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

FIPS 140-2 Non-Proprietary

Security Policy

Document Version 1.0

Brocade Communications

June 25, 2014

Document History

Version	Summary of Changes	Publication Date
1.0	Initial Release	June 25, 2014

1 Module Overview

The Brocade 6510, 6520, 7800, DCX, DCX 8510-8, DCX-4S and DCX 8510-4 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 and 7800 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 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 v7.2.0 (Part Number: 63-1001405-01) 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 v7.2.0

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

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
FCOE10-24 Port Blade	FCOE10-24	80-1002762-04[1] 80-1006991-01[2]	FRU, FCOE BLADE, 10GE X 24P
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), FCOE10-24 (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), FCOE10-24 (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.

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

3.1 Approved mode of operation

The cryptographic module supports the following Approved algorithms:

Approved Algorithm	Certificate Number
RSA	1048, 1049, 1279, 1281
SHS [SHA-1]	749, 1408
SHS [SHA-256]	749, 1408

Table 7 Approved Algorithms available in firmware

*NOTICE: 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.

This cryptographic module is impacted by SP800-131A transition rules effective January 1, 2014. Therefore, the only features that provide 112 bits of equivalent encryption strength is as follows:

- Firmware load test using RSA 2048 SHA-256 (via the Firmware Management service)

The following non-Approved algorithms and protocols are only available in non-FIPS mode of operation:

- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength; non-compliant)
- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
- SNMPv3 KDF (Cryptographic functionality does not meet FIPS requirements and is considered plaintext)
- HMAC-MD5 to support RADIUS authentication (considered as plaintext)
- NDRNG used for seeding RNG
- TLSv1.0 KDF (non-compliant)
- SSHv2 KDF (non-compliant)
- MD5 (used for password hash, considered as plaintext)
- RADIUS PEAP MS-CHAP V2
- AES (non-compliant)
- HMAC SHA-256 (non-compliant)
- HMAC SHA-512 (non-compliant)
- HMAC SHA-1 (non-compliant)
- RNG (non-compliant)
- SHS [SHA-512] (non-compliant)
- Triple-DES (non-compliant)
- RSA digital signature generation (non-compliant)

The initial state of the cryptographic module is not in a FIPS-compliant state. The cryptographic module contains three default accounts: root, 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 by an authorized Crypto-Officer physically present at the boundary; failure to adhere to such guidances is an explicit violation of the Security Policy and as such deems the cryptographic module fully non-compliant and unfit for service in an Approved mode of operation.

1) Login as Crypto-Officer.
2) Perform zeroization operation.
3) Power cycle the module.
4) Change passwords for all existing user accounts.
5) Do not use HTTP, HTTPS, RPC, TLS and SSH.
6) Disable Telnet.
7) Do not use FTP.
    a) Config Upload
    b) Config Download
    c) Support Save
8) Do not use MD5 within Authentication Protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
9) Do not use DH group 0.
10) Do not define FCIP IKE or IPSec policies.
11) Disable Management Interface IPSec/IKE.
12) Disable In-Band Management Interface.
13) Disable In-Flight Encryption.
14) Do not use Radius.
15) Do not use TACACS+ authspec mode.
16) Do not use LDAP.
17) Configure SNMP Access List for read-only access.
18) Enable Self-Tests.
19) Enable Signed FW Download.
20) Disable Boot PROM Access.
21) Disable Root Access.
22) Enable FIPS mode via the “fipscfg – enable fips” command.
23) Power cycle the module.
24) Install removable front cover (as applicable) and apply tamper labels.

The operator can determine if the cryptographic module is running in FIPS vs. non-FIPS mode by issuing the “fipscfg - show” service.

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 between FIPS and non-FIPS mode of operation, the operator is required to perform zeroization of the module's plaintext CSPs.

The following cipher suites are allowed in non-FIPS mode for configuring SSL and TLS:

aes-128-cbc,aes-128-ecb,aes-192-cbc,aes-192-ecb,aes-256-cbc,aes-256-ecb,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

The following message digests functions are allowed in non-FIPS mode: md2, md4, md5, rmd160

The following message authentication algorithms and ciphers are allowed in non-FIPS mode for configuring SSH:

Ciphers: aes-128-ctr,aes-192-ctr,aes-256-ctr,arcfour256,arcfour128,aes-128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes-192-cbc,aes-256-cbc,arcfour

Macs: hmac-md5, hmac-sha-1, umac-64, hmac-ripemd160, hmac-sha-1-96, hmac-md5-96

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

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		FCOE10-24 Port Blade	26
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 for 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 eight 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 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

Role	Type of Authentication	Authentication Data	FOS RBAC Role
Maximum Permissions (for a user-defined role)	Role -based operator authentication	Username and Password	N/A

Table 10 Roles and Required Identification and Authentication

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 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.

