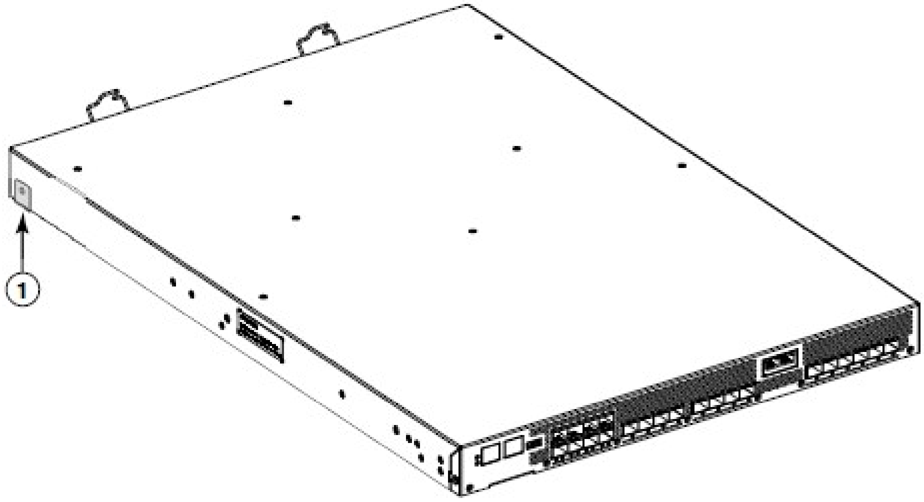

Figure 26 Brocade 7800 left side seal locations

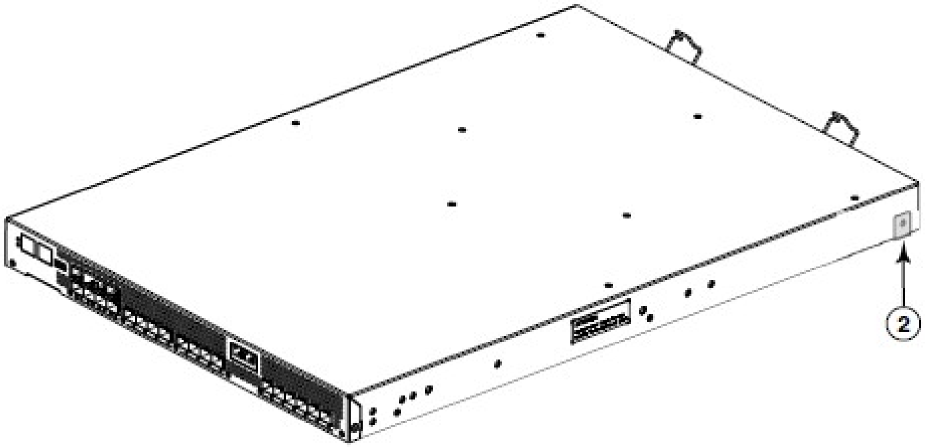

Figure 27 Brocade 7800 right side seal locations

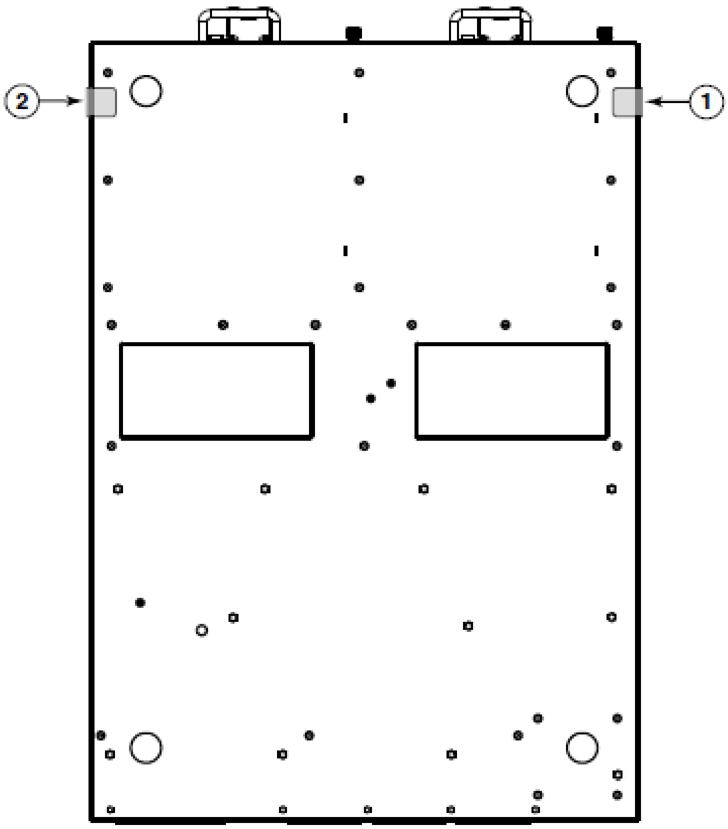

Figure 28 Brocade 7800 bottom seal locations (QTY 2)

Brocade 7840

Twenty-seven (27) tamper evident seals are required to complete the physical security requirements for the Brocade 7840. Steps 1 – 5 below detail the tamper evident seal placement for the Brocade 7840 module.

1. Apply two (2) seals to the front side of the module. See Figure 29 for correct seal placement.
