Brocade® NetIron® CER 2000 Ethernet Routers and Brocade CES 2000 Routers and Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0

July 11, 2016

Brocade Communications

Revision History

Revision Date	Revision	Summary of Changes
7/11/2016	1.0	Initial Draft

This Brocade Communications Systems, Inc. Security Policy for Brocade NetIron CER/CES 2000 series embodies Brocade Communications Systems' confidential and proprietary intellectual property. Brocade Systems retains all title and ownership in the Specification, including any revisions.

This Specification is supplied AS IS and may be reproduced only in its original entirety [without revision]. Brocade Communications Systems makes no warranty, either express or implied, as to the use, operation, condition, or performance of the specification, and any unintended consequence it may on the user environment

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Table of contents:

Table of tables:

Table of figures:

1 Introduction

The Brocade NetIron CER 2000 Series is a family of compact 1U routers that are purpose-built for high-performance Ethernet edge routing and MPLS applications. These fixed-form routers can store a complete Internet table and support advanced MPLS features such as Traffic Engineering and VPLS. They are ideal for supporting a wide range of applications in Metro Ethernet, data center and campus networks. The NetIron CER 2000 is available in 24-port 1 Gigabit Ethernet (GbE) copper and hybrid fiber configurations with two optional 10 GbE uplink ports. To help ensure high performance, all the ports are capable of forwarding IP and MPLS packets at wire speed without oversubscription. With less than 5 watts/Gbps of power consumption, service providers can push up to 136 Gbps of triple-play services through the NetIron CER 2000 while reducing their carbon footprint.

The Brocade NetIron CES 2000 Series is a family of compact 1U, multiservice edge/aggregation switches that combine powerful capabilities with high performance and availability. The switches provide a broad set of advanced Layer 2, IPv4, IPv6, and MPLS capabilities in the same device. As a result, they support a diverse set of applications in metro edge, service provider, mobile backhaul wholesale, data center, and large enterprise networks.

2 Overview

Brocade routers provide high-performance routing to service providers, metro topologies, and Internet Exchange Points. Each router is a multi-chip standalone cryptographic module. Each device has an opaque enclosure with tamper detection tape for detecting any unauthorized physical access to the device. The NetIron family includes both chassis and fixed-port devices.

The cryptographic boundary of CER 2000 series and CES 2000 series devices is the outer perimeter of the metal chassis, including the removable cover. Within the NetIron family, the CER 2000 series and CES 2000 series are fixed-port devices.

For a CER or CES device to operate as a validated cryptographic module, 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 validated cryptographic state after any intentional or unintentional reconfiguration of the physical security measures.

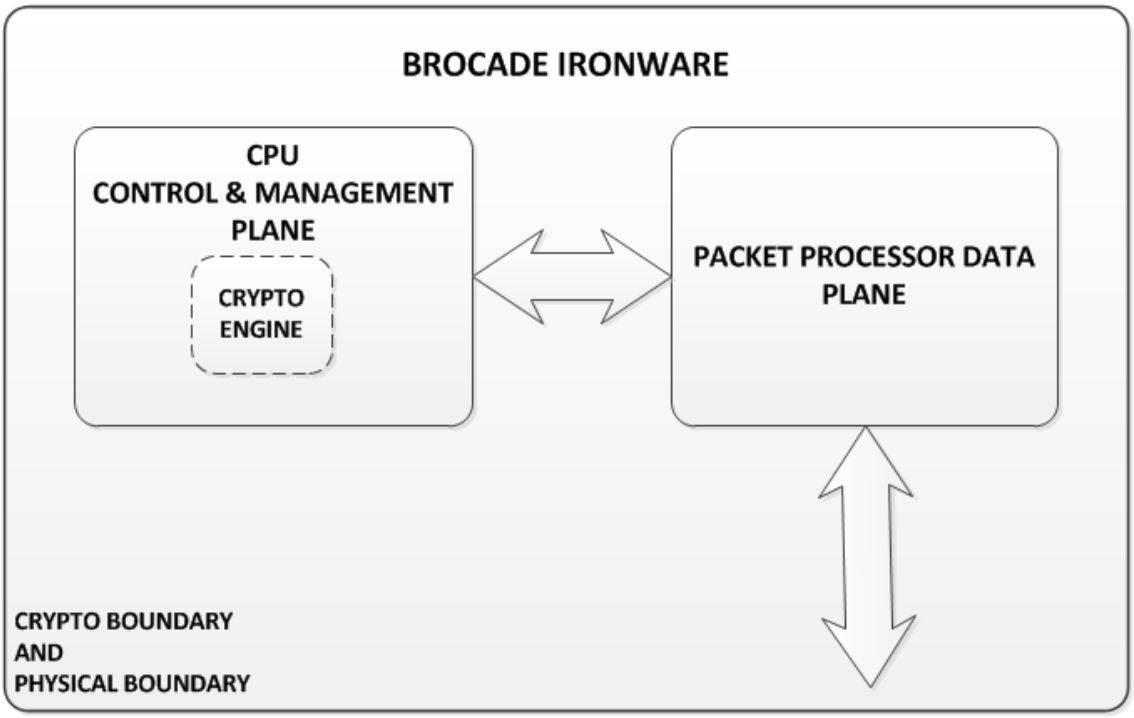

Figure 1 - Block Diagram

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

3 Brocade CER 2000 series

Firmware
Multi-Service IronWare R05.8.00a

Table 1 CER 2000 Series Firmware Version

SKU	MFG Part Number	Brief Description
BR-CER-2024C-4X-RT-AC	P/N:80-1006530-01	Brocade CER2024C-4XRT includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W AC power supply (RPS9)
BR-CER-2024C-4X-RT-DC	P/N:80-1007213-01	Brocade CER2024C-4XRT includes 24 RJ45 ports of 10/100/1000Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W DC power supply (RPS9DC)
BR-CER-2024F-4X-RT-AC	P/N:80-1006529-01	Brocade CER2024F-4XRT includes 24 SFP ports of 100/1000Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W AC power supply (RPS9),
BR-CER-2024F-4X-RT-DC	P/N:80-1007212-01	Brocade CER2024F-4XRT includes 24 SFP ports of 100/1000Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W DC power supply (RPS9DC)

Table 2 CER 2000 Series Part Numbers

SKU	MFG Part Number	Brief Description
RPS9	P/N:80-1003868-01	500W AC PWR SUPPLY FOR NI CER/CES SERIES
RPS9DC	P/N:80-1003869-02	500W DC PWR SUPPLY FOR NI CER/CES SERIES

Table 3 CER Power Supply Module Part Numbers

CER Model	Configuration Details
BR-CER-2024C-4X-RT-AC (P/N: 80-1006530-01)	Base: BR-CER-2024C-4X-RT-AC Interface Module: None License: SW-CER-2024-RTUPG (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)
BR-CER-2024C-4X-RT-DC (P/N: 80-1007213-01)	Base: BR-CER-2024C-4X-RT-DC Interface Module: None License: SW-CER-2024-RTUPG (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)
BR-CER-2024F-4X-RT-AC (P/N: 80-1006529-01)	Base: BR-CER-2024F-4X-RT-AC Interface Module: None License: SW-CER-2024-RTUPG (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)
BR-CER-2024F-4X-RT-DC (P/N: 80-1007212-01)	Base: BR-CER-2024F-4X-RT-DC Interface Module: None License: SW-CER-2024-RTUPG (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)

Table 4 Validated CER 2000 Series Configurations

Figure 2 - BR-CER-2024F-4X-RT-DC with Base: BR-CER-2024F-4X-RT-DC and License: SW-CER-2024-RTUPG

Figure 3 - BR-CER-2024F-4X-RT-DC backside with Power supply RPS9DC (DC Power Supply)

Figure 4 - BR-CER-2024C-4X-RT-DC with Base: BR-CER-2024C-4X-RT-DC and License: SW-CER-2024-RTUPG

Figure 5 - BR-CER-2024C-4X-RT-DC backside with Power supply RPS9DC (DC Power Supply)

Figure 6 - BR-CER-2024F-4X-RT-AC with Base: BR-CER-2024F-4X-RT-AC and License: SW-CER-2024-RTUPG

