BROCADE

Brocade® DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones; 6510 FC Switch; and 7800 Extension Switch with Fabric OS v7.0.0b or Fabric OS v7.0.0b1 Firmware Security Policy

Document Version 2.0

Brocade Communications

August 29, 2012

Table of Contents

1. MODULE OVERVIEW 4
2. SECURITY LEVEL 10
3. MODES OF OPERATION 10
   - Approved mode of operation 10
   - Non-Approved mode of operation 12
4. PORTS AND INTERFACES 13
   - LED Indicators 13
   - DCX-4S, DCX, DCX 8510-4, and DCX 8510-8 blade LED counts: 14
5. IDENTIFICATION AND AUTHENTICATION POLICY 15
   - Assumption of Roles 15
6. ACCESS CONTROL POLICY 17
   - Roles and Services 17
   - Unauthenticated Services 17
   - Definition of Critical Security Parameters (CSPs) 17
   - Definition of Public Keys: 18
   - Definition of CSPs Modes of Access 18
7. OPERATIONAL ENVIRONMENT 19
8. SECURITY RULES 19
9. PHYSICAL SECURITY POLICY 20
   - Physical Security Mechanisms 20
   - Operator Required Actions 20
10. MITIGATION OF OTHER ATTACKS POLICY 20
11. DEFINITIONS AND ACRONYMS 21
12. BROCADE ABBREVIATIONS 21
APPENDIX A: TAMPER LABEL APPLICATION 23
   - Brocade DCX and DCX 8510-8 Backbone 23
   - Brocade DCX-4S and DCX 8510-4 Backbone 27
   - Brocade 6510 29
   - Brocade 7800 31

Table of Tables

Table 1 Firmware Version 4
Table 2 Switch Platforms 4
Table 3 Backbone Models 5
Table 4 Supported Blades 6
Table 5 Backbone Blade Support Matrix 6
Table 6 Module Security Level Specification 10
Table 7 Approved Algorithms available in firmware 10
Table 8 Port/Interface Quantities 14
Table 9 Blade LED Count 14
Table 10 Roles and Required Identification and Authentication 15
Table 11 Strengths of Authentication Mechanisms 16
Table 12 Service Descriptions 16
Table 13 Services Authorized for Roles 17
Table 14 CSP Access Rights within Roles & Services 18
Table 15 Public Key Access Rights within Roles & Services 19
Table 16 Inspection/Testing of Physical Security Mechanisms 20

Table of Figures

Figure 1 DCX-4S and DCX 8
Figure 2 DCX 8510-4 and DCX 8510-8 9
Figure 3 Brocade 6510 9
Figure 4 Brocade 7800 9
Figure 5 Brocade DCX and DCX 8510-8 Backbone chassis right side seal locations 23
Figure 6 Brocade DCX and DCX 8510-8 Backbone port side seal locations 24
Figure 7 Brocade DCX and DCX 8510-8 Backbone non-port side seal locations 25
Figure 8 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application 25
Figure 9 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application 26
Figure 10 Brocade DCX and DCX 8510-8 Backbone filler panel seal application 26
Figure 11 Brocade DCX-4S and DCX 8510-4 Backbone port side seal locations 27
Figure 12 Brocade DCX-4S and DCX 8510-4 Backbone non-port side seal locations 28
Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application 28
Figure 14 Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application 28
Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application 28
Figure 16 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application 28
Figure 17 Brocade 6510 top left port side seal application 29
Figure 18 Brocade 6510 top right port side seal application 29
Figure 19 Brocade 6510 bottom seal application 30
Figure 20 Brocade 7800 top left port side seal application 31
Figure 21 Brocade 7800 top right port side seal application 31
Figure 22 Brocade 7800 bottom seal application 32

1. Module Overview

The Brocade 6510, 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 6510 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 security 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 security officer shall maintain a serial number inventory of all used and unused tamper evident seals. The security 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 security 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 security 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 either Fabric OS v7.0.0b (P/N 63-1000968-01) or Fabric OS v7.0.0b1 (P/N 63-1001098-01) installed on, a switch or backbone and a set of installed blades. The below platforms may be used in a validated module configuration:

Firmware	Part Number
Fabric OS v7.0.0b	63-1000968-01
or	
Fabric OS v7.0.0b1	63-1001098-01

Table 1 Firmware Version

Switch	Part Number	Brief Description
6510	80-1005232-02[1]	6510,24P,16GB SFP,NON-PORT[2] SIDE AIR FLOW
	80-1005267-02[1]	6510,24P,16GB SFP,PORT SIDE[2] AIR FLOW
	80-1005268-02[1]	6510,24P,8GB SFP,NON-PORT SIDE AIR FLOW
	80-1005269-02[1]	6510,24P,8GB SFP,PORT SIDE AIR FLOW
	80-1005271-02	6510,48P,16GB SFP,NON-PORT SIDE AIR FLOW, 24-PORT POD LICENSE
	80-1005272-02	6510,48P,16GB SFP, PORT SIDE AIR FLOW, 24-Port POD LICENSE
7800	80-1002607-06	7800,UPG LIC,22P,16 8 SWL
	80-1002608-06	7800,UPG LIC,22P,16 8 LWL
	80-1002609-06	7800,6P,8GB SWL SFP

Table 2 Switch Platforms

Table 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.