2. Apply twelve (12) seals to the back side of the module. See Figure 30 for correct seal placement.
3. Apply five (5) seals to the left side of the module. These seals will wrap around to the bottom of the module. See Figure 31 for correct seal placement.
4. Apply five (5) seals to the right side of the module. These seals will wrap around to the bottom of the module. See Figure 32 for correct seal placement.
5. Apply three (3) seals to the bottom side of the module near the front side. See Figure 33 for correct seal placement.

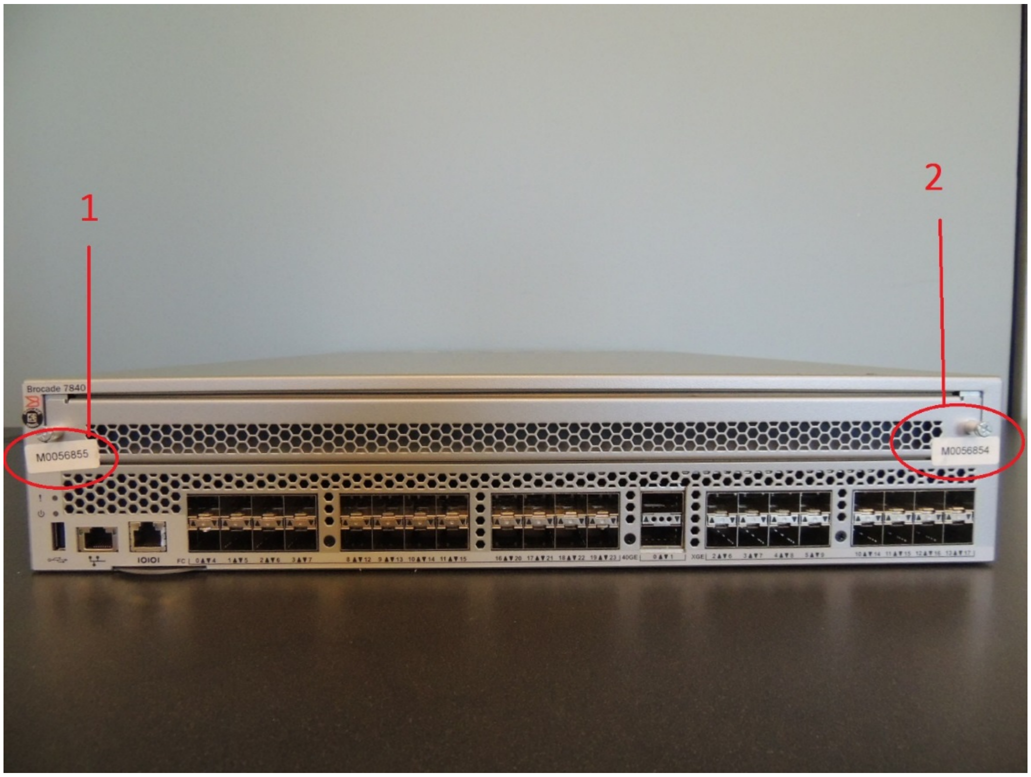

Figure 29: Brocade 7840 front side seal locations (QTY 2)

