BROCADE

VDX® 6710, VDX 6720, VDX 6730, and VDX 8770 with Network OS v3.0.1 Firmware Security Policy

Document Version 1.0

Brocade Communications

November 05, 2013

Table of Contents

Table of Tables

Table of Figures

1. Module Overview

The VDX 6710, VDX 6720, VDX 6730 and VDX 8770 are multiple-chip standalone cryptographic modules, as defined by FIPS 140-2. The module(s) are available in multiple configurations that vary based on the hardware enclosure. Each module is enclosed in a hard opaque commercial grade metal chassis with removable cover. For VDX 6710, VDX 6720 and VDX 6730, the power supply and fan assemblies are no part of the cryptographic boundary. For VDX 8770 modules the power supply and fan assemblies are part of the cryptographic boundary. The module is a 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.

Table 1 Firmware Version

Firmware
Network OS (NOS) v3.0.1

Table 2 Validated Hardware Configurations

Module Label	SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
VDX 6710-54-F	SKU BR-VDX6710-54-F P/N 80-1004843-04	VDX 6710,48P GBE,6P SFP+,AC, NON-PORT SIDE EXHAUST[1]	NOS v3.0.1	XBR-000195
VDX 6710-54-R	SKU BR-VDX6710-54-R P/N 80-1004702-04	VDX 6710,48P GBE,6P SFP+,AC, PORT SIDE EXHAUST[1]	NOS v3.0.1	XBR-000195
VDX 6720-16-F[3]	SKU BR-VDX6720-16-F P/N 80-1004566-07[1], 80-1006701-02[2]	VDX 6720,16P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-16-R[3]	SKU BR-VDX6720-16-R P/N 80-1004567-07[1], 80-1006702-02[2]	VDX 6720,16P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-24-F[3]	SKU BR-VDX6720-24-F P/N 80-1004564-07[1], 80-1006699-02[2]	VDX 6720,24P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-24-R[3]	SKU BR-VDX6720-24-R P/N 80-1004565-07[1], 80-1006700-02[2]	VDX 6720,24P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-40-F[3]	SKU BR-VDX6720-40-F P/N 80-1004570-07[1], 80-1006305-02[2]	VDX 6720,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195

Module Label	SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
VDX 6720-40-R[3]	SKU BR-VDX6720-40-R P/N 80-1004571-07[1], 80-1006306-02[2]	VDX 6720,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-60-F[3]	SKU BR-VDX6720-60-F P/N 80-1004568-07[1], 80-1006303-02[2]	VDX 6720,60P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6720-60-R[3]	SKU BR-VDX6720-60-R P/N 80-1004569-07[1], 80-1006304-02[2]	VDX 6720,60P SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-16-F[3]	SKU BR-VDX6730-16-F P/N 80-1005649-03[1], 80-1006709-02[2]	VDX 6730,16P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-16-R[3]	SKU BR-VDX6730-16-R P/N 80-1005651-03[1], 80-1006711-02[2]	VDX 6730,16P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-24-F[3]	SKU BR-VDX6730-24-F P/N 80-1005648-03[1], 80-1006708-02[2]	VDX 6730,24P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-24-R[3]	SKU BR-VDX6730-24-R P/N 80-1005650-03[1], 80-1006710-02[2]	VDX 6730,24P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-40-F[3]	SKU BR-VDX6730-40-F P/N 80-1005680-03[1], 80-1006719-02[2]	VDX 6730,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-40-R[3]	SKU BR-VDX6730-40-R P/N 80-1005681-03[1], 80-1006720-02[2]	VDX 6730,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-60-F[3]	SKU BR-VDX6730-60-F P/N 80-1005679-03[1], 80-1006718-02[2]	VDX 6730,60P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 6730-60-R[3]	SKU BR-VDX6730-60-R P/N 80-1005678-03[1], 80-1006717-02[2]	VDX 6730,60P,SFP+,AC, PORT SIDE EXHAUST	NOS v3.0.1	XBR-000195
VDX 8770-4	SKU BR-VDX8770-4-BND-AC P/N 80-1005850-02	VDX 8770 4 I/O Slot chassis with three Switch Fabric Modules, one Management Module, two exhaust Fans and two 3000W AC PSU	NOS v3.0.1	XBR-000195
	SKU BR-VDX8770-4-BND-DC P/N 80-1006532-02	VDX 8770 4 I/O Slot chassis with three Switch Fabric Modules, one Management Module, two exhaust Fans and two 3000W DC PSU	NOS v3.0.1	XBR-000195
VDX 8770-8	SKU BR-VDX8770-8-BND-AC P/N 80-1005905-02	VDX 8770 8 I/O Slot chassis with six Switch Fabric Modules, one Management Module, 4 exhaust Fans and three 3000W AC PSU	NOS v3.0.1	XBR-000195

Module Label	SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
	SKU BR-VDX8770-8-BND-DC P/N 80-1006533-02	VDX 8770 8 I/O Slot chassis with six Switch Fabric Modules, one Management Module, 4 exhaust Fans and three 3000W DC PSU	NOS v3.0.1	XBR-000195

Table 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. Port side and non-port side exhaust indicates whether the external fan direction causes air to be draw into the non-port side air vents and exhausted from the port side air vents or vice versa.

The following field removable components: line cards, modules, power supplies and filler panels listed below may be used within validated Brocade VDX 8770-4 and VDX 8770-8 configurations:

Table 3 Components of the VDX 8770

Component of the cryptographic boundary		SKU/MGF Part Number
Field Replaceable Unit – Power Supply Module	AC	SKU XBR-ACPWR-3000 P/N 80-1006540-01
	DC	SKU XBR-DCPWR-3000 P/N 80-1006539-01
Field Replaceable Unit – Filler Panel for Power Supply Slot		SKU XBR-BLNK-PSU P/N 80-1006430-01
Field Replaceable Unit – Fan Module		SKU XBR-FAN-FRU P/N 80-1006080-01
Field Replaceable Unit – Switch Fabric Module		SKU BR-VDX8770-SFM-1 P/N 80-1006295-01
Field Replaceable Unit – Management Module		SKU BR-VDX8770-MM-1 P/N 80-1006294-02
Field Replaceable Unit – Line Card Unit	48X1G Line Card	SKU BR-VDX8770-48X1G-SFP-1 P/N 80-1006049-02
	12X40GE Line Card	SKU BR-VDX8770-12X40G-QSFP-1 P/N 80-1006293-02
	48X10G Line Card	SKU BR-VDX8770-48X10G-SFPP-1 P/N 80-1006048-02
Field Replaceable Unit – Filler Panel for Line Card Slot		SKU XBR-BLNK-FULL P/N 80-1006431-01
Field Replaceable Unit – Half-Slot Filler Panel for Switch Fabric Module Slot or Management Module Slot		SKU XBR-BLNK-HALF P/N 80-1006429-01

Figure 1 through Figure 6 illustrates the cryptographic module configurations. With the exception of VDX 8770-4 and VDX 8770-8 shown below, power supplies and fan assemblies are not within cryptographic boundary.

Figure 1 VDX 6710-54 Switch

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 6710-54.

Figure 2 VDX 6720-16 and VDX 6720-24[1]

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 6720-16 and VDX 6720-24.

Figure 3 VDX 6720-40 and VDX 6720-60[2]

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 6720-40 and VDX 6720-60.

Figure 4 VDX 6730-16 and VDX 6730-24

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 6730-16 and VDX 6730-24.

[1] SW-VDX-6720-24POD-01 license enables the upper eight ports

[2] SW-VDX-6720-60POD-01 and SWVDX-6720-60POD2-01 licenses enable the upper twenty ports

[2] SW-VDX-6720-60POD-01 and SWVDX-6720-60POD2-01 licenses enable the upper twenty ports

Figure 5 VDX 6730-40 and VDX 6730-60[3]

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 6730-40 and VDX 6730-60.

Figure 6 VDX 8770-4 and VDX 8770-8[4]

Table 2 Validated Hardware Configurations lists the hardware configurations for the VDX 8770-4 (Left) and VDX 8770-8 (Right). See ***Table 3 Components of the VDX 8770*** for a list of installable VDX 8770 components.