`

Backbone	Part Number	Brief Description
DCX	80-1001064-08 80-1001064-09[1]	DCX,2PS,0P,2CP,2 CORE,0SFP
	80-1004920-02 80-1004920-03[1]	DCX,2PS,0P,2CP,2 CORE,0 SFP,ENT BUN[2],2 WWN
DCX-4S	80-1002071-08 80-1002071-09[1]	DCX-4S,2PS,0P,2CP,2 CORE,0SFP
	80-1002066-08 80-1002066-09[1]	DCX-4S,2PS,0P,2CP,2 CORE,0SFP,BR,ENT BUN[2]
DCX 8510-4	80-1004697-02 80-1004697-03[1]	DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP
	80-1005158-02 80-1005158-03[1]	DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP,ENT BUN[2]
DCX 8510-8	80-1004917-02 80-1004917-03[1]	DCX8510-8,2PS,0P,2CP,2 16GB,0SFP,ENT BUN[2]

Table 3 Backbone Models

Table Notes

1. Assemblies are equivalent with one exception. The higher dash level assembly incorporated an upgraded blower assembly within the fan module. This change is not security relevant.
2. 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 *	Part Number	Brief Description
CP8 Control Processor Blade	CP8	80-1001070-06	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	FRU, CORE BLADE, DCX-4S
CR8 Core Switch Blade	CR8	80-1001071-02	FRU, CORE BLADE, DCX
FC10-6 Port Blade	FC10-6	80-1000696-01	FRU, 6-PORT 10 GBIT FC BLADE
FC16-32 Port Blade	FC16-32	80-1005166-01	FRU, PORT BLADE,32P,DCX8510,16G SFP
FC16-48 Port Blade	FC16-48	80-1005187-01	FRU,PORT BLADE,48P,DCX8510,16G SFP
FC8-16 Port Blade	FC8-16	80-1001066-01	FRU, PORT BLADE, 16P, DCX, 8G SFP
FC8-32 Port Blade	FC8-32	80-1001067-01	FRU, PORT BLADE, 8P, DCX, 8G SFP
FC8-48 Port Blade	FC8-48	80-1001453-01	FRU, PORT BLADE, 48P, DCX, 8G SFP
FC8-64 Port Blade	FC8-64	80-1003887-01	FRU, PORT BLADE, 48P, DCX, 8G SFP
FCOE10-24 Port Blade	FCOE10-24	80-1002762-04	FRU, FCOE BLADE, 10GE X 24P
FR4-18i Port Blade	FR4-18i	80-1000233-10	FRU, FCIP BLADE, 4G X 16P, 2X1GBE
FX8-24 Port Blade	FX8-24	80-1002839-02	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

** NOTICE: Acronym referenced in Table 5 below*

Each backbone model supports a selected set of blades:

Backbone Model	Blades (max count)
DCX (12 slots) **	CP8 (2), CR8 (2), FC8-16 (8), FC8-32 (8), FC8-48 (8), FC8-64 (8), FC10-6 (1), FR4-18i (4), FX8-24 (1), FCOE10-24 (1), DCX/DCX 8510-8 Filler Panel (10)
DCX 8510-8 (12 slots) **	CP8 (2) **, 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) **	CP8 (2) , CR4S-8 (2), FC8-16 (4), FC8-32 (4), FC8-48 (4), FC8-64 (4), FC10-6 (1), FR4-18i (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) **	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

** NOTICE: Each Backbone Model shall be fully populated with a minimum of two CP8 Control Processor Blades (Part Number: 80-1001070-06), 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 and Figure 2 illustrate representative configurations of the DCX and DCX 8510 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 1 DCX-4S and DCX

Figure 2 DCX 8510-4 and DCX 8510-8

Figure 3 and Figure 4 illustrate the Brocade 6510 and Brocade 7800 cryptographic modules,

Figure 3 Brocade 6510

Figure 4 Brocade 7800

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

Approved mode of operation

The cryptographic module supports the following Approved algorithms:

Table 7 Approved Algorithms available in firmware

Firmware / Approved Algorithm	Fabric OS v7.0.0b	Fabric OS v7.0.0b1
Triple-DES	Cert. #652, #1043	Cert. #652, #1043
AES	Cert. #731, #1595, #1596	Cert. #731, #1595, #1596
SHS [SHA-1]	Cert. #749, #1408	Cert. #749, #1408
SHS [SHA-256]	Cert. #749, #1408	Cert. #749, #1408
SHS [SHA-512]	Cert. #1407, #1408	Cert. #1407, #1408
HMAC SHA-1	Cert. #397, #933, #934	Cert #397, #933, #934
HMAC SHA 256	Cert. #397, #933, #934	Cert. #397, #933, #934
HMAC SHA 512	Cert. #933, #934	Cert. #933, #934
RNG	Cert. #426, #854	Cert. #426, #854
RSA	Cert. #778, #779	Cert. #1048, #1049

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

- RSA Key Wrapping (key establishment methodology; 1024-bit keys provide 80 bits of encryption strength)

- Diffie-Hellman (DH) with 1024 bit or 2048 bit modulus (key agreement; key establishment methodology provides 80 bits of encryption strength)
- SNMPv3 (Cryptographic functionality does not meet FIPS requirements and is considered plaintext)
- HMAC-MD5 to support RADIUS authentication
- NDRNG – used for seeding Approved RNG
- SSHv2 KDF
- TLS KDF with HMAC-MD5
- TLS
- SSHv2
- RSA Key Transport (Key establishment methodology; 1024-bit keys provide 80-bits of encryption strength for TLS, use 2048-bit keys for SSH public key authentication)
- MD5 (used for password hash)
- RADIUS PEAP MS-CHAP V2
- Non-deterministic random number generator for seeding ANSI X9.31 DRNG

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) Perform zeroization operation
2) Change passwords for all existing user accounts.
3) Disable Telnet, HTTP, Remote Procedure Call (RPC)
4) Enable HTTPS, Secure-RPC
5) Do not use FTP
    a) Config Upload
    b) Config Download
    c) Support Save
    d) FW Download
6) Disable Root Access
7) Disable Boot PROM Access
8) Do not use MD5 within Authentication Protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
9) Do not define FCIP IKE or IPSec policies.
10) Disable Management Interface IPSec/IKE
11) Disable In-Band Management Interface
12) Disable In-Flight Encryption
13) Configure LDAP to use certificate-based authentication.
14) Configure SNMP Access List for read-only access.
15) Enable Self-Tests
16) Within Radius, only use PEAP MS-CHAP V2. Configure RADIUS Server to only use PEAP MS-CHAP V2.
17) Enable Signed FW Download
18) Install removable front cover (as applicable) and apply tamper labels
19) Enable FIPS mode via the “fipscfg – enable fips” command

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.”