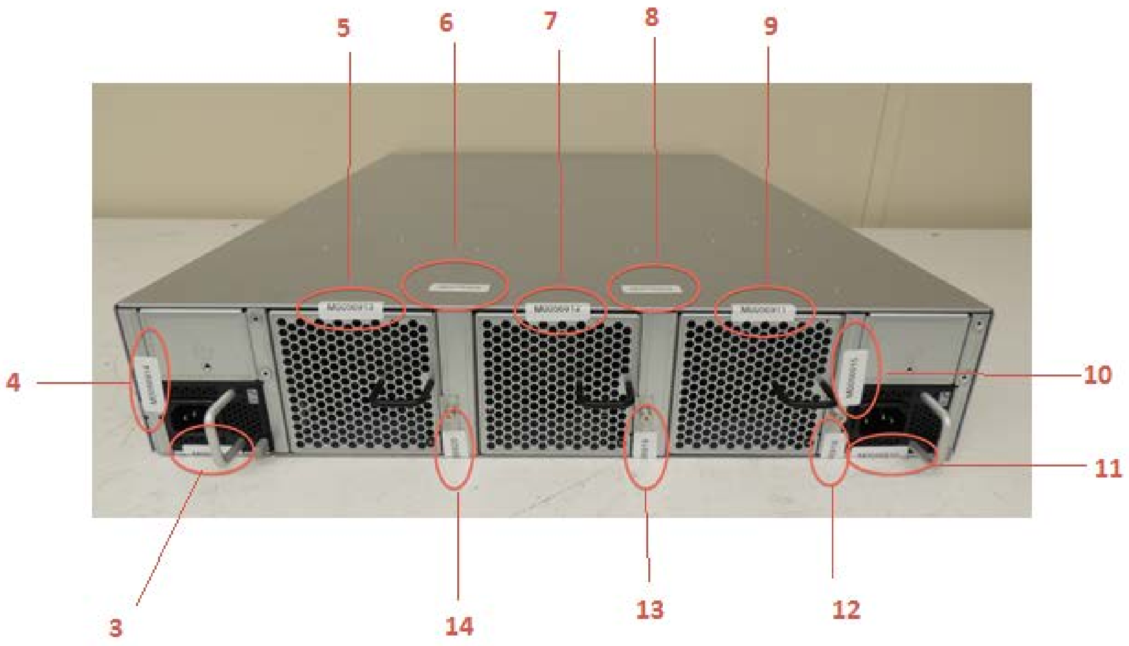

Figure 30: Brocade 7840 back side seal locations (QTY 12)

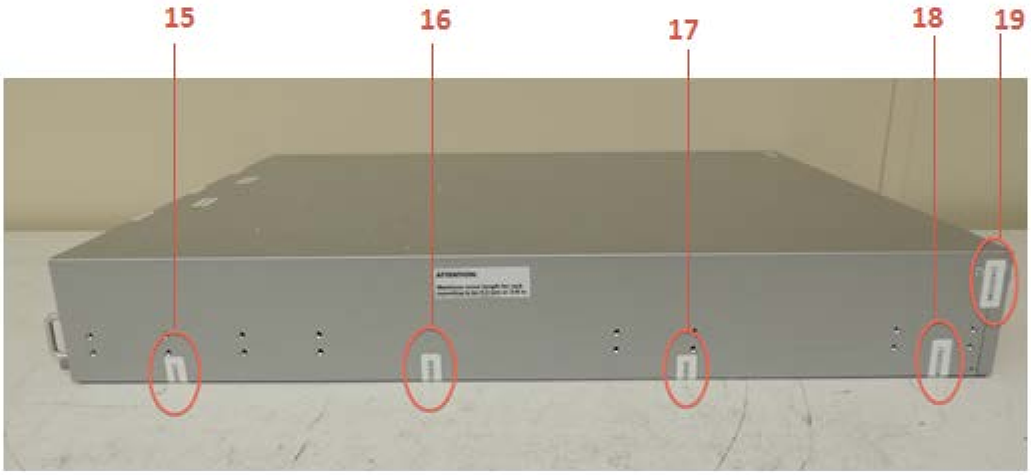

Figure 31: Brocade 7840 left side seal locations (QTY 5)