[3] SW-VDX-6730-60POD-01 and SWVDX-6730-60POD2-01 licenses enable the upper twenty ports

[4] Each removable module in the chassis (except the fans) has a matching filler panel that must be in place if no module is installed in a slot. The two modules shown in this picture are fully populated with management modules, switch fabric modules, line cards, and power supplies per Table 3 Components of the VDX 8770. There are no filler panels for the fans since all fans must be installed on the chassis.

2. Security Level

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

Table 4 Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	2
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

Table 5 FIPS Approved Cryptographic Functions

Label	Cryptographic Function	VDX 6710 VDX 6720 VDX 6730	VDX 8770
AES	Advanced Encryption Algorithm	2283	2285
Triple-DES	Triple Data Encryption Algorithm	1431	1432
SHA	Secure Hash Algorithm	1965	1966
HMAC	Keyed-Hash Message Authentication code	1399	1400
RSA	Rivest Shamir Adleman Signature Algorithm	1174	1175
RNG	Random Number Generator	1135	1136

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

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

- RSA Key Wrapping (key establishment methodology; 1024-bit keys provide 80 bits of encryption strength)
- Diffie-Hellman (DH) for SSHv2 (key agreement; 1024-bit or 2048-bit keys; 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

- SSHv2 KDF
- TLS KDF with HMAC-MD5
- TLS v1.0
- 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, considered as plain text)
- RADIUS PEAP MS-CHAP V2
- Non-deterministic random number generator for seeding ANSI X9.31 DRNG
- Diffie-Hellman (DH) for FC-SP (key agreement, 1024 to 2048 bit keys.
- OSPF is considered as plain text interface (No protection is claimed for protocol data exchange).

The cryptographic module may be configured for FIPS 140-2 mode via execution of the following procedure.

- Install removable front cover (as applicable) and apply tamper labels
- Login as authorized user with admin role.
- Configure the system in standalone or fabric cluster mode as needed.
- Disable Boot PROM Access.
- For LDAP authentication, Configure FIPS 140-2 compliant ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA) for LDAP.
- Configure FIPS 140-2 compliant ciphers (HMAC-SHA1 (mac), , AES128-CBC, AES256-CBC) for SSH.
- Disable root access.
- If TACACS+ is configured, then remove the configuration.
- If dot1x is configured, disable it.
- If vCenter is configured, then remove the configuration.
- *If FC-SP authentication is configured, update DH group to use key sizes greater than 1024.*
- *If autoupload is enabled, disable it.*
- Enable FIPS 140-2 Self tests i.e. Execute ‘fips selftests’
- Execute 'fips zeroize' (automatically reboot(s) the system).
- After reboot, Http, HTTPS, Telnet and some ports of Brocade internal servers must be blocked in FIPS 140-2 mode. Once the switch is in the fips compliant mode, HTTP (80), HTTPS (443), Telnet (23) and Brocade internal server ports (TCP: 2301, 2401, 3016, 3516, 4516, 5016, 7013, 7110, 7710, 9013, 9110, 9710, 9910-10110. UDP: 33351, 36851, 37731, and 50690) must be blocked, and passwords of the default accounts (admin and user) should be changed after every zeroization operation to maintain FIPS 140-2 compliance.
    - Note:
        - If SSH access is required, configure to open ports 22 and 830(netconf).
        - If remote access is required, such as through SCP or LDAP, configure to allow UDP and TCP traffic on ports 1024 through 65535.
- For LDAP authentication, import minimum 1024 bits RSA LDAP CA certificate.
- For Radius authentication, configure the Radius server with PEAP-MSCHAPv2 mode and shared secret.
- If secure sys log is needed, import minimum 1024 bits RSA CA certificate. In FIPS 140-2 compliant state,
    - Do not use FTP for following operations
    - Config Upload
    - Config Download
    - Support Save
    - FW Download

- Do not use outbound SSH and telnet commands (clients).
- With regards to SCP client on the switch, remote SCP server must employ RSA host keys with minimum length of 1024 bits and DH with minimum length of 1024 bit. FIPS 140-2 compliant ciphers (HMAC-SHA1 (mac), AES128-CBC, AES256-CBC) are enforced on the client side.

NOTES:

1. Firmware packages are always signed at build time and validated during the firmwaredownload operation.
2. USB interface: Authorized operator is required to maintain the physical possession (at all times) of the USB token and shall not provide to unauthorized individuals/entities.

The operator can determine if the cryptographic module is running in FIPS 140-2 vs. non-FIPS mode by performing the following operations

- Display the status of self-tests, and accounts.
- Display the status of boot prom access.
- Display of cipherset configuration.
- Display of radius-server configuration.
- Display of IP ACLs configuration.
- Confirm LDAP server's root CA certificate.

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 140-2 and non-FIPS mode of operation, the operator is required to zeroize the module's plaintext CSPs, by calling "fips zeroize".

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 chippers 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 list of all cryptographic modules along with physical ports and logical interfaces are captured below:

1. VDX 6710-48-F and VX6710-48-R
    a. 10GE (Qty. 6) Data Input, Data Output, Control Input, Status Output
    b. Gig-E (Qty. 48): Data Input, Data Output, Control Input, Status Output
    c. Management Ethernet Ports (Qty. 1): Control Input, Status Output
    d. Serial port (Qty. 1): Control Input, Status Output
    e. RLOM Ethernet Ports (Qty. 1): (Inactive)
    f. USB (Qty. 1): Data Input, Data Output, Status Output
        i. Brocade USB flash device, XBR-DCX-0131

g. Power Supply Connectors (Qty. 2): Power Input, Data Output, Status Input
h. Fan Tray Connectors (Part of Power Supply FRU) (Qty. 2): Control Output, Status Input
i. LEDs: Status Output

2. VDX 6720-24-F and VDX 6720-24-R
    a. 10GE (Qty. 24) Data Input, Data Output, Control Input, Status Output
    b. Management Ethernet Ports (Qty. 2): Control Input, Status Output
    c. Serial port (Qty. 1): Control Input, Status Output
    d. RLOM Ethernet Ports (Qty. 1): (Inactive)
    e. USB (Qty. 1): Data Input, Data Output, Status Output
        i. Brocade USB flash device, XBR-DCX-0131
    f. Power Supply Connectors (Qty. 2): Power Input, Control Output, Status Input
    g. Fan Tray Connectors (Part of Power Supply FRU) (Qty. 2): Control Output, Status Input
    h. LEDs: Status Output
3. VDX 6720-60-F and VDX 6720-60-R
    a. 10GE (Qty. 60): Data Input, Data Output, Control Input, Status Output
    b. Management Ethernet Ports (Qty. 2): Control Input, Status Output
    c. Serial port (Qty. 1): Control Input, Status Output
    d. USB (Qty. 1): Data Input, Data Output, Status Output
        i. Brocade USB flash device, XBR-DCX-0131
    e. Power Supply Connectors (Qty. 2): Power Input, Control Output, Status Input
    f. Fan Tray Connectors (Qty. 2 – Part of Power Supply FRUs +3 – FAN FRUs): Control Output, Status Input
    g. LEDs: Status Output
4. VDX 6730-24-F and VDX 6730-24-R
    a. 10GE (Qty. 24): Data Input, Data Output, Control Input, Status Output
    b. Fibre Channel (Qty. 8): Data Input, Data Output, Control Input, Status Output
    c. Management Ethernet Ports (Qty. 2): Control Input, Status Output
    d. Serial port (Qty. 1): Control Input, Status Output
    e. RLOM Ethernet Ports (Qty. 1): (Inactive)
    f. USB (Qty. 1): Data Input, Data Output, Status Output
        i. Brocade USB flash device, XBR-DCX-0131
    g. Power Supply Connectors (Qty. 2): Power Input, Control Output, Status Input
    h. Fan Tray Connectors (Part of Power Supply FRU) (Qty. 2): Control Output, Status Input
    i. LEDs: Status Output
5. VDX 6730-60-F and VDX 6730-60-R
    a. 10GE (Qty. 60): Data Input, Data Output, Control Input, Status Output
    b. Fibre Channel (Qty. 16): Data Input, Data Output, Control Input, Status Output
    c. Management Ethernet Ports (Qty. 2): Control Input, Status Output
    d. Serial port (Qty. 1): Control Input, Status Output
    e. RLOM Ethernet Ports (Qty. 1): (Inactive)
    f. USB (Qty. 1): Data Input, Data Output, Status Output
        i. Brocade USB flash device, XBR-DCX-0131
    g. Power Supply Connectors (Qty. 2): Power Input, Control Output, Status Input
    h. Fan Tray Connectors (Qty. 2-Part of Power Supply FRUs + 3 FAN FRUs): Control Output, Status Input