Table 11 Strengths of Authentication Mechanisms

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
User Management	User and password management.	passwd passwdconfig userconfig

Table 12 Service Descriptions

6 Access Control Policy

6.1 Roles and Services

	User	Admin	Security Admin	Maximum Permissions
FIPSCfg		X	X	X

Zeroize		X	X	X
FirmwareManagement	X	X	X	X
UserManagement		X	X	X

Table 13 Services Authorized for Roles

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)

- Passwords

6.4 Definition of Public Keys:

The following are the public keys contained in the module:

- FW Download Public Key (RSA 2048)

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

	Passwords
FIPSCfg	N
Zeroize	Z
FirmwareManagement	N
UserManagement	RW

Table 14 CSP Access Rights within Roles & Services

.

	Firmware Download Public Key
FIPSCfg	N
Zeroize	N
FirmwareManagement	RW

	Firmware Download Public Key
User Management	N

Table 15 Public Key Access Rights within Roles & Services

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 signed by RSA 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) RSA 1024 SHA-1 Verify KAT
        (2) RSA 2048 SHA-256 Sign/Verify KAT
    ii) Firmware Integrity Test (128-bit EDC)
    iii) Critical Functions Tests:
        (1) RSA 2048 Encrypt/Decrypt KAT
    b) Conditional Self-Tests:
    i) Continuous Random Number Generator (RNG) test – N/A
    ii) Continuous Random Number Generator test – N/A
    iii) Pairwise Consistency Test – N/A
    iv) Firmware Load Test (RSA 1024 SHA-1 and RSA 2048 SHA-256 Signature Verification) (NOTICE: This submission is impacted by SP800-131A transitions effective January 1, 2014. The use of RSA 1024 SHA-1 provides 80 bits of equivalent encryption strength. The use of RSA 2048 SHA-256 provides 112 bits of equivalent encryption strength.)
    v) Bypass Test: N/A
    vi) 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 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
KAT	Known Answer Test
LED	Light Emitting Diode
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NTP	Network Time Protocol
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
SSH	Secure Shell Protocol
TDES	Triple Data Encryption Standard
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

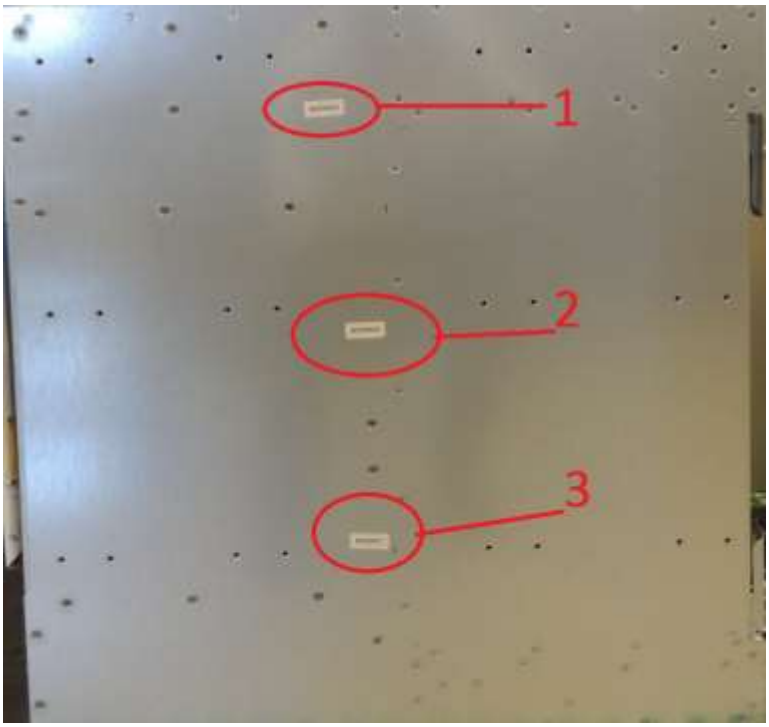
0P	No port blades
0SFP	Zero SFP devices provided
2CP	Two Control processor blades (see Table 4)
2 CORE	Two core switch blades (see Table 4)
ENT BUN	Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized (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
FCOE	Fiber Channel over Ethernet
FCOE10-24	10G, 24 port, FCoE 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.

