VDX 6710, VDX 6720, VDX 6730, VDX 6740, VDX 6740T and VDX 8770 Switches

FIPS 140-2

Non-Proprietary

Security Policy

Document Version 1.0

Brocade Communications

10/21/2014

Revision History

Revision Date	Revision	Summary of Changes
10/21/2014	1.0	Initial Draft

Table of Contents

Table of Tables

Table of Figures

1   Module Overview

The VDX 6710, VDX 6720, VDX 6730, VDX 6740, VDX6740T and VDX 8770 are multi-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 the VDX 6710, VDX 6720, VDX 6730, VDX 6740, and VDX 6740T the power supply and fan assemblies are not 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	Part Number
Network OS (NOS) v4.0.1	63-1001271-01

Table 2 Validated VDX 6710 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6710-54-F P/N: 80-1004843-04	VDX 6710,48P GBE,6P SFP+,AC, NON-PORT SIDE EXHAUST[1]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6710-54-R P/N: 80-1004702-04	VDX 6710,48P GBE,6P SFP+,AC, PORT SIDE EXHAUST[1]	NOS v4.0.1	XBR-000195

Table 2 Notes:

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

Table 3 Validated VDX 6720 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6720-16-F[3] P/N: 80-1004566-07[1], 80-1006701-02[2]	VDX 6720,16P,SFP+,AC, NON-PORT SIDE EXHAUST[4]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6720-16-R[3] P/N: 80-1004567-07[1], 80-1006702-02[2]	VDX 6720,16P,SFP+,AC, PORT SIDE EXHAUST[4]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6720-24-F[3] P/N: 80-1004564-07[1], 80-1006699-02[2]	VDX 6720,24P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6720-24-R[3] P/N: 80-1004565-07[1], 80-1006700-02[2]	VDX 6720,24P,SFP+,AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6720-40-F[3] P/N: 80-1004570-07[1], 80-1006305-02[2]	VDX 6720,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6720-40-R[3] P/N: 80-1004571-07[1], 80-1006306-02[2]	VDX 6720,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6720-60-F[3] P/N: 80-1004568-07[1], 80-1006303-02[2]	VDX 6720,60P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6720-60-R[3] P/N: 80-1004569-07[1], 80-1006304-02[2]	VDX 6720,60P SFP+,AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195

Table 3 Notes:

1. Serviceable assembly

2. Production assembly.

3. Serviceable and production assemblies are functionally equivalent. The part number assigned to each production assembly was created to support the release of updated logos and marks on the agency label.

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

Table 4 Validated VDX 6730 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6730-16-F[3] P/N: 80-1005649-03[1], 80-1006709-02[2]	VDX 6730,16P,SFP+,AC, NON-PORT SIDE EXHAUST[4]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-16-R[3] P/N: 80-1005651-03[1], 80-1006711-02[2]	VDX 6730,16P,SFP+,AC, PORT SIDE EXHAUST[4]	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6730-24-F[3] P/N: 80-1005648-03[1], 80-1006708-02[2]	VDX 6730,24P,SFP+,AC, NON-PORT SIDE EXHAUST, SW-VDX-6730-24POD-01 LIC	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-24-R[3] P/N: 80-1005650-03[1], 80-1006710-02[2]	VDX 6730,24P,SFP+,AC, PORT SIDE EXHAUST, SW-VDX-6730-24POD-01 LIC	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-32-FCOE-F P/N: BR-VDX6730-24-F with BR-VDX6730-24VCS-01 and BR-VDX6730-24FCOE-01 License	VDX 6730, BUNDLE, 24P SFP+, 8 8G FC, VCS LIC, FCOE LIC, AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-32-FCOE-R P/N: BR-VDX6730-24-R with BR-VDX6730-24VCS-01 and BR-VDX6730-24FCOE-01 License	VDX 6730, BUNDLE, 24P SFP+, 8 8G FC, VCS LIC, FCOE LIC, AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6730-40-F[3] P/N: 80-1005680-03[1], 80-1006719-02[2]	VDX 6730,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-40-R[3] P/N: 80-1005681-03[1], 80-1006720-02[2]	VDX 6730,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-60-F[3] P/N: 80-1005679-03[1], 80-1006718-02[2]	VDX 6730,60P,SFP+,AC, NON-PORT SIDE EXHAUST, SW-VDX-6730-60POD-01 LIC, SWVDX-6730-60POD2-01 LIC	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-60-R[3] P/N: 80-1005678-03[1], 80-1006717-02[2]	VDX 6730,60P,SFP+,AC, PORT SIDE EXHAUST, SW-VDX-6730-60POD-01 LIC, SWVDX-6730-60POD2-01 LIC	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-76-FCOE-F P/N: BR-VDX6730-60-F with BR-VDX6730-60VCS-01 and BR-VDX6730-60FCOE-01 License	VDX 6730, BUNDLE, 60P SFP+, 16 8G FC, VCS LIC, FCOE LIC, AC, NON-PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195
SKU: BR-VDX6730-76-FCOE-R P/N: BR-VDX6730-60-R with BR-VDX6730-60VCS-01 and BR-VDX6730-60FCOE-01 License	VDX 6730, BUNDLE, 60P SFP+, 16 8G FC, VCS LIC, FCOE LIC, AC, PORT SIDE EXHAUST	NOS v4.0.1	XBR-000195

Table 4 Notes:

1. Serviceable assembly

2. Production assembly.

3. Serviceable and production assemblies are functionally equivalent. The part number assigned to each production assembly was created to support the release of updated logos and marks on the agency label.

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

Table 5 Validated VDX 6740 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6740-24-F P/N: 80-1007295-01	VDX6740,24-Port, AC, Non-port side exhaust[1]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6740-24-R P/N: 80-1007294-01	VDX6740, 24-Port, AC, Port side exhaust[1]	NOS v4.0.1	XBR-000195
SKU: BR-VDX6740-48-F P/N: 80-1007483-01	VDX6740,24-Port, AC, SW- VDX-24POD10G LIC, Non-port side exhaust	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6740-48-R P/N: 80-1007481-01	VDX6740, 48-Port, AC, SW-VDX-24POD10G LIC, Port side exhaust	NOS v4.0.1	XBR-000195

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6740-64-ALLSW-F P/N: 80-1007484-01	VDX6740,64-Port, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01,SWVDX-24POD10G and SW-VDX-4POD40G LIC, Non-port side exhaust	NOS v4.0.1	XBR-000195
SKU: BR-VDX6740-64-ALLSW-R P/N: 80-1007482-01	VDX6740,64-Port, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01,SWVDX-24POD10G and SW-VDX-4POD40G LIC, Port side exhaust	NOS v4.0.1	XBR-000195

Table 5 Notes:

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

Table 6 Validated VDX 6740T Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX-6740T-24-F P/N: 80-1007273-01	VDX 6740T, 24-Port, 10GB-T, AC, Non-port side exhaust[1]	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6740T-24-R P/N: 80-1007274-01	VDX 6740T, 24-Port, 10GB-T, AC, Port side exhaust[1]	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6740T-48-F P/N: 80-1007485-01	VDX 6740T, 48-Port, 10GB-T, AC, SW-VDX-24POD10G LIC, Non-port side exhaust	NOS v4.0.1	XBR-000195
SKU: BR-VDX-6740T-48-R P/N: 80-1007487-01	VDX 6740T, 48-Port, 10GB-T, AC, SW-VDX-24POD10G LIC Port side exhaust	NOS v4.0.1	XBR-000195
SKU: BR-VDX6740T-64-ALLSW-F P/N: 80-1007486-01	VDX6740T,64-Port, 10GB-T, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Non-port side exhaust	NOS v4.0.1	XBR-000195
SKU: BR-VDX6740T-64-ALLSW-R P/N: 80-1007488-01	VDX6740T,64-Port, 10GB-T, FCOE,AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Port side exhaust	NOS v4.0.1	XBR-000195

Table 6 Notes:

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

Table 7 Validated VDX 8770 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
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 v4.0.1	XBR-000195
SKU: BR-VDX8770-4-BND-DC P/N: 80-1006532-03	VDX 8770 4 I/O Slot chassis with three Switch Fabric Modules, one Management Module, two exhaust Fans and two 3000W DC PSU	NOS v4.0.1	XBR-000195
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 v4.0.1	XBR-000195
SKU: BR-VDX8770-8-BND-DC P/N: 80-1006533-03	VDX 8770 8 I/O Slot chassis with six Switch Fabric Modules, one Management Module, 4 exhaust Fans and three 3000W DC PSU	NOS v4.0.1	XBR-000195

The following Field Replaceable Units (FRU) [i.e. Power Supply Module, Filler Panel for Power Supply Slot, Fan Module, Switch Fabric Module, Management Module, Line Card Unit, Filler Panel for Line Card Slot, Half-Slot Filler Panel for Switch Fabric Module Slot or Management Module Slot] may be used within validated Brocade VDX 8770-4 and VDX 8770-8 configurations:

Table 8 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:80-1006539-02
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

Table 8 Components of the VDX 8770 continued

Component of the cryptographic boundary		SKU/MGF Part Number
	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 8 illustrate 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 lists the validated configurations for the VDX 6710-54.

Figure 2 VDX 6720-16 and VDX 6720-24

Table 3 lists the validated configurations for the VDX 6720-16 and VDX 6720-24[1].

Figure 3 VDX 6720-40 and VDX 6720-60

Table 3 lists the validated configurations for the VDX 6720-40 and VDX 6720-60[2].