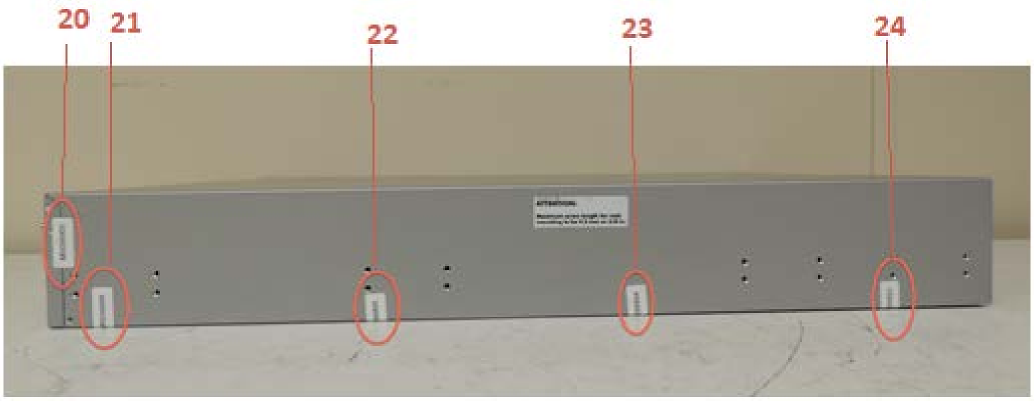

Figure 32: Brocade 7840 right side seal locations (QTY 5)

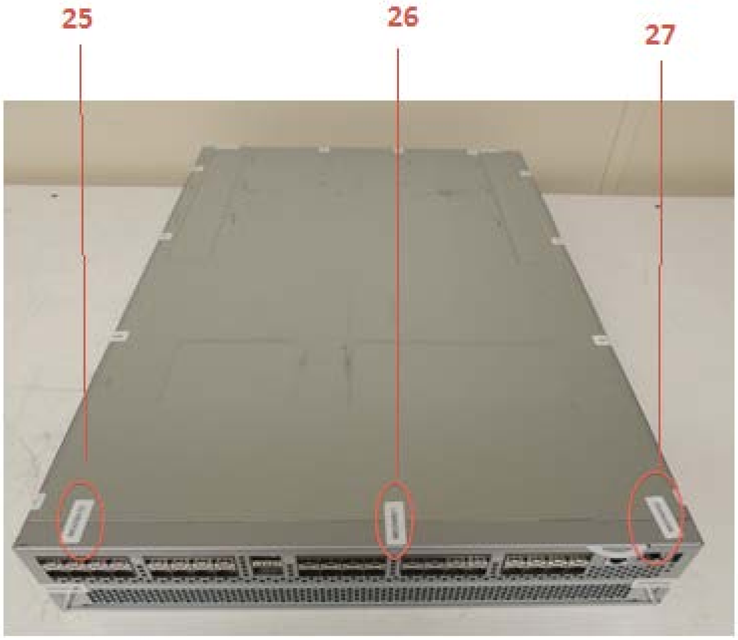

Figure 33: Brocade 7840 bottom side seal locations (QTY 3)

