Brocade® MLXe® and Brocade NetIron® CER 2000 Series
Ethernet Routers, Brocade NetIron CES 2000 Series
Ethernet Switches

FIPS 140-2 Non-Proprietary Security Policy

Level 2 with Design Assurance Level 3 Validation

Document Version 1.0

February 14, 2014

Revision History

Revision Date	Revision	Summary of Changes
2/14/14	1.0	Initial Draft

Introduction

Brocade MLXe Series routers feature industry-leading 100 Gigabit Ethernet (GbE), 10 GbE, and 1 GbE wire-speed density; rich IPv4, IPv6, Multi-VRF, MPLS, and Carrier Ethernet capabilities without compromising performance; and advanced Layer 2 switching. Built upon Brocade's sixth-generation architecture and terabit-scale switch fabrics, the Brocade MLXe Series has a proven heritage with more than 9000 routers deployed worldwide. Internet Service Providers (ISPs), transit networks, Content Delivery Networks (CDNs), hosting providers, and Internet Exchange Points (IXPs) rely on these routers to meet skyrocketing traffic requirements and to reduce the cost per bit. By leveraging the Brocade MLXe Series, mission-critical data centers can support more traffic, achieve greater virtualization, and provide cloud services using less infrastructure—thereby simplifying operations and reducing costs. Moreover, the Brocade MLXe Series can reduce complexity in large campus networks by collapsing core and aggregation layers, as well as providing connectivity between sites using MPLS/VPLS.

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 and 48-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.

1   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.

Brocade MLXe series devices are chassis devices. Each MLXe chassis contains slots for MR and MR2 management cards, Switch Fabric Modules (SFM), and interface modules. The SFM pass data packets between the various modules. The interface modules themselves forward data without any cryptographic operation or pass data packets to a management module, if any cryptographic operation has to be performed.

The cryptographic boundary of a Brocade MLXe series device is a chassis with two like management cards; one management module runs in active mode while the other is in standby mode. The fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. The power supplies are not part of the cryptographic boundary. Unpopulated switch fabric module and interface modules slots are covered by opaque filler panels, which are part of the cryptographic boundary.

The cryptographic boundary of a 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 an MLXe, 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.

2   Brocade MLXe series

Table 1 MLXe Series Firmware Version

Firmware
Multi-Service IronWare R05.5.00ca

Table 2 MLXe Series Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-4-MR-M-AC	P/N: 80-1006853-01	Brocade MLXe-4 AC system with 2 high speed switch fabric modules, 1 AC 1200 W power supply, 4 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-4-MR-M-DC	P/N: 80-1006854-01	Brocade MLXe-4 DC system with 2 high speed switch fabric modules, 1 DC 1200 W power supply, 4 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-8-MR-M-AC	P/N: 80-1004809-04	Brocade MLXe-8 AC system with 2 high speed switch fabric modules, 2 AC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-8-MR-M-DC	P/N: 80-1004811-04	Brocade MLXe-8 DC system with 2 high speed switch fabric modules, 2 DC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included
BR-MLXE-16-MR-M-AC	P/N: 80-1006820-02	Brocade MLXe-16 AC system with 3 high speed switch fabric modules, 4 AC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-16-MR-M-DC	P/N: 80-1006822-02	Brocade MLXe-16 DC system with 3 high speed switch fabric modules, 4 DC 1200 W power supplies, 2 exhaust fan assembly kits and air filter. MLX management module included.
BR-MLXE-4-MR2-M-AC	P/N: 80-1006870-01	Brocade MLXe-4, AC system with 1 MR2 management module, 2 high speed switch fabric modules, 1 AC 1800 W power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.

SKU	MFG Part Number	Brief Description
BR-MLXE-4-MR2-M-DC	P/N:80-1006872-01	Brocade MLXe-4, DC system with 1 MR2 management module, 2 high speed switch fabric modules, 1 1800 W DC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-8-MR2-M-AC	P/N:80-1007225-01	Brocade MLXe-8 AC system with 1 MR2 management module, 2 high speed switch fabric modules, 2 1800 W AC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-8-MR2-M-DC	P/N:80-1007226-01	Brocade MLXe-8 DC system with 1 MR2 management module, 2 high speed switch fabric modules, 21800 W DC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-16-MR2-M-AC	P/N:80-1006827-02	Brocade MLXe-16 AC system with 1 MR2 management module, 3 high speed switch fabric modules, 4 AC1800 W power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-16-MR2-M-DC	P/N:80-1006828-02	Brocade MLXe-16 DC system with 1 MR2 management module, 3 high speed switch fabric modules, 4 DC 1800 W power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included