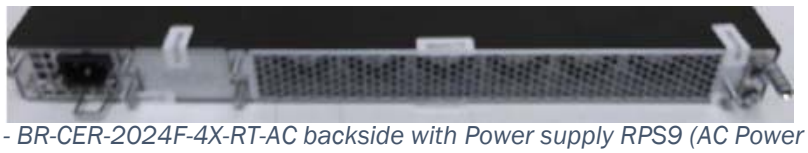

Figure 7 - BR-CER-2024F-4X-RT-AC backside with Power supply RPS9 (AC Power Supply)

Figure 8 - BR-CER-2024C-4X-RT-AC with Base: BR-CER-2024C-4X-RT-AC and License: SW-CER-2024-RTUPG

Figure 9 - BR-CER-2024C-4X-RT-AC backside with Power supply RPS9 (AC Power Supply)

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

4 Brocade CES 2000 Series

Firmware
Multi-Service IronWare R05.8.00a

Table 5 CES 2000 Series Firmware Version

SKU	MFG Part Number	Brief Description
BR-CES-2024C-4X-AC	P/N:80-1000077-01	Brocade CES 2024C-4X includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet ports, 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W AC power supply.
BR-CES-2024C-4X-DC	P/N:80-1007215-01	Brocade CES2024C-4X includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet Ports, 4 fixed ports of 10Gigabit Ethernet SFP+, 500W DC power Supply.
BR-CES-2024F-4X-AC	P/N:80-1000037-01	Brocade CES 2024F-4X includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet ports, 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W AC power supply
BR-CES-2024F-4X-DC	P/N:80-1007214-01	Brocade CES 2024F-4X, includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet ports, 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W DC power supply

Table 6 CES 2000 Series Part Numbers

SKU	MFG Part Number	Brief Description
RPS9	P/N:80-1003868-01	500W AC PWR SUPPLY FOR NI CER/CES SERIES
RPS9DC	P/N:80-1003869-02	500W DC PWR SUPPLY FOR NI CER/CES SERIES

Table 7 CES 2000 Series Power Supply Module Part Numbers

CES Model	Configuration Details
BR-CES-2024C-4X-AC	Base: BR-CES-2024C-4X-AC Interface module: None Power supply: RPS9 (P/N: 80-1003868-01)(1)
BR-CES-2024C-4X-DC	Base: BR-CES-2024C-4X-DC Interface module: None Power supply: RPS9DC (P/N: 80-1003869-02)(1)
BR-CES-2024F-4X-AC	Base: BR-CES-2024F-4X-AC Interface module: None Power supply: RPS9 (P/N: 80-1003868-01)(1)
BR-CES-2024F-4X-DC	Base: BR-CES-2024F-4X-DC Interface module: None Power supply: RPS9DC (P/N: 80-1003869-02)(1)

Table 8 Validated CES 2000 Series Configurations

Figure 10 - Front view of BR-CES-2024C-4X-AC

Figure 11 - BR-CES-2024C-4X-AC backside with Power supply: RPS9 (AC Power supply)

Figure 12 - Front view of BR-CES-2024C-4X-DC

Figure 13 - BR-CES-2024C-4X-DC backside with Power supply: RPS9DC (DC Power supply)

Figure 14 - Front view of BR-CES-2024F-4X-AC

Figure 15 - BR-CES-2024F-4X-AC backside with Power supply: RPS9 (AC Power supply)

Figure 16 - Front view of BR-CES-2024F-4X-DC

Figure 17 - BR-CES-2024F-4X-DC backside with Power supply: RPS9DC (DC Power supply)

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5 Ports and Interfaces

Each CER 2000 and CES 2000 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces they provide for Data input, Data output, Control input, and Control output.

The table below shows the correspondence between the physical interfaces of NetIron devices (CER, and CES) and logical interfaces defined in FIPS 140-2.

Physical Interface	Logical Interface
Data ports	Data input
Management port (Mgmt port)	
Console (serial port)	
Data ports	Data output
Management port (Mgmt port)	
Console (serial port)	
Data ports	Control input
Management port (Mgmt port)	
Console (serial port)	
Data ports	Status output
Management port (Mgmt port)	
Console (serial port)	
LED	
Power plugs	Power

Table 9 Physical/Logical Interface Correspondence

Models in the Brocade NetIron CER 2000 series provide 24 Gigabit Ethernet ports. Models in the Brocade NetIron CES 2000 series provide 24 Gigabit Ethernet ports and four fixed 10GbE ports. Each series supports both copper and fiber connecters with some models supporting combination ports. Some models support 10 Gigabit Ethernet uplink ports. All models have an out-of-band Ethernet management port (Gigabit Ethernet RJ-45 connector) and a console port (serial connector).

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5.1 Status LEDs

LED	Position	State	Meaning
AC PS1 (labeled P1)	Left side of front panel	Off	Power supply 1 is not installed or is not providing power.
		Amber	Power supply 1 is installed, but not connected or a fault is detected.
		Green	Power supply 1 is installed and is functioning normally.
AC PS1 (labeled P2)	Right side of front panel	Off	Power supply 2 is not installed or is not providing power.
		Amber	Power supply 2 is installed, but not connected or a fault is detected.
		Green	Power supply 2 is installed and is functioning normally.
Fan (labeled Fn)	Right side of front panel	Green	The fan tray is powered on and is operating normal
		Amber or Green blinking	The fan tray is not plugged in.
		Amber	The fan tray is plugged in but one or more fans are faulty.

Table 10 Power and fan status LEDs for the CER 2024 and CES 2024 models

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5.2 Modes of Operation

The NetIron validated cryptographic module has two modes of operation: FIPS Approved mode and non-Approved mode. Both these modes enforce digital signature based firmware load test. Section 7 describes services and cryptographic algorithms available in FIPS Approved mode.

Section 9.1.1.1 describes how to invoke FIPS Approved mode.

5.3 Module Validation Level

The module meets an overall FIPS 140-2 compliance of security level 2 with Design Assurance level 3.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic 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
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 11 NetIron Security Levels

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6 Roles

In FIPS Approved mode, NetIron devices support three authenticated roles: Crypto-officer, Port Configuration Administrator, and User:

1. Crypto-officer Role: The Crypto-officer role on the device in FIPS Approved mode is equivalent to administrator or super-user in non-Approved mode. Hence, the Crypto-officer role has complete access to the system.
2. Port Configuration Administrator Role: The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-Approved mode. Hence, the Port Configuration Administrator role has read-and-write access for specific ports but not for global (system-wide) parameters.
3. User Role: The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

The User role has read-only access to the cryptographic module while the Crypto-officer role has access to all device commands. NetIron modules do not have a maintenance interface.

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LEDs. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests by power cycling a NetIron device.

For all other services, an operator must authenticate to the device as described in Section 8.2 Authentication.

NetIron devices provide services for remote communication (SSHv2, SCP, SNMPv3 and Console) for management and configuration of cryptographic algorithms.

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSPs) associated with the service.

The table below summarizes the available FIPS Approved cryptographic algorithms. Refer to Table 16 for more information on modes, key sizes and certificate numbers for below FIPS Approved cryptographic functions.

Label	Cryptographic Algorithm
AES	Advanced Encryption Standard
CVL	SSHv2 and TLS v1.0/1.1 and TLS v1.2 Key Derivation Function, SNMPv3 KDF NOTE: TLS v1.0/1.1 and TLS v1.2 are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
DRBG	SP800-90A Deterministic Random Bit Generator
HMAC	Keyed-Hash Message Authentication Code
RSA	Rivest Shamir Adleman Signature Algorithm
SHS	Secure Hash Standard
Triple-DES	Triple Data Encryption Algorithm NOTE: Triple-DES is NOT available within any service in the Approved mode of operation.

Table 12 FIPS Approved Cryptographic Algorithms

The table below lists cryptographic algorithms that while not FIPS Approved are allowed in FIPS Approved mode of operation. Note that cryptographic algorithms listed in this table **ARE NOT** exposed to the operator:

Label	Cryptographic Algorithm
DH	Diffie-Hellman (within SCP/SSHv2 protocol) (key agreement; key establishment methodology provides 112 bits of encryption strength)
HMAC-MD5	Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
HMAC-SHA1-96	Used for OSPFv3 authentication
MD5	Message-Digest Algorithm - Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
NDRNG	Nondeterministic Random Number Generator used for generation of seeds for DRBG only

Table 13 Non-Approved Cryptographic Algorithms Allowed in FIPS Approved Mode

7.1 FIPS Approved Mode Services

Services in FIPS Approved mode of operation are described in this section.