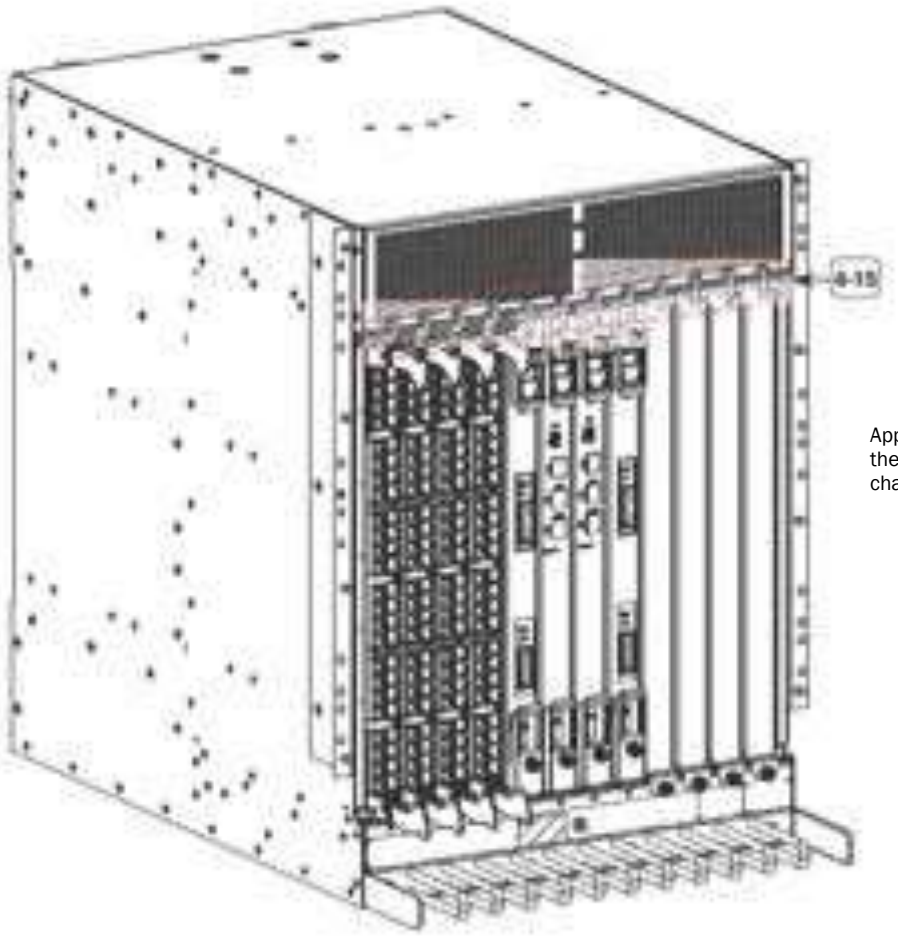
Brocade DCX and DCX 8510-8 Backbone

Twenty-two tamper evident seals are required to complete the physical security requirements.