i. LEDs: Status Output

6. VDX 8770-4 and VDX 8770-8
    a. Line card:
        i. BR-VDX8770-48X10G-SFPP-1 (48x10G):
            a. 10GbE port (quantity 48): Data Input, Data Output
            b. LEDs: Status Output
                i. Status LED (quantity 1)
                ii. Power LED (quantity 1)
                iii. Status Port LED (quantity 48)
        ii. BR-VDX8770-12X40G-QSFP-1 (12x40G):
            a. 40GbE port (quantity 12): Data Input, Data Output
            b. LEDs: Status Output
                i. Status LED (quantity 1)
                ii. Power LED (quantity 1)
        iii. Status Port LED (quantity 12)
        iv. BR-VDX8770-48X1G-SFP-1:
            a. 1GbE port (quantity 48): Data Input, Data Output
            b. LEDs: Status Output
                i. Status LED (quantity 1)
                ii. Power LED (quantity 1)
                iii. Status Port LED (quantity 48)
    b. Management Module (MM) (half-slot) :
        i. USB port (quantity 1): Data Input, Data Output
        ii. Console Port (RJ45 - serial) (quantity 1):Control Input, Status Output
        iii. Ethernet port (Mgmt IP) (RJ45) (quantity 1): Control Input, Status Output
        iv. Ethernet port (Service IP) (quantity 1): Control Input, Status Output
        v. LEDs: Status Output
            1. Status LED (quantity 1)
            2. Power LED (quantity 1)
            3. Active LED (quantity 1)
            4. Ethernet management link (upper left) (quantity 1)
            5. Ethernet management link activity (upper right) (quantity 1)
    c. Switch Fabric Module (SFM)
        i. LEDs: Status Output
            1. Status LED (quantity 1)
            2. Power LED (quantity 1)
    d. Power Supply
        i. AC Inlet (quantity 1): Power
        ii. LEDs: Status Output
            1. AC power input LED (AC OK) (quantity 1)
            2. DC power output LED (DC OK) (quantity 1)
            2. Alarm LED (ALM) (quantity 1)
    e. Fan Assembly
        i. LEDs: Status Output
            1. Power LED (quantity 1)
            2. Fault LED (quantity 1)

NOTE: LEDs display power status and port activity status.

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports five 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 forty (40) characters. The password is an alphanumeric string of eight (8) to forty (40) characters randomly chosen from the ninety-six (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.

Forty-eight (48) concurrent operators are allowed on the switch.

Table 6 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer): Admin role has the permission to access and execute all the available services.	Role-based operator authentication	Username and Password
User (User role): User role has the permission to display general configuration.	Role-based operator authentication	Username and Password
Maximum Permissions (for a custom role): A custom role can be created and assigned the custom permissions.	Role -based operator authentication	Username and Password
LDAP: If LDAP is configured, LDAP server authenticates to the cryptographic module.	Role-based operator authentication	LDAP Root CA certificate
RADIUS: If RADIUS is configured, RADIUS server authenticates to the cryptographic module.	Role -based operator authentication	RADIUS Shared Secret

Table 7 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.

Authentication Mechanism	Strength of Mechanism
Knowledge of a Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The maximum possible authentication attempts within a minute are 16. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Table 8 Service Descriptions

Service Name	Description
User Management	User and password management.
Login Session Management	Controls the user session management,
RADIUS	RADIUS configuration functions
LDAP	LDAP configuration functions.
FIPS	Control FIPS mode operation and related functions
Zeroize	Zeroize all CSPs
Firmware Management	Control firmware management.
PKI	Import LDAP root CA certificate.
Clock Management	Clock and Time zone Management
Debug & Diagnostics	Debug & Diagnostics tools.
CLI Management	CLI Management tools
Platform	Platform tools
Display	Display configuration and operational commands
Terminal Configuration	Terminal configuration operations
Ethernet	Ethernet Management
License	License Management
VCS®	Cluster services
vCenter	VMware-ESX hosts Management
SNMP	SNMP
System Monitor	Status configuration & monitoring

6. Access Control Policy

Roles and Services

Table 9 Services Authorized for Roles

SERVICE / ROLE	User	Admin	Maximum Permissions	RADIUS	LDAP
User Management		X	X		
Login Session Management		X	X		
PKI	X	X	X		
Firmware Management	X	X	X		
FIPS		X	X		
Zeroize		X	X		
Clock Management		X	X		
Debug & Diagnostics		X	X		
CLI Management		X	X		
Platform		X	X		
Display		X	X		
Login Session Management / RADIUS-server		X	X	X	
Login Session Management / LDAP-server		X	X		X
Terminal Configuration		X	X		
Ethernet		X	X		
License		X	X		
VCS		X	X		
vCenter		X	X		
SNMP		X	X		
System Monitor		X	X		
FCSP		X	X		
Switch Connection Policy		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 1024/2048 bit modulus in SSHv2.
- SSH/SCP/SFTP Session Keys- 128 and 256 bit AES CBC
- SSH/SCP/SFTP Authentication Key
- SSH KDF Internal State
- SSH DH Shared Secret Key
- SSH 2048 RSA Private Key
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS PRF Internal State
- TLS Session Key – 128 bit AES
- TLS Authentication Key for HMAC-SHA-1
- Approved RNG Seed Material
- ANSI X9.31 DRNG Internal State
- Passwords
- RADIUS Secret
- DH Keys for use from 1024 to 2048 bit modulus in FC-SP

Definition of Public Keys:

The following are the public keys contained in the module:

- DH Public Key (1024/2048 bit modulus)
- DH Peer Public Key (1024/2048 bit modulus)
- TLS v1.0 Public Key (RSA 1024)
- TLS v1.0Peer Public Key (RSA 1024)
- FW Download Key (RSA 1024)
- LDAP ROOT CA certificate (RSA 1024)
- SSH RSA 1024/2048 bit Public Key

Definition of Service Categories:

Table 10 Services and Command Line Instructions (CLI)

Services	CLIs
User Management	Username role password-attributes rule encryption-level unlock
Login Session Management	radius-server tacacs-server ldap-server aaa logout banner ssh telnet

Services	CLIs
PKI	Certutil
Firmware Management	Firmware
Fips	fips selftests cipherset prom-access
Zeroize	fips zeroize
Clock Management	Clock Ntp
Debug & Diagnostics	Debug diag ping l2traceroute traceroute top undebug
CLI Mgmt	no delete configure dir exit help history quit rename abort do pwd unhide unhide fips prompt1 prompt2 rbridge-id
Platform	reload chassis clear copy fastboot usb logging service switch-attributes support auditlog autoupload beacon cidrecov df ha oscmd power-off power-on linecard
Display	Show

Services	CLIs
Terminal Configuration	send terminal end line
Ethernet	dot1x cee-map interface ip ipv6 lacp mac mac-address-table port-profile protocol qos rmon sflow vlan monitor arp class-map mac-rebalance police-priority-map policy-map resequence reserved-vlan route-map router system-max fabric fcoe bp-rate-limit zoning
License	License Dpod
VCS	Vcs
vCenter	Vcenter Vnetwork
SNMP	snmp-server
System Monitor	system-monitor system-monitor-mail threshold-monitor
FCSP	Fcsp
Switch connection policy	secpolicy

Table 11 CSP Access Rights within Roles & Services

	SSH and SCP CSPs[5]	TLS CSPs[6]	RNG Seed Key[7]	Passwords	RADIUS Secret	FCSP Secret	SSH RSA 1024/2048 Public Key
Login Session Management	N	N	N	RW	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	N
Firmware Management	R	N	N	N	N	N	N
PKI	RW	N	N	N	N	N	RW
RADIUS	N	N	N	RW	RW	N	N
User Management	N	N	N	RW	N	N	N
FCSP	N	N	N	N	N	RW	N