7.1.1 User Role Services

The User management privilege level allows access to the User EXEC, and Privileged EXEC commands, but only with read access.

7.1.1.1 SSHv2

The module supports SSHv2. This service provides a secure session between a NetIron device and an SSHv2 client. The NetIron device authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface. The following cipher sequence is supported for SSHv2:

- AES-CTR with a 256-bit key (aes-256-ctr),
- AES-CTR with a 192-bit key (aes-192-ctr),
- AES-CTR with a 128-bit key (aes-128-ctr),
- AES-CBC with a 256-bit key (aes-256-cbc),
- AES-CBC with a 192-bit key (aes-192-cbc) and
- AES-CBC with a 128-bit key (aes-128-cbc).

NetIron devices support three kinds of SSHv2 client authentication: password, keyboard interactive and public-key authentication.

For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The NetIron device authenticates operator with passwords stored on the device, on a TACACS+ server, or on a RADIUS server. Section 8.2 provides authentication details.

The keyboard interactive (KI) authentication goes one step further. It allows multiple challenges to be issued by the NetIron device, using the backend RADIUS or TACACS+ server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the NetIron device.

For public key authentication, possession of a private key serves as an authentication method. In PKI (Public Key Infrastructure), each private key has its corresponding public key and they are referred to as a key pair. Every key pair is unique. The cryptographic module uses a database of client public keys and its associated user names and roles to support public key authentication. The SSHv2 client which possesses the private key sends a signature (over some data from the request including the user name) created using the private key. The cryptographic module uses the public key corresponding to the user and verifies the signature to authenticate the user.

In the User role, the client is given access to three commands: enable, exit and terminal. The enable command allows the operator to re-authenticate using a different role. If the role is the same, based on the credentials given during the enable command, the operator has access to a small subset of commands that can perform ping, traceroute, outbound SSHv2 client in addition to show commands.

7.1.1.2 SNMP

SNMPv1 and SNMPv2c are blocked in FIPS mode. Only SNMPv3 in authPriv mode is allowed while other modes are blocked. SNMP service within the User role allows read-only access to the SNMP MIB within the NetIron device. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for read-only access (status output).

7.1.1.3 Console

Console connections occur via a directly connected RS-232 serial cable. Once authenticated in the User role, the module provides console commands to display information about a NetIron device and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available are the same as the list mentioned in the SSHv2 service.

7.1.2 Port Configuration Administrator Role Services

The Port Configuration Administrator management privilege level allows read-and-write access for port configuration, but not for global (system-wide) parameters.

7.1.2.1 SSHv2

This service is described above in Section 7.1.1.1.

The port configuration administrator will have 7 commands, which allows this user to run show commands, run ping or traceroute and the enable command which allows this user to re-authenticate as described in Section 7.1.1.1. Within the configuration mode, this role provides access to all the port configuration commands. That is, all sub-commands within “interface eth 1/1” command. This operator cannot transfer and store software images and configuration files between the network and the system. However, this operator can review the configuration.

7.1.2.2 SNMP

This service is described above in Section 7.1.1.2.

The SNMP service is not available for the Port Configuration Administrator role.

7.1.2.3 Console

This service is described above in Section 7.1.1.3.

Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. The commands available to operator within the Port Configuration Administrator role are same as those mentioned in the SSHv2 service Section 7.1.1.1.

7.1.3 Crypto-officer Role Services

The Crypto-officer management privilege level allows complete read-and-write access to the system. This is generally for system administrators and is the only management privilege level that allows one to configure passwords. The Crypto-officer role is able to perform firmware loading for the device as it has complete access to the system.

7.1.3.1 SSHv2

This service is described above in Section 7.1.1.1.

The Crypto-officer can perform configuration changes to the module. This role has full read and write access to the NetIron device.

7.1.3.2 SCP

This is a secure copy service that works over SSHv2 protocol. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary files can be copied and installed similarly to TFTP operation (that is, upload from device to host and download from host to device). SCP automatically uses the

authentication methods, encryption algorithm, and data compression level configured for SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use could be to copy configuration to/from the cryptographic module.

7.1.3.3 SNMP

This service is described above in Section 7.1.1.2.

The SNMP service within Crypto-officer role allows access to the SNMP MIB within the NetIron device as per the capability of the SNMP agent, using SNMPv3 version in authPriv security mode. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for access similar to non-Approved mode of operation.

7.1.3.4 Console

This service is described in Section 7.1.1.3 above.

Console commands provide an authenticated Crypto-officer complete access to all the commands within the NetIron device. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access; afterwards the operator may securely import additional pairs of RSA host keys over a secured SSHv2 connection.

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7.2 Non-Approved Mode Services

Certain services are available within the non-Approved mode of operation, which are otherwise not available in the FIPS Approved mode of operation. They are:

Algorithm/Service	Role(s)	Additional Details
SNMP	Crypto-officer Role, User Role	Simple Network Management Protocol SNMPv1 and SNMPv2c. SNMPv3 noAuthNoPriv, authNoPriv modes. SNMPv3 authPriv mode using DES 56 bit. SNMPv3 KDF (non-compliant)
SSHv2	Crypto-officer Role, Port Configuration Administrator Role, User Role	Secure Shell (SSHv2) is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way. Key size / Mode: 1024 bit RSA Key size / Mode: 1024 bit DSA Key sizes / Mode: Three-key Triple-DES (non-compliant) SSHv2 KDF (non-compliant)
TACACS	Crypto-officer Role, Port Configuration Administrator Role, User Role	TACACS (Terminal Access Controller Access Control System) is an authentication protocol running over UDP which allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Telnet	Crypto-officer Role, Port Configuration Administrator Role, User Role	Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
TFTP	Crypto-officer Role	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Algorithm/Service	Role(s)	Additional Details
TLS	Crypto-officer Role, Port Configuration Administrator Role, User Role	OpenFlow: OpenFlow protocol allows a network device to support remote abstraction of flow table by an OpenFlow controller. This allows remote controller to manipulate the device's forwarding table. TLS v1.0/1.1 - RSA 2048 (non-compliant) - SP800-135 TLS v1.0/1.1 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant) TLS v1.2 - RSA 2048 (non-compliant) - SP800-135 TLS v1.2 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant), HMAC-SHA-256 (non-compliant) Syslog: System Log allows auditing and logging of selective events within a networking device to be recorded by a remote entity. This uses industry standard Syslog protocol for this purpose. TLS v1.0/1.1 - RSA 2048 (non-compliant) - SP800-135 TLS v1.0/1.1 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant) TLS v1.2 - RSA 2048 (non-compliant) - SP800-135 TLS v1.2 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant), HMAC-SHA-256 (non-compliant) TACACS+: Terminal Access Controller Access-Control System (TACACS+) is used to handle authentication, authorization and accounting service for a network device using a remote centralized server. TLS v1.0/1.1 - RSA 2048 (non-compliant) - SP800-135 TLS v1.0/1.1 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant) TLS v1.2 - RSA 2048 (non-compliant) - SP800-135 TLS v1.2 KDF (non-compliant) - AES-CBC (non-compliant) - HMAC-SHA-1 (non-compliant), HMAC-SHA-256 (non-compliant)

Table 14 FIPS non-Approved Cryptographic Algorithms and Protocols only available in non-Approved Mode

8 Policies

8.1 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 2 security requirements. After configuring a NetIron device to operate in FIPS Approved mode the Crypto-officer must execute the "fips self-tests" command to validate the integrity of the firmware installed on the device. If an error is detected during the self-test, the error must be corrected prior to rebooting the device.