Apply three seals are to the right side of the chassis

Figure 6 Brocade DCX and DCX 8510-8 Backbone chassis right side seal locations



Apply twelve seals are to the port side of the chassis

Figure 7 Brocade DCX and DCX 8510-8 Backbone port side seal locations

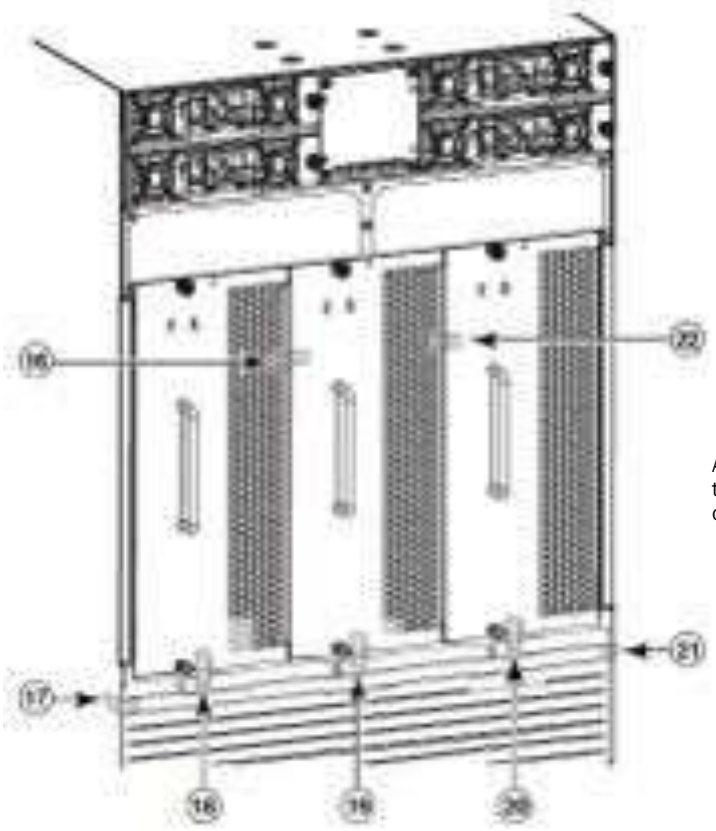


Figure 8 Brocade DCX and DCX 8510-8 Backbone non-port side seal locations

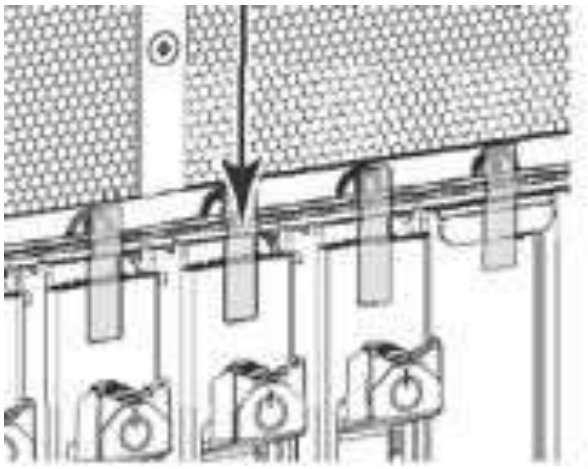


Figure 9 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application

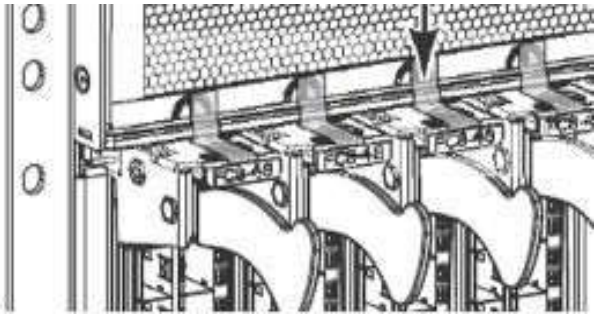


Figure 10 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application

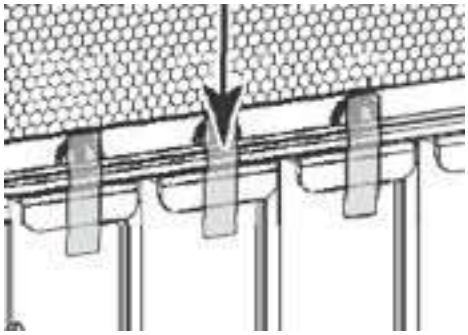


Figure 11 Brocade DCX and DCX 8510-8 Backbone filler panel seal application

Brocade DCX-4S and DCX 8510-4 Backbone

Nineteen tamper evident seals are required to complete the physical security requirements.

