BROCADE

VDX 6710, VDX 6720, VDX 6730 with Network OS v2.1.0 Firmware Security Policy

Document Version 2.0

Brocade Communications

August 29, 2012

Table of Contents

Table of Tables

Table of Figures

1. Module Overview

The VDX 6710, VDX 6720 and VDX 6730 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. Power supply /fan assemblies are not 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 FIPS Kit (Part Number: 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) v2.1.0	63-1000931-01

Table 2 Validated Hardware Configurations

Module Label	Part Number	Product Description	Firmware	FIPS Kit
VDX6710-54-F	80-1004843-02	VDX6710,48P GBE,6P SFP+,AC, NON-PORT SIDE EXHAUST[1]	NOS v2.1.0	All modules with FIPS Kit (Part Number: Brocade XBR-000195
VDX6710-54-R	80-1004702-02	VDX6710,48P GBE,6P SFP+,AC, PORT SIDE EXHAUST[1]	NOS v2.1.0	
VDX6720-16-F	80-1004566-05	VDX6720,16P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-16-R	80-1004567-05	VDX6720,16P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-24-F	80-1004564-05	VDX6720,24P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-24-R	80-1004565-05	VDX6720,24P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-40-F	80-1004570-05	VDX6720,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-40-R	80-1004571-05	VDX6720,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-60-F	80-1004568-05	VDX6720,60P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6720-60-R	80-1004569-05	VDX6720,60P SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-16-F	80-1005649-01	VDX6730,16P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-16-R	80-1005651-01	VDX6730,16P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-24-F	80-1005648-01	VDX6730,24P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-24-R	80-1005650-01	VDX6730,24P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-40-F	80-1005680-01	VDX6730,40P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-40-R	80-1005681-01	VDX6730,40P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-60-F	80-1005679-01	VDX6730,60P,SFP+,AC, NON-PORT SIDE EXHAUST	NOS v2.1.0	
VDX6730-60-R	80-1005678-01	VDX6730,60P,SFP+,AC, PORT SIDE EXHAUST	NOS v2.1.0	

Table Notes

1. 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.

Figure 1 through Figure 5 illustrate the cryptographic module configurations. For each module, power supplies and fan assemblies are not within cryptographic boundary.

Figure 1 Brocade VDX 6710-54 Switch (80-1004843-02, 80-1004702-02)

Figure 2 Brocade VDX 6720-16 (80-1004566-05, 80-1004567-05) and Brocade VDX 6720-24[1] (80-1004564-05, 80-1004565-05)

Figure 3 Brocade VDX 6720-40 (80-1004570-05, 80-1004571-05) and Brocade VDX 6720-60[2] (80-1004568-05, 80-1004569-05)

Figure 4 Brocade VDX 6730-16 (80-1005649-01, 80-1005651-01) and Brocade VDX 6730-24[3] (80-1005648-01, 80-1005650-01)

[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
[3] SW-VDX-6730-24POD-01 license enables the upper eight ports

Figure 5 Brocade VDX 6730-40 (80-1005680-01, 80-1005681-01) and Brocade VDX 6730-60[4] (80-1005679-01, 80-1005678-01)

2. Security Level

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

Table 3 Module Security Level Specification

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

3. Modes of Operation

Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware

- Triple-DES (Cert. #652)
- AES (Cert. #731,#1595)
- SHA-1 (Cert. #749)
- SHA-256 (Cert. #749)
- SHA 512 (Cert.#1407)
- HMAC SHA-1 (Cert #397,#933)
- HMAC SHA 256 (Cert. #397,#933)
- HMAC SHA 512 (Cert. #933)
- RNG (Cert. #426)

[4] SW-VDX-6730-60POD-01 and SWVDX-6720-60POD2-01 licenses enable the upper twenty ports

- RSA (Cert #342, #778)

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 (key agreement; key establishment methodology provides 80 or 112 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

The cryptographic module may be configured for FIPS 140-2 mode via execution of the following procedure. For further information, review the FIPS support information in Chapter 9 of the Network OS Administrator's Guide (53-1002339-01).