7. Operational Environment

The cryptographic module supports a limited operational environment; only trusted, validated code signed by RSA 1024 with SHA1 digest 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 FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide five 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:
        i. Cryptographic algorithm tests:
            (1) Triple-DES CBC KAT (encrypt/decrypt)
            (2) AES CBC KAT (encrypt/decrypt)
            (3) HMAC SHA-1 KAT
            (4) ANSI X9.31 DRNG KAT

[5] Includes the following CSPs: DH Private Keys for use with 1024 bit modulus in SSHv2; SSH/SCP/SFTP Session Keys- 128, 192, and 256 bit AES CBC or Triple-DES 3 key; SSH/SCP/SFTP Authentication Key; SSH KDF Internal State; SSH DH Shared Secret Key; SSH 2048 RSA Private Key

[6] Includes the following CSPs: TLS Private Key (RSA 1024); TLS Pre-Master Secret; TLS Master Secret; TLS PRF Internal State; TLS Session Key – 128 bit AES; TLS Authentication Key for HMAC-SHA-1

[7] Includes the following CSPs: Approved RNG Seed Material; ANSI X9.31 DRNG Internal State

(5) SHA-1 KAT
(6) HMAC SHA-256 KAT (SHA-256 tested within this self-test)
(7) HMAC SHA-512 KAT (SHA-512 tested within this self-test)
(8) RSA 1024 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 – performed on Non-deterministic hardware based random number generator and ANSI X9.31 DRNG
ii. RSA 1024/ 2048 SHA- 1 Pair wise Consistency Test (Sign/Verify & Encrypt/Decrypt)
iii. RSA 1024/2048 Pair wise Consistency Test (Encrypt/Decrypt)
iv. Firmware Load Test (RSA 1024 SHA-1 Signature Verification)
v. Bypass Test: N/A
vi. Manual Key Entry Test: N/A

5. 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 by rebooting the module.
6. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. FC-SP authentication is supported only on VDX 6730 switches.

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 must periodically inspect the tamper evident seals applied to the modules within the operator's scope of responsibility for evidence of tampering.

Table 12 Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test
Tamper Evident Seals	12 months

10. Mitigation of Other Attacks Policy

These modules have 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
MM	Management Module
NTP	Network Time Protocol
NOS	Network Operating System
PKI	Public Key Infrastructure
PROM	Programmable read-only memory
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SSH	Secure Shell Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security Protocol

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.

VDX 6710-54

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6710-54. See Figure 7 and Figure 8 for details on how to position each seal.

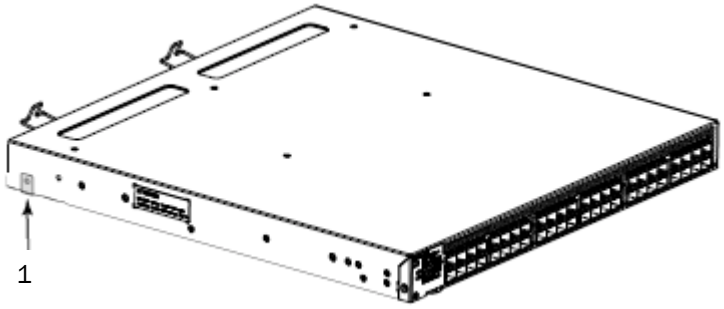

Figure 7 VDX 6710-54 left side seal location

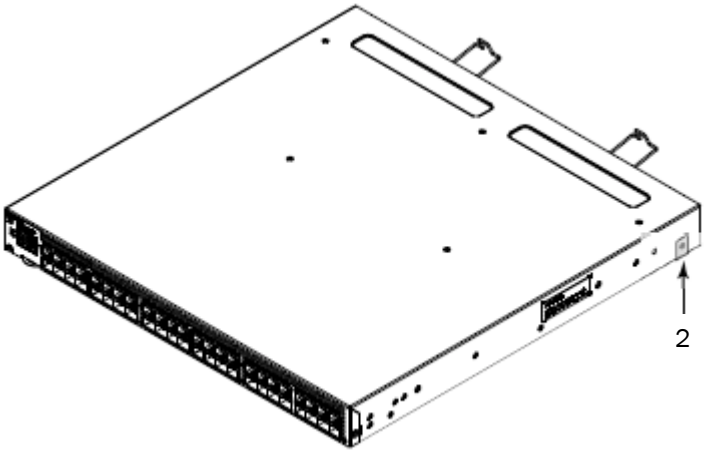

Figure 8 VDX 6710-54 right side seal location

VDX 6720-16 and VDX 6720-24

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6720-16 and VDX 6720-24. See Figure 9 and Figure 10 for details on how to position each seal.

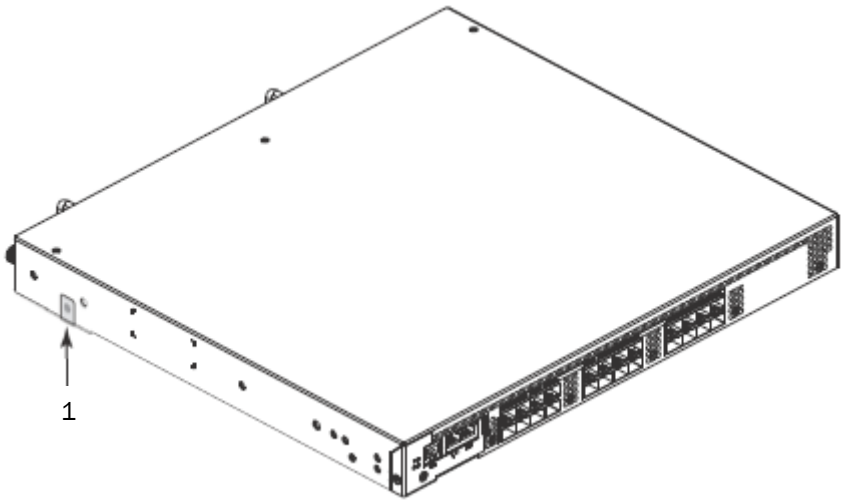

Figure 9 VDX 6720-16 and VDX 6720-24 left side seal location

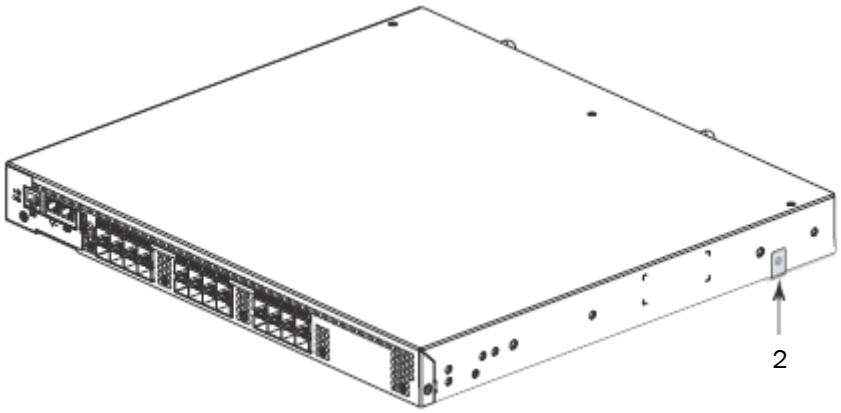

Figure 10 VDX 6720-16 and VDX 6720-24 right side seal location

VDX 6720-40 and VDX 6720-60

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6720-40 and VDX 6720-60. See Figure 11 and Figure 12 for details on how to position each seal.