1) The cryptographic module provides role-based authentication.
2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSPs).
3) The cryptographic module fully implements DRBG Health Tests performed as part of self-tests, and therefore meets the requirements of SP800-90A Section 11.3.
4) The cryptographic module performs the following tests:
   a) Power up Self-Tests:
      (i) Cryptographic Known Answer Tests (KAT):
         (1) Three-Key Triple-DES KAT (encrypt)
         (2) Three-Key Triple-DES KAT (decrypt)
         (3) AES-128, 192, 256-bit key sizes KAT (encrypt)
         (4) AES-128, 192, 256-bit key sizes KAT (decrypt)
         (5) SHA-1, 256, 384, 512 KAT (hashing)
         (6) HMAC-SHA-1, 256 KAT (hashing)
         (7) RSA 2048 bit key size KAT (encrypt)
         (8) RSA 2048 bit key size KAT (decrypt)
         (9) RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature generation)
         (10) RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature verification)
         (11) SP800-90A DRBG KAT
         (12) SP800-135 TLS v1.0/1.1 KDF KAT
         (13) SP800-135 SSHv2 KDF KAT
         (14) SP800-135 TLS v1.2 KDF KAT
         (15) SP800-135 SNMPv3 KDF KAT
      (ii) Firmware Integrity Test: (CRC 16)
      (iii) Critical functions test: RSA 2048 encrypt/decrypt

      If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

      ```
      Crypto module initialization and Known Answer Test (KAT) Passed.
      ```

      (iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

```
Crypto Module Failed <Reason String>
```

b) Conditional Self-Tests:

(i) Continuous Test: Non-Deterministic Random Number Generator (NDRNG) Test performed on non-Approved NDRNG.

(ii) Continuous Test: Random Number Generator Test performed on Approved DRBG.

(iii) Pairwise Consistency Test: RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

(iv) Pairwise Consistency Test: RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

(v) Firmware Load Test: RSA 2048 SHA-256 Signature Verification

(vi) Bypass Test: N/A

(vii) Manual Key Entry Test: N/A

5) At any time the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-tests by executing the “fips self-tests” command.

6) Data output to services defined in Section 7 is inhibited during key generation, self-tests, zeroization, and error states.

7) Status information does not contain CSPs or sensitive data that if used could compromise the module.

8) The following protocols have not been reviewed or tested by the CAVP nor CMVP:

a) TLS v1.0/1.1 (NOTE: TLS v1.0/1.1 is latent functionality that “IS NOT” available within any service in the Approved mode of operation.)

b) SSHv2

c) TLS v1.2 (NOTE: TLS v1.2 is latent functionality that “IS NOT” available within any service in the Approved mode of operation.)

d) SNMPv3

8.1.1 Cryptographic Module Operational Rules

In order to operate a CER 2000 series and CES 2000 series device securely, an operator should be aware of the following rules for FIPS Approved mode of operation.

Do not make external communication channels/ports available before initialization of a CER 2000 series or CES 2000 series device.

CER 2000 series and CES 2000 series devices use a SP800-90A FIPS Approved DRBG random number generator, implementing the algorithm in CTR mode. Note that the algorithm has also been certified for Hash_Based DRBG but not used within any service in the module.

CER 2000 series and CES 2000 series ensures that the random number seed and seed key input do not have same value. The devices generate seed keys and do not accept a seed key entered manually.

CER 2000 series and CES 2000 series devices use FIPS Approved key generation methods:

- RSA public and private keys

CER 2000 series and CES 2000 series devices test the prime numbers generated for RSA keys using Miller-Rabin Test.

CER 2000 series and CES 2000 series devices restrict key entry and key generation to authenticated roles.

8.2 Authentication

NetIron devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS+, RADIUS and local configuration database. Moreover, NetIron supports multiple authentication methods for each service.

To implement one or more authentication methods for securing access to the device, an operator in the Crypto-officer role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (SSHv2, SNMP, and so on) and the order in which the device tries one or more of the following authentication methods:

1. Line password authentication,
2. Enable password authentication,
3. Local user authentication,
4. RADIUS authentication with exec authorization and command authorization, and
5. TACACS+ authentication with exec authorization and command authorization

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a TACACS+ server) the device tries the next method until a method in the list is available or all methods have been tried.

NetIron devices allow multiple concurrent operators through SSHv2 and the console. One operator's configuration changes can overwrite the changes of another operator.

8.2.1 Line Authentication Method

The line method uses the Telnet password to authenticate an operator.

To use line authentication, a Crypto-officer must set the Telnet password. Please note that when operating in FIPS Approved mode, Telnet is disabled and Line Authentication is not available.

8.2.2 Enable Authentication Method

The enable method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-config password to the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto-officer Role.

To use enable authentication, a Crypto-officer must set the password for each privilege level.

8.2.3 Local Authentication Method

The local method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The NetIron device assigns the role associated with the user name to the operator when authentication is successful.

To use local authentication, a Crypto-officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

8.2.4 RADIUS Authentication Method

The RADIUS method uses one or more RADIUS servers to verify user names and passwords. The NetIron device prompts an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server does not respond, the NetIron device will send the user name and password information to the next configured RADIUS server.

NetIron series devices support additional command authorization with RADIUS authentication. The following events occur when RADIUS command authorization takes place.

1. A user previously authenticated by a RADIUS server enters a command on the NetIron device.
2. The NetIron device looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3. If the command belongs to a privilege level that requires authorization, the NetIron device looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the NetIron device. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the NetIron device.

To use RADIUS authentication, a Crypto-officer must configure RADIUS server settings along with authentication and authorization settings.

8.2.5 TACACS+ Authentication Method

The TACACS+ methods use one or more TACACS+ servers to verify user names and passwords. For TACACS+ authentication, the NetIron device prompts an operator for a user name, which the device uses to get a password prompt from the TACACS+ server. The operator enters a password, which the device relays to the server for validation. Upon successful authentication, the TACACS+ server supports both exec and command authorization similar to RADIUS authorization described above.

To use TACACS+ authentication, a Crypto-officer must configure TACACS+ server settings along with authentication and authorization settings.

8.2.6 Strength of Authentication

NetIron devices minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18), for a total of 80 characters. Therefore, the probability of a successful random attempt is 1/80^8, which is less than 1/1,000,000.

The module enforces a one second delay for each attempted password verification, therefore the maximum number of random attempts per minute is 60. Thus, the probability of a successful random attempt within a one minute period is 60/80^8, which is less than 1/100,000.

RADIUS and TACACS+ support minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18), for a total of 80 characters. Therefore, the probability of a successful random attempt is 1/80^8, which is less than 1/1,000,000.

A user gets three attempts before lockdown. When lockdown occurs, the user is locked out until the device is rebooted. Rebooting takes longer than one minute. Therefore, the maximum number of attempts per minute is 3. Thus, the probability of a successful random attempt within a one minute period is 3/80^8, which is less than 1/100,000.

8.3 Access Control and Critical Security Parameters (CSPs)

Table 15 summarizes the access operators in each role have to critical security parameters. Blank table cells indicate no security relevance between the role and the CSP. The table entries have the following meanings:

- r – Operator can read the value of the item,
- w – Operator can write a new value for the item,
- x – Operator can use the value of the item (for example encrypt with an encryption key), and
- d – Operator can delete the value of the item (zeroize) by executing a `fips zeroize all` command. See item 4a in Section 9.1.1.1 for further details.

NOTE: Refer to section 13, Appendix B: Critical Security Parameters, for more information on the CSPs.

ROLE➔	Crypto-officer				User			Port Administrator	
Services / CSP	SSHv2	SCP	SNMP	Console	SSHv2	SNMP	Console	SSHv2	Console
SSHv2 Host RSA Private Key (2048 bit)	xwd	x		wd	x			x	
SSHv2 Client RSA Private Key	xwd	x		wd	x			x	
SSHv2 DH Group-14 Private Key (2048 bit)	xwd	x		wd	x			x	
SSHv2 DH Shared Secret Key (2048 bit)	x	x		xd	x			x	
SSHv2/SCP Session Keys (128 and 256 bit AES CBC)	x	x		xd	x			x	
SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	x	x		xd	x			x	
SSHv2 KDF Internal State	x	x		xd	x			x	
DRBG Seed	x	x		xd	x			x	
DRBG Value V	x	x		xd	x			x	
DRBG Key	x	x		xd	x			x	
DRBG Internal State	xd	x		xd	x			x	
User Password	xrwd	xrwd	x	xrwd	x	x	x		
Port Administrator Password	xrwd	xrwd		xrwd				x	x
Crypto-officer Password	xrwd	xrwd		xrwd					
RADIUS Secret	xrwd	xrwd		xrwd	x		x	x	x
TACACS+ Secret	xrwd	xrwd		xrwd	x		x	x	x
Firmware Load RSA Public Key	x			xd					

ROLE➔	Crypto-officer				User			Port Administrator	
Services / CSP	SSHv2	SCP	SNMP	Console	SSHv2	SNMP	Console	SSHv2	Console
SSHv2 Host RSA Public key	xrwd	xrw		rwd	x			x	
SSHv2 Client RSA Public Key	xrwd	xrwd		xrwd	x			x	
SSHv2 DH Public Key	x	x		xd	x			x	
SSHv2 DH Peer Public Key	x	x		xd	x			x	

Table 15 Access Control Policy and Critical Security Parameters (CSPs)

8.3.1 CSP Zeroization

The SSHv2 session key is transient. It is zeroized at the end of a session and recreated at the beginning of a new session.