Table 3 MLXe Management Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-MLX-MR	P/N:80-1006778-01	NetIron MLX Series management module with 1 GB ECC memory, dual PCMCIA slots, EIA/TIA-232 (RS- 232) serial console port and 10/100/1000 Ethernet port for out-of band management
BR-MLX-MR2-M	P/N:80-1005643-01	MLXE/MLX GEN2, Management module for 4, 8 and 16-Slot Systems. Includes 4 GB RAM, 1 internal Compact Flash

Table 4 MLXe Switch Fabric Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-X-4-HSF	P/N:80-1003891-02	MLXe/MLX/XMR high speed switch fabric module for 4-slot chassis
NI-X-16-8-HSF	P/N:80-1002983-01	MLXe/MLX/XMR high speed switch fabric module for 8-slot and 16-slot chassis

Table 5 MLXe Power Supply Module Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-ACPWR-1800	P/N:80-1003971-01	16-slot, 8-slot and 4-slot MLXe AC 1800W power supply
BR-MLXE-DCPWR-1800	P/N:80-1003972-01	16-slot, 8-slot and 4-slot MLXe DC 1800W power supply
NI-X-ACPWR	P/N:80-1003811-02	16-slot, 8-slot and 4-slot MLXe AC 1200W power supply
NI-X-DCPWR	P/N:80-1002756-03	16-slot, 8-slot and 4-slot MLXe DC 1200W power supply

Table 6 MLXe Fan Module Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-4-FAN	P/N:80-1004114-01	MLXe-4 exhaust fan assembly kit
BR-MLXE-8-FAN	P/N:80-1004113-01	MLXe-8 exhaust fan assembly kit
BR-MLXE-16-FAN	P/N:80-1004112-01	MLXe-16 exhaust fan assembly kit

Table 7 MLXe Filler Panel Part Numbers

SKU	MFG Part Number	Brief Description
NI-X-MPNL	P/N:80-1004760-02	NetIron XMR/MLX Series management module blank panel
NI-X-IPNL	P/N: 80-1006511-02	NetIron XMR/MLX Series interface module blank panel
NI-X-SF3PNL	P/N:80-1004757-02	NetIron XMR/MLX switch fabric module blank panel for 16- and 8-slot chassis
NI-X-SF1PNL	P/N:80-1003009-01	NetIron XMR/MLX switch fabric module blank panel for 4-slot chassis
NI-X-PWRPNL	P/N:80-1003052-01	NetIron XMR/MLX power supply blank panel for 16-and 8-slot chassis
NI-X-PWRPNL-A	P/N: 80-1003053-01	NetIron XMR/MLX power supply blank panel for 4-slot chassis

Table 8 Validated MLXe Configurations

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**

MLXe-4	Chassis: BR-MLXE-4-MR-M-AC (P/N: 80-1006853-01)
	    Management Module: NI-MLX-MR (P/N: 80-1006778-01) (2)
	    Management Module Filler Panels: None
	    Switch Fabric Modules: NI-X-4-HSF (P/N: 80-1003891-02) (2)
	    Switch Fabric Module Filler Panels: NI-X-SF1PNL (P/N: 80-1003009-01) (1)
	    Interface Modules: None
	    Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (4)
	    Fan Modules: BR-MLXE-4-FAN (P/N: 80-1004114-01) (4)
	    AC Power Supply Modules: NI-X-ACPWR (P/N: 80-1003811-02) (1)
	    Power Supply Filler Panels: NI-X-PWRPNL-A (P/N: 80-1003053-01) (3)