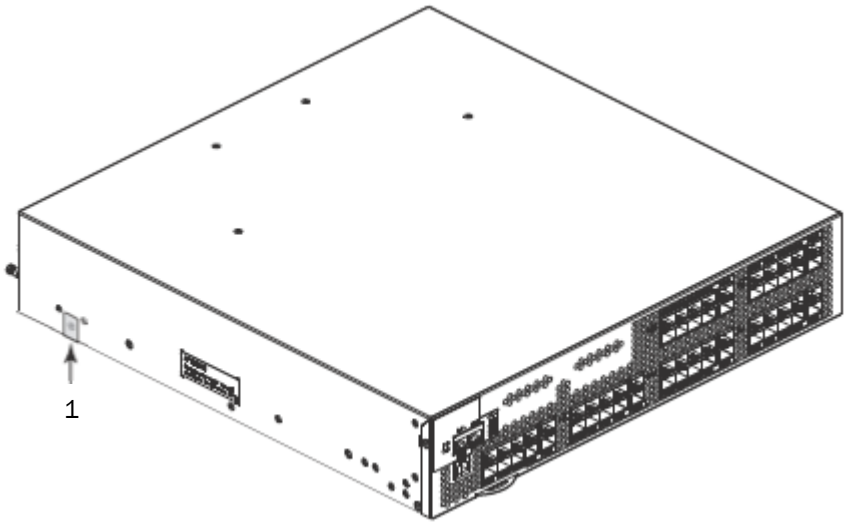

Figure 11 VDX 6720-40 and VDX 6720-60 left side seal location

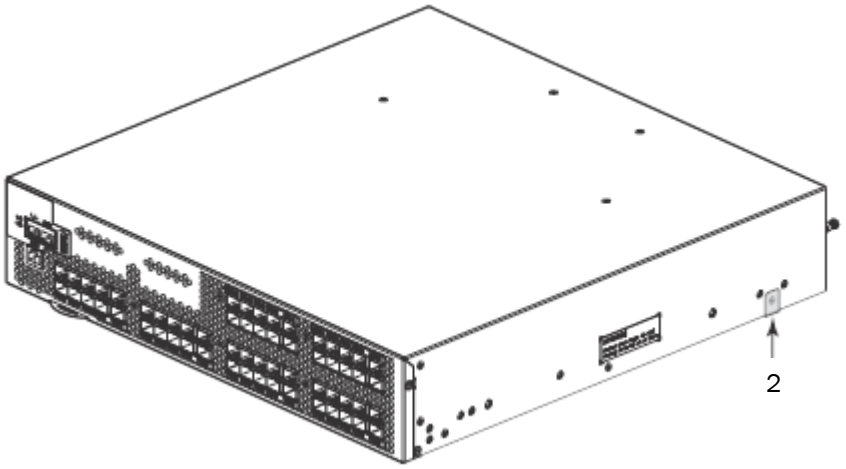

Figure 12 VDX 6720-40 and VDX 6720-60 right side seal location

VDX 6730-16 and VDX 6730-24

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6730-16 and VDX 6730-24. See Figure 13 and Figure 14 for details on how to position each seal.

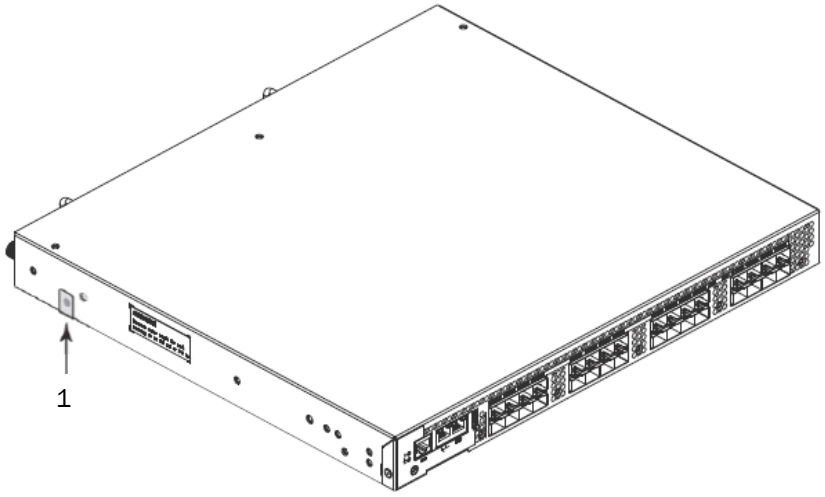

Figure 13 VDX 6730-16 and VDX 6730-24 left side seal location

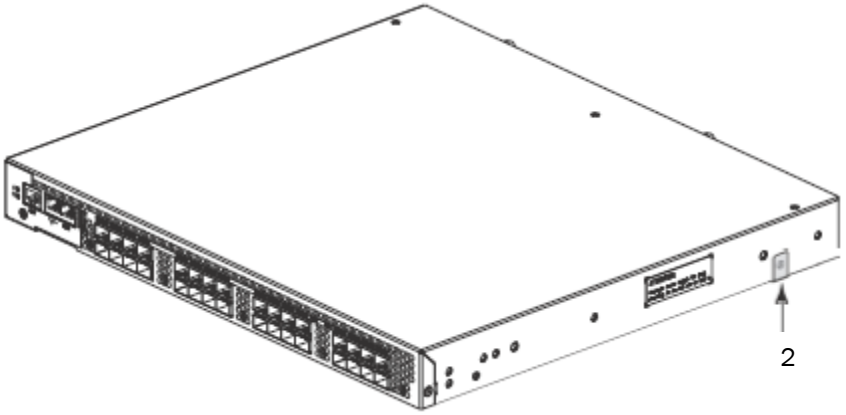

Figure 14 VDX 6730-16 and VDX 6730-24 right side seal location

VDX 6730-40 and VDX 6730-60

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6730-40 and VDX 6730-60. See Figure 15 and Figure 16 for details on how to position each seal.

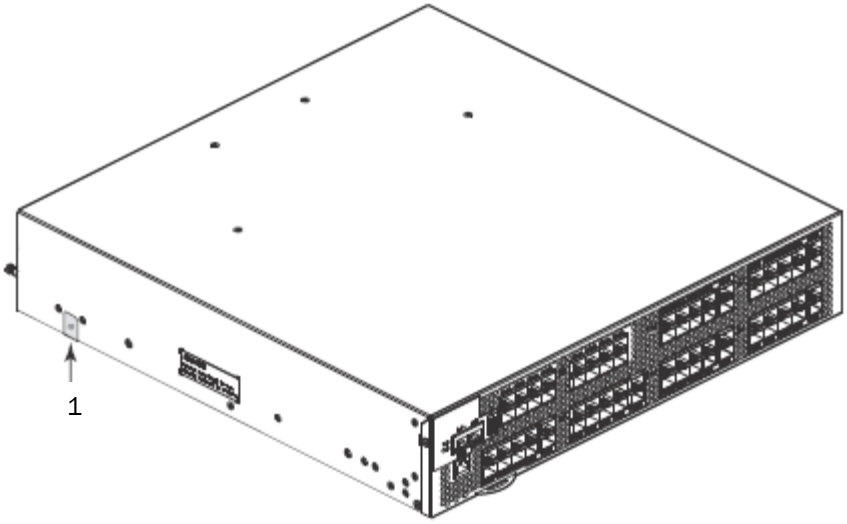

Figure 15 VDX 6730-40 and VDX 6730-60 left side seal location

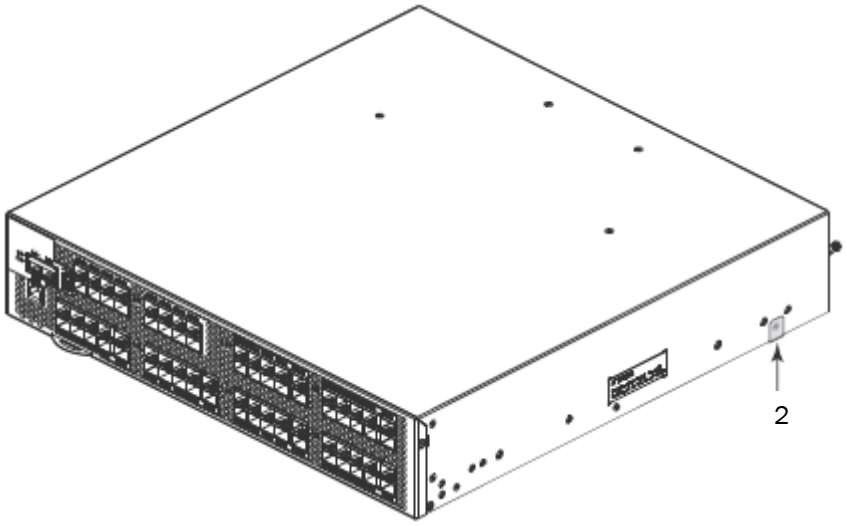

Figure 16 VDX 6720-40 and VDX 6720-60 right side seal location

VDX 8770-8

Thirty-six (36) tamper evident seals are required to complete the physical security requirements illustrated in Figure 17 and Figure 18.