The DRBG seed and CTR_DRBG Entropy is recomputed periodically on 100 millisecond intervals. Each time this occurs, four bytes of the seed are written into an 8K buffer. When the buffer is full the DRBG V and Key values are regenerated and the buffer is zeroized.

The DH private exponent is generated at the beginning of DH KEX. A new random number overwrites the memory location used to store the value each time a new session is initiated.

For SSHv2, the RSA private key is stored in a locally generated file on flash during the key generation process. The file is removed during zeroization. The crypto key zeroize command removes the keys.

Executing the "`no fips enable`" command zeroizes all host key pairs.

All other CSPs can be zeroized by executing the "`fips zeroize all`" command.

8.4 Physical Security

NetIron devices require the Crypto-officer to install tamper evident labels (TELs) in order to meet FIPS 140-2 Level 2 Physical Security requirements. The TELs are available from Brocade under part number XBR-000195. The Crypto-officer shall follow the Brocade FIPS Security Seal application procedures prior to operating the module in FIPS Approved mode. The FIPS seal application procedure is available in Appendix A.

9 Crypto-officer Guidance

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.

9.1 Mode Status

NetIron devices provide the "`fips show`" command to display status information about the device's configuration. This information includes the status of administrative commands for security policy, the status of security policy enforcement, and security policy settings. The "`fips enable`" command changes the status of administrative commands; see also Section 9.1.1 FIPS Approved Mode.

The following example shows the output of the "`fips show`" command before an operator enters a "`fips enable`" command. Administrative commands for security policy are unavailable (administrative status is off) and the device is not enforcing a security policy (operational status is off). The command displays the security policy settings.

```
Not a FIPS Validated Cryptographic Module
FIPS Version: BRCD-IP-CRYPTO-VER-3.0
FIPS mode   : Administrative status OFF: Operational status OFF
```

The following example shows the output of the "`fips show`" command after an operator enters the fips enable command. Administrative commands for security policy are available (administrative status is on) but the device is not enforcing a security policy yet (operational status is off). The command displays the security policy settings.

```
FIPS Validated Cryptographic Module
FIPS Version: BRCD-IP-CRYPTO-VER-3.0
FIPS mode   : Administrative status ON: Operational status OFF
Some shared secrets inherited from non-fips mode may not be fips compliant
and has to be zeroized.
The system need to be reloaded to operationally enter FIPS mode.

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                  : Disabled
Telnet client                  : Disabled
TFTP client                    : Disabled
SNMP v1, v2, v2c               : Disabled
SNMP Access to security objects: Disabled
```

```
Password Display              : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                         : Clear
```

The status 'Clear' refers to the fact that when FIPS Approved mode is disabled at a later point in time, the corresponding CSPs will be affected based on the FIPS policy settings for that CSP.

The following example shows the output of the "fips show" command after the device reloads successfully in the default strict FIPS Approved mode. Administrative commands for security policy are available (administrative status is on) and the device is enforcing a security policy (operational status is on): The command displays the policy settings.

```
FIPS Validated Cryptographic Module
FIPS Version: BRCD-IP-CRYPTO-VER-3.0
FIPS mode   : Administrative status ON: Operational status ON

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                 : Disabled
Telnet client                 : Disabled
TFTP client                   : Disabled
SNMP v1, v2, v2c              : Disabled
SNMP Access to security objects: Disabled
Password Display              : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                         : Clear
```

9.1.1 FIPS Approved Mode

This section describes the FIPS Approved mode of operation and the sequence of actions that put a NetIron device in FIPS Approved mode. FIPS Approved mode does the following:

1. Remove "telnet server" configuration command to disable Telnet access.
2. Remove "enable aaa console" command to disable AAA authentication for the console. This allows console access to configure SSH parameters. This command can be enabled after SSH is confirmed to be operational.
3. Remove command "ip ssh scp disable" to allow SCP operation in FIPS mode.
4. Disable TFTP access
5. Disable SNMP access to CSP MIB objects
6. Disable access to all commands that allow debugging of memory content within the monitor mode

Entering FIPS Approved mode also clears:

1. Protocol shared secret and host passwords

FIPS Approved mode enables:

1. SCP

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES)	128, 192, and 256-bit keys, ECB, CBC and CTR	#2715
Advanced Encryption Standard (AES)	CFB128	#3143
Component Test Key Derivation Function (CVL)	SNMPv3 KDF	#403
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and SSHv2 KDF NOTE: TLS v1.0/1.1 is latent functionality that "IS NOT" available within any service in the Approved mode of operation.	#173
Component Test Key Derivation Function (CVL)	TLS v1.2 KDF NOTE: TLS v1.2 is latent functionality that "IS NOT" available within any service in the Approved mode of operation.	#394
Deterministic Random Bit Generator (DRBG) NOTE: The algorithm was also certified for Hash_Based DRBG, but the DRBG runs in CTR mode. Hash_Based DRBG is not available within any service in Approved mode of operation.	SP800-90A CTR_DRBG	#452
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256	#1694
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: The module does not support 1024-bit keys in FIPS Mode. 1024-bit key size is only allowed in non-Approved mode.	1024-bit and 2048-bit keys	#1411
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	#2280
Triple Data Encryption Algorithm (Triple- DES) NOTE: Triple-DES is NOT available within any service in the Approved mode of operation.	KO 1, 2 ECB and CBC mode	#1632

Table 16 Algorithm Certificates for the CER and CES 2000 Series

Operators 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.

NOTE: The module does not allow the use of 1024-bit RSA or 1024-bit DSA keys in the FIPS Approved mode of operation due to the SP800-131A transition effective January 1, 2014.
RSA 1024-bit and DSA 1024-bit key sizes are used only in non-Approved mode.

The following non-Approved but allowed cryptographic methods are allowed within limited scope in the FIPS Approved mode of operation:

1. Diffie-Hellman (within SCP/SSHv2 protocol) (key agreement; key establishment

methodology provides 112 bits of encryption strength)

2. MD5 – Message-Digest Algorithm - Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
3. HMAC-MD5 – Used to support RADIUS for operator authentication (HMAC-MD5 is not exposed to the operator)
4. HMAC-SHA1-96 - Used for OSPFv3 authentication (Note: The latent OSPFv3 authentication implemented by the module does not provide cryptographic protection, and is considered plaintext).
5. NDRNG – Non-deterministic random number generator used for generation of seeds for DRBG only.

9.1.1.1 Invoking FIPS Approved Mode for Brocade NetIron CER 2000 Series and CES 2000 Series Devices

To invoke the FIPS Approved mode of operation, perform the following steps from the console terminal.

1) Assume Crypto-officer role
2) Copy signature files of all the affected images to the flash memory.
3) Enter command: `fips enable`
   a) The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.
4) Enter command: `fips zeroize all`
   a) The device zeroizes the shared secrets used by various networking protocols including host access passwords and SSHv2 Host keys.
5) Save the running configuration: `write memory`
   a) The device saves the running configuration as the startup configuration
6) Reload the device
   a) The device resets, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
7) Enter command: `fips show`
   a) The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
8) Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

9.1.1.2 Negating FIPS Approved Mode for Brocade CER 2000 Series and CES 2000 Series Devices

To exit the FIPS Approved mode of operation, perform the following steps from the console terminal.

1) Enter command: `no fips enable`
   a) This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.
   b) The device zeroizes the shared secrets used by various networking protocols including host access passwords, SSHv2 client keys and SSHv2 server keys.
   c) "`write memory`" to save the updated configuration
   d) Reload the device to begin non-Approved mode of operation.

10 Mitigation of other attacks

This module is not designed to mitigate against any attacks outside the scope of FIPS 140-2.