1. Install removable front cover (as applicable) and apply tamper labels
2. Login as authorized user with admin role.
3. If the system is not in standalone mode, configure it in standalone mode.
4. Disable Boot PROM Access.
5. 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), Triple-DES-CBC, AES128-CBC, AES192-CBC, AES256-CBC) for SSH.

1. Disable root access.
2. If TACACS+ is configured, then remove the configuration.
3. If dot1x is configured, disable it.
4. Enable FIPS 140-2 Self tests i.e. Execute 'fips selftests'
5. Execute 'fips zeroize' (automatically reboot(s) the system).
6. 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, HTTPS, Telnet and some ports of Brocade internal servers 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.
7. Note: Consult 2.1.0 FIPS admin manual for the specific port numbers.
8. For LDAP authentication, import only RSA 1024 LDAP CA certificate.
9. For Radius authentication, configure the Radius server with PEAP-MSCHAPv2 mode and shared secret.
10. In FIPS 140-2 compliant state, do not use FTP for following operations
    a. Config Upload
    b. Config Download
    c. Support Save
    d. FW Download

NOTE: Firmware packages are always signed at build time and validated during the firmwaredownload operation.

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

1. Display the status of self tests, and root account
2. Display the status of bootprom access
3. Display of cipherset configuration
4. Display of radius-server configuration.
5. Display of IP ACLs configuration.
6. 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 (by calling "fips zeroize") the module's plaintext CSPs.

The following cipher suites are allowed in non-FIPS mode for configuring SSL and TLS: aes-128-cbc,aes-128-ecb,aes-192-cbc,aes-192-ecb,aes-256-cbc,aes-256-ecb,bf,bf-cbc,bf-cfb,bf-ecb,bf-ofb,cast,cast-cbc,cast5-cbc,cast5-cfb,cast5-ecb,cast5-ofb,des,des-cbc,des-cfb,des-ecb,des-ede,des-ede-cbc,des-ede-cfb,des-ede-ofb,des-ede3,des-ede3-cbc,des-ede3-cfb,des-ede3-ofb,des-ofb,des3,desx,rc2,rc2-40-cbc,rc2-64-cbc,rc2-cbc,rc2-cfb,rc2-ecb,rc2-ofb,rc4,rc4-40

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

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

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

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

4. Ports and Interfaces

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

1. VDX6710-48-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. VDX6720-24-F and VDX6720-24-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. VDX6720-60-F and VDX6720-60-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. VDX6730-24-F and VDX6730-24-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. VDX6730-60-F and VDX6730-60-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

    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 40 characters. The password is an alphanumeric string of eight to 40 characters randomly chosen from the 96 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the context of the module. At the end of a session, the operator must log-out.
Sixty-four concurrent operators are allowed on the switch.

Table 4 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	Role -based operator authentication	RADIUS Shared Secret

authenticates to the cryptographic module.		

Table 5 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 is 16. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Table 6 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
FirmwareManagement	Control firmware management.
PKI	Import LDAP root CA certificate.
Clock Management	Clock and Timezone Management
Debug & Diagnostics	Debug & Diagnostics tools.
CLI Mgmt	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 7 Services Authorized for Roles

	User	Admin	Maximum Permissions	RADIUS	LDAP
Login Session Management		X	X		
FIPS		X	X		
Zeroize		X	X		
FirmwareManagement	X	X	X		
PKI	X	X	X		
Login Session Management / radius-server		X	X	X	
Login Session Management / ldap-server		X	X		X
UserManagement		X	X		
Clock Management		X	X		
Debug & Diagnostics		X	X		
CLI Mgmt		X	X		
Platform		X	X		
Display		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		

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

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

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- DH Private Keys for use with 1024 bit or 2048 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
- 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

Definition of Public Keys:

The following are the public keys contained in the module:

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

Definition of Service Categories:

Table 8 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
PKI	Certutil
Firmware Management	Firmware
Fips	ips selftests cipherset prom-access
Zeroize	fips zeroize
Clock Management	Clock Ntp
Debug & Diagnostics	Debug diag ping l2traceroute traceroute top