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: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128, aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour

Macs:hmac-md5,hmac-sha1,umac-64,hmac-ripemd160,hmac-sha1-96,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)

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	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
7800	16	8	1	1	1	2	32

Table 8 Port/Interface Quantities

DCX-4S, DCX, DCX 8510-4, and DCX 8510-8 blade LED counts:

Blade	LED
CP8 Control Processor	8
CR16-4 Core Switch Blade	4
CR16-8 Core Switch Blade	4
CR4S-8 Core Switch Blade	6
CR8 Core Switch Blade	4
FC10-6 Port Blade	8
FC16-32 Port Blade	34
FC16-48 Port Blade	50
FC8-16 Port Blade	18
FC8-32 Port Blade	34
FC8-48 Port Blade	50
FC8-64 Port Blade	66
FCOE10-24 Port Blade	26
FR4-18i Port Blade	20
FX8-24 Port Blade	26

Table 9 Blade LED Count

5. Identification and Authentication Policy

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, 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

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.
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. 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	fipgscfg --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

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

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.

Definition of Critical Security Parameters (CSPs)

- DH Private Keys for use with 1024 bit or 2048 bit modulus
- Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 1024, 2048)
- SSH/SCP/SFTP Session Keys - 128, 192, and 256 bit AES CBC or TDES 3 key CBC
- SSH/SCP/SFTP Authentication Key for HMAC-SHA-1
- SSH KDF Internal State
- SSH DH Shared Secret 1024 – 8192 bits
- SSH 2048 RSA Private Key
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS PRF Internal State
- TLS Session Keys – 128, 256 bit AES CBC, TDES 3 key CBC
- TLS Authentication Key for HMAC-SHA-1

- RNG Seed Material
- ANSI X9.31 DRNG Internal State
- Passwords
- RADIUS Secret
- RPC Shared Secret

Definition of Public Keys:

The following are the public keys contained in the module:

- DH Public Key (1024 bit or 2048 bit modulus)
- DH Peer Public Key (1024 bit or 2048 bit modulus)
- FCAP Public Key (RSA 1024)
- FCAP Peer Public Key (RSA 1024)
- TLS Public Key (RSA 1024)
- TLS Peer Public Key (RSA 1024)
- FW Download Public Key (RSA 1024)
- SSH RSA 1024/2048 bit Public Key
- LDAP ROOT CA certificate (RSA 1024)

Definition of CSPs Modes of Access

Table 12 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

	SSH/SCP/SFTP CSPs	TLS CSPs	RNG Seed Material/Internal State	Passwords	RADIUS Secret	FCAP Private Key	FCSP CHAP Secret
Fabric Element Authentication	N	N	RW	N	N	RW	RW
FIPSCfg	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	N	N	N	N	N	N
PKI	RW	N	RW	N	N	N	N
RADIUS	N	N	N	RW	RW	N	N
UserManagement	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	SSH RSA 1024/2048 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
LDAP	N	N	N	N	N	RW
UserManagement	N	N	N	N	N	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) TDES CBC KAT (encrypt/decrypt)
            (2) AES CBC KAT (encrypt/decrypt)
            (3) HMAC SHA-1 KAT
            (4) HMAC SHA-256 KAT
            (5) HMAC SHA-512 KAT
            (6) ANSI X9.31 DRNG KAT
            (7) SHA-1 KAT
            (8) SHA-256 KAT
            (9) SHA-512 KAT
            (10) RSA 1024 SHA-1 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 – performed on non-approved RNG.

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

iii) RSA 1024/2048 SHA-1 Pairwise Consistency Test (Sign/Verify)

iv) RSA 1024/2048 Pairwise Consistency Test (Encrypt/Decrypt)

v) Firmware Load Test (RSA 1024 SHA-1 Signature Verification

vi) Bypass Test: N/A

vii) 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.

9. Physical Security Policy

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.

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	Blade server
CBC	Cipher Block Chaining
CLI	Command Line interface
CSP	Critical Security Parameter
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
FOS	Fabric Operating System
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
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
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 foot note for Table 2 & 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
FR4-18i	4G, 18 port, FCIP, routing and extension 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.