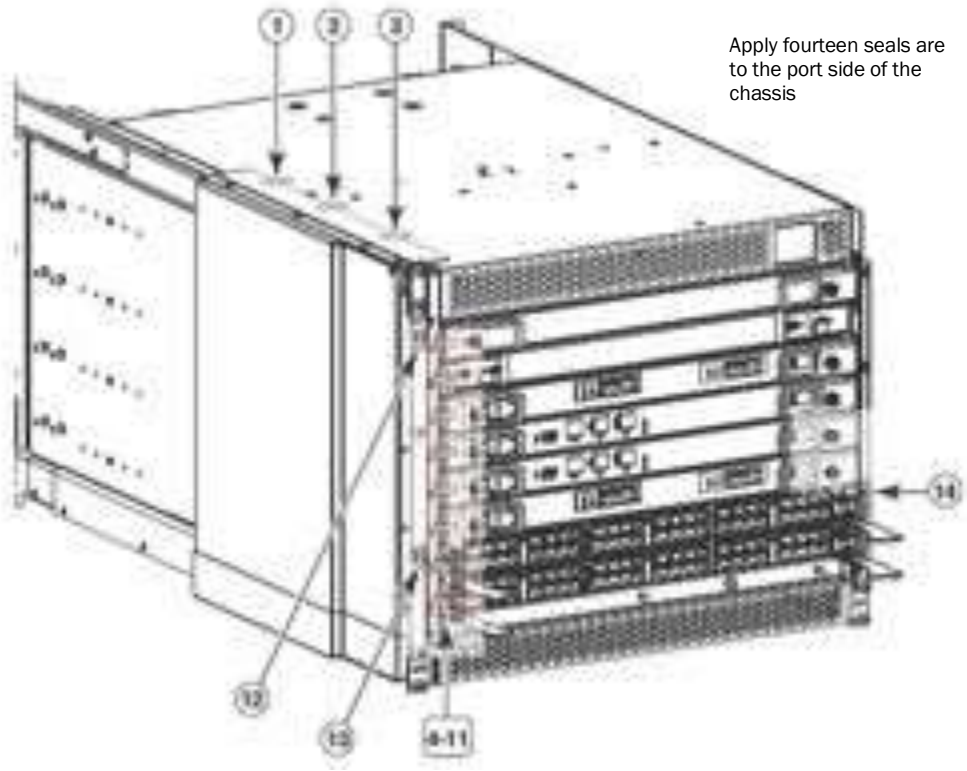


Figure 12 Brocade DCX-4S and DCX 8510-4 Backbone port side seal locations

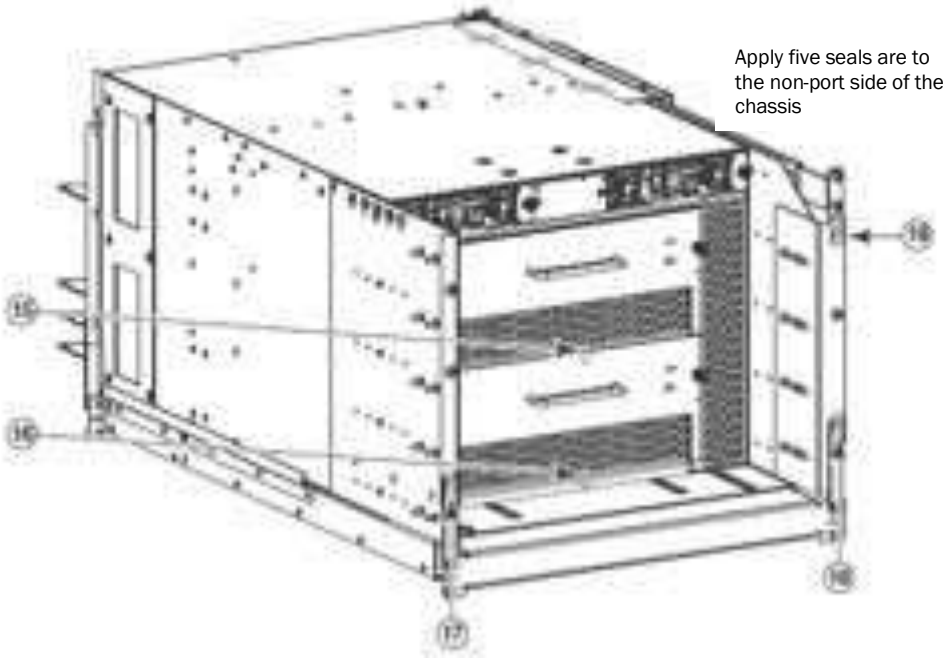


Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone non-port side seal locations

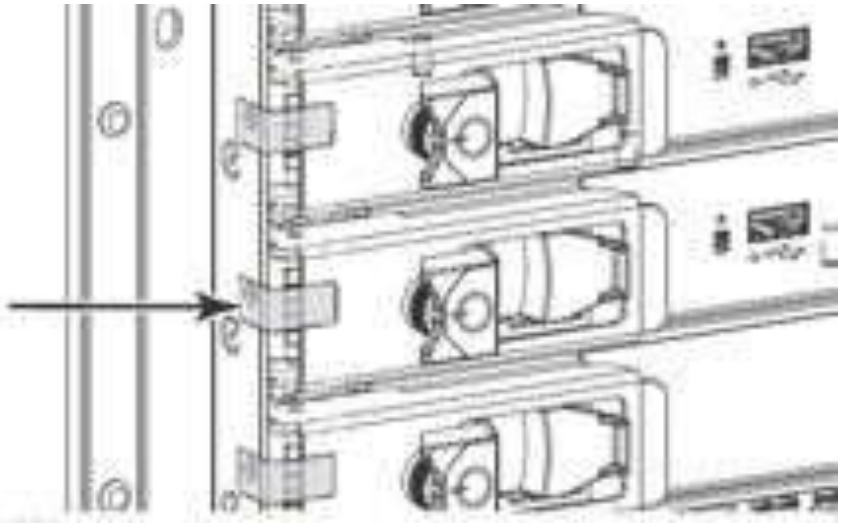


Figure 14 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application

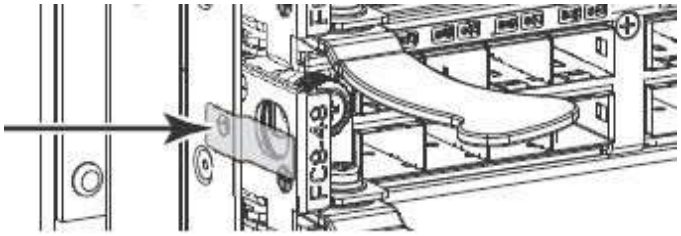


Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application

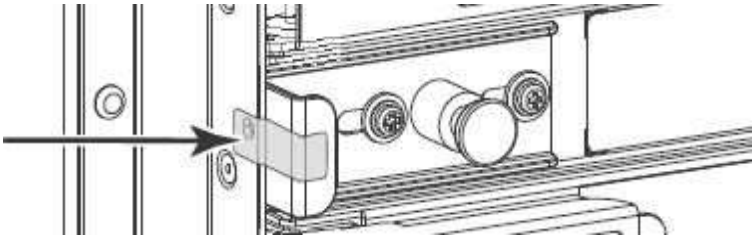


Figure 16 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application

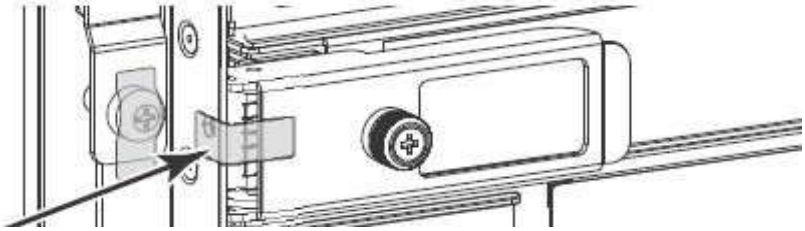


Figure 17 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application

Brocade 6510

Two tamper evident seals are required to complete the physical security requirements.