---

[1] SW-VDX-6720-24POD-01 license enables additional ports

2 SW-VDX-6720-60POD-01 and SWVDX-6720-60POD2-01 licenses enable additional ports.

Figure 4 VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE

Table 4 lists the validated configurations for the VDX 6730-16, VDX 6730-24[3] and VDX 6730-32-FCOE[4].

Figure 5 VDX 6730-40, VDX 6730-60 and VDX 6730-76-FCOE

Table 4 lists the validated configurations for the VDX 6730-40, VDX 6730-60[5] and VDX 6730-76-FCOE[6].

Figure 6 VDX 6740-24, VDX 6740-48 and VDX 6740-64

Table 5 lists the validated configurations for the VDX 6740-24, VDX 6740-48[7] and VDX 6740-64[8].

Table 5 Notes:

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

---

[3] SW-VDX-6730-24POD-01 license enables additional ports.

[4] SW-VDX-6730-24POD-01, BR-VDX6730-24VCS-01 and BR-VDX6730-24FCOE-01 licenses enable additional ports and features.

[5] SW-VDX-6730-60POD-01 and SWVDX-6730-60POD2-01 licenses enable additional ports.

[6] SW-VDX-6730-60POD-01 and SWVDX-6730-60POD2-01, BR-VDX6730-60VCS-01 and BR-VDX6730-60FCOE-01 licenses enable additional ports and features.

[7] The SW-VDX-24POD10G license enables additional ports

[8] SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G licenses enable additional ports and features

Figure 7 VDX 6740T-24, VDX 6740T-48[9] and VDX 6740T-64[10]

Table 6 lists the validated configurations for the VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64.

Figure 8 VDX 8770-4 and VDX 8770-8[11]

Table 7 Validated VDX 8770 Configurations lists the hardware configurations for the VDX 8770-4 (Left) and VDX 8770-8 (Right). See Table 8 Components of the VDX 8770 for a list of installable VDX 8770 components.

1.1   Security Level Definitions

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

Table 9 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

2   Modes of Operation

2.1   FIPS Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware

Table 10 FIPS Approved Cryptographic Functions for the VDX 6710, VDX 6720 and VDX 6730

Label	Cryptographic Function	VDX 6710 VDX 6720 VDX 6730
AES	Advanced Encryption Algorithm	2283
Triple-DES	Triple Data Encryption Algorithm	1431
SHS	Secure Hash Algorithm	1965
HMAC	Keyed-Hash Message Authentication code	1399
RSA	Rivest Shamir Adleman Signature Algorithm	1358, 1359
RNG	Random Number Generator	1135
CVL	SP800-135 KDF	131

Table 11 FIPS Approved Cryptographic Functions for the VDX 8770

Label	Cryptographic Function	VDX 8770
AES	Advanced Encryption Algorithm	2285
Triple-DES	Triple Data Encryption Algorithm	1432
SHS	Secure Hash Algorithm	1966
HMAC	Keyed-Hash Message Authentication code	1400
RSA	Rivest Shamir Adleman Signature Algorithm	1358, 1359
RNG	Random Number Generator	1136
CVL	SP800-135 KDF	131

Table 12 FIPS Approved Cryptographic Functions for the VDX 6740 and VDX 6740T

Label	Cryptographic Function	VDX 6740	VDX 6740T
AES	Advanced Encryption Algorithm	2285	2285
Triple-DES	Triple Data Encryption Algorithm	1432	1432
SHS	Secure Hash Algorithm	1966	1966
HMAC	Keyed-Hash Message Authentication code	1400	1400

Label	Cryptographic Function	VDX 6740	VDX 6740T
RSA	Rivest Shamir Adleman Signature Algorithm	1356, 1357	1356, 1357
RNG	Random Number Generator	1136	1136
CVL	SP800-135 KDF	130	130

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

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

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman for SSHv2 (key agreement: key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman for FC-SP (key agreement: key establishment methodology provides 112 bits of encryption strength)
- MD5 (used for password hash, considered as plaintext)
- Non-deterministic random number generator for seeding ANSI X9.31 DRNG
- 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.
- Do not enable SNMPv3
- 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 2048.*
- *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.
  - o   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 2048 bits RSA LDAP CA certificate.

- If secure sys log is needed, import minimum 2048 bits RSA CA certificate. In FIPS 140-2 compliant state,
  - o Do not use FTP for following operations
  - o Config Upload
  - o Config Download
  - o Support Save
  - o FW Download
  - o Do not use outbound SSH and telnet commands (clients).
  - o With regards to SCP client on the switch, remote SCP server must employ RSA host keys with minimum length of 2048 bits and DH with minimum length of 2048 bit. FIPS 140-2 compliant ciphers (HMAC-SHA1 (mac), AES128-CBC, AES256-CBC) are enforced on the client side.

- The use of the "disable cipherconfig" command is not allowed in FIPS mode.
- Externally generated RSA key pairs shall only be imported if they are RSA 2048 and SHA-256.
- Do not expire Admin account.
- Do not enable Admin lockout.

NOTES:

1. Firmware packages are always signed at build time and validated during the firmware download 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-Approved 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 IP ACLs configuration.
- Confirm LDAP server's root CA certificate.

2.2 Non-Approved Mode of Operation

In non-Approved mode, an operator will have no access to CSPs used within the FIPS Approved mode. When switching from FIPS Approved mode to a non-Approved 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-Approved 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-Approved mode:

md2, md4, md5, rmd160

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

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

Macs: hmac-md5, hmac-sha-1, umac-64, hmac-ripemd160, hmac-sha1-96, hmac-md5-96

The following can only be used in the non-Approved mode of operation:

SNMPv3 KDF (non-compliant)

3   Ports and Interfaces

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

1. VDX 6710-54-F and VDX 6710-54-R

    a. 10 GbE (Qty. 6) Data Input, Data Output, Control Input, Status Output

    b. 1 GbE (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. USB (Qty. 1): Data Input, Data Output, Status Output

        •   Brocade USB flash device, XBR-DCX-0131

    f. Power Supply and Fan Assembly (Qty. 2)

        •   Assembly Connectors (Qty. 2): Power Input, Control Input

        •   Assembly Status LED (Qty. 2): Status Output

    g. Switch Status LEDs (Qty. 2): Status Output

        •   System Status (Qty. 1)

        •   System Power (Qty. 1)

2. VDX 6720-16-F, VDX 6720-16-R, VDX 6720-24-F and VDX 6720-24-R

    a. The VDX 6720-16 and VDX 6720-24 utilize the same hardware platform. Licensing is used to enable more than the base sixteen 10 GbE ports.

    b. Data Ports (Qty. 24) : Data Input, Data Output, Control Input, Status Output

        •   GbE SFP+ (Qty. 24)

    c. Management Ethernet Ports (Qty. 1): Control Input, Status Output

    d. RLO Management Ethernet Ports (Qty. 1): (Inactive)

    e. Serial port (Qty. 1): Control Input, Status Output

    f. USB (Qty. 1): Data Input, Data Output, Status Output

        •   Brocade USB flash device, XBR-DCX-0131

    g. Power Supply and Fan Assembly (Qty. 2)

        •   Assembly Connectors (Qty. 2): Power Input, Control Input

        •   Assembly Status LED (Qty. 2): Status Output

    h. Switch Status LEDs (Qty. 2): Status Output

        •   System Status (Qty. 1)

        •   System Power (Qty. 1)

3. VDX 6720-40-F, VDX 6720-40-R, VDX 6720-60-F and VDX 6720-60-R

    a. The VDX 6720-40 and VDX 6720-60 utilize the same hardware platform. Licensing is used to enable more than the base forty 10 GbE ports.

    b. Data Ports (Qty. 60): Data Input, Data Output, Control Input, Status Output

        •   GbE SFP+ (Qty. 60)

    c. Management Ethernet Ports (Qty. 1): Control Input, Status Output

d. RLO Management Ethernet Ports (Qty. 1): (Inactive)

e. Serial port (Qty. 1): Control Input, Status Output

f. USB (Qty. 1): Data Input, Data Output, Status Output

- Brocade USB flash device, XBR-DCX-0131
  g. Power Supply (Qty. 2)
    - Power Supply Connectors (Qty. 2): Power Input, Control Input
    - Power Supply Status LED (Qty. 2): Status Output
  h. Fan Assembly (Qty. 3)
    - Fan Tray Connectors (Qty. 3): Control Input
    - Fan Status LED (Qty. 3): Status Output
  i. Switch Status LEDs (Qty. 2): Status Output
    - System Status (Qty. 1)
    - System Power (Qty. 1)

4. VDX 6730-16-F, VDX 6730-16-R, VDX 6730-24-F, VDX 6730-24-R, VDX 6730-32-FCOE

  a. The VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE utilize the same hardware platform. Licensing is used to enable more than the base sixteen 10 GbE ports.
  b. Data Ports (Qty. 32): Data Input, Data Output, Control Input, Status Output
    - GbE SFP+ (Qty. 24)
    - 8G Fibre Channel (Qty. 8)
  c. Management Ethernet Ports (Qty. 1): Control Input, Status Output
  d. RLO Management Ethernet Ports (Qty. 1): (Inactive)
  e. Serial port (Qty. 1): Control Input, Status Output
  f. USB (Qty. 1): Data Input, Data Output, Status Output
    - Brocade USB flash device, XBR-DCX-0131
  g. Power Supply and Fan Assembly (Qty. 2)
    - Assembly Connectors (Qty. 2): Power Input, Control Input
    - Assembly Status LED (Qty. 2): Status Output
  h. Switch Status LEDs (Qty. 2): Status Output
    - System Status (Qty. 1)
    - System Power (Qty. 1)