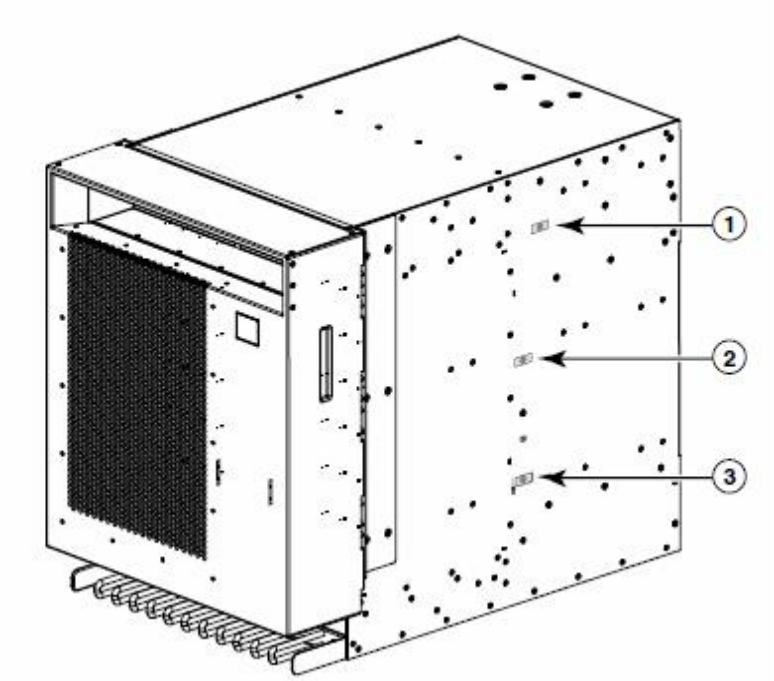

Figure 5 Brocade DCX and DCX 8510-8 Backbone chassis right side seal locations

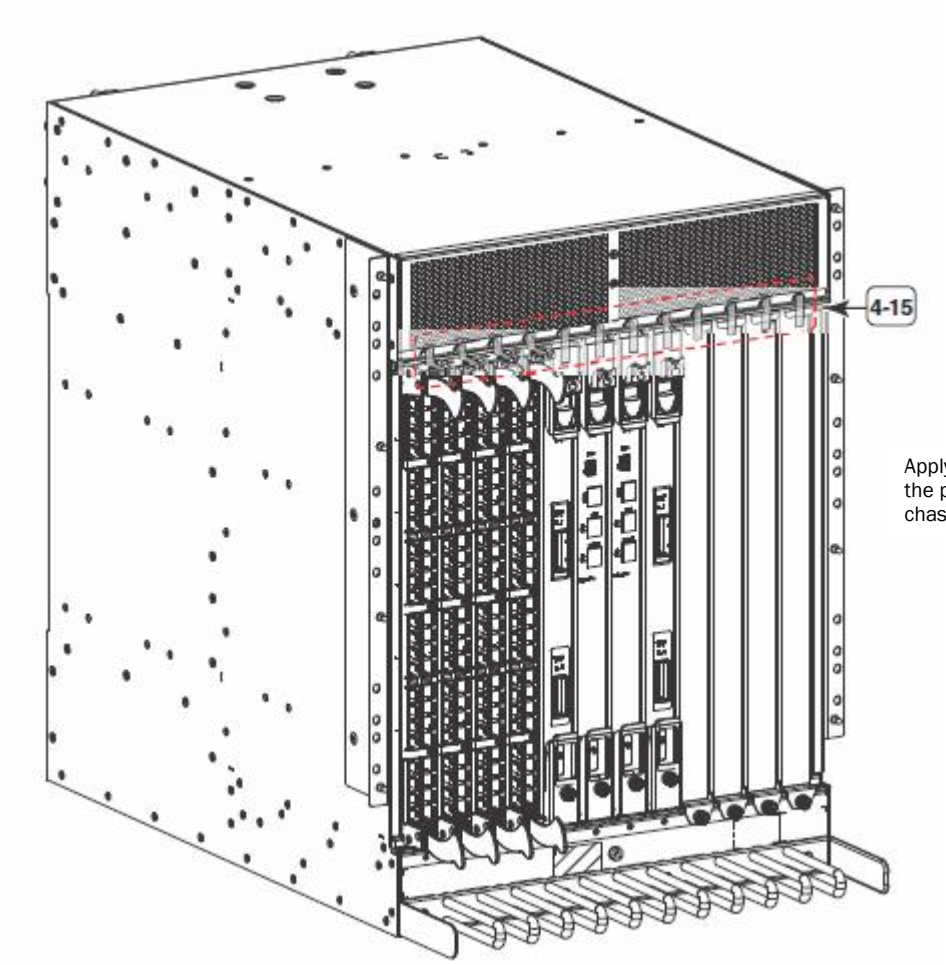

Figure 6 Brocade DCX and DCX 8510-8 Backbone port side seal locations

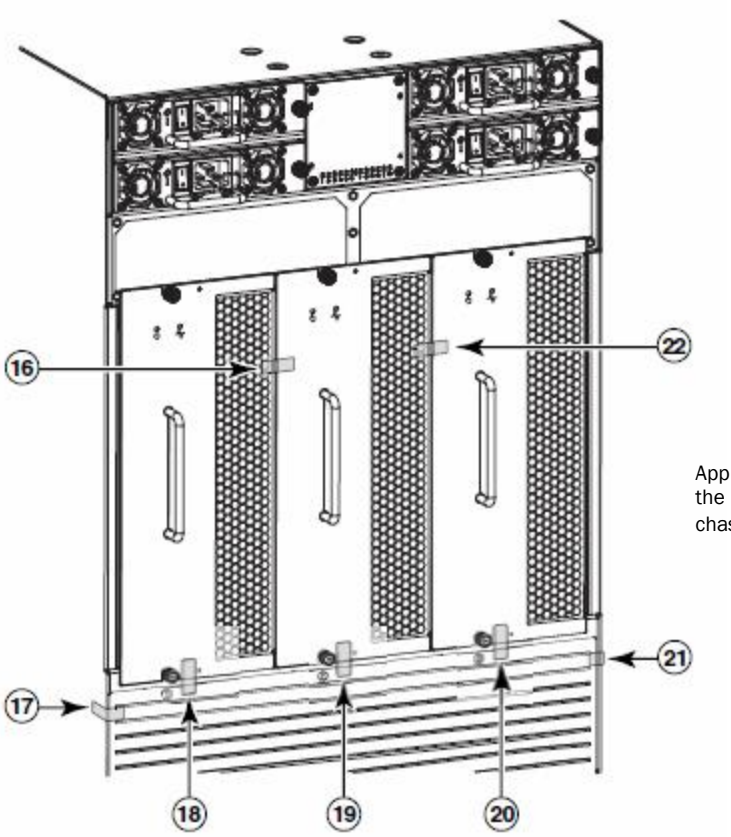

Figure 7 Brocade DCX and DCX 8510-8 Backbone non-port side seal locations

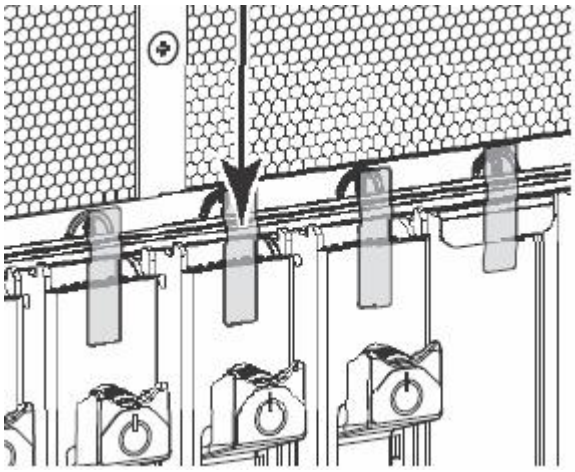

Figure 8 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application