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**
MLXe-4	Chassis: BR-MLXE-4-MR-M-DC (80-1006854-01) 　Management Module: NI-MLX-MR (P/N: 80-1006778-01)(2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-4-HSF (P/N: 80-1003891-02) (2) 　Switch Fabric Module Filler Panels: NI-X-SF1PNL (P/N: 80-1003009-01) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (4) 　Fan Modules: BR-MLXE-4-FAN (P/N: 80-1004114-01) (4) 　DC Power Supply Modules: NI-X-DCPWR (P/N: 80-1002756-03) (1) 　Power Supply Filler Panels: NI-X-PWRPNL-A (P/N: 80-1003053-01) (3)
MLXe-4	Chassis: BR-MLXE-4-MR2-M-AC (P/N: 80-1006870-01) 　Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-4-HSF (P/N: 80-1003891-02) (2) 　Switch Fabric Module Filler Panels: NI-X-SF1PNL (P/N: 80-1003009-01) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (4) 　Fan Modules: BR-MLXE-4-FAN (P/N: 80-1004114-01) (4) 　AC Power Supply Modules: BR-MLXE-ACPWR-1800 (P/N: 80-1003971-01) (1) 　Power Supply Filler Panels: NI-X-PWRPNL-A (P/N: 80-1003053-01) (3) Chassis: BR-MLXE-4-MR2-M-DC (P/N: 80-1007225-01) 　Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-4-HSF (P/N: 80-1003891-02) (2) 　Switch Fabric Module Filler Panels: NI-X-SF1PNL (P/N: 80-1003009-01) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (4) 　Fan Modules: BR-MLXE-4-FAN (P/N: 80-1004114-01) (4) 　DC Power Supply Modules: BR-MLXE-DCPWR-1800 (P/N: 80-1003972-01) (1) 　Power Supply Filler Panels: NI-X-PWRPNL-A (P/N: 80-1003053-01) (3)
MLXe-8	Chassis: BR-MLXE-8-MR-M-AC (P/N: 80-1004809) 　Management Module: NI-MLX-MR (P/N: 80-1006778-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (2) 　Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02)(1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (9) 　Fan Modules: BR-MLXE-8-FAN (P/N: 80-1004113-01) (2) 　AC Power Supply Modules: NI-X-ACPWR (P/N: 80-1003811-02) (2) 　Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (2)

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**
MLXe-8	Chassis: BR-MLXE-8-MR-M-DC (8-1004811-04) 　Management Module: NI-MLX-MR (P/N: 80-1006778-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (2) 　Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (9) 　Fan Modules: BR-MLXE-8-FAN (P/N: 80-1004113-01) (2) 　DC Power Supply Modules: NI-X-DCPWR (P/N: 80-1002756-03) (2) 　Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01)(2)
MLXe-8	Chassis: BR-MLXE-8-MR2-M-AC (P/N: 80-1007225-01) 　Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2) 　Management Module Filler Panel: None 　Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (2) 　Switch fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (9) 　Fan Modules: BR-MLXE-8-FAN (P/N: 80-1004113-01) (2) 　AC Power Supply Modules: BR-MLXE-ACPWR-1800 (P/N: 80-1003971-01) (2) 　Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (2) Chassis: BR-MLXE-8-MR2-M-DC (P/N: 80-1007226-01) 　Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (2) 　Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (9) 　Fan Modules: BR-MLXE-8-FAN (P/N: 80-1004113-01) (2) 　DC Power Supply Modules BR-MLXE-DCPWR-1800 (P/N: 80-1003972-01) (2) 　Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (2)
MLXe-16	Chassis: BR-MLXE-16-MR-M-AC (P/N: 80-1006820-02) 　Management Module: NI-MLX-MR (P/N: 80-1006778-01) (2) 　Management Module Filler Panels: None 　Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (3) 　Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1) 　Interface Modules: None 　Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (16) 　Fan Modules: BR-MLXE-16-FAN (P/N: 80-1004112-01) (2) 　AC Power Supply Modules: NI-X-ACPWR (P/N: 80-1003811-02) (4), 　Power Supply Filler Panels: NI-X-PWRPNL(P/N: 80-1003052-01) (4)

Validated MLXe Configurations	
MLXe Model	**SKUs (Count)**

MLXe-16	Chassis: BR-MLXE-16-MR-M-DC (P/N: 80-1006822-02)
	    Management Module: NI-MLX-MR (P/N: 80-1006778-01) (2)
	    Management Module Filler Panels: None
	    Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (3)
	    Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1)
	    Interface Modules: None
	    Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (16)
	    Fan Modules: BR-MLXE-16-FAN (P/N: 80-1004112-01) (2)
	    DC Power Supply Modules: NI-X-DCPWR (P/N: 80-1002756-03) (4),
	    Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (4)