VDX 8770-8 Port Side Tamper Evident Seal Application Procedure

Twenty-eight tamper evident seals are required to complete the physical security requirements illustrated in Figure 17. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

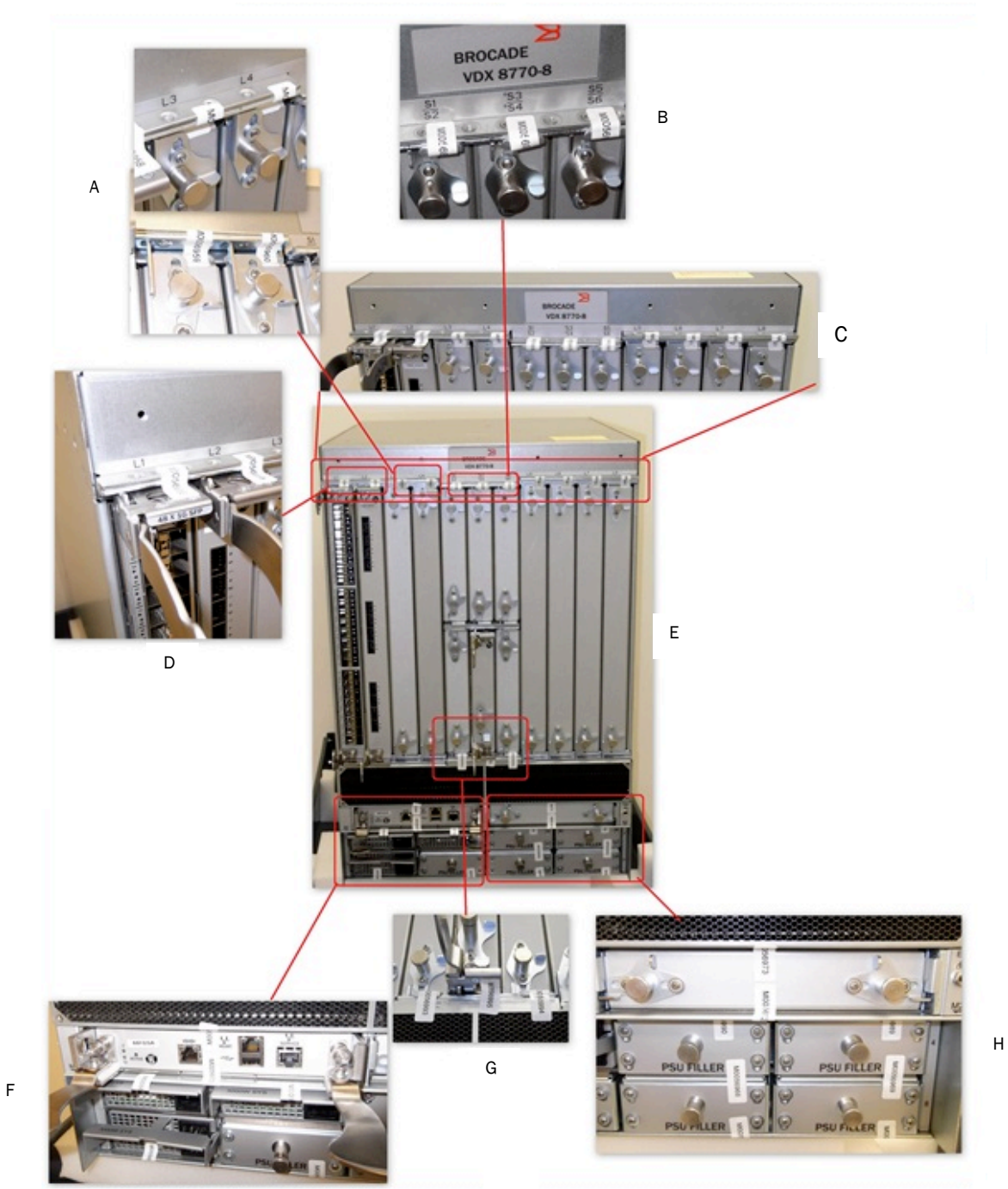

Figure 17 Brocade VDX 8770-8 Switch port side seal locations

1. Apply one (1) seal to each blade or filler panel installed in line card slots L1 through L8. Eight (8) seals are required to complete this step. See Figures 17A, 17C, 17D and 17E for details on how to position each seal.
2. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S1, S3 and S5. Three (3) seals are required to complete this step. See Figure 17B and 17E for details on how to position each seal.
3. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S2, S4 and S6. Three (3) seals are required to complete this step. See Figure 17E and 17G for details on how to position each seal.
4. Apply two (2) seal to each Management Module (MM) or filler panel installed in MM slots M1 and M2. Four (4) seals are required to complete this step. See Figure 17E, 17F and 17H for details on how to position each seal.

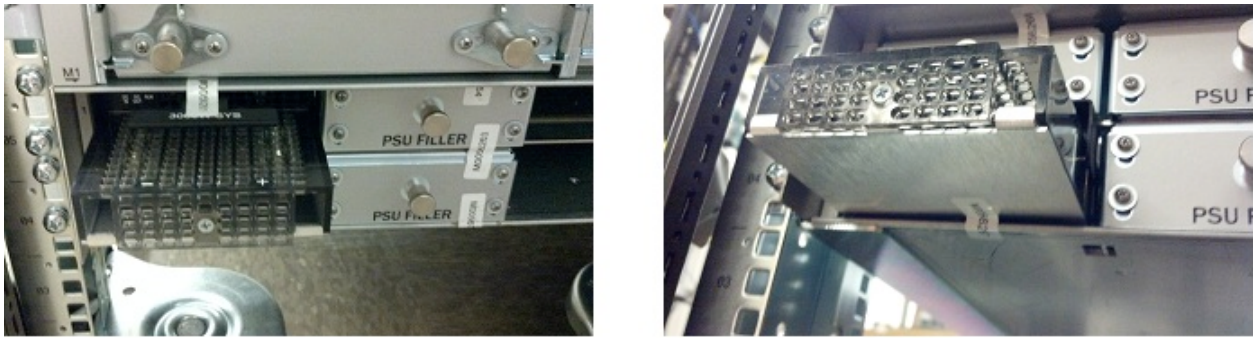

Figure 18 Brocade VDX 8770-8 DC PSU seal locations

5. The VDX 8770-8 accepts both AC and DC power supply module. For AC configurations, complete steps 5a and 5b. For DC configurations, complete steps 5b, 5c and 5d, as appropriate.
    a. For a VDX 8770-8 with AC Power Supply Units (PSU) apply one (1) seal to each Power Supply Unit (PSU) installed in PSU slots P1 through P8. For the configuration shown in Figure 17, PSUs are installed in PSU slots P1, P2 and P5. Therefore, three (3) seals are required to complete this step, for this configuration. See Figure 17E, 17F and 17H for details on how to position each seal.
    b. Apply one (1) seal to each PSU filler panel installed in PSU slots P1 through P8. Apply an additional seal that spans the gap between vertically stacked PSU filler panels. For this example, PSU filler panels are installed in PSU slots P3, P4, P6, P7 and P8. Therefore, seven (7) seals are required to complete this step, for this configuration. See Figure 17E, 17F and 17H for details on how to position each seal
    c. For a VDX 8770-8 with DC Power Supply Units (PSU) in slots P1 through P4 apply one (1) seal to the ejector handle of the PSU that spans the gap between the chassis and the PSU ejector handle. See Figure 18 for details on how to position the seal.
    d. For a VDX 8770-8 with DC Power Supply Units (PSU) in slots P5 through P8 apply one (1) seal to the sheet metal on the bottom of the PSU that spans the gap between the chassis and the PSU sheet metal housing. See Figure 18 for details on how to position the seal.