Other Attacks	Mitigation mechanism	Specific Limitations
N/A	N/A	N/A

Table 17 Mitigation of other attacks

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

11 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CER	Carrier Ethernet Router
CES	Carrier Ethernet Switch
CLI	Command Line Interface
CFP	C Form-factor Pluggable
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
LP	Line Processor
Mbps	Megabits per second
MP	Management Processor
NDRNG	Non-Deterministic Random Number Generator
NI	NetIron platform
OC	Optical Carrier
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SFP	Small Form-factor Pluggable
SFPP	Small Form-factor Plus Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SSHv2	Secure Shell
TACACS	Terminal Access Control Access-Control System
TACACS+	Terminal Access Control Access-Control System Plus
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
XFP	10 Gigabit Small Form Factor Pluggable

Table 18 Glossary

12 Appendix A: Tamper Evident Seal Application Procedure

The FIPS Kit (SKU XBR-000195) contains the following items:

- Tamper Evident Security Seals
  - Count 120
  - Checkerboard destruct pattern with ultraviolet visible “Secure” image

Use 99% isopropyl alcohols to clean the surface area at each tamper evident seal placement location. Isopropyl alcohol is not provided in the kit. However, 99% isopropyl alcohol is readily available for purchase from a chemical supply company. Prior to applying a new seal to an area, that shows seal residue, use consumer strength adhesive remover to remove the seal residue. Then use additional alcohol to clean off any residual adhesive remover before applying a new seal.

12.1 Applying Tamper Evident Seals to Brocade NetIron CER 2024C-4X-RT devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024C-4X-RT.

Brocade NetIron CER 2024C-4X-RT device require the placement of eighteen (18) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 18). See Figure 18 for correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). The orientation and placement of seals on the left and right sides mirrors each other. See Figure 19 and Figure 20 for correct seal orientation.
- Rear: Affix six (6) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 13 wraps from the top cover to the filler panel. Seals 15 and 16 wrap from the top cover to the fan module. See Figure 21 for correct seal placement. Seal 12 touches both the power supply module and filler panel before wrapping onto the bottom of the chassis. Seals 14 and 17 wrap from the fan module to the bottom of the chassis. See Figure 22 for correct seal placement.

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

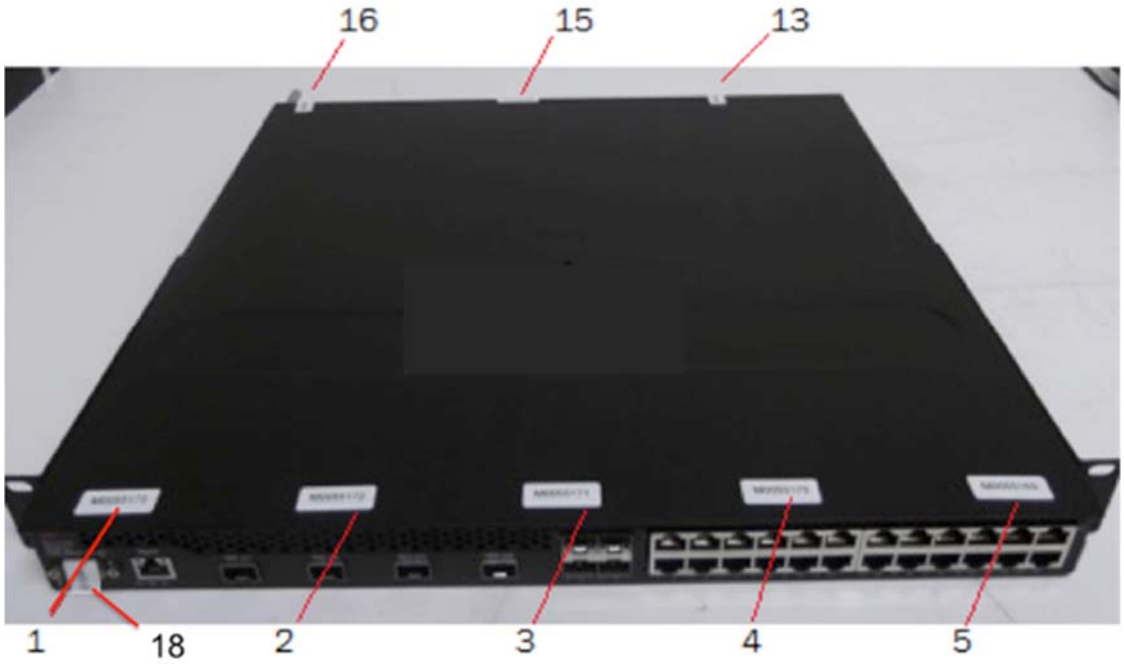

Figure 18 - Top front view of Brocade CER 2024C-4X-RT device with security seals

Figure 19 - Right view of Brocade CER 2024C-4X-RT device with security seals

Figure 20 - Left side view of Brocade CER 2024C-4X-RT device with security seals

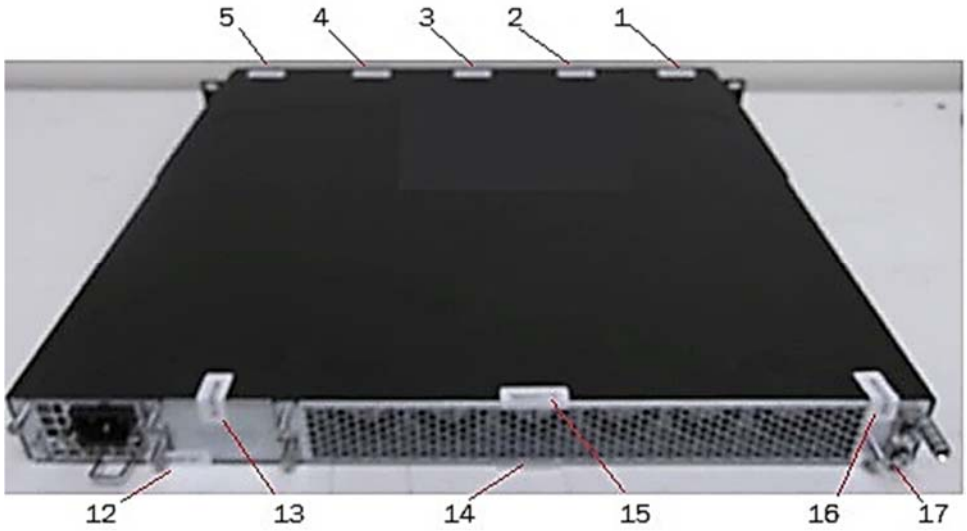

Figure 21 - Rear view of Brocade CER 2024C-4X-RT device with security seals

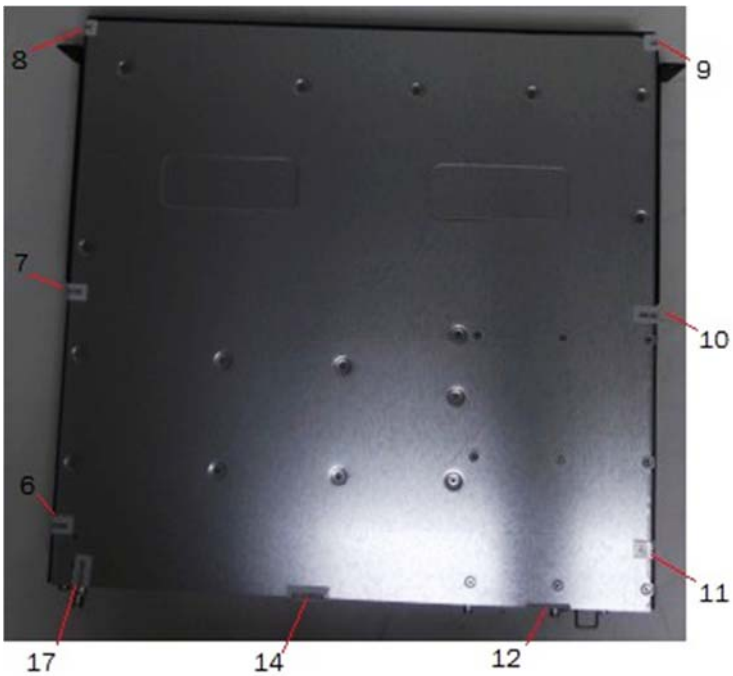

Figure 22 - Bottom view of Brocade CER 2024C-4X-RT device with security seals

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

12.2 Applying Tamper Evident Seals to Brocade NetIron CER 2024F-4X-RT devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024F-4X-RT. Brocade NetIron CER 2024F-4X-RT devices require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). 1 seal is placed vertically over the console port (Seal 20). See Figure 23 for correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). The orientation and placement of seals on the left and right sides mirrors each other. See Figure 24 and Figure 25 for correct seal orientation.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the filler panel to the bottom of the chassis. Seal 14 wraps from power supply module to the bottom of the chassis. Seal 15 wraps from the top cover to the power supply module. Seals 16 and 19 wrap from the top cover to the fan module. Seal 17 and 18 wrap from the fan module to the bottom side of the chassis. See Figure 26 and Figure 27 for correct seal orientation and positioning.