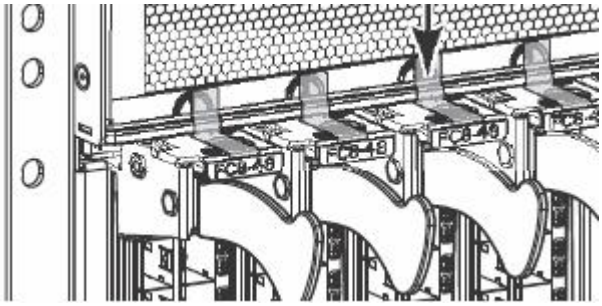

Figure 9 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application

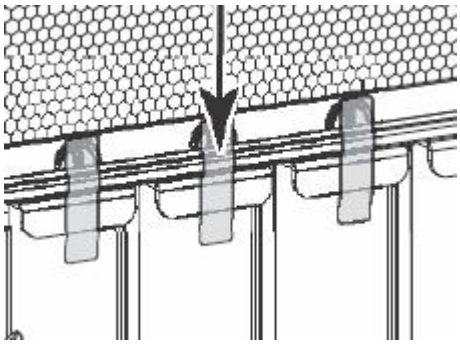

Figure 10 Brocade DCX and DCX 8510-8 Backbone filler panel seal application

Brocade DCX-4S and DCX 8510-4 Backbone

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

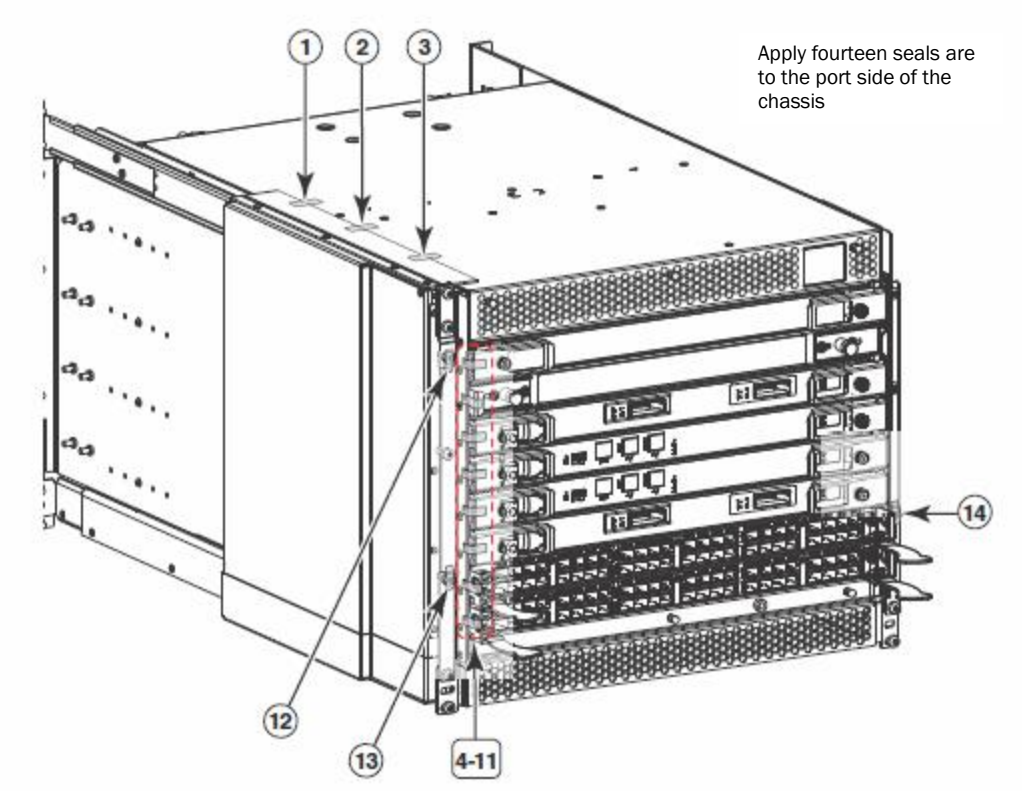

Figure 11 Brocade DCX-4S and DCX 8510-4 Backbone port side seal locations