5. VDX 6730-40-F, VDX 6730-40-R, VDX 6730-60-F, VDX 6730-60-R, VDX 6730-76-FCOE-F, VDX 6730-76-FCOE-R

  a. The VDX 6730-40, VDX 6730-60 and VDX 6730-76-FCOE utilize the same hardware platform. Licensing is used to enable more than the base forty 10 GbE ports.
  b. Data Ports (Qty. 72): Data Input, Data Output, Control Input, Status Output
    - GbE SFP+ (Qty. 60)
    - 8G Fibre Channel (Qty. 16)
  c. Management Ethernet Ports (Qty. 1): Control Input, Status Output
  d. RLO Management Ethernet Ports (Qty. 1): (Inactive)
  e. Serial port (Qty. 1): Control Input, Status Output
  f. USB (Qty. 1): Data Input, Data Output, Status Output
    - Brocade USB flash device, XBR-DCX-0131
  g. Power Supply (Qty. 2)
    - Power Supply Connectors (Qty. 2): Power Input, Control Input
    - Power Supply Status LED (Qty. 2): Status Output
  h. Fan Assembly (Qty. 3)
    - Fan Tray Connectors (Qty. 3): Control Input

- Fan Status LED (Qty. 3): Status Output

    i. Switch Status LEDs (Qty. 2): Status Output

- System Status (Qty. 1)

- System Power (Qty. 1)

6. VDX 6740-24-F, VDX 6740-24-R, VDX 6740-48-F, VDX 6740-48-R, VDX 6740-64-ALLSW-F, VDX 6740-64-ALLSW-R

    a. Data Port (Qty. 64): Data Input, Data Output, Control Input, Status Output

- 1G/10G SFP+ ports (Qty. 48) supporting both 1G and 10G data rates

    - Thirty-two of the forty-eight ports are 10G universal ports which can be configured as Ethernet ports (1G/10G) or Fiber Channel ports (8G/16G)

- QSFP ports (Qty. 4)

    - 40G QSFP ports can be used as a native 40G Ethernet port or as four 16G Fiber Channel ports

    b. Management Ethernet Ports (Qty. 1): Control Input, Status Output

    c. Serial port (Qty. 1): Control Input, Status Output

    d. USB (Qty. 1): Data Input, Data Output, Status Output

- Brocade USB flash device, XBR-DCX-0131

    e. Power Supply and Fan Assembly (Qty. 2)

- Assembly Connectors (Qty. 2): Power Input, Control Input

- Assembly Status LED (Qty. 2): Status Output

    f. LEDs: Status Output

- System Power LED (Qty. 1)

- System Status LED (Qty. 1)

- Power Supply and Fan Status LED (Qty. 2)

7. VDX 6740T-24-F, VDX 6740T-24-R, VDX 6740T-48-F, VDX 6740T-48-R, VDX 6740T-64-ALLSW-F, VDX 6740T-64-ALLSW-R

    a. Data Port (Qty. 64): Data Input, Data Output, Control Input, Status Output

- 1G/10G SFP+ ports (Qty. 48) supporting both 1G and 10G data rates

      o Thirty-two of the forty-eight ports are 10G universal ports which can be configured as Ethernet ports (1G/10G) or Fiber Channel ports (8G/16G)

- QSFP ports (Qty. 4)

      o 40G QSFP ports can be used as a native 40G Ethernet port or as four 16G Fiber Channel ports

    b. Management Ethernet Ports (Qty. 1): Control Input, Status Output

    c. Serial port (Qty. 1): Control Input, Status Output

    d. USB (Qty. 1): Data Input, Data Output, Status Output

- Brocade USB flash device, XBR-DCX-0131

    e. Power Supply and Fan Assembly (Qty. 2)

- Assembly Connectors (Qty. 2): Power Input, Control Input
- Assembly Status LED (Qty. 2): Status Output

    f. LEDs

- System Power LED (Qty. 1)

- System Status LED (Qty. 1)
- Power Supply and Fan Status LED (Qty. 2) 8.

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

- o   LEDs: Status Output
  - o   Power LED (Qty. 1)
  - o   Fault LED (Qty. 1)

NOTE: LEDs display power status and port activity status.

4   Identification and Authentication Policy

4.1   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 13 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. This role is able to load new firmware.	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

Table 14 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 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 15 Service Descriptions

Service Name	Description
User Management	User and password management.
Login Session Management	Controls the user session management,
LDAP	LDAP configuration functions.
FIPS	Control FIPS mode operation and related functions
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
System Monitor	Status configuration & monitoring
FCSP	Fibre Channel Security Protocol
Zeroize	Destroy CSPs
Switch Connection Policy	Switch connection policy

5   Access Control Policy

5.1   Roles and Services

Table 16 Services Authorized for Roles

SERVICE ROLE	User	Admin	Maximum Permissions	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 / LDAP-server		X	X	X
Terminal Configuration		X	X	
Ethernet		X	X	
License		X	X	
VCS		X	X	
vCenter		X	X	
System Monitor		X	X	
FCSP		X	X	
Switch Connection Policy		X	X	

5.2   Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

5.3   Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Note: Zeroization can be performed by session termination or by issuing command "fips zeroize".

- o DH Private Keys for use with 2048 bit modulus in SSHv2
  - • Used in SSH to establish a Shared Secret
- o SSH/SCP/SFTP Session Keys- 128 and 256 bit AES CBC
  - • AES encryption key used to secure SSH/SCP/SFTP sessions
- o SSH/SCP/SFTP Authentication Key (HMAC-SHA-1)
  - • Session Authentication Key used to authenticate and provide integrity of SSH sessions
- o SSH KDF Internal State
  - • Used to generate encryption and Authentication Key
- o SSH DH Shared Secret Key
  - • 2048 bit keys used in SSH KDF to derive Session Keys
- o SSH 2048 RSA Private Key
  - • Used to authenticate SSH server to client
- o TLS Private Key (RSA 2048)
  - • RSA key used to establish TLS sessions
- o TLS Pre-Master Secret
  - • Secret value used to establish the Session and Authentication Key
- o TLS Master Secret
  - • Secret value used to establish the Session and Authentication Key
- o TLS PRF Internal State
  - • Values of the PRF Internal HMAC-SHA-1 and HMAC-MD5
- o TLS Session Keys – 128 , 256 bit AES CBC, TDES 3 key CBC
  - • TDES or AES key used to secure TLS sessions
- o TLS Authentication Key for HMAC-SHA-1
  - • HMAC-SHA-1 key used to provide data authentication for TLS sessions
- o Approved RNG Seed Material
  - • ANSI X9.31 DRNG seed key
- o ANSI X9.31 DRNG Internal State
  - • DRNG Internal state
- o Passwords
  - • Passwords used to authenticate operators (8 to 40 characters)
- o DH Keys for 2048 bit modulus in FC-SP
  - • Used to establish a Shared Secret

5.4 Definition of Public Keys:

The following are the public keys contained in the module:

- o SSH DH Public Key (2048 bit modulus)
- o SSH DH Peer Public Key (2048 bit modulus)
- o DH Keys for 2048 bit modulus in FC-SP
- o TLS v1.0 Public Key (RSA 2048)
- o TLS v1.0 Peer Public Key (RSA 2048)
- o Firmware Download Key (RSA 2048 SHA 256)
- o LDAP ROOT CA certificate (RSA 2048)
- o SSH RSA 2048 bit Public Key
- o SSH RSA 2048 bit host key

5.5   Definition of Service Categories:

Table 17 Services and Command Line Instructions (CLI)

Services	CLIs
PKI	Certutil
Firmware Management	Firmware
User Managment	Username role password-attributes rule encryption-level unlock
Login Session Management	tacacs-server ldap-server aaa logout banner ssh telnet
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
System Monitor	system-monitor system-monitor-mail threshold-monitor
FCSP	Fcsp
Switch connection policy	secpolicy

Table 18 CSP Access Rights within Roles & Services

	SSH and SCP CSPs[12]	TLS CSPs[13]	RNG Seed Key[14]	Passwords	FCSP Secret	SSH RSA 2048 Public Key
Login Session Management	N	N	N	RW	N	N
Zeroize	Z	Z	Z	Z	Z	N
Firmware Management	R	N	N	N	N	N
PKI	RW	N	N	N	N	RW
User Management	N	N	N	RW	N	N
FCSP	N	N	N	N	RW	N

6   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 2048 with SHA-256 digest may be executed.

6.1   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) Three Key Triple-DES CBC KAT (encrypt/decrypt)

      (2) AES (128, 192, 256) CBC KAT (encrypt/decrypt)

      (3) HMAC SHA-1 KAT

      (4) ANSI X9.31 DRNG KAT

      (5) SHA-1 KAT

---

[12] Includes the following CSPs: DH Private Keys for use with 2048 bit modulus in SSHv2; SSH/SCP/SFTP Session Keys- 128, 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

[13] Includes the following CSPs: TLS Private Key (RSA 2048); TLS Pre-Master Secret; TLS Master Secret; TLS PRF Internal State; TLS Session Key – 128 bit AES; TLS Authentication Key for HMAC-SHA-1

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

    (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 2048 SHA 256 Sign/Verify KAT

    (9) SP800-135 SSH KDF KAT

    (10) SP800-135 TLS KDF 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 2048 SHA- 256 Pairwise Consistency Test (Sign/Verify & Encrypt/Decrypt)

    iii. Firmware Load Test (RSA 2048 SHA-256 Signature Verification)

    iv. Bypass Test: N/A

    v. 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. The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.

