Brocade DCX Backbone and 48000 Director Security Policy

Document *Version 1.2*

Brocade Communications

November 11, 2009

TABLE OF CONTENTS

1. Module Overview

The Brocade DCX Backbone and 48000 Director is a multiple-chip standalone cryptographic module, as defined by FIPS 140-2. The module is available in two configurations that vary based on the hardware enclosure. Each is enclosed in a hard, opaque, commercial grade metal chassis. The module is a Fibre-channel and Gigabit Ethernet routing switch that provides secure network services and network management.

The validated configurations are as follows:

Brocade DCX Backbone configuration:
FW Version Fabric OS v6.0.0, HW P/N Brocade DCX Version C

Brocade 48000 Director configuration:
FW Version Fabric OS v6.0.0, HW P/N Brocade 48000 Version L

The figures below illustrate the cryptographic module configurations.

Figure 1 - DCX Chassis

Figure 2 – 48000 Chassis

2. Security Level

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

Table 1 - Module Security Level Specification

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

3. Modes of Operation

Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware (OpenSSL):

- AES (Cert. #731)
- Triple-DES (Cert. #652)
- SHA-1 (Cert. #749)
- SHA-256 (Cert. #749)
- HMAC-SHA-1 (Cert. #397)
- HMAC-SHA-256 (Cert. #397)
- RNG - ANSI x9.31 with 2 key TDES (Cert. #426)
- RSA (Cert. #342)

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) (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

The following algorithm is non-Approved and shall not be used as a security function in the Approved mode of operation.

- RC4

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

1. Disable Telnet, HTTP, Remote Procedure Call (RPC)
2. Enable HTTPS, Secure-RPC
3. Do not use FTP
   - Config Upload
   - Config Download
   - Support Save
   - FW Download
4. Disable Root Access
5. Do not use MD5 within Authentication Protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
6. Do not define IKE or IPSec policies
7. Disable LDAP
8. Configure SNMP Access List for read-only access.
9. Enable Self-Tests
10. Within Radius, only use PEAP MS-CHAP V2

11. Enable Signed FW Download
12. Apply tamper seals (reference Section 9 for additional information).
13. 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 zeroize (by calling FIPSCfg –zeroize) the module's plaintext CSPs.

4. Ports and Interfaces

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

- Fiber Channel (Qty. 128): Data Input, Data Output, Control Input, Status Output
- Gig-E (Qty. 4): Data Input, Data Output, Control Input, Status Output
- Ethernet Ports (Qty. 2): Control Input, Status Output
- Serial port (Qty. 2): Control Input, Status Output
- Power Supply Connectors (Qty. 4): Power Input, Control Input, Status Output
- (48000 only) Fan Tray Connectors (Qty. 3): Control Input, Status Output
- LEDs: Status Output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports four 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 and five Radius servers that may be allocated the following roles:

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer)	Role-based operator authentication	Username and Password
User (User role)	Role-based operator authentication	Username and Password
Security Admin (Other role)	Role-based operator authentication	Username and Password
Fabric Admin (Other role)	Role-based operator authentication	Username and Password
Host/Server/Peer Switch (Other role)	Role-based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum 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 one 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 5 – Service Descriptions

Service Name	Description
Authentication	Fabric element authentication, including selection of authentication protocols, protocol configuration selection and setting authentication secrets.
FIPSCfg	Control FIPS mode operation and related functions; zeroize all CSPs
FirmwareManagement	Control firmware management.
PKI	PKI configuration functions, including FOS switch certificates and SSL certificates.
RADIUS	RADIUS configuration functions.
UserManagement	User and password management.

6. Access Control Policy

Roles and Services

Table 6 – Services Authorized for Roles

	User	Admin	FabricAdmin	SecurityAdmin	Host/Server/Peer Switch
Authentication		X		X	X
FIPSCfg		X		X	
Firmware Management	X	X	X	X	
PKI	X	X	X	X	

	User	Admin	FabricAdmin	SecurityAdmin	Host/Server/Peer Switch
RADIUS		X		X	
UserManagement		X		X	

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)

The following are CSPs contained in the module:

- DH Private Keys for use with 1024 bit modulus.
- Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Fibre-Channel Authentication Protocol (FCAP) Private Key(RSA 1024)
- SSH Session Key - 128, 192, and 256 bit AES CBC or TDES 2 and 3 key
- Secure Copy (SCP) Session Key - 128, 192, and 256 bit AES CBC or TDES 2 and 3 key
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret
- TLS Session Key – 128 bit AES
- TLS Authentication Key for HMAC-SHA-1
- RNG Seed Material
- Passwords
- Radius Secret

Definition of Public Keys

The following are the public keys contained in the module:

- DH Public Key (1024 bit modulus)
- DH Peer Public Key (1024 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 Key (RSA 1024)

Definition of CSPs Modes of Access

Table 6 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

Table 7 – CSP Access Rights within Roles & Services

	SSH and SCP CSPs	TLS CSPs	RNG Seed Key	Passwords	RADIUS Secret	FCAP Private Key	FCSP CHAP Secret
Authentication	N	N	N	RW	N	RW	RW
FIPSCfg	Z	Z	Z	Z	Z	Z	Z
Firmware Management	R	N	N	N	N	N	N
PKI	RW	N	N	N	N	N	N
RADIUS	N	N	N	RW	RW	N	N
UserManagement	N	N	N	RW	N	N	N

7. Operational Environment

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

8. Security Rules

The cryptographic module's 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 FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide four distinct operator roles.
2. The cryptographic module shall provide role-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests:
        1. Cryptographic algorithm tests:
            a. TDES KAT
            b. AES KAT
            c. HMAC SHA-1 KAT
            d. SHA-1 KAT
            e. HMAC SHA-256 KAT (SHA-256 tested within this self-test)
            f. RNG KAT
            g. RSA Sign/Verify KAT
            h. RSA Encrypt/Decrypt KAT
        2. Firmware Integrity Test (128-bit EDC)
        3. Critical Functions Tests: N/A
    B. Conditional Self-Tests:
        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and RNG
        2. RSA Pairwise Consistency Test (Sign/Verify & Encrypt/Decrypt)
        3. Firmware Load Test (RSA Signature Verification)
5. Results of power-up and conditional self-tests are recorded in the system log or are output to the local console. This includes logging both passing and failing results.
    A. Status is indicated by the listing of the test condition and then "successful" (e.g.,

"AES encryption/decryption...successful")

B. Failure is indicted by error code and the listing of the failure condition (e.g., "24557:error:2A068065:lib(42):FIPS_selftest_aes:selftest failed")

6. 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. Power-up self tests will be initiated by power cycling the module.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

To operate in FIPS Approved mode the tamper evident seals shall be installed as indicated.

The cryptographic boundary of the DCX Backbone configuration is defined as being the outer perimeter of the enclosure excluding the power supply field replaceable units (FRUs) and front cover. The cryptographic boundary of the 48000 Director configuration is defined as being the outer perimeter of the enclosure excluding the power supply FRUs, fan FRUs, and front cover. The excluded components are non-security relevant.

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. Reference Appendix A for detailed instructions on tamper seal placement.

The module must be configured as follows in order to operate in an Approved mode.

- For the DCX chassis, verify that the CP blades are installed in slots 6 and 7and Core blades are installed in slots 5 and 8.
- For the 48000 chassis, verify that the CP blades are installed in slots 5 and 6.
- Any chassis slot that is not populated with a module must have a filler plate installed. The slot covers are included with each chassis, and additional slot covers may be ordered. Reference Appendix A for detailed instructions on tamper seal placement.
- After the switch has been configured to meet FIPS 140-2 Level 2 requirements, the switch cannot be accessed without indicating signs of tampering.
- Reference Appendix A for detailed instructions on how to install tamper seals.

Operator Required Actions

The operator is required to periodically inspect tamper evident seals.

Table 8 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	12 months	The removed seal shows a checkerboard destruct pattern. The graphics printed within the seal are uniquely split between the removed seal and the residue left on the surface. The residue is visible under ultraviolet light.

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.

Appendix A - Brocade DCX Backbone and 48000 Director Tamper Seal Placement

To operate in FIPS Approved mode the tamper evident seals shall be installed as indicated.

To operate in FIPS Approved mode, the tamper evident seals shall be installed as follows:

Seal Application Instructions

For all seal applications, observe the following instructions.

- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not use bare fingers to handle the seals. Slowly peel the backing from each seal, taking care not to touch the adhesive.
- When applying the seal, use a firm pressure across the entire seal surface to ensure maximum adhesion. Allow at last 30 minutes for the adhesive to cure. Tamper evidence may not be apparent until the adhesive cures.

DCX Backbone Chassis (18 Tamper Evident Seals)

Right side of the Brocade DCX chassis

Figure A.1 below illustrates seal placement for the right side of the DCX Chassis

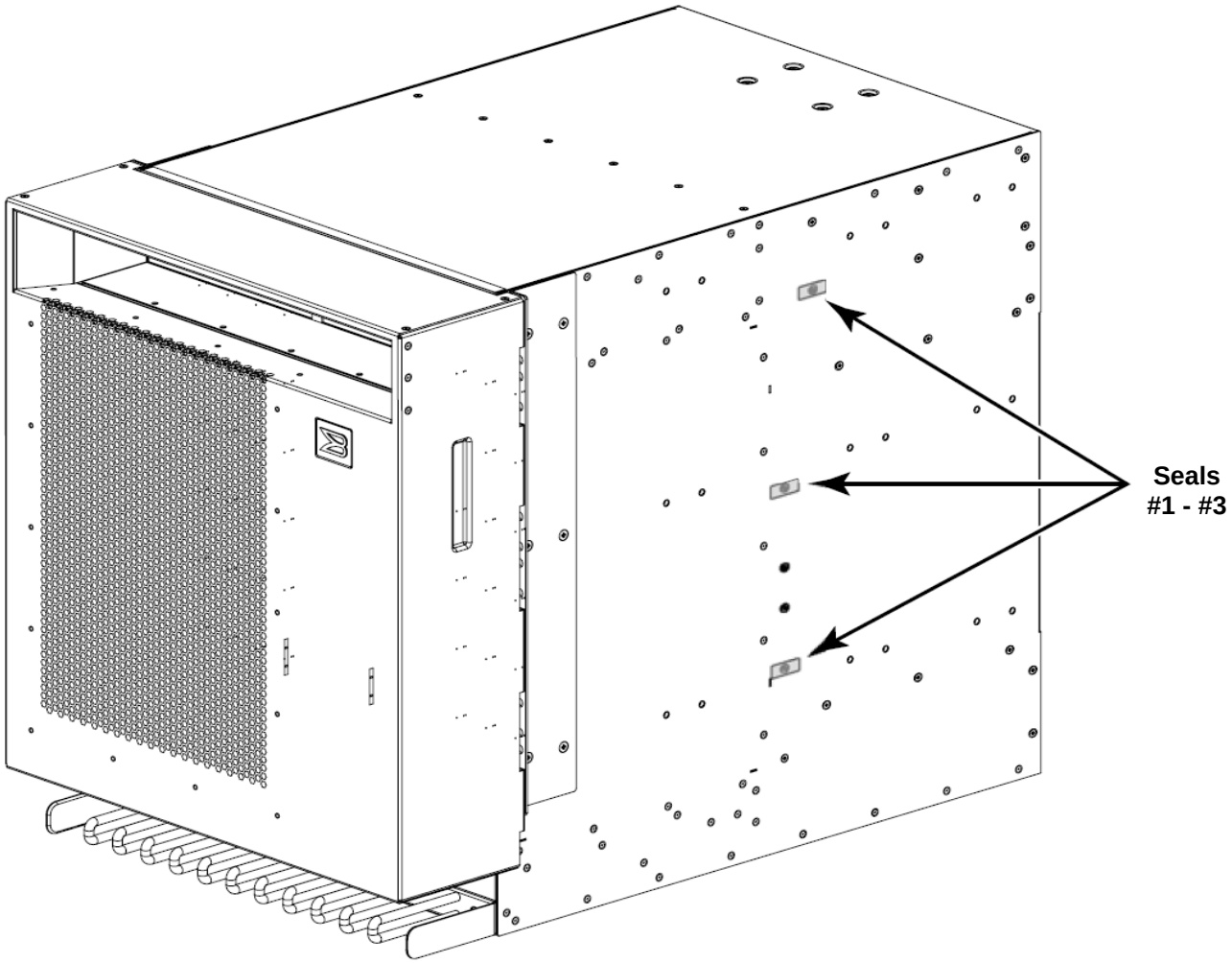

Figure A.1 – Brocade DCX Chassis Right Side Seal Location

Locate the three (3) screws on the right side of the chassis enclosure specified in Figure A.1. Attach one (1) seal (#1 - #3) that covers each screw head completely. Ensure that the seal is firmly affixed.