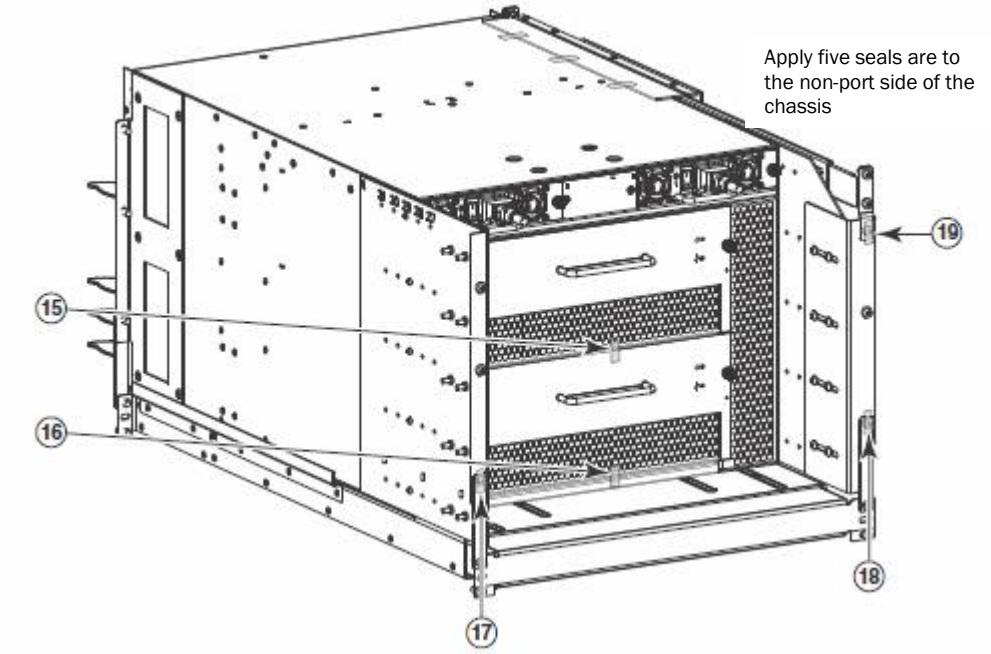

Figure 12 Brocade DCX-4S and DCX 8510-4 Backbone non-port side seal locations

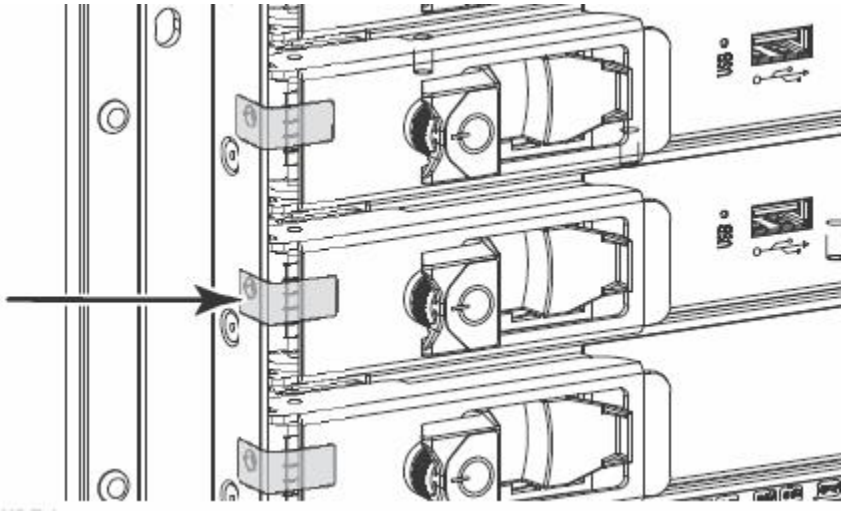

Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application

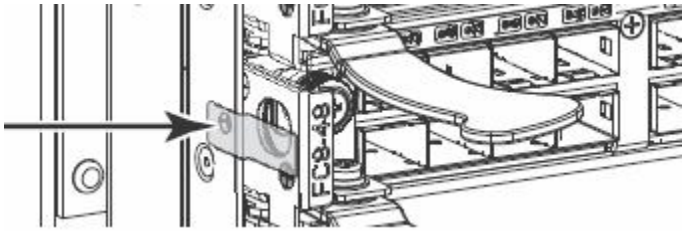

Figure 14 Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application

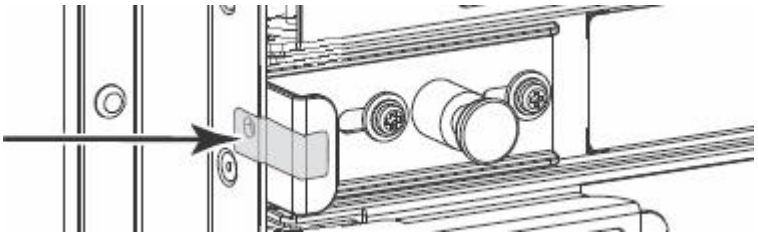

Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application

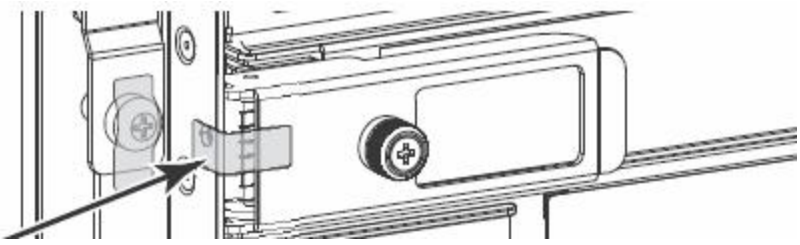

Figure 16 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application

Brocade 6510

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

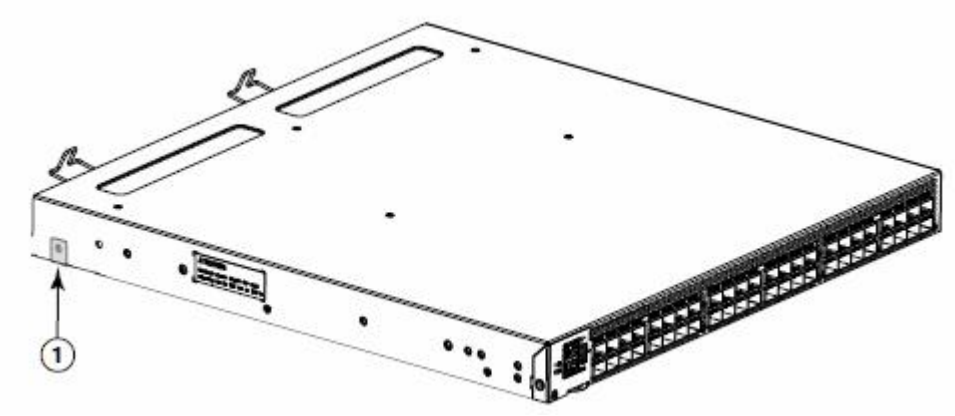

Figure 17 Brocade 6510 top left port side seal application

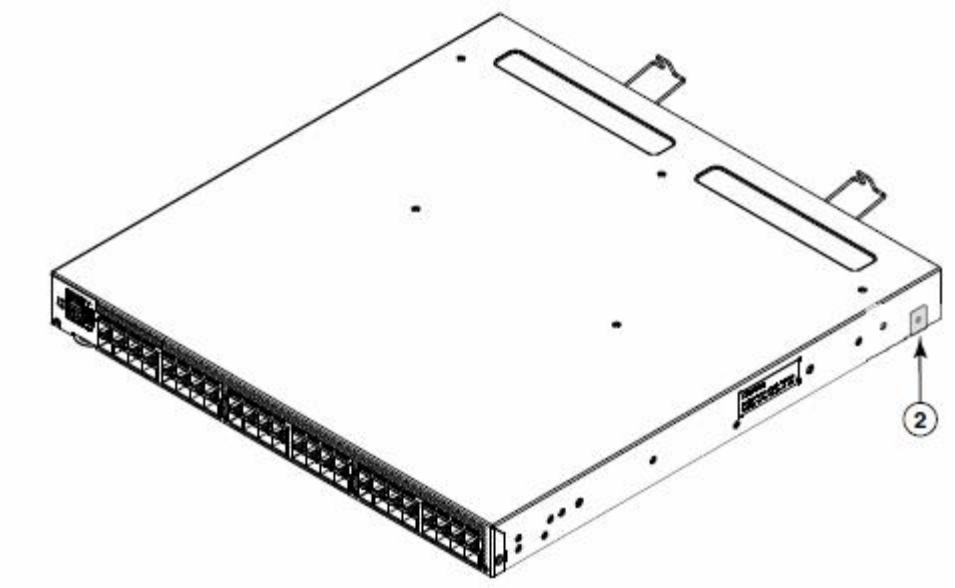

Figure 18 Brocade 6510 top right port side seal application