10. In the event of a self-test or conditional test failure, the operator will see the following message: "<Algorithm under test>...FAILED!"

7   Physical Security Policy

7.1   Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:
- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals.

7.2   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 19 Inspection/Testing of Physical Security Mechanisms

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

8   Mitigation of Other Attacks Policy

These modules have not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

9   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

KDF   Key Derivation Function

LED   Light Emitting Diode

LDAP   Lightweight Directory Access Protocol

LIC   License

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 Evident Seal Application Procedures

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.

NOTICE: After performing the tamper evident seal application procedures as defined below, the removal of any tamper seal from the cryptographic boundary is explicitly prohibited by this Security Policy. The cryptographic module does not support a maintenance role or a maintenance interface.

Therefore, any such removal of a tamper evident seal from the cryptographic boundary (including but not limited to the removal of a seal from a component described in this Security Policy as "field replaceable") is an explicit violation of the Security Policy.

Removal of a tamper evident seal results in an instantaneous invalidation of the cryptographic module, deeming said module no longer FIPS validated and incapable of being placed back into FIPS mode thereafter in perpetuity; such a cryptographic module shall be zeroized, immediately removed from service and immediately returned to Brocade.

Applying seals to the Brocade VDX 6710-54

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6710-54. See Figure 9 and Figure 10 for details on how to position each seal.
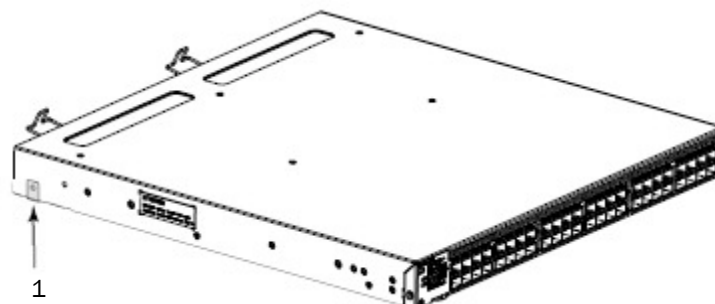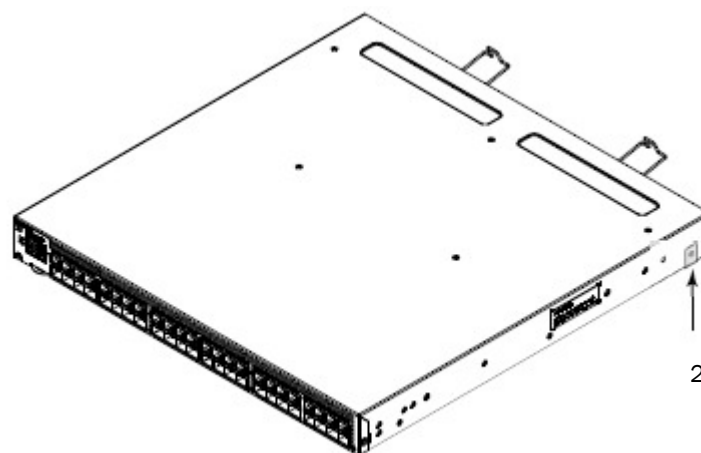

Figure 9 VDX 6710-54 left side seal location

Figure 10 VDX 6710-54 right side seal location

Applying seals to the Brocade 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 11 and Figure 12 for details on how to position each seal.
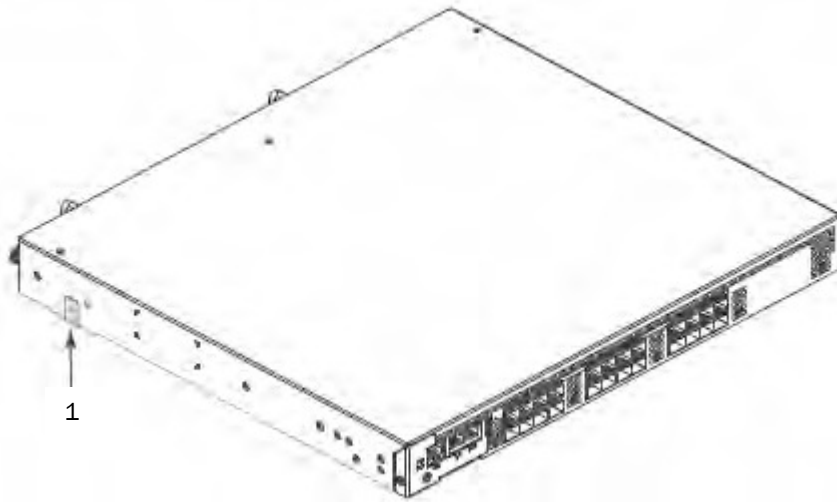

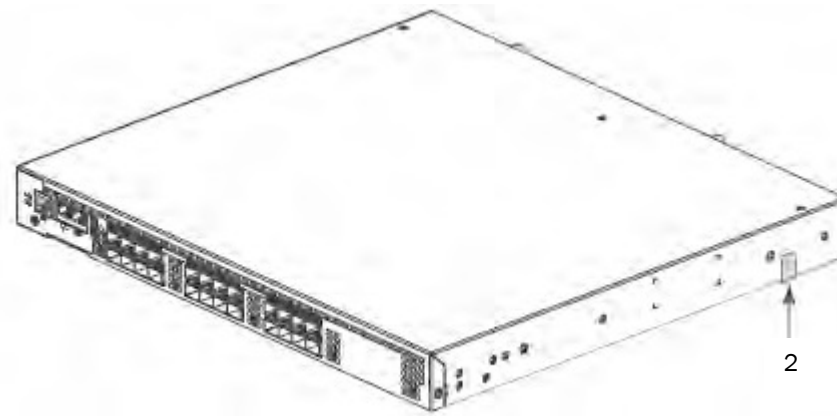**Figure 11 VDX 6720-16 and VDX 6720-24 left side seal location**

Figure 12 VDX 6720-16 and VDX 6720-24 right side seal location

Applying seals to the Brocade 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 13 and Figure 14 for details on how to position each seal.

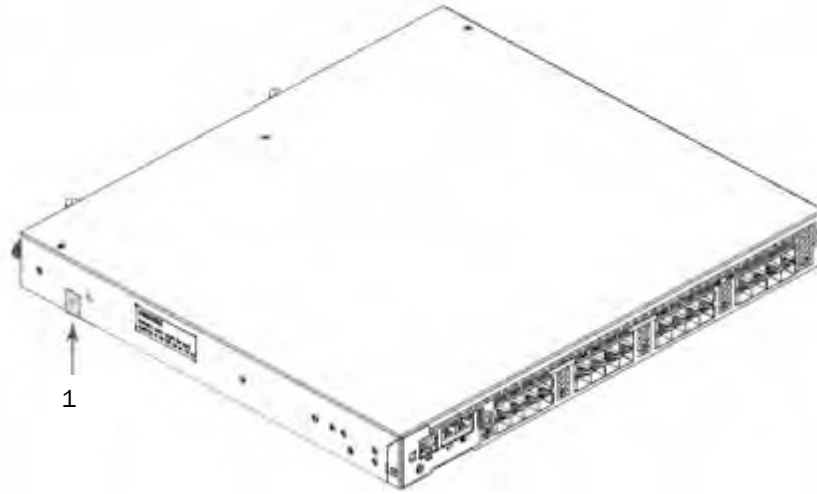**Figure 13 VDX 6720-40 and VDX 6720-60 left side seal location**

Figure 14 VDX 6720-40 and VDX 6720-60 right side seal location

Applying seals to the Brocade VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE. See Figure 15 and Figure 16 for details on how to position each seal.

Figure 15 VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE left side seal location
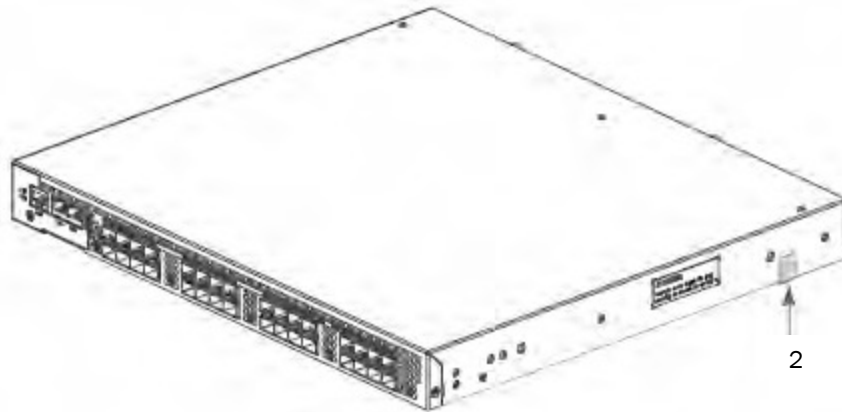