Figure 18 Brocade 6510 top left port side seal application

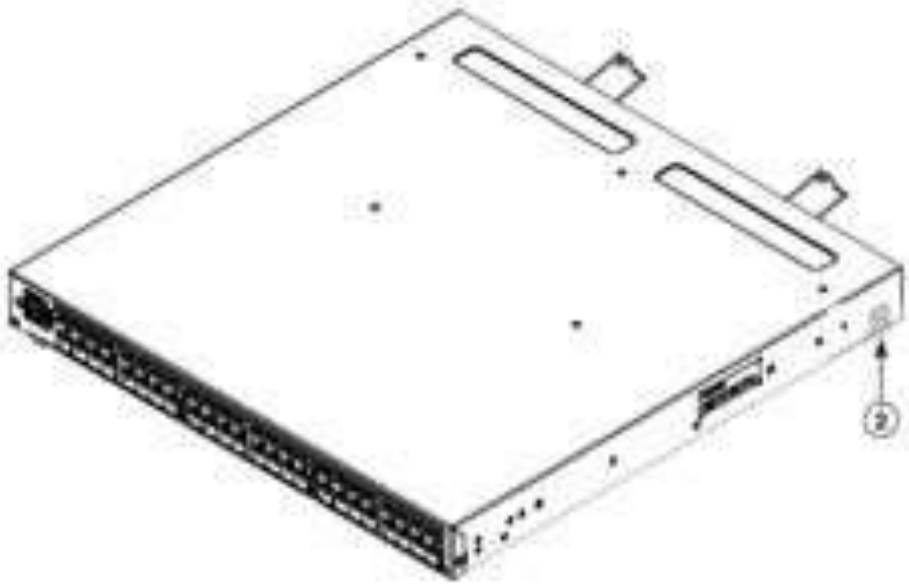


Figure 19 Brocade 6510 top right port side seal application

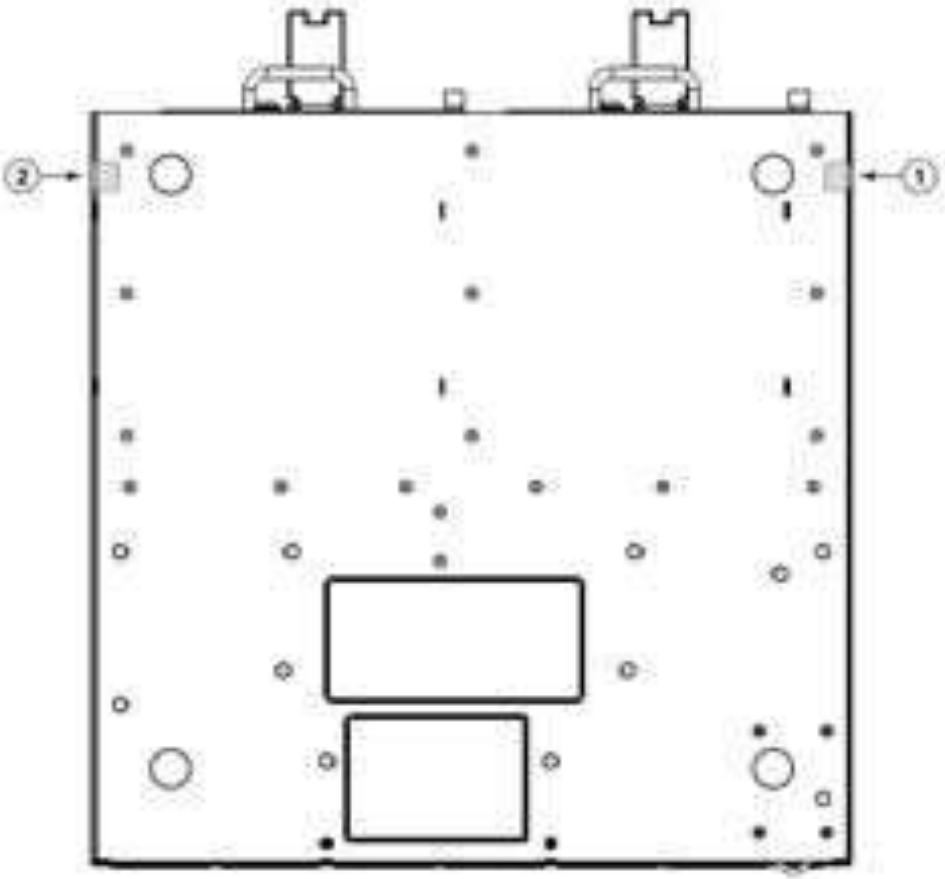


Figure 20 Brocade 6510 bottom seal locations

Brocade 6520

Twenty-six (26) tamper evident seals are required to complete the physical security requirements.

1. Relative to the port 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 21 for details on how to position each seal.
2. Relative to the port 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 21 for details on how to position each seal.