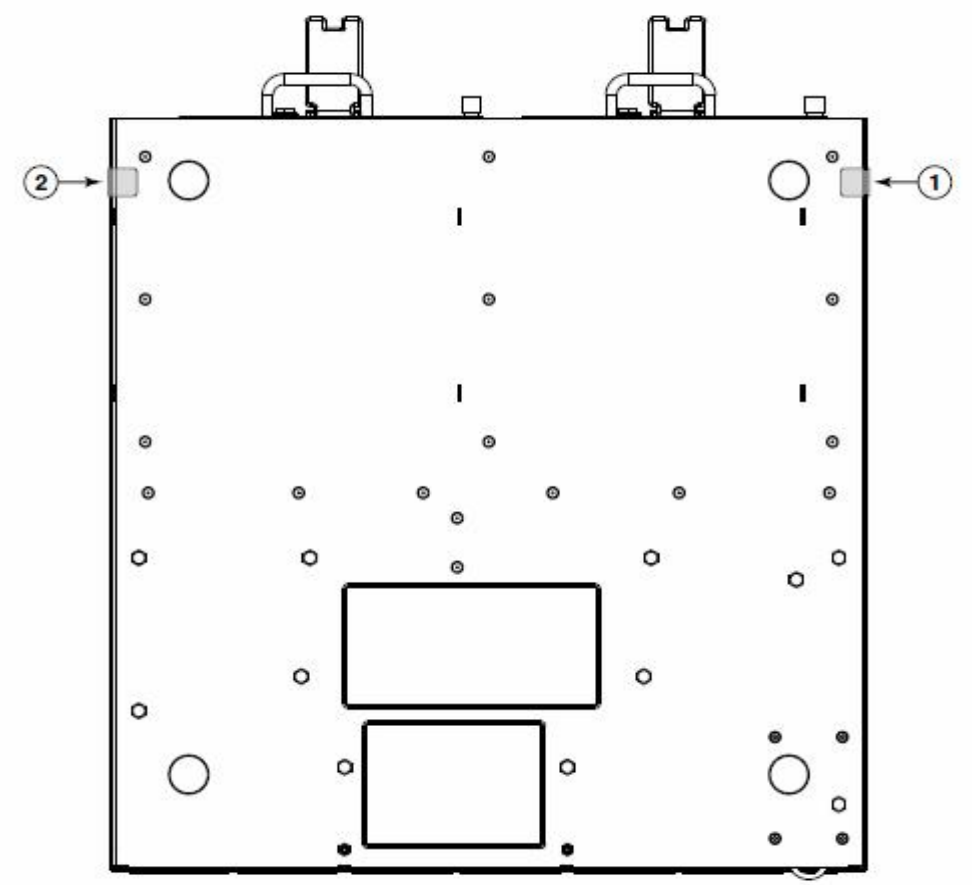

Figure 19 Brocade 6510 bottom seal application

Brocade 7800

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

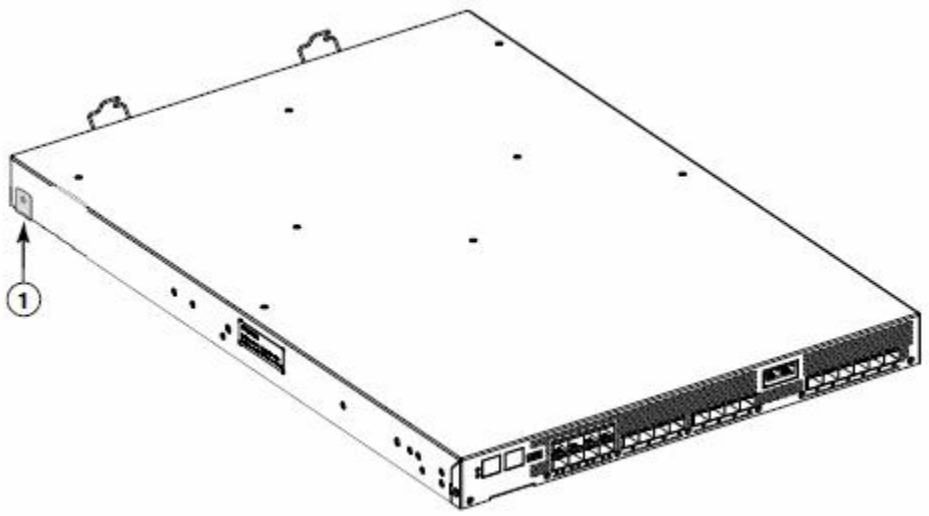

Figure 20 Brocade 7800 top left port side seal application

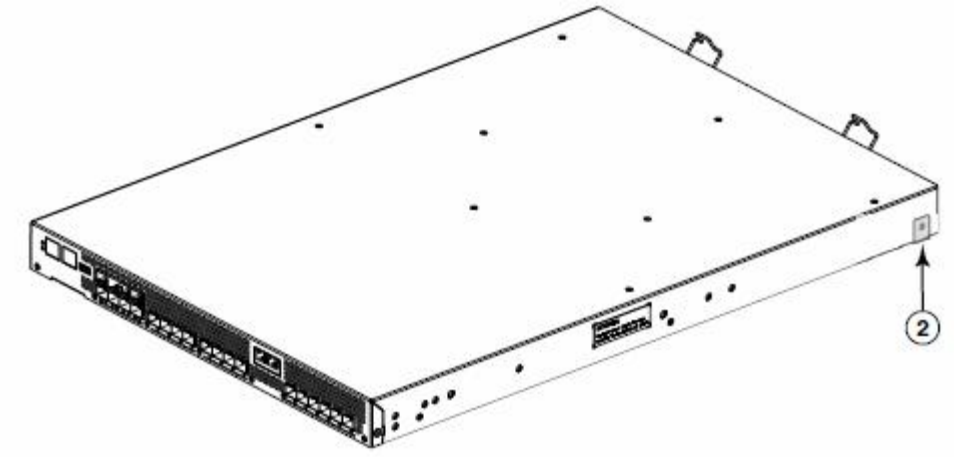

Figure 21 Brocade 7800 top right port side seal application

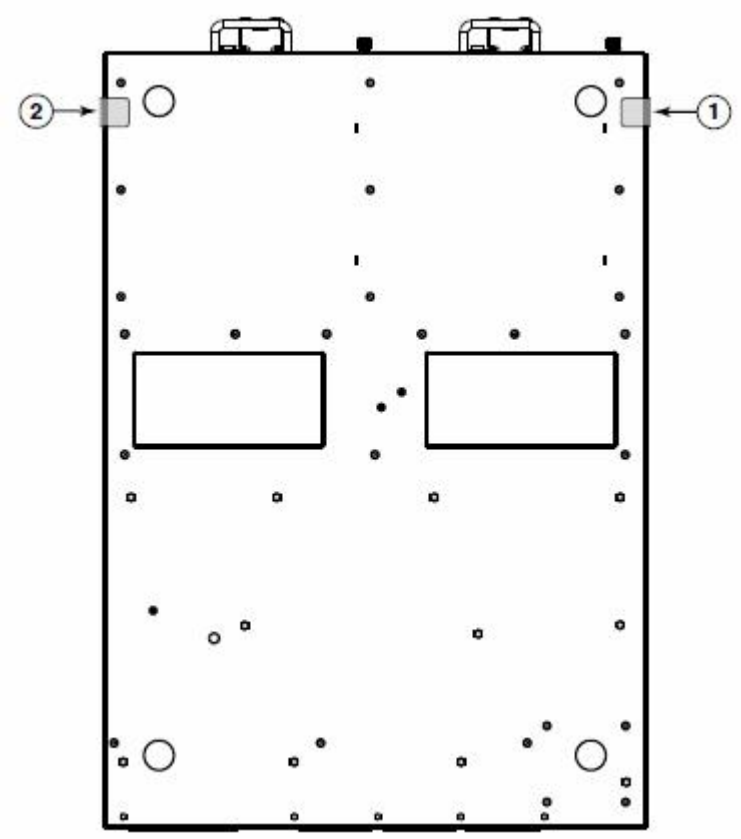

Figure 22 Brocade 7800 bottom seal application1024