Figure 16 VDX 6730-16, VDX 6730-24 and VDX 6730-32-FCOE right side seal location

Applying seals to the Brocade VDX 6730-40, VDX 6730-60 and VDX 6730-72-FCOE

Two (2) tamper evident seals are required to complete the physical security requirements for the VDX 6730-40, VDX 6730-60 and VDX 6730-72-FCOE. See Figure 17 and Figure 18 for details on how to position each seal.
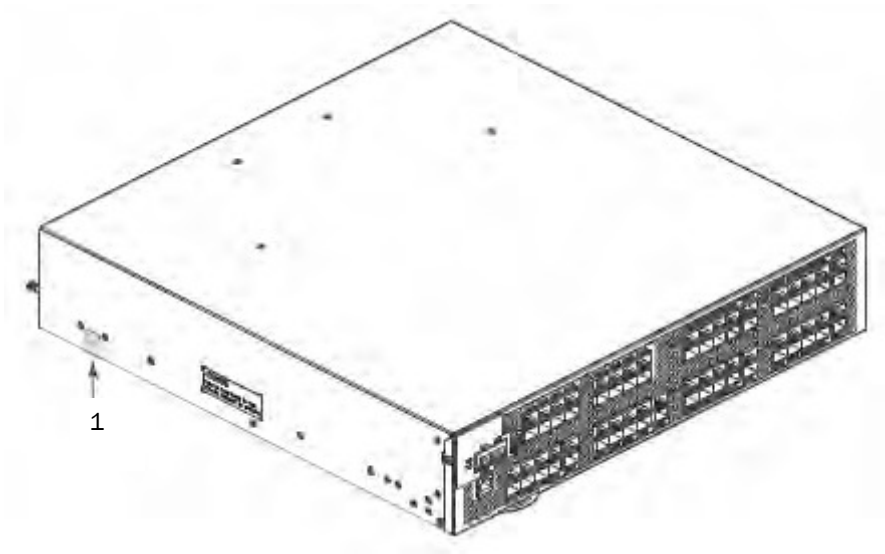

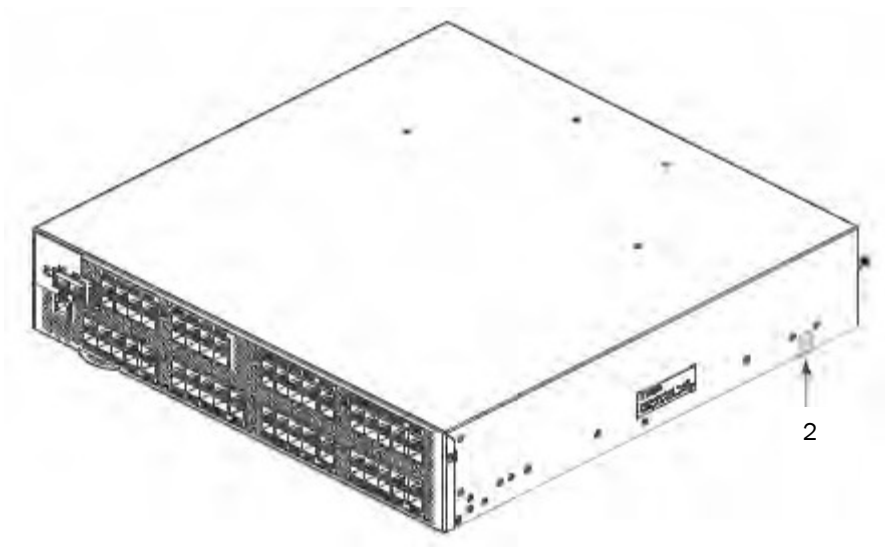**Figure 17 VDX 6730-40, VDX 6730-60 and VDX 6730-72-FCOE left side seal location**

Figure 18 VDX 6730-40, VDX 6730-60 and VDX 6730-72-FCOE right side seal location

Applying seals to the Brocade VDX 6740

Twenty (20) tamper evident seals are required to complete the physical security requirements for the –R and –F configurations of the BR-VDX 6740-24, BR-VDX 6740-48 and BR-VDX 6740-64-ALLSW. See Figure 19 through Figure 23 for details on how to position each seal.

1. Apply one (1) seal over the screws along the bottom port side surface of the chassis. Five (5) seals, 1 to 5, are required to complete this step. See Figure 19 for details on how to position each seal.

2. Apply three (3) seals, 6 to 8, across the seam between the left side of the top cover and the bottom side of the chassis. Each seal must wrap across a 90 degree angle from the bottom of the chassis to the side of the top cover.   See Figure 20 on how to position each seal.

3. Apply three (3) seals, 9 to 11, across the seam between the right side of the top cover and the bottom of the chassis. Each seal must wrap across a 90 degree angle from the bottom of the chassis to the side of the top cover.   See Figure 21 on how to position each seal.

4. Six (6) seals, 12 to 17, are required to complete this step. Seals 13, 14 and16 must wrap across a 90 degree angle from the top of the chassis to the external surface of the combination power supply and fan module. Seals 15 and 17 must wrap across a 90 degree angle from the bottom of the chassis to the external surface of the combination power supply and fan module.   Seal 12 bridges the seam between the chassis the combination power supply and fan module on the left side of the non-port side of the chassis. See Figure 22 for details on how to position each seal.

5. Apply one (1) seal over the screws along the top port side surface of the chassis. Three (3) seals, 18 to 20, are required to complete this step. See Figure 23 for details on how to position each seal.
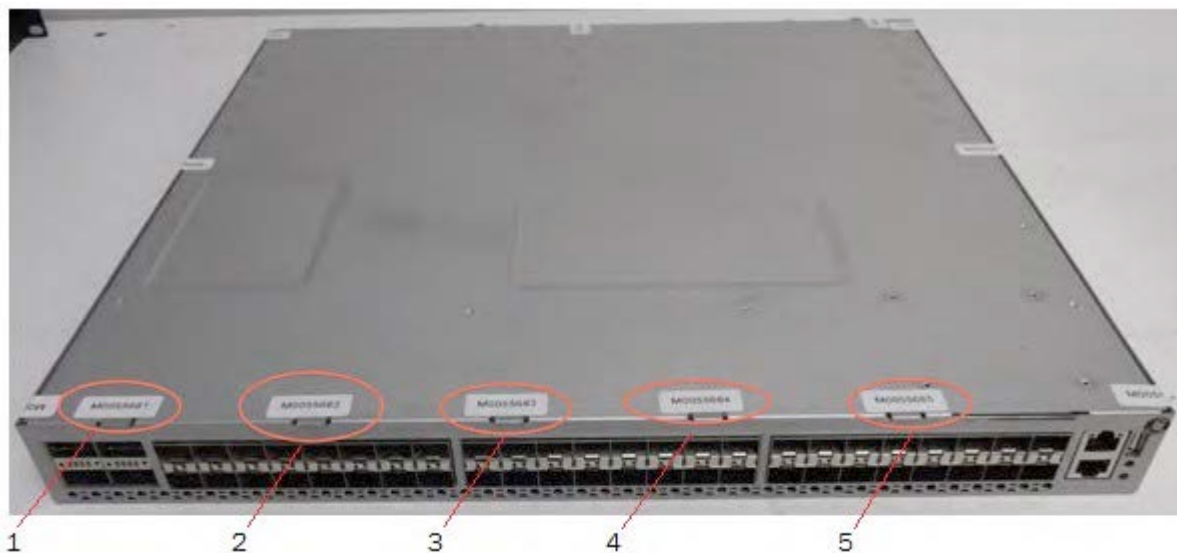

Figure 19 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom port side seal locations

Figure 20 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom left side seal locations

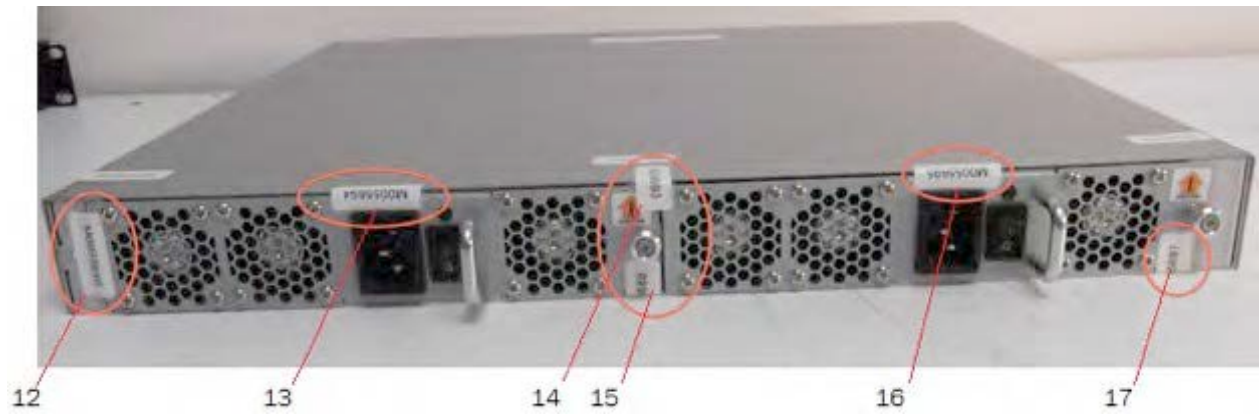**Figure 21 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom right side seal locations**