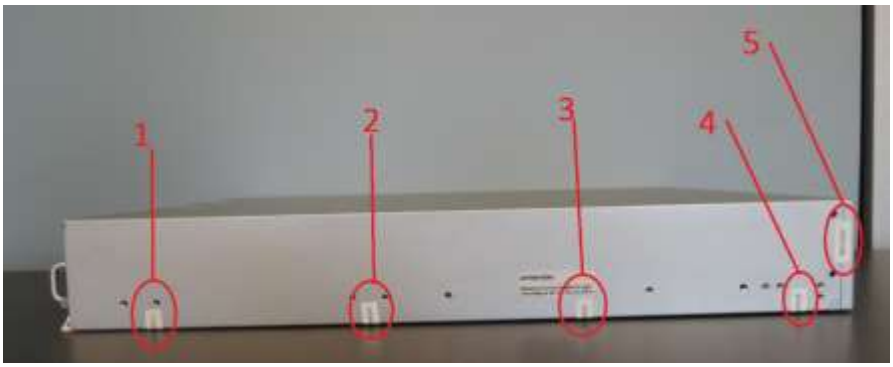


Figure 21 Brocade 6520 left port side seal locations

3. Relative to the port 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 22 for details on how to position each seal.
4. Relative to the port 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 22 for details on how to position each seal.

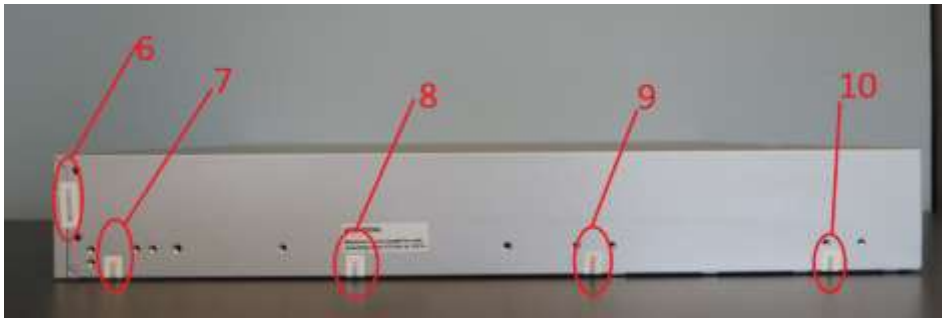


Figure 22 Brocade 6520 right port side seal locations

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 23A 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 23 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 23 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 23 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 23 for details on how to position each seal. Three (3) seals are required to complete this step.

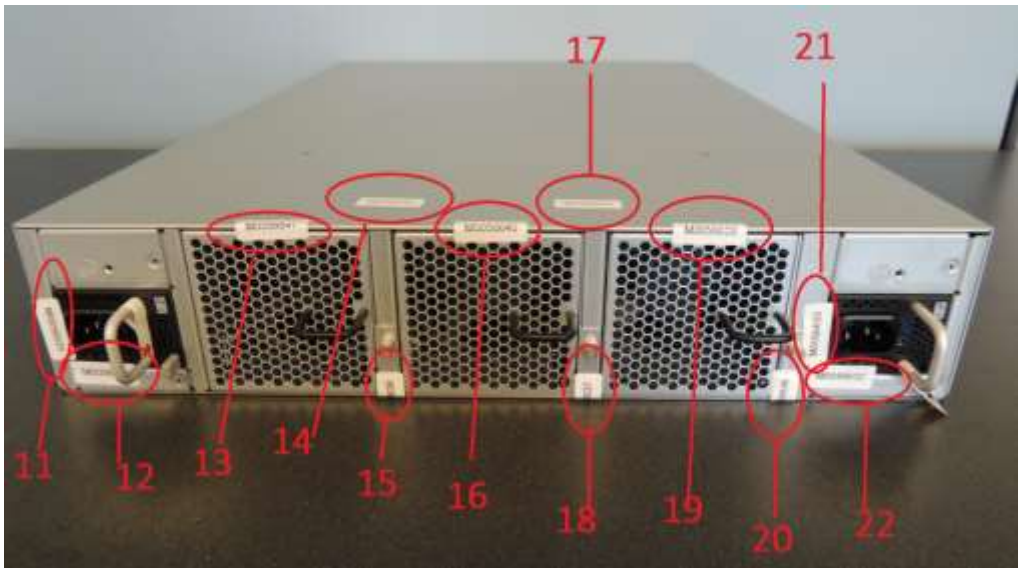


Figure 23 Brocade 6520 top and non-port side seal locations

9. Relative to the port 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 24 for details on how to position each seal.