Non-Port side Seal Placement for the Brocade DCX Chassis.

Figure A.2 below illustrates seal placement for the DCX fan FRUs.

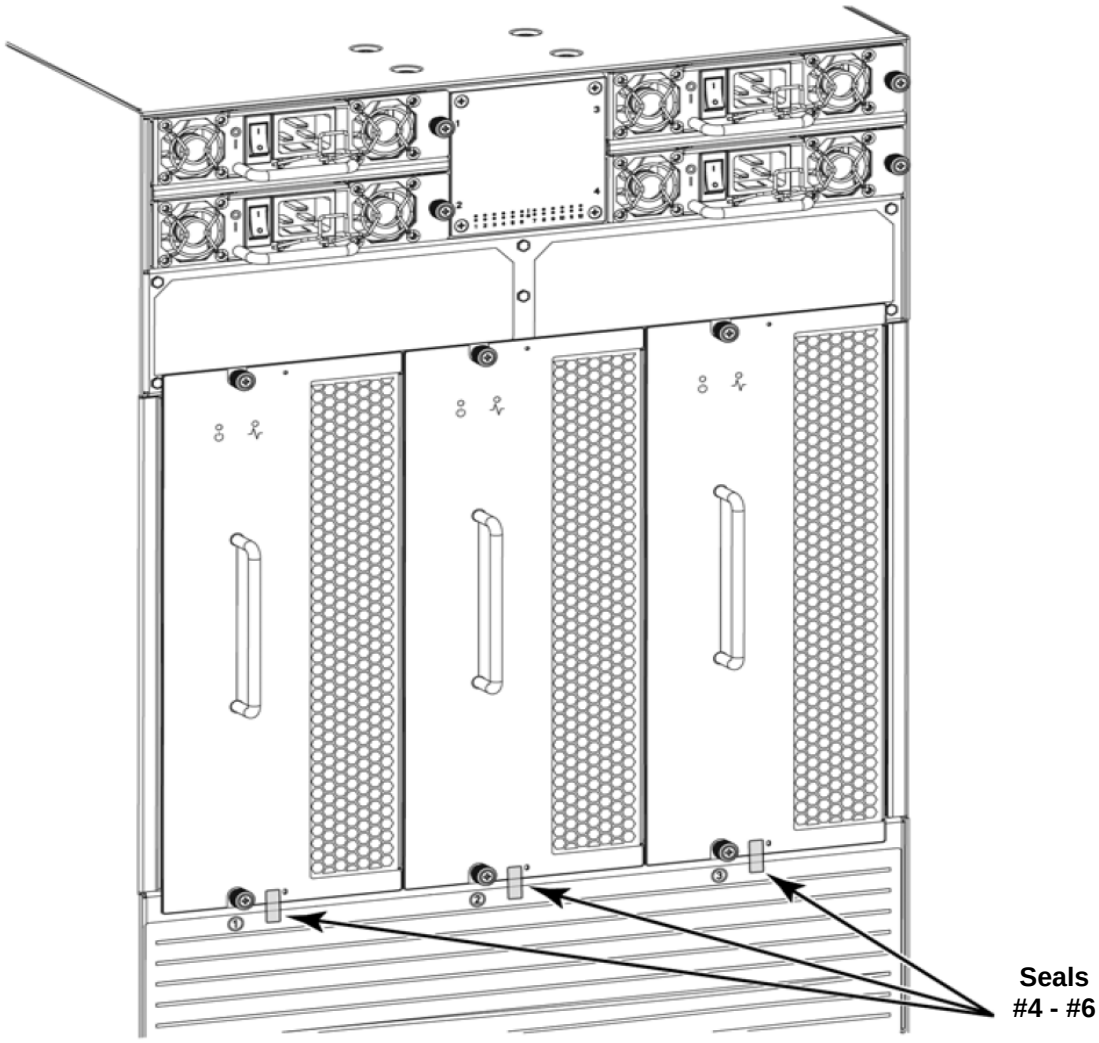

Figure A.2 –Rear Chassis Seal Location

Locate the joint between the bottom of each fan FRU and the lower part of the chassis enclosure. Attach one (1) seal (#4 - #6) mounted vertically that bridges the seam between each fan FRU and the chassis enclosure. Ensure that the seal is firmly affixed to both the fan FRUs and the chassis enclosure. You must apply one seal per fan FRU.