MLXe-16	Chassis: BR-MLXE-16-MR2-M-AC (P/N: 80-1006827-02)
	    Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2)
	    Management Module Filler Panels: None
	    Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (3)
	    Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1)
	    Interface Modules: None
	    Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (16)
	    Fan Modules: BR-MLXE-16-FAN (P/N: 80-1004112-01) (2)
	    AC Power Supply Modules: BR-MLXE-ACPWR-1800 (P/N: 80-1003971-01) (4)
	    Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (4)
	
	Chassis: BR-MLXE-16-MR2-M-DC (P/N: 80-1006828-02)
	    Management Module: BR-MLX-MR2-M (P/N: 80-1005643-01) (2)
	    Management Module Filler Panels: None
	    Switch Fabric Modules: NI-X-16-8-HSF (P/N: 80-1002983-01) (3)
	    Switch Fabric Module Filler Panels: NI-X-SF3PNL (P/N: 80-1004757-02) (1)
	    Interface Modules: None
	    Interface Module Filler Panels: NI-X-IPNL (P/N: 80-1006511-02) (16)
	    Fan Modules: BR-MLXE-16-FAN (P/N: 80-1004112-01) (2)
	    DC Power Supply Modules: BR-MLXE-DCPWR-1800 (P/N: 80-1003972-01) (4)
	    Power Supply Filler Panels: NI-X-PWRPNL (P/N: 80-1003052-01) (4)

Figure 1 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-AC (AC Power Supply)

Figure 2 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-AC backside

Figure 3 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-DC (DC Power Supply)

Figure 4 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-DC backside

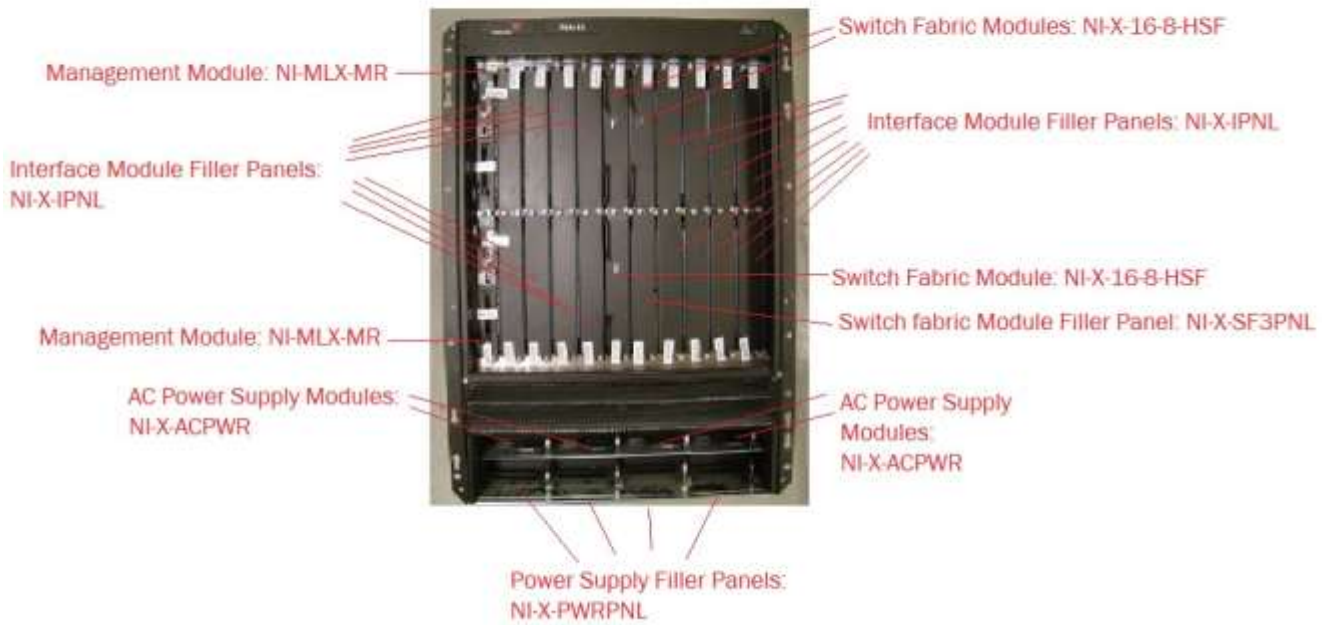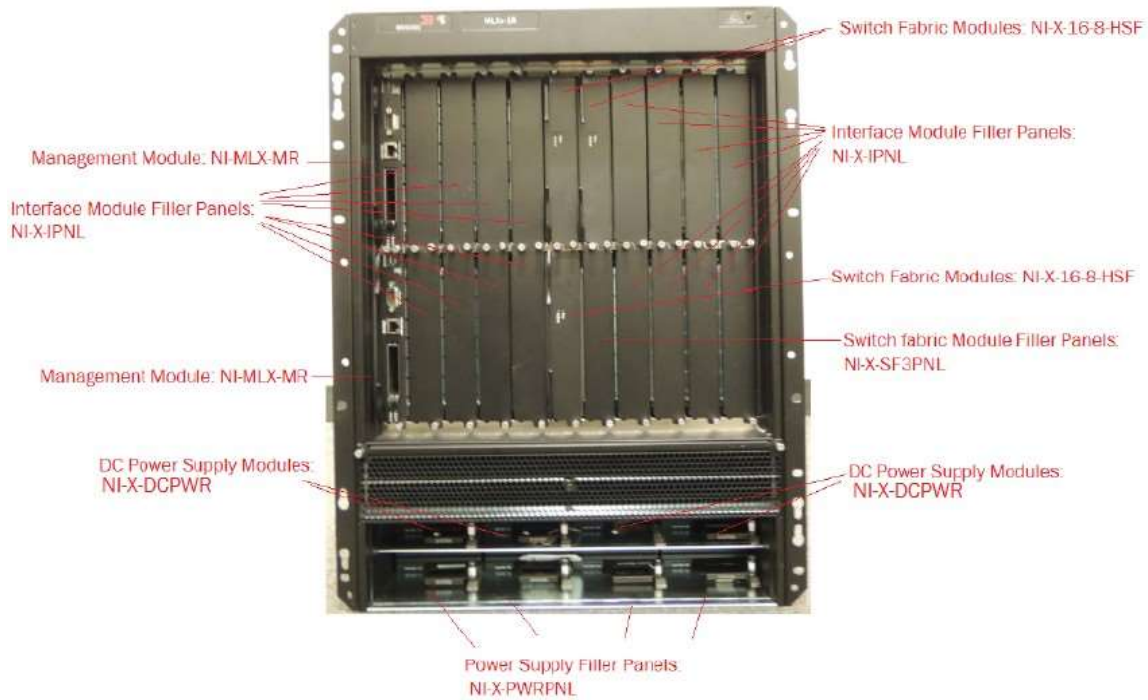Figure 5 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR2-M-AC (AC Power Supply)