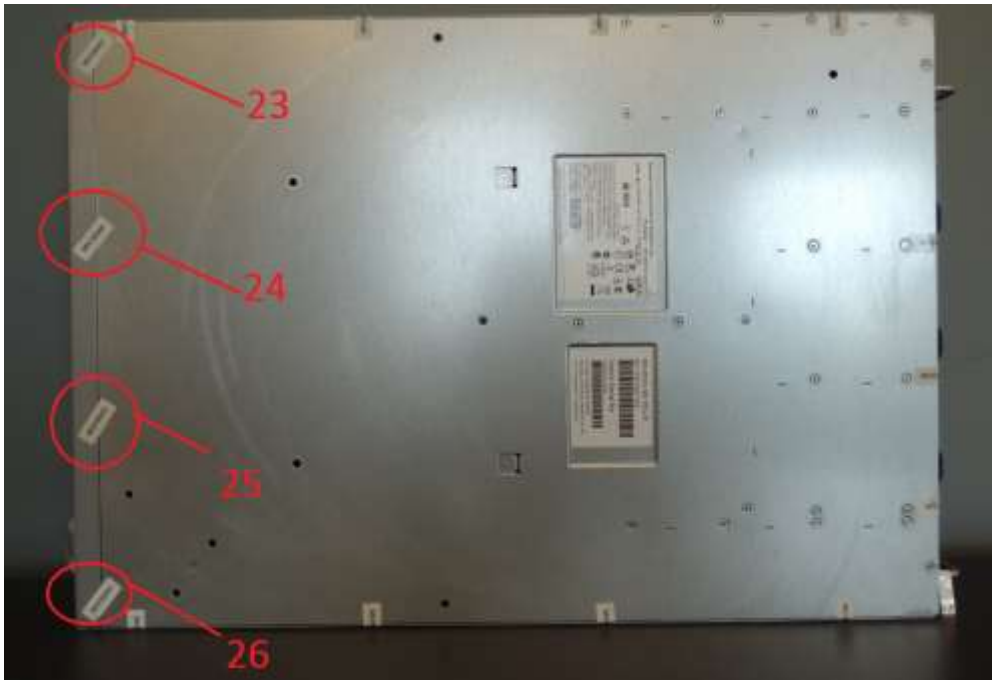


Figure 24 Brocade 6520 bottom seal locations

Brocade 7800

Two tamper evident seals are required to complete the physical security requirements.

Figure 25 Brocade 7800 top left port side seal locations

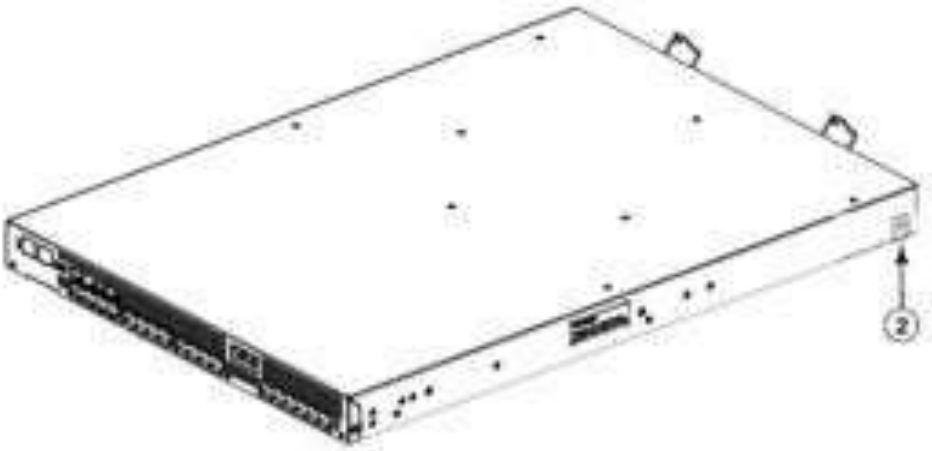


Figure 26 Brocade 7800 top right port side seal locations

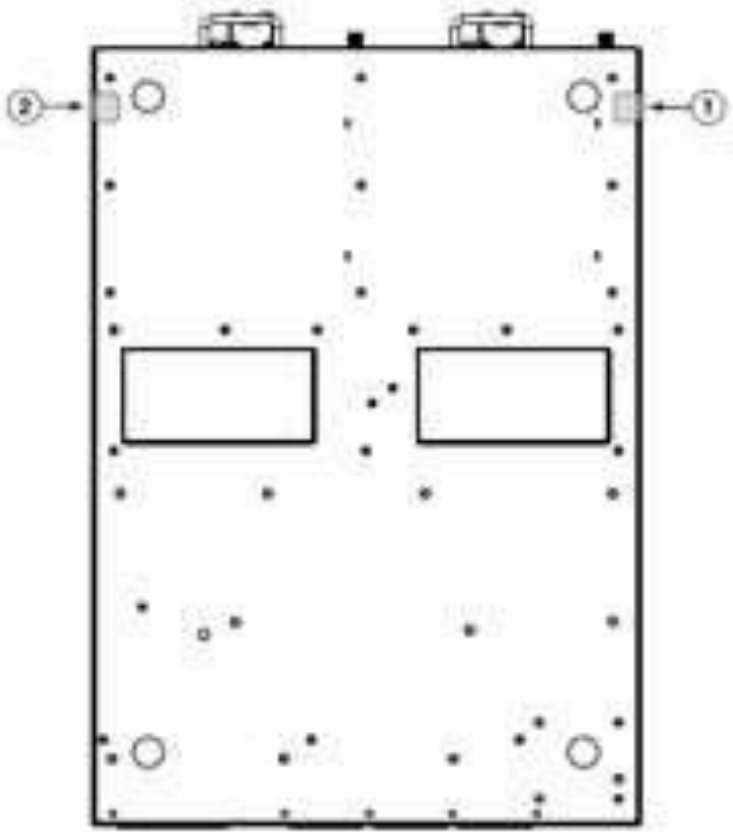


Figure 27 Brocade 7800 bottom seal locations