VDX 8770-8 Non-Port Side Tamper Evident Seal Application Procedure

Eight (8) tamper evident seals are required to complete the physical security requirements illustrated in Figure 18. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

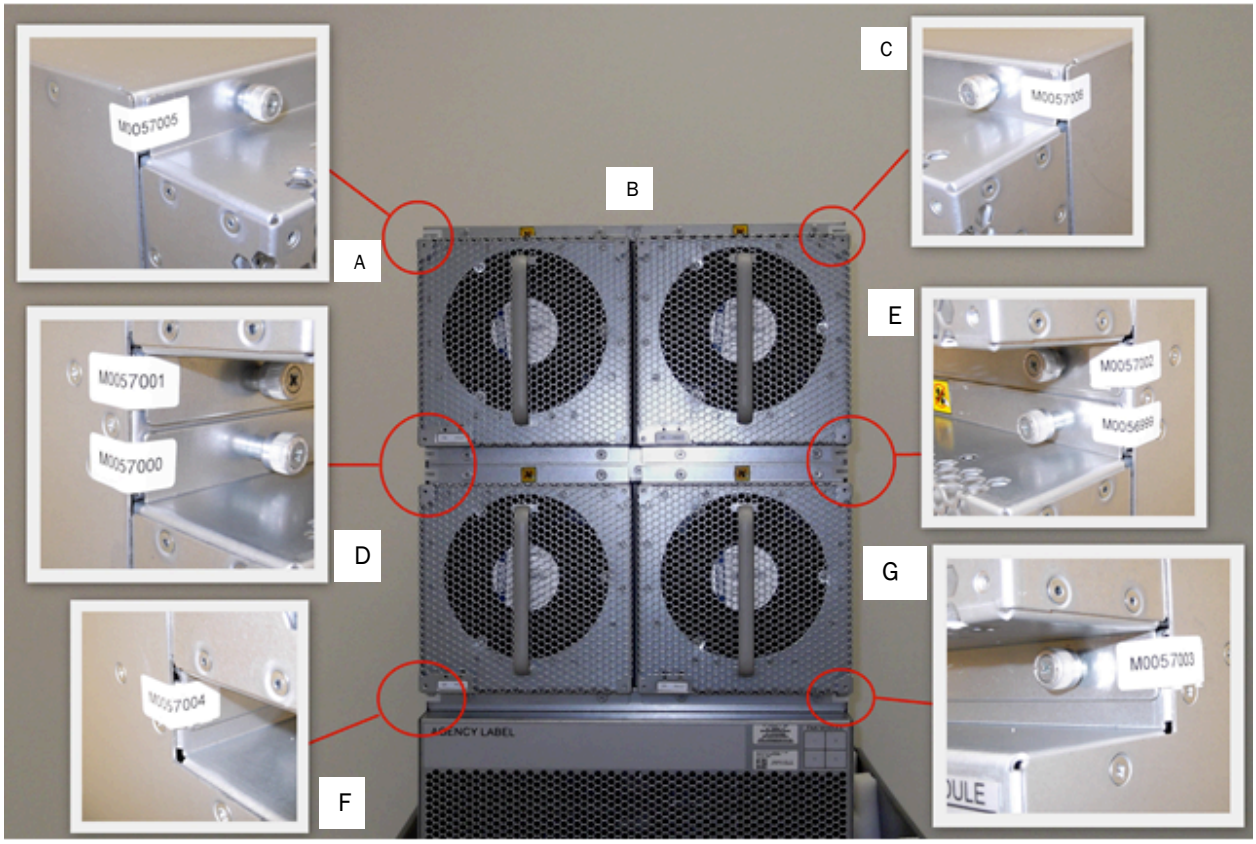

Figure 19 Brocade VDX 8770-8 non-port side seal locations

1. Apply two (2) seals to each FAN FRU or FAN FRU filler panel installed in the non-port side of the VDX 8770-8. Eight (8) seals are required to complete this step. See Figures 19A-G for details on how to position each seal.

VDX 8770-4

Twenty-three (23) tamper evident seals are required to complete the physical security requirements illustrated in Figure 20, Figure 21, Figure 22 and Figure 23.

VDX 8770-4 Port Side Tamper Evident Seal Application Procedure

Fifteen (15) tamper evident seals are required to complete the physical security requirements illustrated in Figure 20 and Figure 21. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