Services	CLIs
CLI Mgmt	no delete configure dir exit help history quit rename abort do pwd help unhide unhide fips
Platform	reload chassis clear copy fastboot firmware fos usb logging service switch-attributes support
Display	Show
Terminal Configuration	send terminal end line
Ethernet	Sequence dot1x cee-map interface ip ipv6 lacp mac mac-addresstable port-profile protocol qos rmon sflow vlan monitor
License	License Dpod
Vcs	Vcs
Vcenter	Vcenter Vnetwork

Services	CLIs
SNMP	snmp-server
System Monitor	system-monitor system-monitor-mail

Table 9 CSP Access Rights within Roles & Services

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- R: Read
- W: Write
- N: No Access
- Z: Zeroize

	SSH and SCP CSP[5]s	TLS CSPs[6]	RNG Seed Key[7]	Passwords	RADIUS Secret
Login Session Management	N	N	N	RW	N
Zeroize	Z	Z	Z	Z	Z
FirmwareManagement	R	N	N	N	N
PKI	RW	N	N	N	N
RADIUS	N	N	N	RW	RW
UserManagement	N	N	N	RW	N

[5] Includes the following CSPs: DH Private Keys for use with 1024 bit or 2048 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

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code signed by RSA 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) 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. The module provides status of power-up and conditional self-tests (Success or Fail) via the "Show Status" service.

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 10 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
NTP	Network Time Protocol
NOS	Network Operating System
PKI	Public Key Infrastructure
PROM	Programmable read-only memory
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SFP	Small form-factor pluggable
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 tamper evident seals are required to complete the physical security requirements for the VDX 6710-54

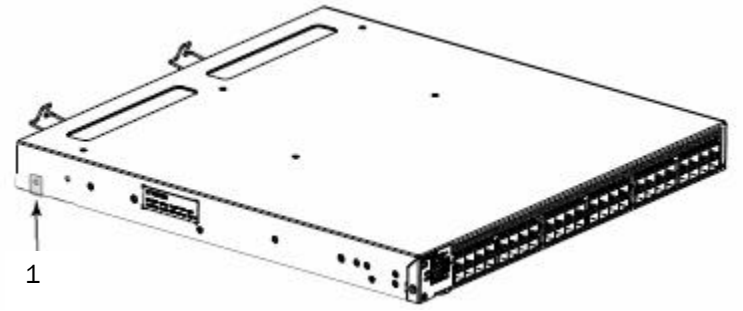

Figure 6 VDX 6710-54 left side seal location

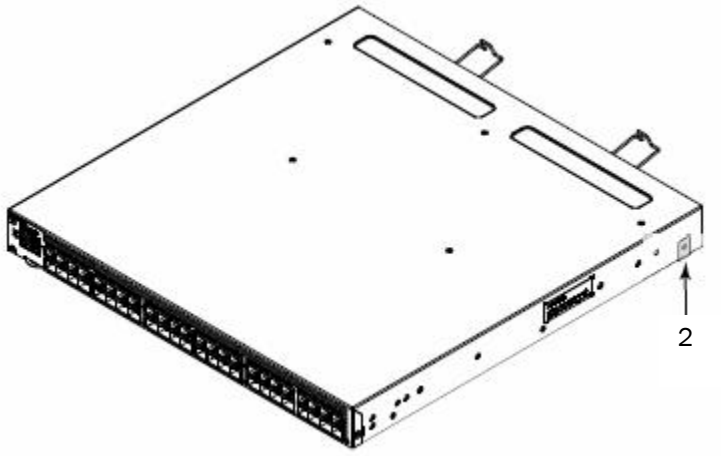

Figure 7 VDX 6710-54 right side seal location

VDX 6720-16 and VDX 6720-24

Two tamper evident seals are required to complete the physical security requirements for the VDX 6720-16 and VDX 6720-24