Front Panel Seal Placement

Figure A.3 below illustrates seal placement for all blades and filler panels.

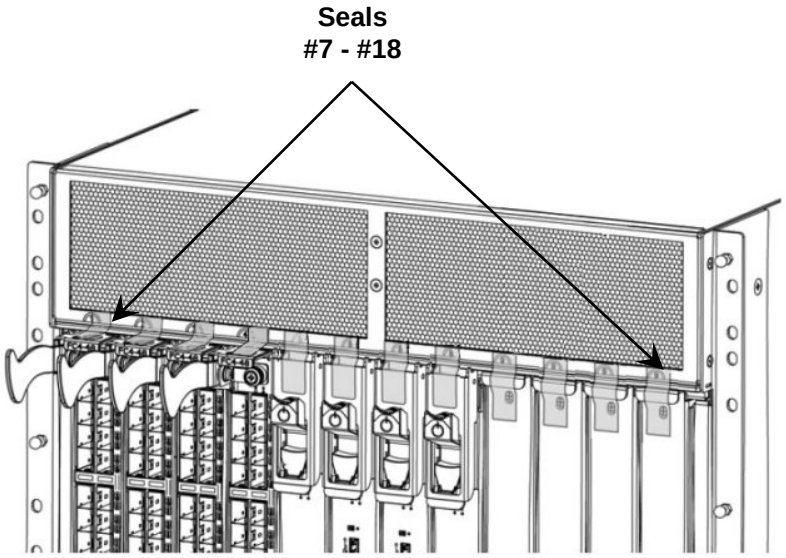

Figure A.3 – Brocade DCX Front Blade Panel

Placement of seals (#7 - #18) in Figure A.3 shows the front blade panel with the proper placement of tamper seals. Each slot must be populated with a filler panel, control blade, core blade or port blade.

Blade Seal Placement - Flat Ejector Handle on the Brocade DCX

Figure A.4 below illustrates seal placement for flat ejector handle blades.

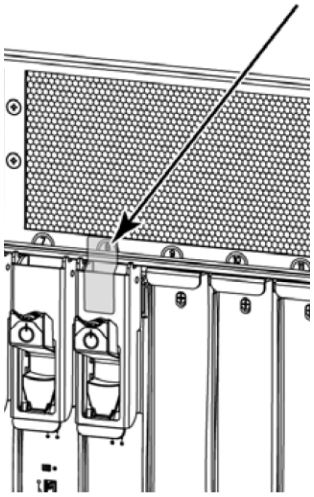

Figure A.4 – Flat Ejector Handle Seal Placement for the Brocade DCX

Attach one (1) seal beginning on the lower frame of the exhaust vent, spanning the gap between the frame and the blade, extending on to the upper blade ejector, and ending just before the thumbscrew. Apply one (1) seal to every blade that has a flat ejector handle. Ensure the seal is firmly affixed to the exhaust vent frame and the blade ejector. NOTE: Be sure that the seal does not cover either the micro-switch or the thumbscrew.

Blade Seal Placement - Stainless Steel Ejector Handle on the Brocade DCX

Figure A.5 below illustrates seal placement for the stainless steel ejector handle blades.

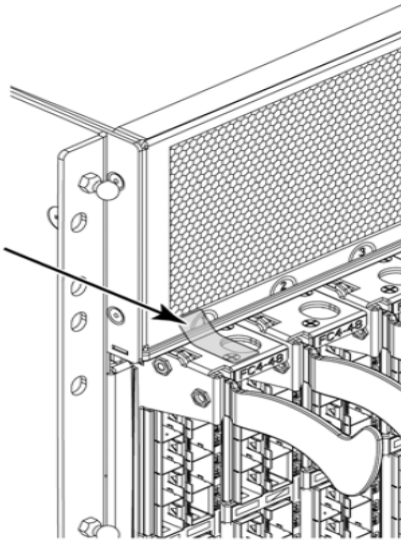

Figure A.5 – Stainless Steel Ejector Seal Placement

Attach one (1) seal beginning on the lower frame of the exhaust vent and curving down onto the upper surface of the pull tab of the blade. Attach one (1) seal to each blade that has stainless steel ejectors. Ensure the seal is firmly affixed to both the exhaust vent frame and the top of the pull tab.