Appendix B: Block Diagram

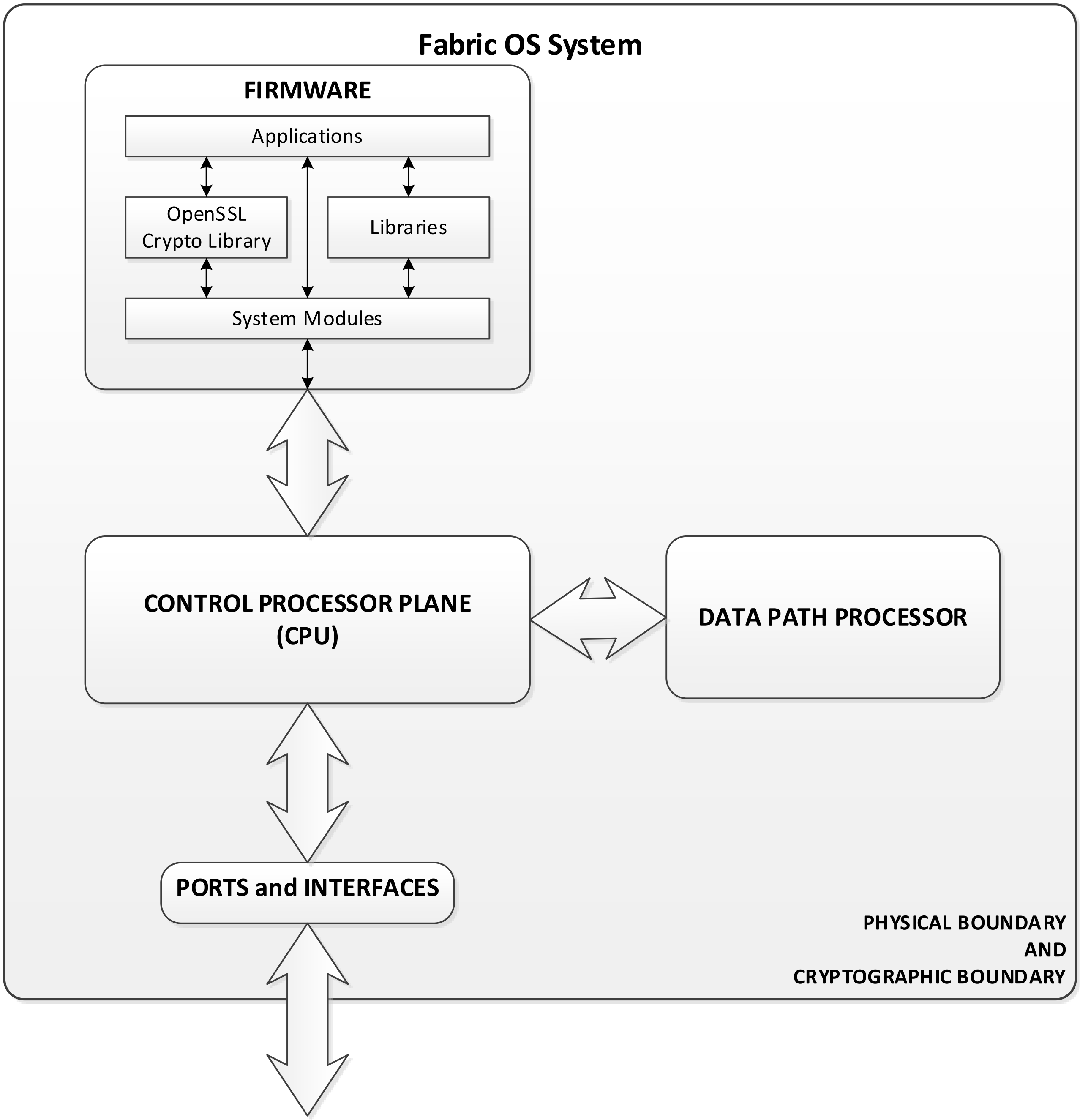

Figure 34: Block Diagram

Appendix C: Critical Security Parameters and Public Keys:

The module supports the following CSPs:

1. DH Private Keys (256 bits) for use with 2048 bit modulus
- Description: Used in DHCHAP, and 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 ANSI X9.31 DRNG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination and "fipscfg –zeroize" command

2. Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Description: Shared secret used for authentication in FC-Security Protocol
- Generation: N/A
- Storage: Plaintext in RAM, Compact Flash
- Entry: Configured by an operator during the secauthsecret command
- Output: N/A
- Destruction: "secauthsecret --remove" command

3. Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- 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 ANSI X9.31 DRNG; this is Approved as per SP800-56A.
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Destruction: "fipscfg --zeroize" command

4. SSHv2/SCP/SFTP Session Keys - 128, 192, and 256 bit AES CBC or Triple-DES 3 key CBC
- Description: AES or TDES encryption key used to secure SSHv2/SCP/SFTP sessions
- 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
- Destruction: Session termination or "fipscfg --zeroize" command

5. SSHv2/SCP/SFTP Authentication Key (HMAC-SHA-1)
- Description: Session authentication key 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
- Destruction: Session termination or “fipscfg –zeroize” command

6. 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: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fipscfg --zeroize” command

7. SSHv2 DH Shared Secret Key (2048 bits)
- 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
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fipscfg --zeroize” command

8. SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- Description: Shared secret from the EC DH 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
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fipscfg –zeroize” command

9. SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- Description: ECDH private key
- 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 ANSI X9.31 DRNG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A as per IG 7.7
- Output: N/A
- Storage: Plaintext in RAM
- Key-To-Entity: Process
- Destruction: Session termination or “fipscfg –zeroize” command

10. SSHv2 2048 RSA Private Key
- 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.
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fipscfg –zeroize” command

11. Value of K during SSHv2 256 ECDSA session
- Description: Used to authenticate generate keys that signs and verify
- Generation: ANSI X9.31 RNG, as per FIPS 186-4
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fipscfg --zeroize” command

12. 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
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg --zeroize" command

13. 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 6.2, key generation is performed as per FIPS 186-4; this is an allowed method as per FIPS 140-2 IG D.9

Establishment: RSA key wrapped over TLS session; allowed as per FIPS 140-2 IG D.9
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Destruction: "fipscfg –zeroize" command

14. TLS Pre-Master Secret
- Description: Secret value used to establish the Session and Authentication key
- Generation: N/A
- 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: N/A
- Destruction: Session termination or “fipscfg –zeroize” command

15. 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
- Destruction: Session termination or “fipscfg –zeroize” command

16. 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
- Destruction: Session termination or “fipscfg –zeroize” command

17. TLS Session Keys - 128, 256 bit AES CBC, TDES 3 key CBC
- Description: TDES or 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
- Destruction: Session termination

18. TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256
- Description: HMAC-SHA-1, 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
- Destruction: Session termination

- - - RNG Seed CSPs- - -

19. Approved RNG Seed Material
- Description: ANSI X9.31 DRNG seed and seed key
- Generation: Internally generated; raw random data from NDRNG
- Storage: Plaintext in RAM
- Entry: N/A

- Output: N/A
- Destruction: Session termination or “fipscfg --zeroize” command

20. ANSI X9.31 DRNG Internal State
- Description: DRNG Internal State
- Generation: ANSI X9.31 DRNG seeded by RNG Seed Material from NDRNG
- Storage: RAM (plaintext)
- Entry: N/A
- Output: N/A
- Destruction: "fipscfg --zeroize" command

21. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A
- Storage: MD5 digest (plaintext) in Compact Flash
- Entry: Configured by the operator during account maintenance and authentication
- Output: MD5 hashed to associated devices
- Destruction: "fipscfg --zeroize" command

22. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Configured by an operator during the "aaaconfig --add" command
- Output: CLI through "aaaconfig -show" and "configupload"
- Destruction: "fipscfg --zeroize" command

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

23. DH Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- 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 ANSI X9.31 DRNG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext

24. DH Peer Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- Generation: N/A
- Storage: Plaintext in RAM
- Entry: plaintext
- Output: N/A

25. FCAP Public Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- Generation: N/A
- Storage: Plaintext in DRAM
- Entry: plaintext
- Output: plaintext

26. FCAP Peer Public Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- Generation: N/A
- Storage: Plaintext in DRAM
- Entry: plaintext
- Output: N/A

27. TLS Public Key (RSA 2048)
- Description: Used by client to encrypt TLS Pre-Master secret
- Generation: As per SP800-133 Section 6.2, key generation is performed as per FIPS 186-4; this is an allowed method as per FIPS 140-2 IG D.9.

- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext

28. TLS Peer Public Key (RSA 2048)
- Description: Used to authenticate the client
- Generation: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext during TLS handshake protocol
- Output: N/A

29. FW Download Public Key (RSA 2048)
- Description: Used to update the FW of the module.
- Generation: N/A Generated outside the module
- Storage: Plaintext in Compact Flash
- Entry: Through firmwarekeyupdate cmd or through FW Update.
- Output: Through firmwarekeyshow cmd.

30. SSHv2 RSA 2048 bit Public Key
- Description: Used to authenticate the SSHv2 server to the 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.
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext during SSHv2 handshake

31. LDAP ROOT CA certificate (RSA 2048)
- Description: Used to authenticate LDAP server
- Generation: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext
- Output: N/A

32. 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
- Entry: N/A
- Output: plaintext during SSHv2 handshake
- Key-To-Entity: User

33 SSHv2 ECDH Public Key (P-256, P-384 and P-521)
- 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 ANSI X9.31 DRNG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM
- Key-To-Entity: Process
- Destruction: N/A

Ref. 3