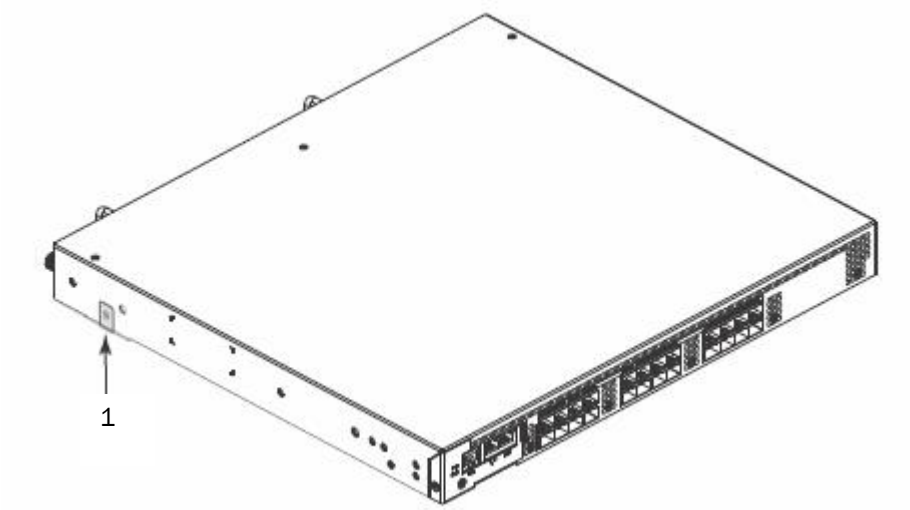

Figure 8 VDX 6720-16 and VDX 6720-24 left side seal location

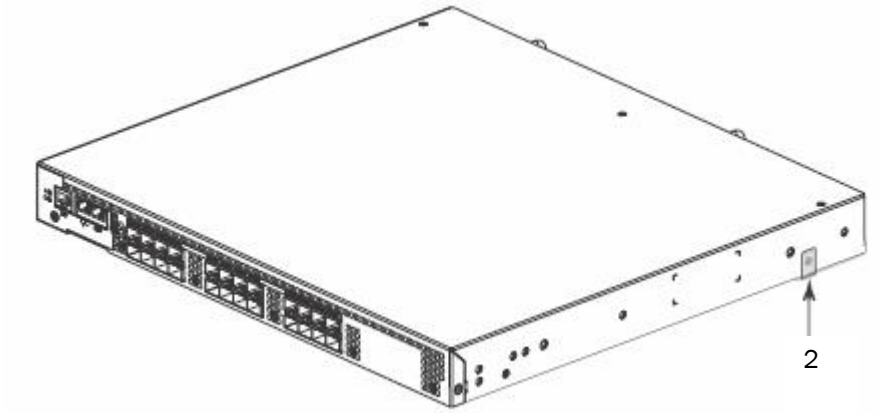

Figure 9 VDX 6720-16 and VDX 6720-24 right side seal location

VDX 6720-40 and VDX 6720-60

Two tamper evident seals are required to complete the physical security requirements for the VDX 6720-40 and VDX 6720-60