Blade Seal Placement – Filler panel seal location on the Brocade DCX

Figure A.6 below illustrates the filler panel seal placement on the Brocade DCX.

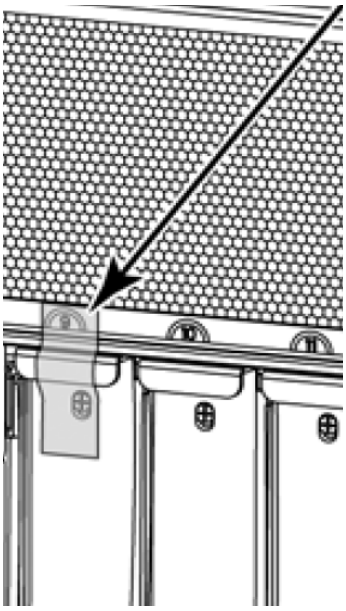

Figure A.6 – Filler Panel Seal Placement

Insert the new filler panel for all unpopulated slots. Attach one (1) seal to each filler panel, beginning on the lower frame of the exhaust vent, extending across the pull tab at the top of the filler plate, and spanning down to the surface of the filler panel. The seal may have to "tent" over the gap between the pull tab and the surface of the filler panel. Be sure that the seal does not cover any of the exhaust vent. It must make contact only with the frame. Ensure the seal is firmly affixed to the exhaust vent frame, the pull tab, and the surface of the filler panel.

48000 Director Chassis (11 Tamper Evident Seals)

Non-Port side Seal Placement for the Brocade 48000 Director

Figure A.7 below illustrates the seal placement for the non-port side of the Brocade 48000 Director. Refer to the following figure to perform the procedure.

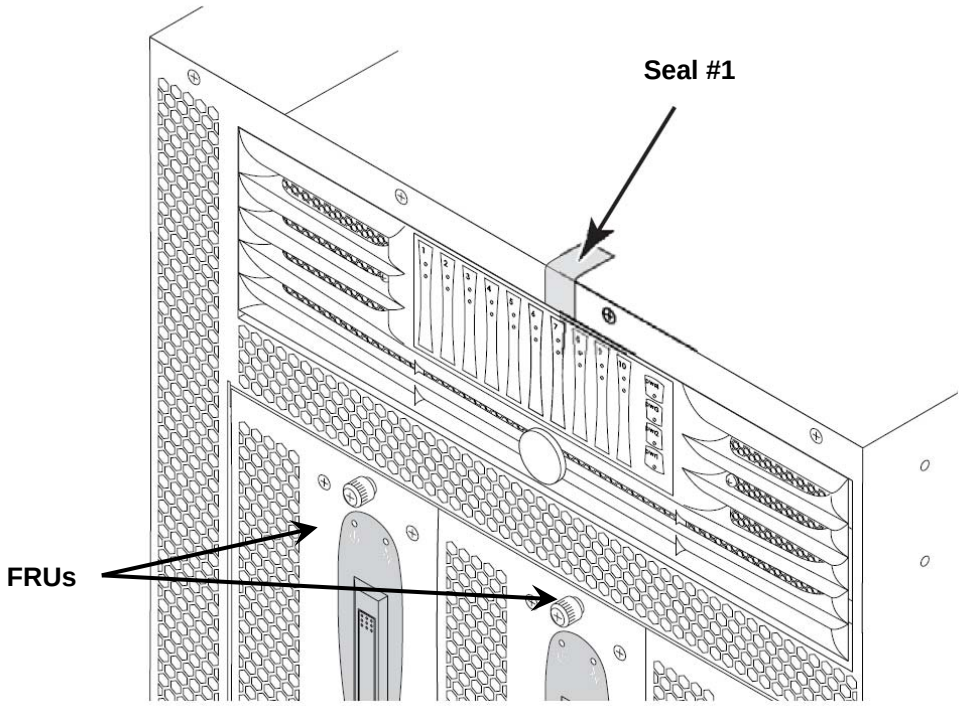

Figure A.7 – Brocade 48000 Upper Non-Port Side Seal Location

Locate the seam between the frame and the upper surface of the chassis enclosure. Attach one (1) seal (#1) mounted vertically that begins on the frame, covers the seam between the frame and the upper chassis enclosure, and extends on to the upper surface of the enclosure. Ensure that none of the indicator LEDs on the bezel are covered by the seal. Ensure that the seal is firmly affixed to the frame and the upper chassis enclosure.