Figure 6 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR2-M-AC backside

Figure 7 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR2-M-DC (DC Power Supply)

Figure 8 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR2-M-DC backside

Figure 9 MLXe-8 cryptographic module with Chassis: BR-MLXE-8-MR-M-AC (AC power supply).

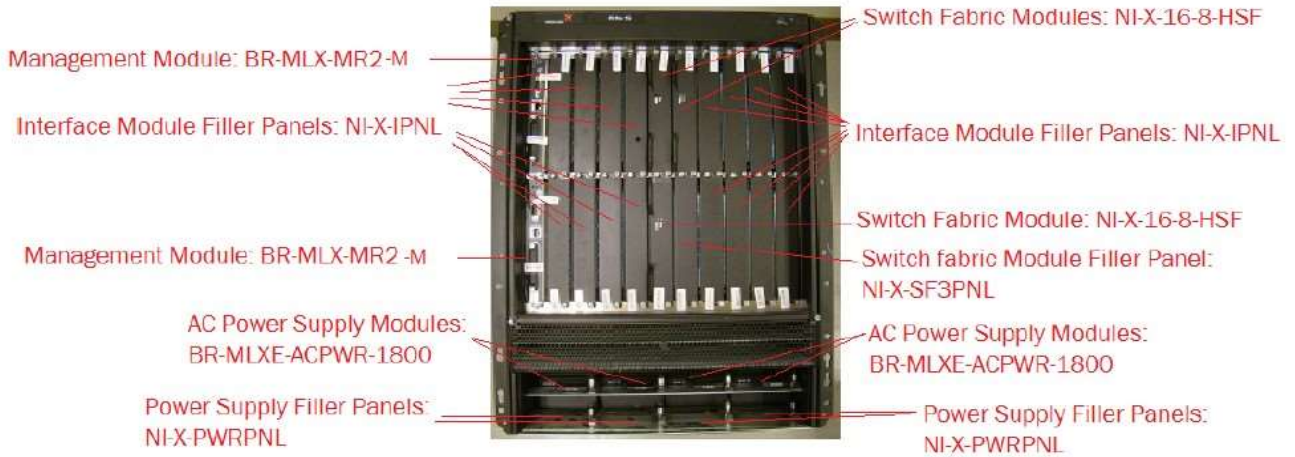FIgure 10 MLXe-8 cryptographic module with Chassis: BR-MLXE-8-MR-M-AC backside