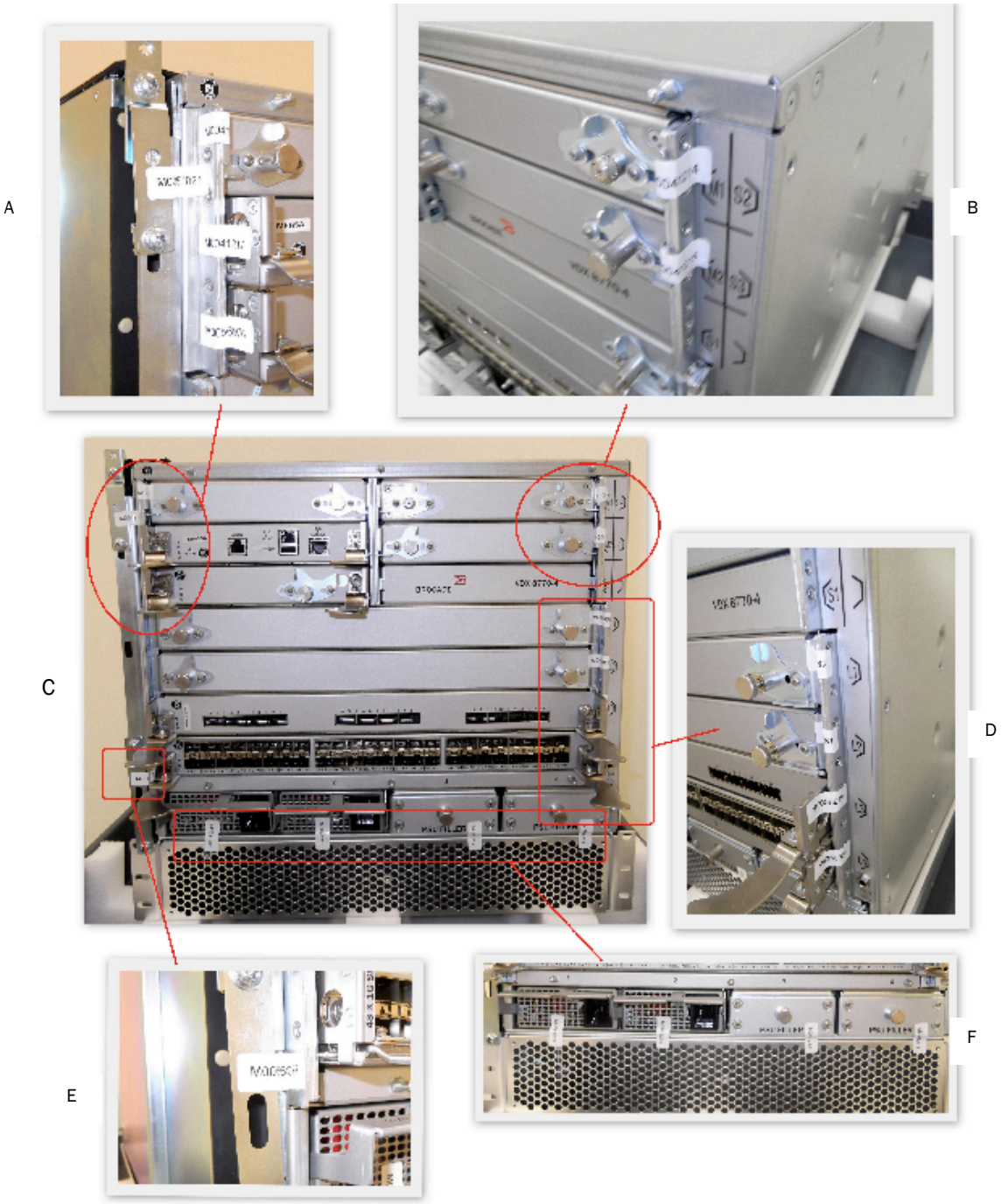

Figure 20 Brocade VDX 8770-4 Switch port side seal locations

Figure 21 Brocade VDX 8770-4 DC PSU seal locations

1. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S1, S2 and S3. Three (3) seals are required to complete this step. See Figure 20A, 20A and 20C for details on how to position each seal.
2. Apply one (1) seal to each Management Module (MM) or filler panel installed in MM slots M1 and M2. Two (2) seals are required to complete this step. See Figure 20A, 20A and 20C for details on how to position each seal.
3. Apply one (1) seal to each blade or filler panel installed in line card slots L1 through L4. Four (4) seals are required to complete this step. See Figures 20C, 20D and 20E for details on how to position each seal.
4. The VDX 8770-4 accepts both AC and DC power supply module. Depending on the type of installed power supply module complete step 4a or 4b.
    a. For a VDX 8770-4 with AC Power Supply Units (PSU) apply one (1) seal to each AC PSU or PSU filler panel installed in PSU slots P1 through P4. For this example, an AC PSUs are installed in slots P1 and P2. PSU filler panels are installed in slots P3 and P4. Four (4) seals are required to complete this step. See Figure 20C and 20F for details on how to position each seal.
    b. For a VDX 8770-4 with DC Power Supply Units (PSU) apply one (1) seal to each DC PSU or PSU filler panel installed in PSU slots P1 through P4. For this example, a DC PSUs are installed in slot P1. A PSU filler panels are installed in slot P2. Four (4) seals are required to complete this step. See Figure 21 for details on how to position each seal.
5. Apply one (1) seal on each FIPS bracket. The upper left FIPS bracket is shown in Figure 20A and 20C. The lower left FIPS bracket is shown in Figure 20E and 20C. Two (2) seals are required to complete this step. See Figure 20A, 20C and 20E for details on how to position each seal.

VDX 8770-4 Non-Port Side Tamper Evident Seal Application Procedure

Five (5) tamper evident seals are required to complete the physical security requirements illustrated in Figure 22. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

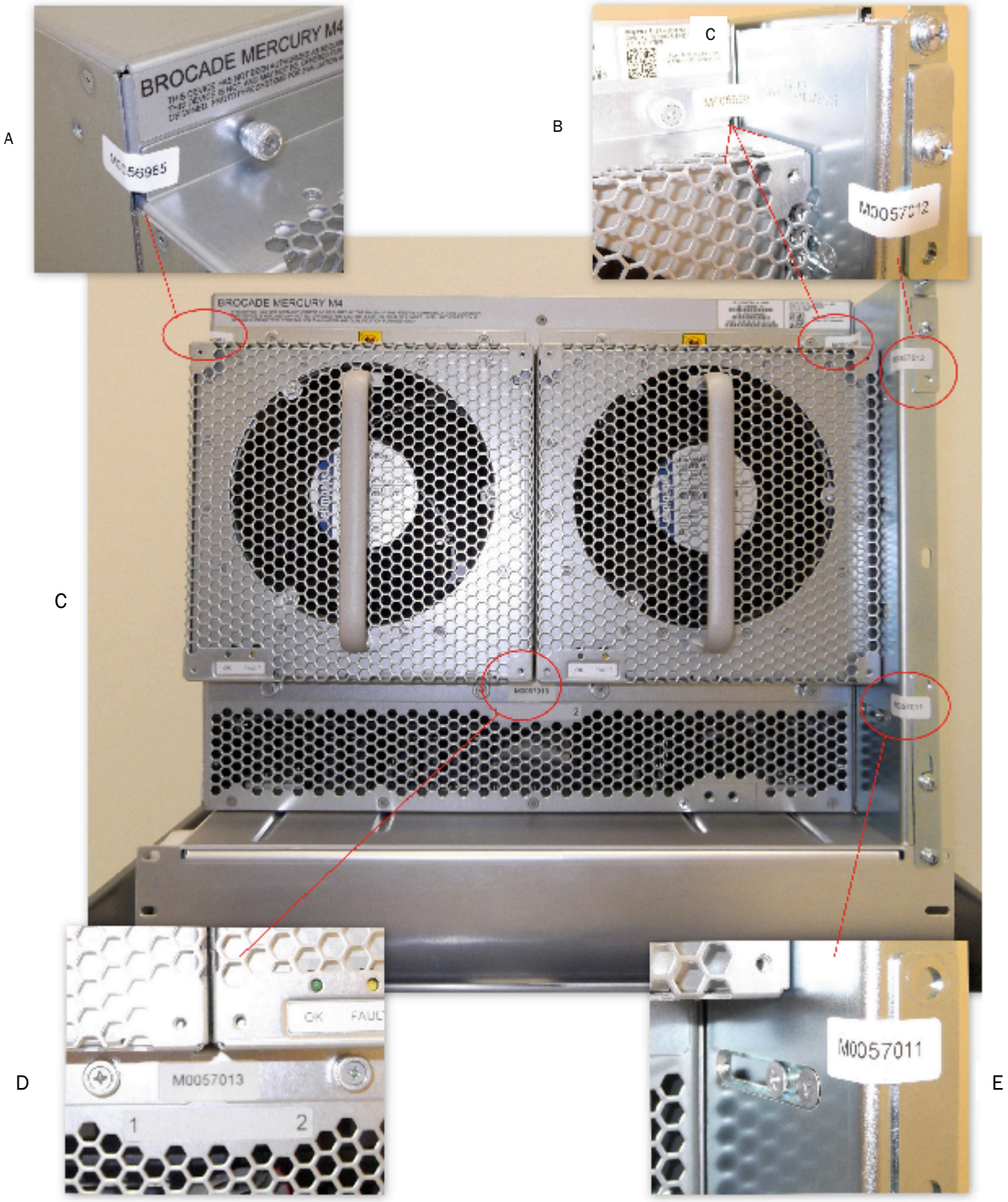

Figure 22 Brocade VDX 8770-4 Non-port side seal locations

1. Apply one (1) seals to each FAN FRU or FAN FRU filler panel installed in the non-port side of the VDX 8770-4. For the FAN FRU on the left the seal wraps from the flange on the FAN FRU or filler around the outside corner of the chassis. For the FAN FRU on the right the seal wraps from the flange on the FAN FRU or filler around the inside corner of the chassis. Two (2) seals are required to complete this step. See Figures 22A-C for details on how to position each seal.
2. Apply one (1) seals that bridges the gap between the FAN FRU positions installed in the non-port side of the VDX 8770-4. One (1) seals are required to complete this step. See Figures 22C and 22D for details on how to position each seal.
3. Apply one (1) seal on each FIPS bracket. The upper right FIPS bracket is shown in Figure 22B and 22C. The lower right FIPS bracket is shown in Figure 22C and 22E. Two (2) seals are required to complete this step. See Figure 22B, 22C and 22E for details on how to position each seal.

VDX 8770-4 Air Duct Tamper Evident Seal Application Procedure

Three (3) tamper evident seals are required to complete the physical security requirements illustrated in Figure 23. Relative to the port side of the VDX 8770-4 chassis the air duct is secured to the left side of the chassis.

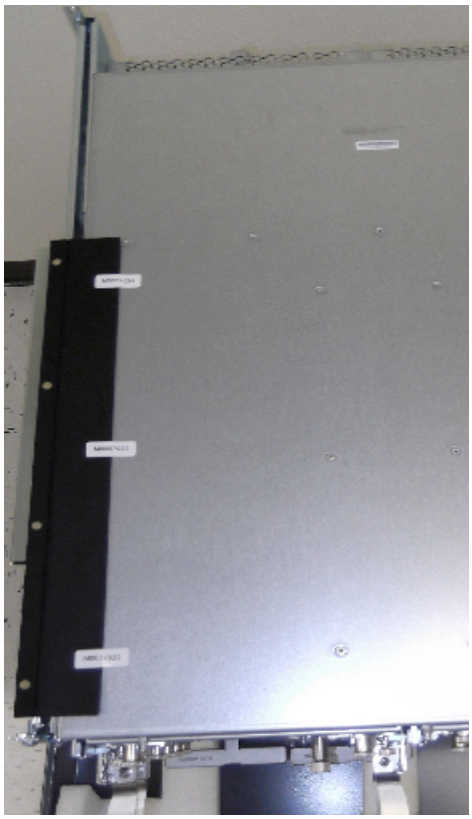

Figure 23 Brocade VDX 8770-4 Air Duct side seal locations

1. Apply thee (3) seals to the rubber flap that touches the top of the VDX 8770-4. Position each seal such that approximately half of each seal adheres to the rubber flap and half of each seal adheres to the top of the chassis. Three (3) seals are required to complete this step. See Figures 23 for details on how to position each seal.