Front 48000 Panel Seal Placement

Figure A.8 below illustrates seal placement for all front blades and panels.

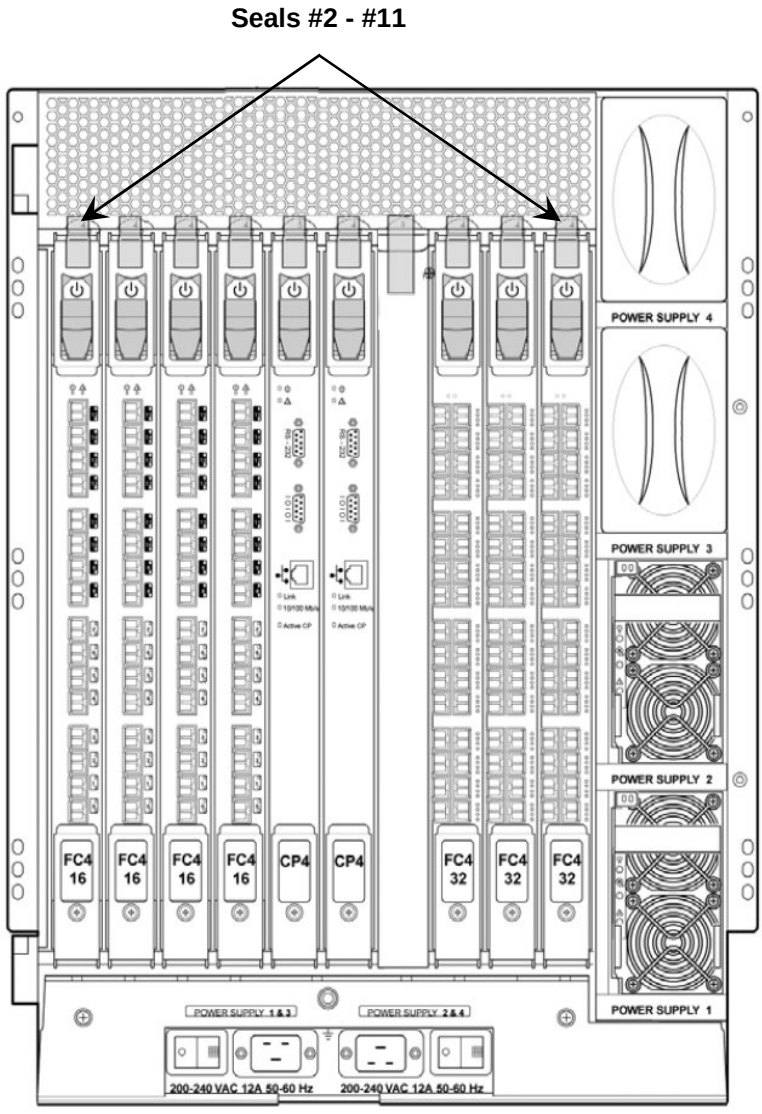

Figure A.8 – All Blades and Panels (Port Side)

Blade Seal Placement – Flat Ejector Handle Seal Placement

Figure A.9 below illustrates seal placement for both a control blade and a port blade.