Figure 22 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW top non-port side fan and power supply seal locations
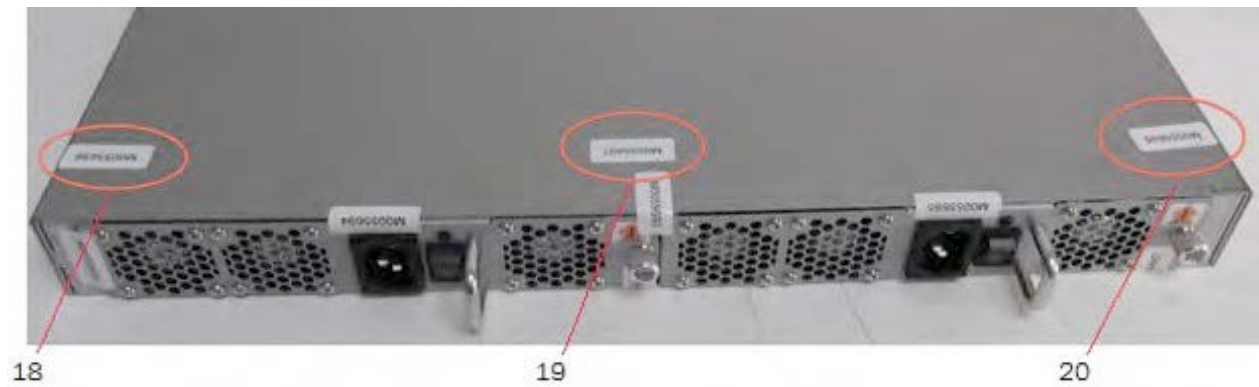

Figure 23 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW top non-port side top cover seal locations

Applying seals to the Brocade VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64

Twenty Nine (29) tamper evident seals are required to complete the physical security requirements for the VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64. See Figure 24 through Figure 28 for details on how to position each seal.

Figure 24 VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64 bottom/front seal locations

Figure 25 VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64 bottom left side seal locations

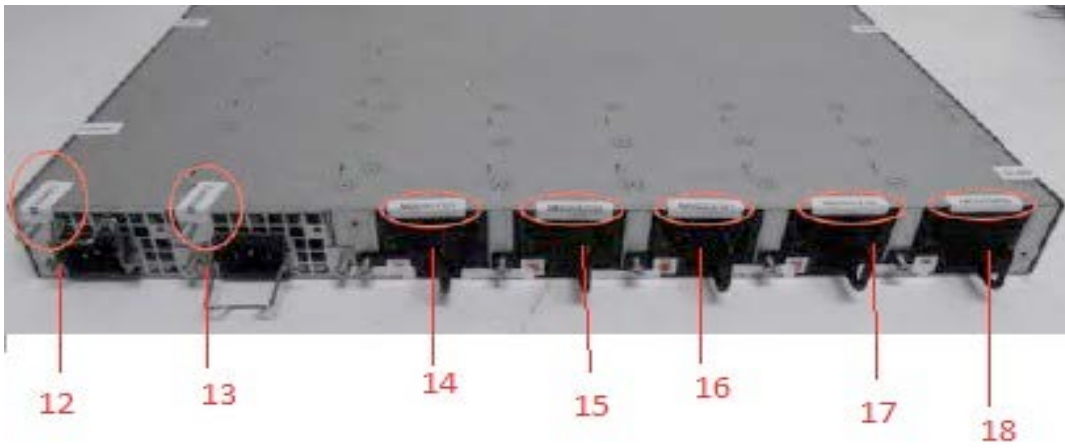**Figure 26 VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64 bottom right side seal locations**

Figure 27 VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64 bottom back side seal locations
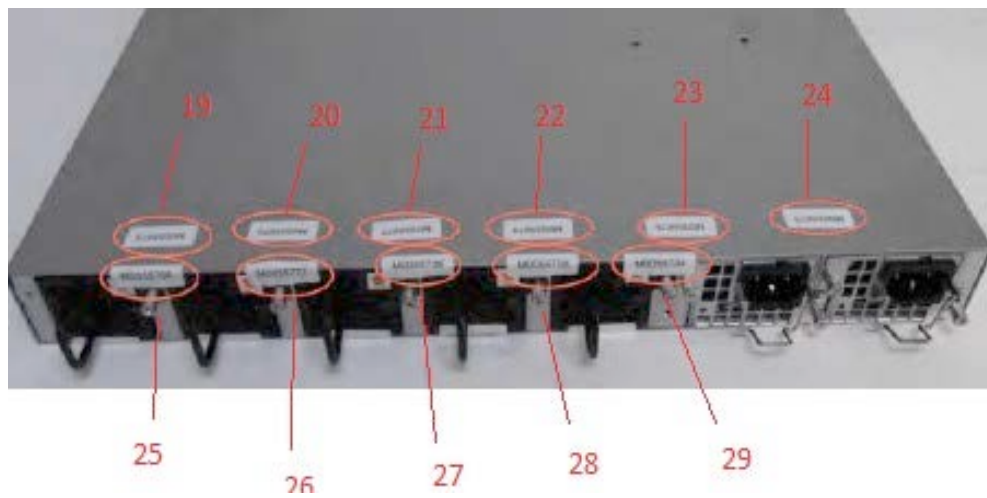

Figure 28 VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64 top back side seal locations

Applying seals to the Brocade VDX 8770-8 with AC and DC Power Supply

Thirty-six (36) tamper evident seals are required to complete the physical security requirements illustrated in Figure 29 to Figure 31.

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

Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 29. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

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 29A, 29C, 29D and 29E 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 29B and 29E 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 29E and 29G for details on how to position each seal.

4. Apply two (2) seals 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 29E, 29F and 29H for details on how to position each seal.

5. For VDX 8770-8 with AC Power Supply Units (PSU) see Figures 29E and 29F for details on how to position seals 14-17. Four (4) seals are required to complete this step.

6. See Figure 29E and 29H for details on how to position seals 21-26. Six (6) seals are required to complete this step.
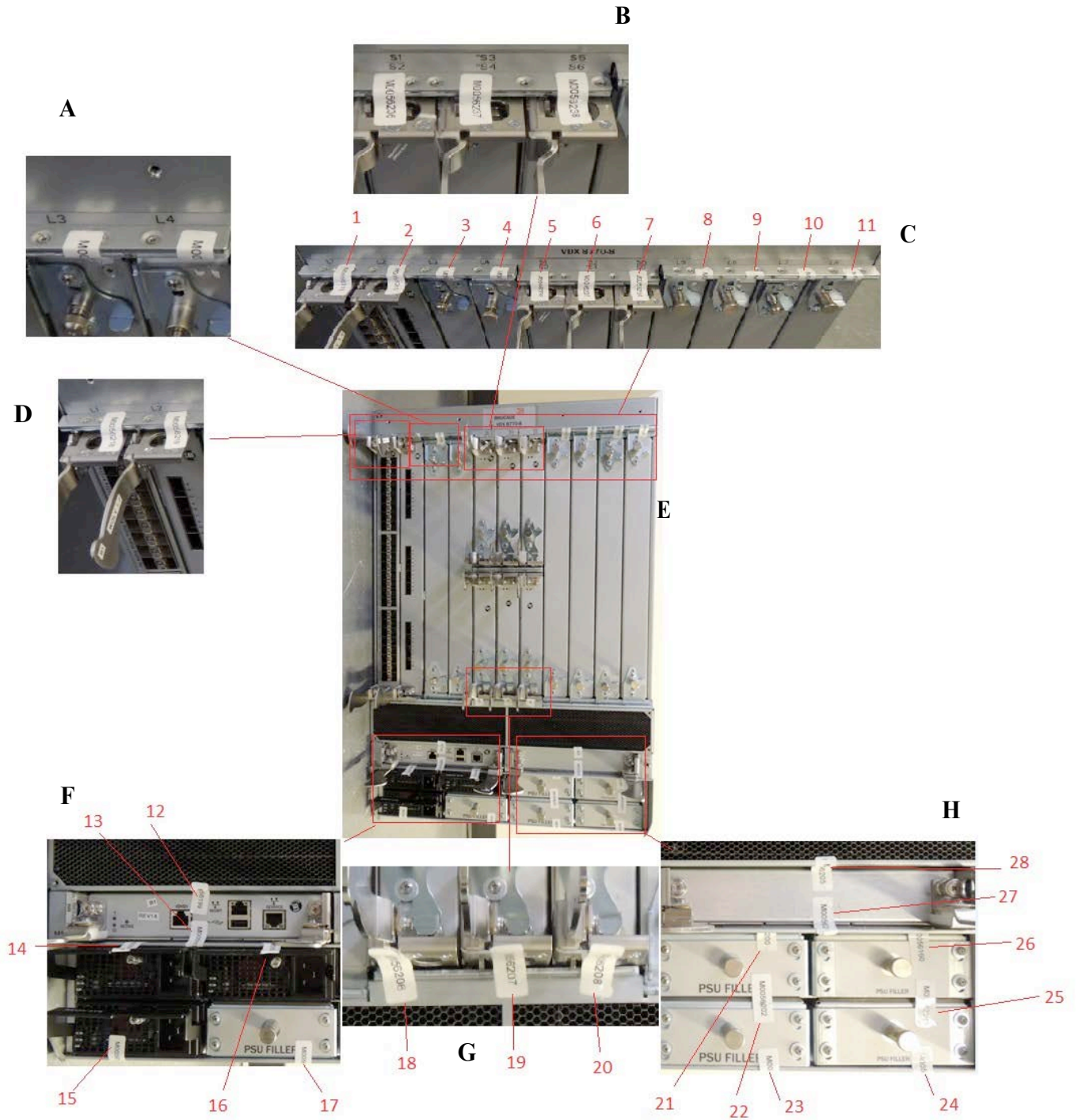
Figure 29 Brocade VDX 8770-8 AC port side seal locations

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

Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 30. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

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 30A, 30C, 30D and 30E 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 30B and 30E 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 30E and 30H for details on how to position each seal.