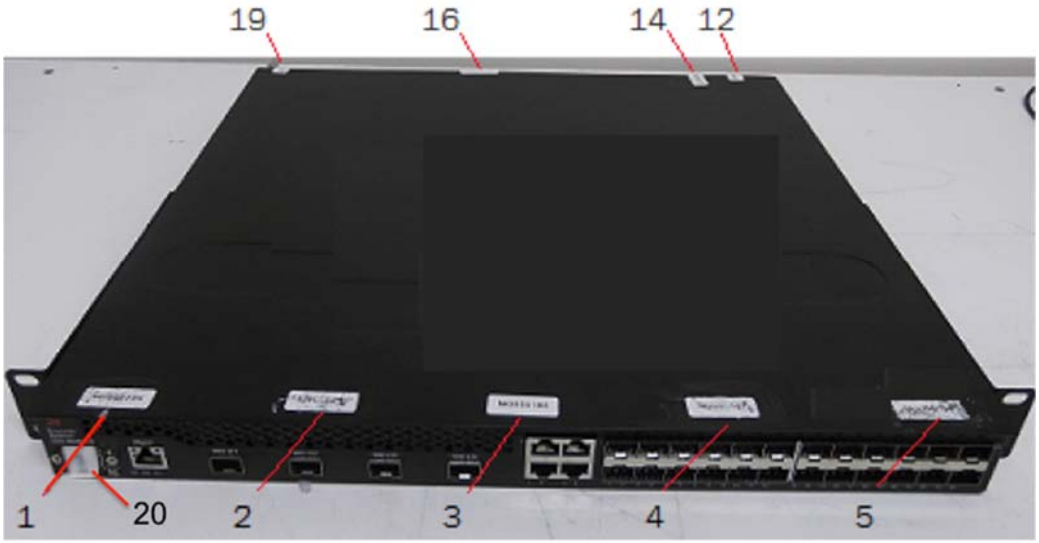

Figure 23 - Top front view of Brocade CER 2024F-4X-RT device with security seals

Figure 24 - Right side view of Brocade CER 2024F-4X-RT device with security seals

Figure 25 - Left side view of Brocade CER 2024F-4X-RT device with security seals

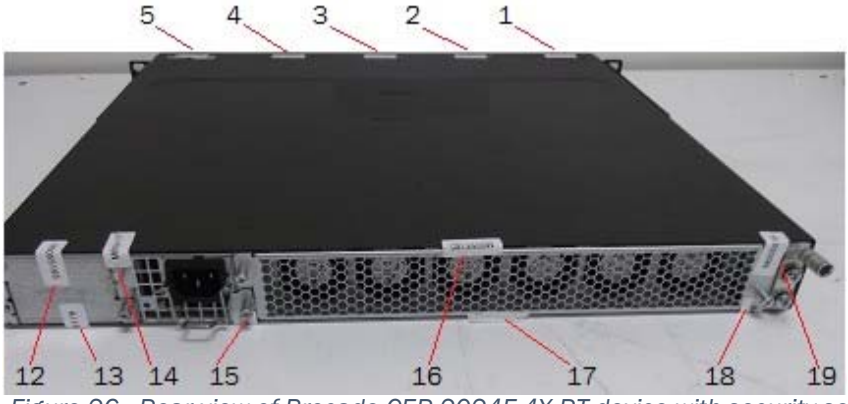

Figure 26 - Rear view of Brocade CER 2024F-4X-RT device with security seals

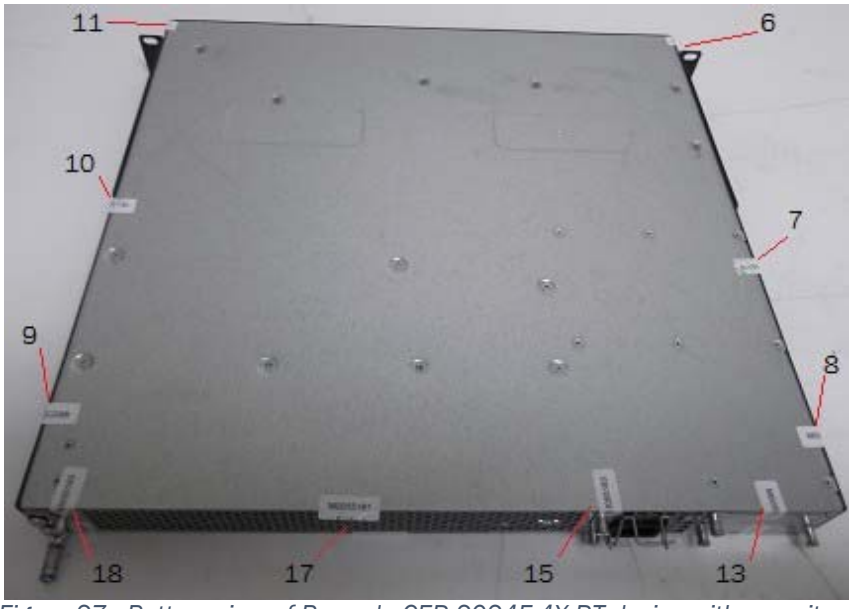

Figure 27 - Bottom view of Brocade CER 2024F-4X-RT device with security seals

REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

12.3 Applying Tamper Evident Seals to Brocade NetIron CES 2024C-4X devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CES 2024C-4X device.

Brocade NetIron CES 2024C-4X device require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 20). See Figure 28 for the correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). See Figure 29 and Figure 30 for correct seal orientation. The orientation and placement of seals on the left and right sides mirrors each other.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the bottom cover of the chassis to the filler panel. Seal 14 wraps from the top cover to the power supply module. Seals 16 and 18 wrap from the top cover to the fan module. Seal 15 touches both the power supply module before wrapping onto the bottom of the chassis. Seals 17 and 19 wrap from the fan module to the bottom of the chassis. See Figure 31 and Figure 32 for correct seal orientation and positioning.