Figure 11 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR-M-DC (DC Power Supply)

FIgure 12 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR-M-DC backside

Figure 13 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR2-M-AC (AC Power Supply)

Figure 14 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR2-M-AC backside

Figure 15 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR2-M-DC (DC Power Supply)

FIgure 16 MLXe-8 Cryptographic Module with Chassis: BR-MLXE-8-MR2-M-DC backside

Figure 17 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-AC (AC Power supply)

Figure 18 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-AC backside

Figure 19 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-DC (DC Power Supply)

Figure 20 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-DC backside

FIgure 21 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR2-M-AC (AC Power Supply)

Figure 22 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR2-M-AC backside

Figure 23 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR2-M-DC (DC Power Supply)

Figure 24 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR2-M-DC backside

3   Brocade CER 2000 series

Table 9 CER 2000 Series Firmware Version

Firmware
Multi-Service IronWare R05.5.00ca

Table 10 CER 2000 Series Part Numbers

SKU	MFG Part Number	Brief Description
NI-CER-2048F-ADVPREM-AC	P/N:80-1003769-07	NetIron CER 2048F includes 48 SFP ports of 100/1000 Mbps Ethernet. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software)
NI-CER-2048F-ADVPREM-DC	P/N:80-1003770-08	NetIron CER 2048F includes 48 SFP ports of 100/1000 Mbps Ethernet. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software)
NI-CER-2048FX-ADVPREM-AC	P/N:80-1003771-07	NetIron CES 2048FX includes 48 SFP ports of 100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software)
NI-CER-2048FX-ADVPREM-DC	P/N:80-1003772-08	NetIron CES 2048FX includes 48 SFP ports of 100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software)
NI-CER-2024F-ADVPREM-AC	P/N:80-1006902-02	NetIron CER 2024F includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W AC power supply (RPS9), and Advanced Services software
NI-CER-2024F-ADVPREM-DC	P/N:80-1006904-02	NetIron CER 2024F includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2024C-ADVPREM-AC	P/N:80-1007032-02	NetIron CER 2024C includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W AC power supply (RPS9), and Advanced Services software

SKU	MFG Part Number	Brief Description
NI-CER-2024C-ADVPREM-DC	P/N:80-1007034-02	NetIron CER 2024C includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. Optional slot for 2 ports of 10 Gigabit Ethernet XFP, 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2048C-ADVPREM-AC	P/N:80-1007039-02	NetIron CER 2048C includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. The router also includes 500W AC power supply (RPS9), and Advanced Services software
NI-CER-2048C-ADVPREM-DC	P/N:80-1007040-02	NetIron CER 2048C includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and Advanced Services software
NI-CER-2048CX-ADVPREM-AC	P/N:80-1007041-02	NetIron CER 2048CX includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W AC power supply (RPS9), and ADV_PREM (Advanced Services software
NI-CER-2048CX-ADVPREM-DC	P/N:80-1007042-02	NetIron CER 2048CX includes 48 RJ45 ports of 10/100/1000 Mbps Ethernet with 2 ports of 10 Gigabit Ethernet XFP for uplink connectivity. The router also includes 500W DC power supply (RPS9DC), and ADV_PREM (Advanced Services software
BR-CER-2024F-4X-RT-DC	P/N:80-1007212-01	Brocade CER2024F-4XRT includes 24 SFP ports of 100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with 4 fixed ports of 10 Gigabit Ethernet SFP+, 500W DC power supply (RPS9DC)
BR-CER-2024C-4X-RT-DC	P/N:80-1007213-01	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 DC power supply (RPS9DC)
BR-CER-2024F-4X-RT-AC	P/N:80-1006529-01	Brocade CER2024C-4XRT includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4 combination RJ45/SFP Gigabit Ethernet with4 fixed ports of 10 Gigabit Ethernet SFP+, 500W AC power supply (RPS9),
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)