4. Apply two (2) seals 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 30E, 30F and 30I for details on how to position each seal.

5. For VDX 8770-8 with DC Power Supply Units (PSU) refer to Figures 30E, 30F and 30G for details on how to position seals 14-17. Four (4) seals are needed to complete this step.

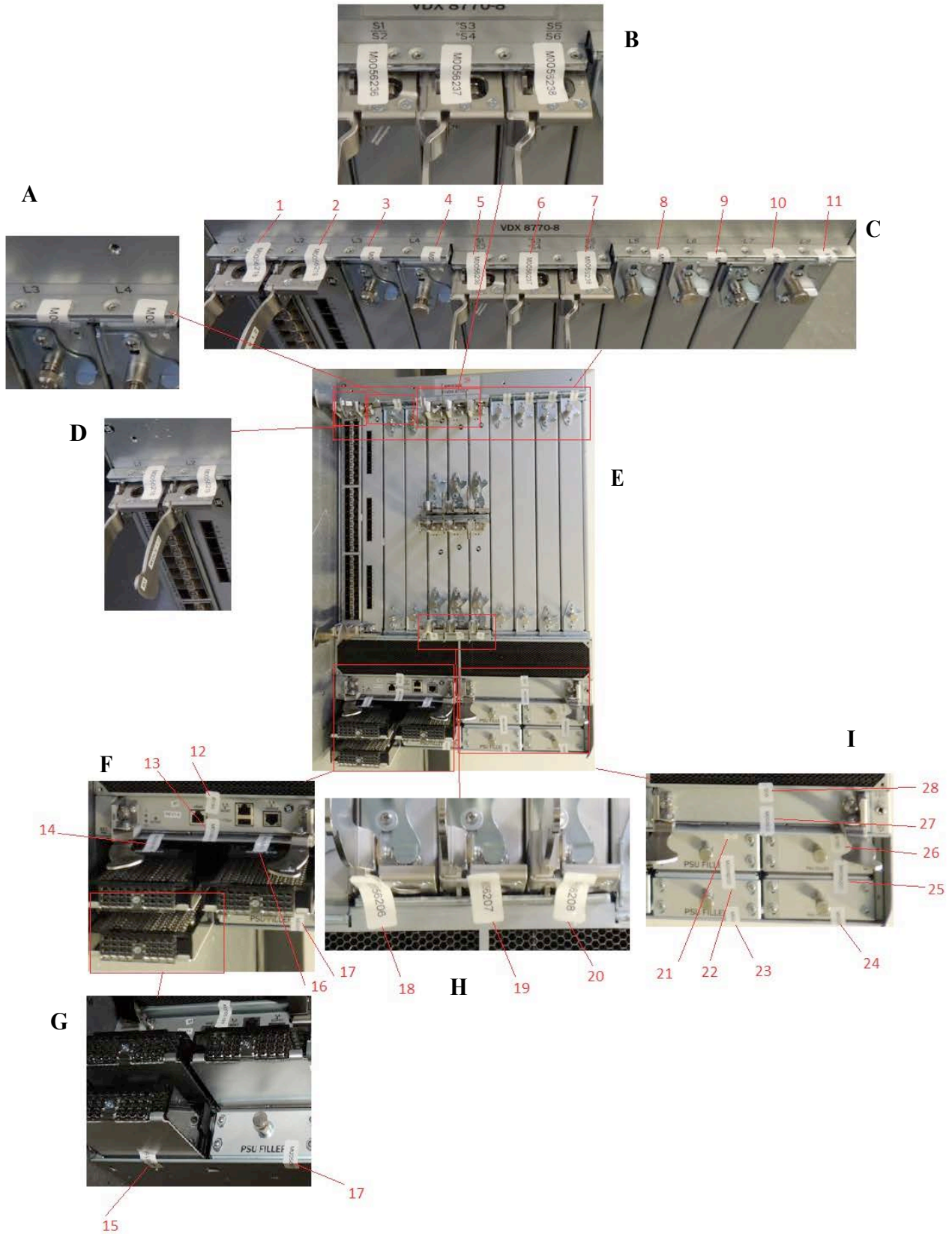6. See Figures 30E and 30I on how to position seals 21-26. Six (6) seals are required to complete this step.

Figure 30 Brocade VDX 8770-8 DC PSU seal locations

VDX 8770-8 Non-Port Side Tamper Evident Seal Application Procedure for AC and DC modules

Eight (8) tamper evident seals are required to complete the physical security requirements illustrated in Figure 31. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.
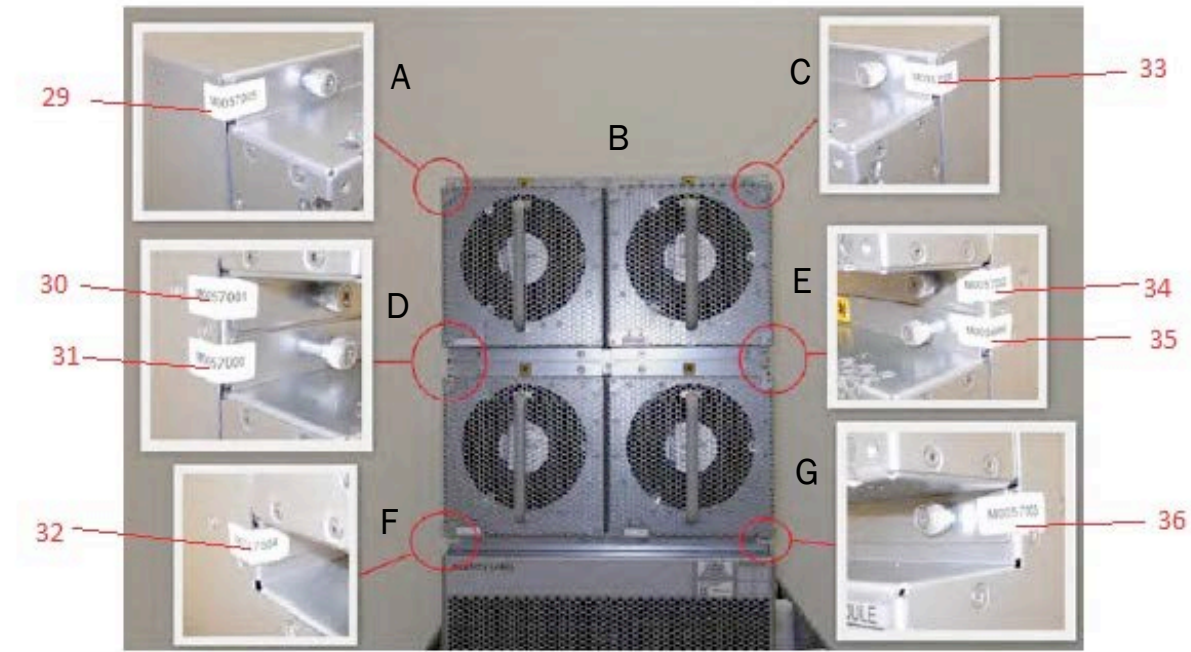

Figure 31 Brocade VDX 8770-8 non-port side seal locations

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 Figure 31A-G for details on how to position each seal.

Applying seals to the Brocade VDX 8770-4

Twenty-three (23) tamper evident seals are required to complete the physical security requirements illustrated in Figure 32, Figure 33, Figure 34 and Figure 35.