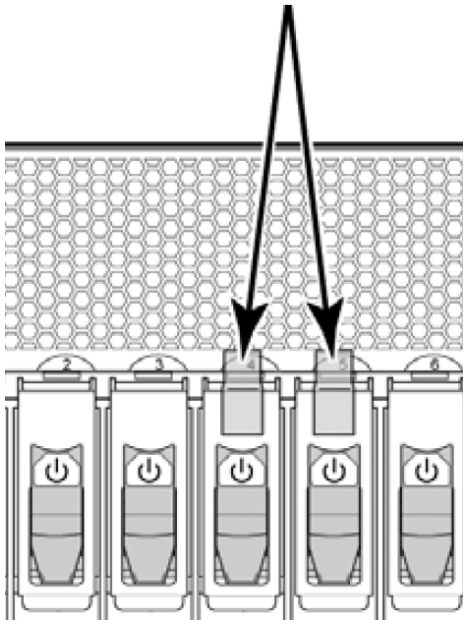

Figure A.9 – Flat Ejector Handle Seal Locations for the Brocade 48000

Attach one (1) seal beginning on the lower frame of the exhaust vent, spanning the gap between the frame and the blade, extending on to the upper blade ejector, and ending just before the thumbscrew. Apply one (1) seal to every blade. Ensure the seal is firmly affixed to the exhaust vent frame and the blade ejector.

NOTE: Be sure that the seal does not cover either the micro-switch or the thumbscrew.

Blade Seal Placement – Stainless Steel Ejector Handle Seal Placement

Figure A.10 below illustrates the seal placement for blades that have stainless steel ejector handles on the Brocade 48000 Director.

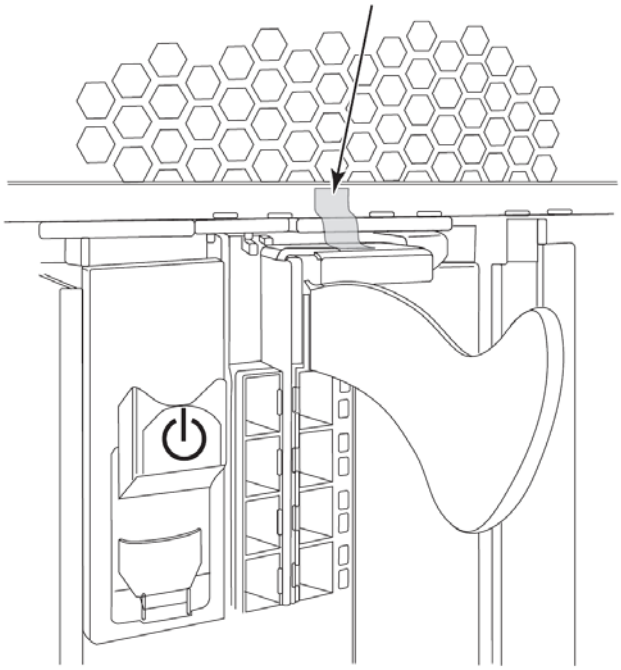

Figure A.10 - Brocade 48000 Stainless Steel Blade Ejector Seal Location

Attach one (1) seal beginning on the lower frame of the exhaust vent and curving down onto the upper surface of the pull tab of the blade. Attach one (1) seal for each blade that has stainless steel ejectors. Ensure the seal is firmly affixed to both the exhaust vent frame and the top of the pull tab.

Blade Seal Placement – Filler Plate Seal Placement

Figure A.11 below illustrates the filler panel seal placement on the Brocade 48000 Director. Refer to the following figure to perform the procedure.

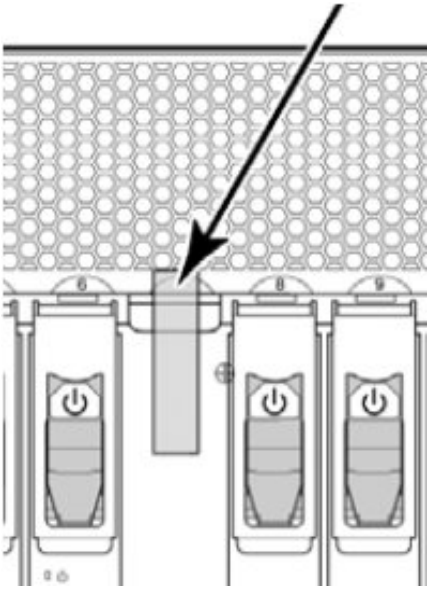

Figure A.11 – Brocade 48000 Filler Panel Seal Location

Insert the new filler panel if necessary. Attach one (1) seal beginning on the lower frame of the exhaust vent, bypassing the pull tab, and spanning down to the surface of the filler panel. Apply one (1) seal for each filler panel. Be sure that the seal does not cover any of the exhaust vents. It must make contact only with the frame. Ensure the seal is firmly affixed to the exhaust vent frame and to the surface of the filler panel.