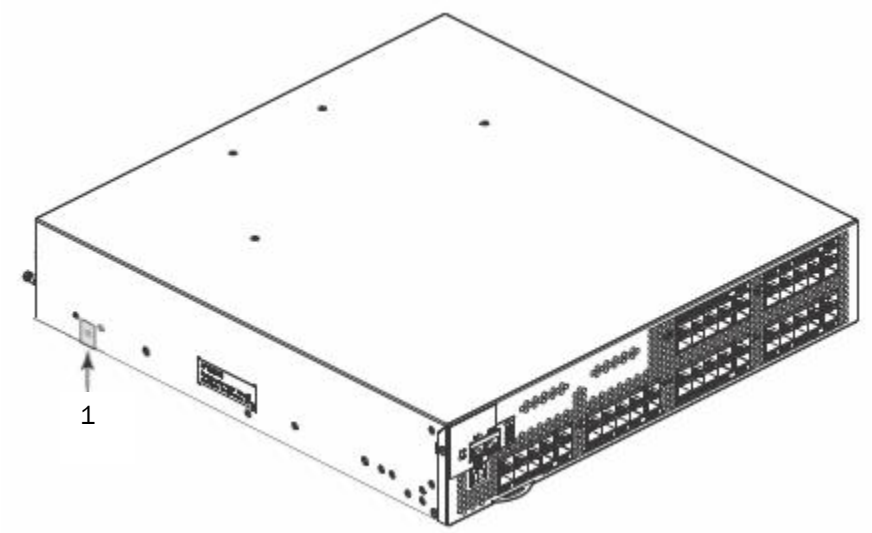

Figure 10 VDX 6720-40 and VDX 6720-60 left side seal location

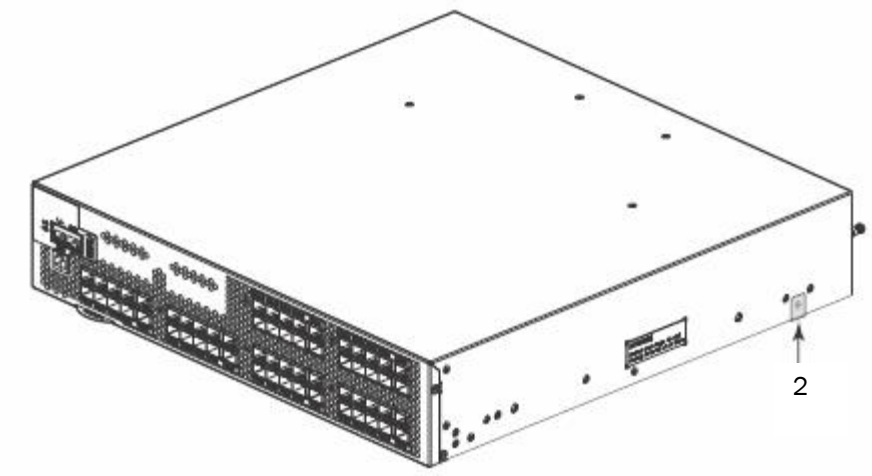

Figure 11 VDX 6720-40 and VDX 6720-60 right side seal location

VDX 6730-16 and VDX 6730-24

Two tamper evident seals are required to complete the physical security requirements for the VDX 6730-16 and VDX 6730-24.