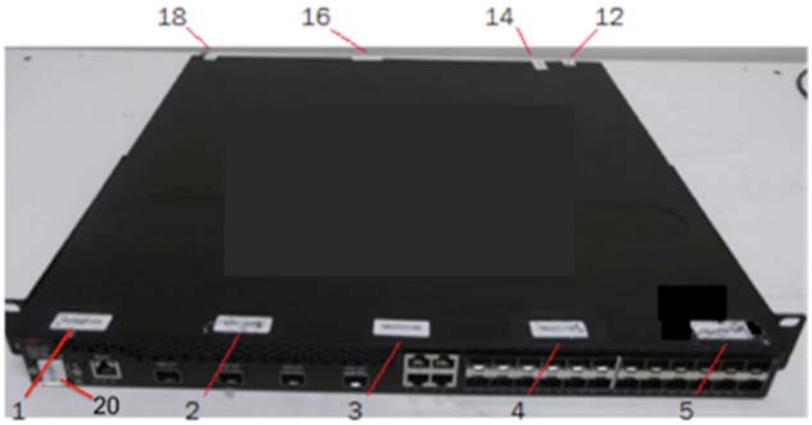

Figure 28 - Top front view of Brocade CES 2024C-4X device with security seals

Figure 29 - Right side view of Brocade CES 2024C-4X device with security seals

Figure 30 - Left side view of Brocade CES 2024C-4X device with security seals

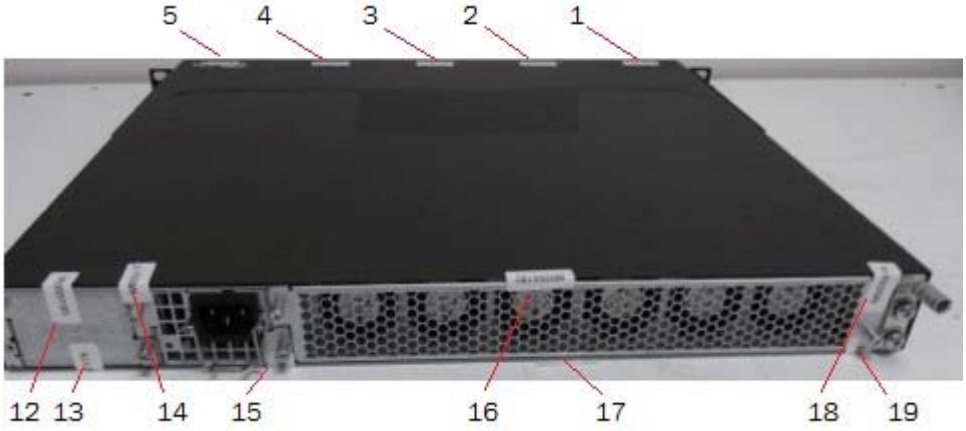

Figure 31 - Rear view of Brocade CES 2024C-4X device with security seals

Figure 32 - Bottom view of Brocade CES 2024C-4X device with security seals

12.4 Applying Tamper Evident Seals to Brocade NetIron CES 2024F-4X devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CES 2024F-4X device. Brocade NetIron CES 2024F-4X device require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 20). See Figure 33 for the correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. 6 seals are needed to complete this step of the procedure (Seals 6 through 11). See Figure 34 and Figure 35 for correct seal orientation. The orientation and placement of seals on the left and right sides mirrors each other.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the bottom of the chassis to the filler panel. Seal 14 wraps from the top cover to the power supply module. Seals 16 and 18 wrap from the top cover to the fan module. Seal 15 touches the power supply module before wrapping onto the bottom of the chassis. Seals 17 and 19 wrap from the fan module to the bottom of the chassis. See Figure 36 and Figure 37 for correct seal orientation and positioning.

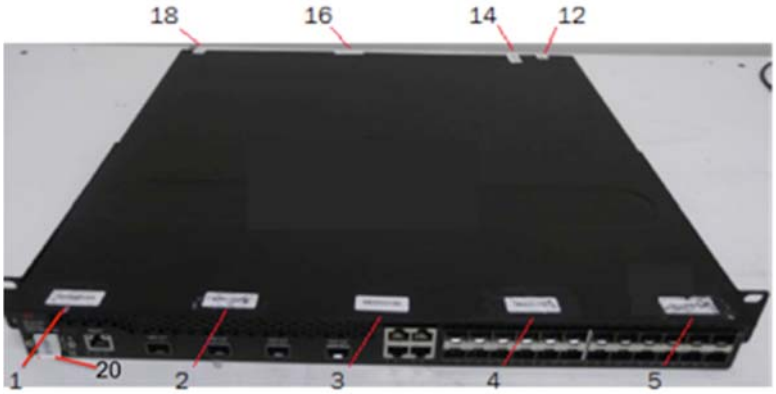

Figure 33 - Top front view of Brocade CES 2024F-4X device with security seals

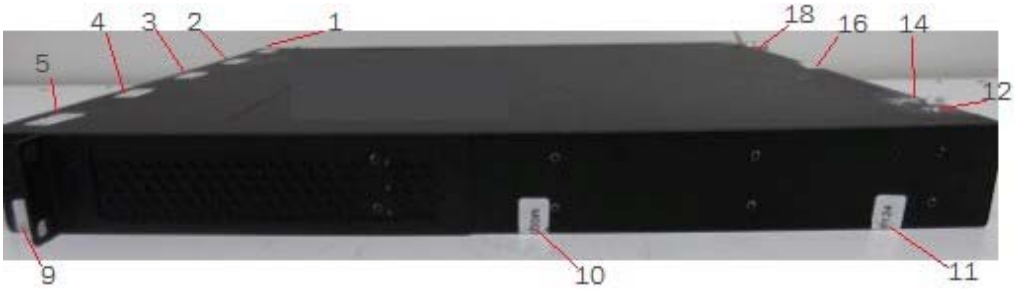

Figure 34 - Right side view of Brocade CES 2024F-4X device with security seals

Figure 35 - Left side view of Brocade CES 2024F-4X device with security seals

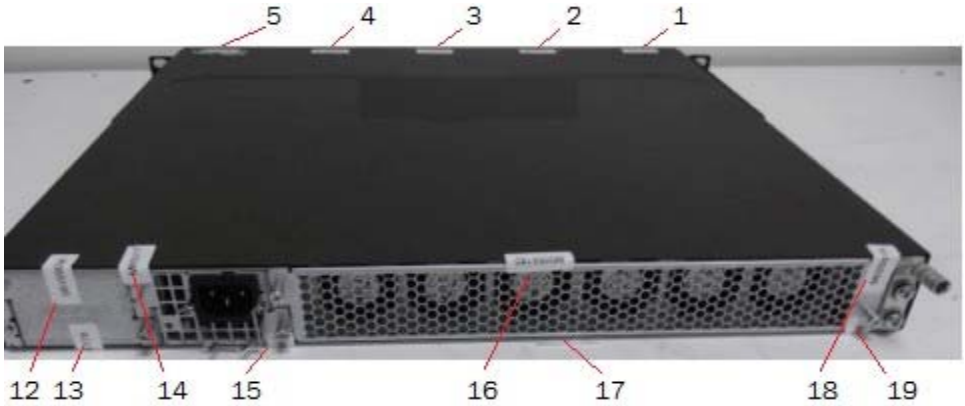

Figure 36 - Rear side view of Brocade CES 2024F-4X device with security seals

Figure 37 - Bottom view of Brocade CES 2024F-4X device with security seals

13 Appendix B: Critical Security Parameters

The module supports the following CSPs and public keys:

1) SSHv2 Host RSA Private Key (2048 bit)
- Description: Used to authenticate SSHv2 server to client
- Type: RSA Private Key
- Generation: N/A
- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Entry: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: N/A
- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

2) SSHv2 Client RSA Private Key (2048 bit)
- Description: Used to establish shared secrets (SSHv2)
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

3) SSHv2 DH Group-14 Private Key (2048 bit)
- Description: Used in SCP and SSHv2 to establish a shared secret
- Type: DH Private Key
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Session termination and "fips zeroize all" command

4) SSHv2 DH Shared Secret Key (2048 bit)
- Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- Type: DH Shared Secret Key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

5) SSHv2/SCP Session Keys (128, 192 and 256 bit (AES CBC and AES CTR))
- Description: AES encryption key used to secure SSHv2/SCP
- Type: AES CBC Key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A

- Output: N/A
- Storage: Plaintext in RAM
-Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

6) SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)
- Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
- Type: HMAC-SHA-1
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

7) SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Type: KDF
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

8) DRBG Seed
- Description: Seeding material for the SP800-90A CTR_DRBG
- Type: DRBG Seed material
- Generation: Internally generated using the NDRNG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Session termination and "fips zeroize all" command

9) DRBG Value V
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

10) DRBG Key
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

11) DRBG Internal State
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

12) User Password
- Description: Password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

13) Port Administrator Password
- Description: Password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

14) Crypto-officer Password
- Description: Password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

15) RADIUS Secret
- Description: Used to authenticate the RADIUS server (8 to 64 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

16) TACACS+ Secret
- Description: Used to authenticate the TACACS+ server (8 to 64 characters)
- Type: Authentication data

- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

**********Public Keys**********

17) Firmware Load RSA Public Key
- Description: RSA 2048-bit public key used to verify signature of firmware of the module
- Type: RSA Public Key
- Generation: N/A, Generated outside the module
- Establishment: N/A
- Entry: Through firmware update
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

18) SSHv2 Host RSA Public Key
- Description: (2048 bit); Used to establish shared secrets
- Type: RSA Public Key
- Generation: N/A, generated outside the module
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

19) SSHv2 Client RSA Public Key
- Description: (2048 bit); Used to establish shared secrets
- Type: RSA Public Key
- Generation: N/A, generated outside the module
- Establishment: N/A
- Entry: Configured by the operator, entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

20) SSHv2 DH Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)
- Type: DH Public Key
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

21) SSHv2 DH Peer Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)
- Type: DH Peer Public Key
- Generation: N/A
- Establishment: N/A
- Entry: Plaintext
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process