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 32 and Figure 33. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.
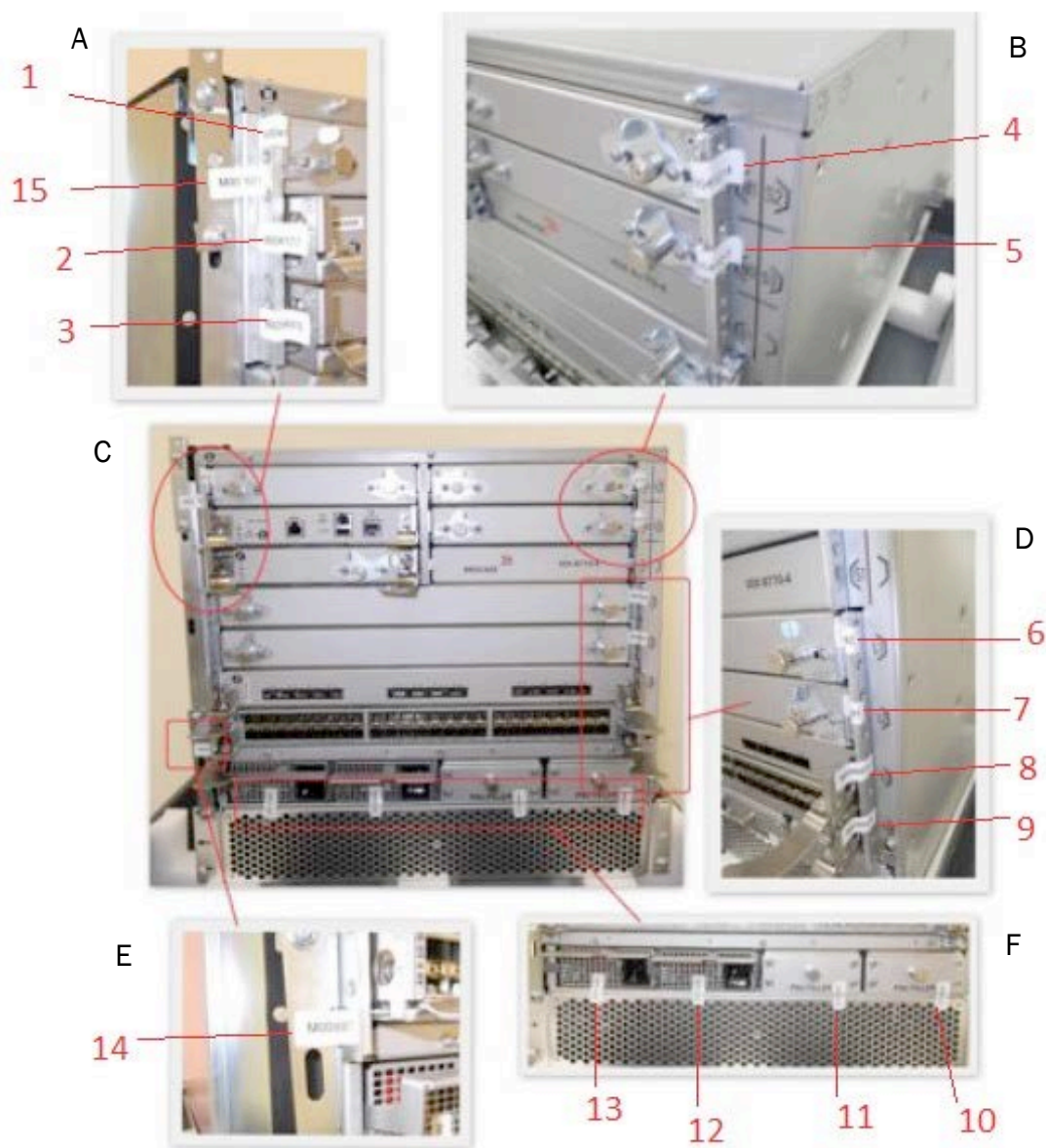

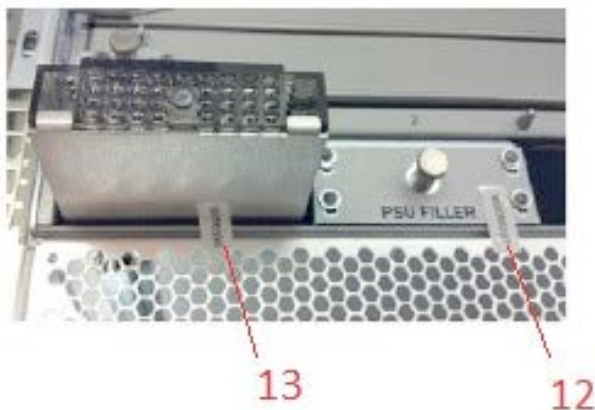**Figure 32 Brocade VDX 8770-4 port side seal locations**

Figure 33 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 32A and 32C 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 32B and 32C 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 Figure 32C and 32D 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 32C and 32F 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. PSU filler panels are installed in slot P2. Four (4) seals are required to complete this step. See Figure 33--seals 12 and 13, Figure 32C and 32F--seals 10 and 11 for how to position the labels.

5. Apply one (1) seal on each FIPS bracket. The upper left FIPS bracket is shown in Figure 32A and 32C. The lower left FIPS bracket is shown in Figure 32C and 32E. Two (2) seals are required to complete this step. See Figure 32A, 32C and 32E 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 34. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.
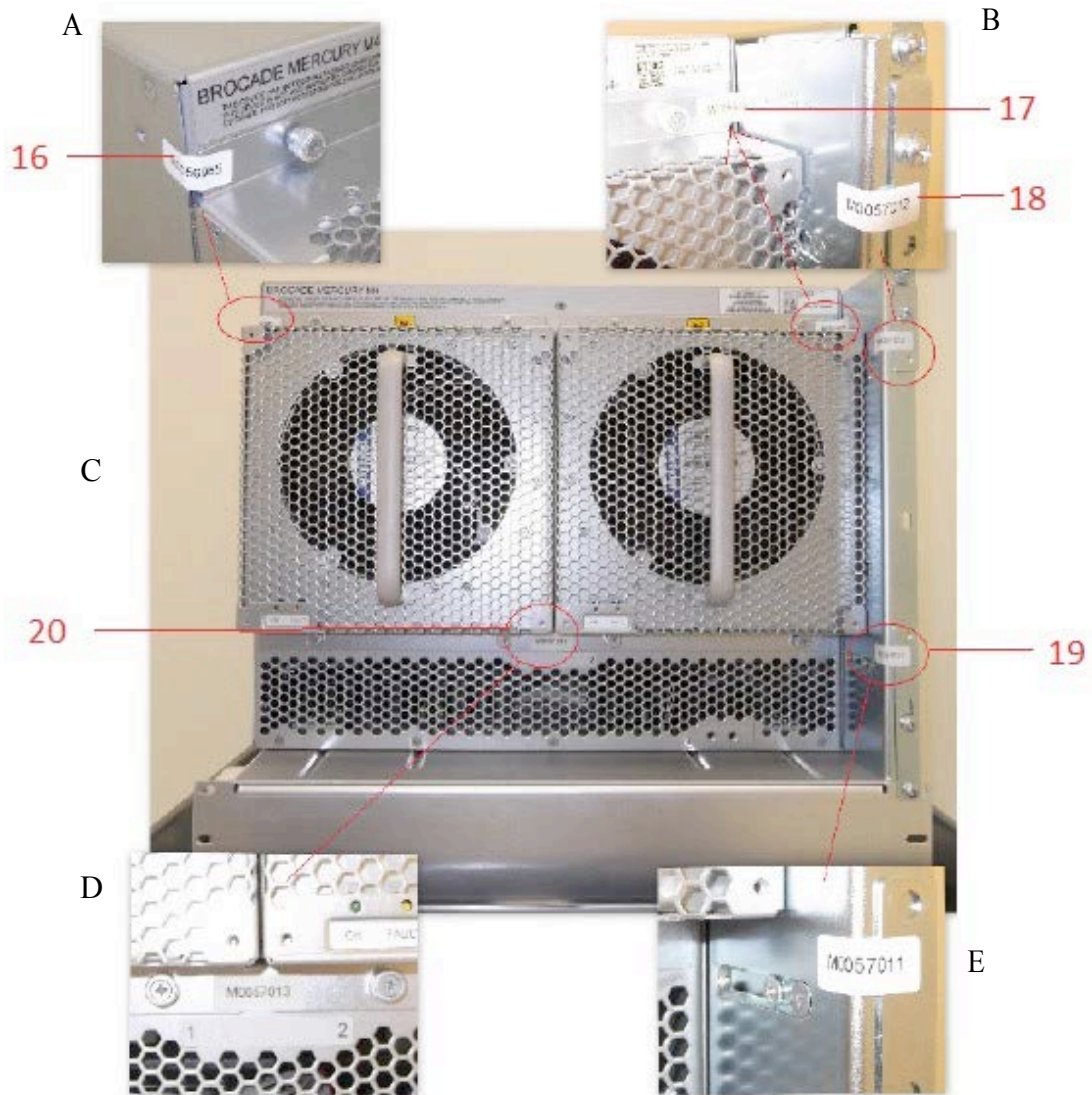
Figure 34 Brocade VDX 8770-4 Non-port side seal locations

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 Figure 34A, 34B and 34C 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 Figure 34C and 34D 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 34B and 34C. The lower right FIPS bracket is shown in Figure 34C and 34E. Two (2) seals are required to complete this step. See Figure 34B, 34C and 34E 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 35. Relative to the port side of the VDX 8770-4 chassis the air duct is secured to the left side of the chassis.
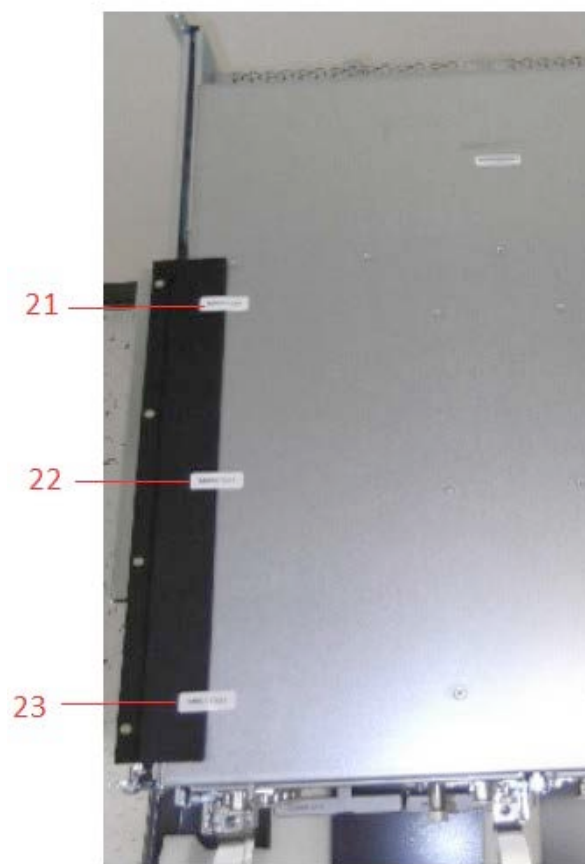

Figure 35 Brocade VDX 8770-4 Air Duct side seal locations

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 Figure 35 for details on how to position each seal.