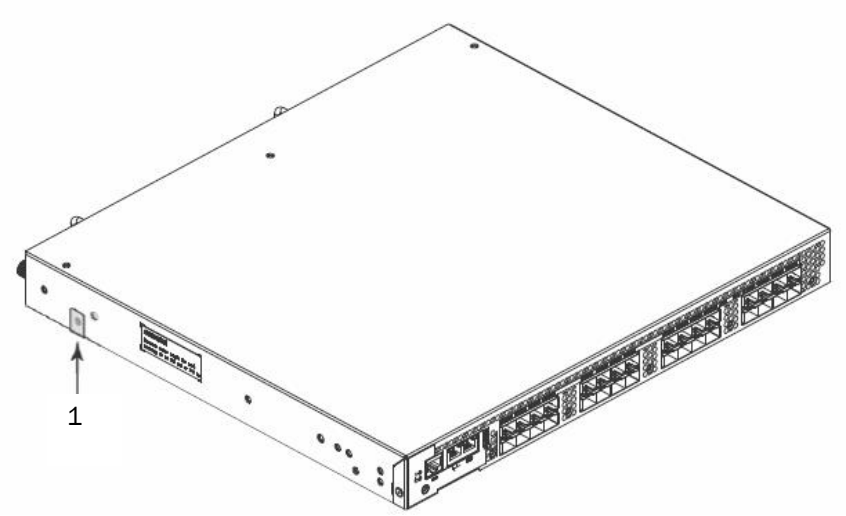

Figure 12 VDX 6730-16 and VDX 6730-24 left side seal location

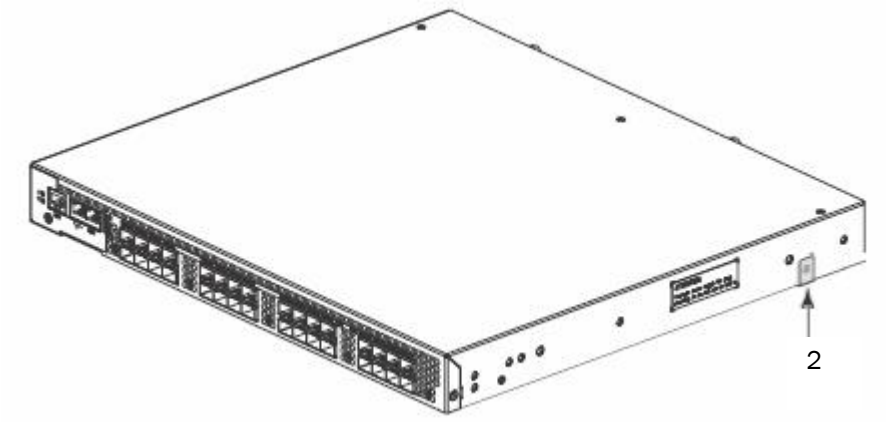

Figure 13 VDX 6730-16 and VDX 6730-24 right side seal location

VDX 6730-40 and VDX 6730-60

Two tamper evident seals are required to complete the physical security requirements for the VDX 6730-40 and VDX 6730-60

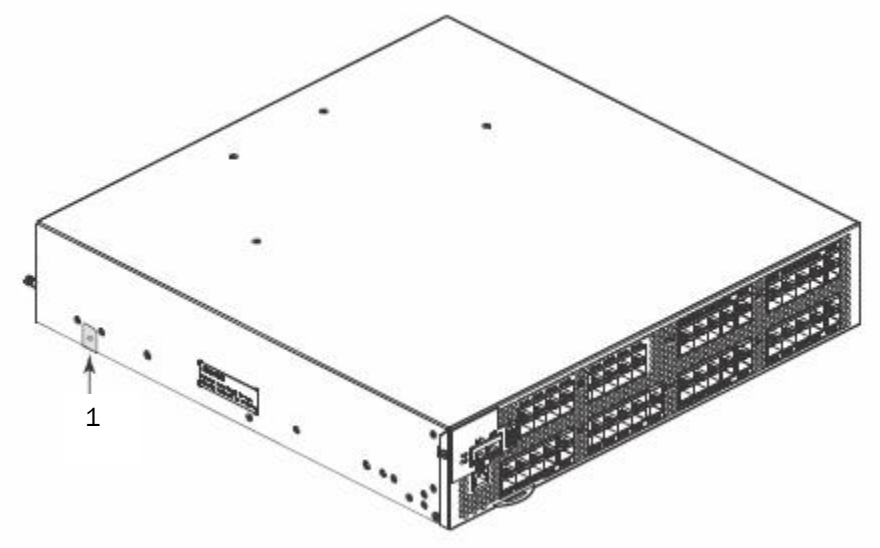

Figure 14 VDX 6730-40 and VDX 6730-60 left side seal location

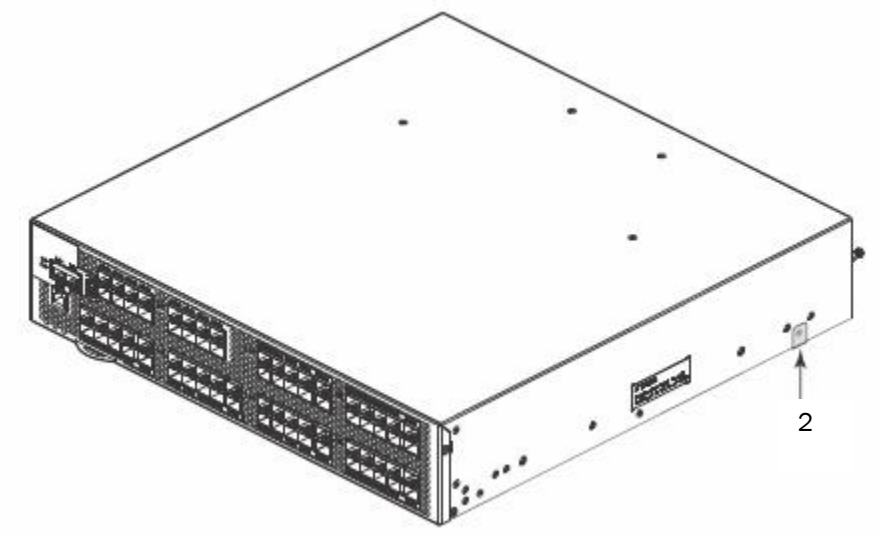

Figure 15 VDX 6720-40 and VDX 6720-60 right side seal location