Table 11 CER Interface Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-CER-2024-2X10G	P/N:80-1003719-03	NetIron CER 2000 Series 2x10G XFP uplink

***Note: The following non-security relevant components have been excluded from the requirements of FIPS 140-2 as they do not have access to CSPs and perform no security relevant function:
> -AC Power Supply
> -DC Power Supply
> -2X10GXFP Uplink

Table 12 CER Power Supply Module 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 13 Validated CER 2000 Series Configurations

Validated CER 2000 Series Configurations		
CER Model	Configuration 1, SKUs (Count)	Configuration 2, SKUs (Count)
NI-CER-2048F-ADVPREM-AC (P/N: 80-1003769-07)	Base: NI-CER-2048F-AC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	N/A
NI-CER-2048F-ADVPREM-DC (P/N: 80-1003770-08)	Base: NI-CER-2048F-DC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	N/A
NI-CER-2048FX-ADVPREM-AC (P/N: 80-1003771-07)	Base: NI-CER-2048FX-AC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	N/A
NI-CER-2048FX-ADVPREM-DC (P/N: 80-1003772-08)	Base: NI-CER-2048FX-DC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	N/A
NI-CER-2024F-ADVPREM-AC (P/N: 80-1006902-02)	Base: NI-CER-2024F-AC Interface Module: None License: SW-CER-2024-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	Base: NI-CER-2024F-AC Interface Module: NI-CER-2024-2X10G (P/N: 80-1003719-03) (1) License: SW-CER-2024-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)
NI-CER-2024F-ADVPREM-DC (P/N: 80-1006904-02)	Base: NI-CER-2024F-DC Interface Module: None License: SW-CER-2024-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	Base: NI-CER-2024F-DC Interface Module: NI-CER-2024-2X10G (P/N: 80-1003719-03) (1) License: SW-CER-2024-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)

NI-CER-2024C-ADVPREM-AC (P/N: 80-1007032-02)	Base: NI-CER-2024C-AC Interface Module: None License: SW-CER-2024-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	Base: NI-CER-2024C-AC Interface Module: NI-CER-2024-2X10G (P/N: 80-1003719-03) (1) License: SW-CER-2024-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)
NI-CER-2024C-ADVPREM-DC (P/N: 80-1007034-02)	Base: NI-CER-2024C-DC Interface Module: None License: SW-CER-2024-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	Base: NI-CER-2024C-DC Interface Module: NI-CER-2024-2X10G (P/N: 80-1003719-03) (1) License: SW-CER-2024-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)
NI-CER-2048C-ADVPREM-AC (P/N: 80-1007039-02)	Base: NI-CER-2048C-AC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	N/A
NI-CER-2048C-ADVPREM-DC (P/N: 80-1007040-02)	Base: NI-CER-2048C-DC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	N/A
NI-CER-2048CX-ADVPREM-AC (P/N: 80-1007041-02)	Base: NI-CER-2048CX-AC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)	N/A
NI-CER-2048CX-ADVPREM-DC (P/N: 80-1007042-02)	Base: NI-CER-2048CX-DC Interface Module: None License: SW-CER-2048-ADVU (1) Power Supply: RPS9DC (P/N: 80-1003869-02) (1)	N/A
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)	N/A
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)	N/A
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)	N/A
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)	N/A

Figure 25 NI-CER-2048F-ADVPREM-AC with Base: NI-CER-2048F-AC and License: SW-CER-2048-ADVU

Figure 26 NI-CER-2048F-ADVPREM-AC backside with Power supply: RPS9 (AC Power supply)

Figure 27 NI-CER-2048F-ADVPREM-DC with Base: NI-CER-2048F-DC and License: SW-CER-2048-ADVU

Figure 28 NI-CER-2048F-ADVPREM-DC backside with Power supply: RPS9DC (DC Power supply)

Figure 29 NI-CER-2048FX-ADVPREM-AC with Base: NI-CER-2048FX-AC and License: SW-CER-2048-ADVU

Figure 30 NI-CER-2048FX-ADVPREM-AC backside with Power supply: RPS9 (AC Power Supply)

Figure 31 NI-CER-2048FX-ADVPREM-DC with Base: NI-CER-2048FX-DC and License: SW-CER-2048-ADVU

FIgure 32 NI-CER-2048FX-ADVPREM-DC backside with Power supply: RPS9DC (DC Power supply)

Figure 33 NI-CER-2024F-ADVPREM-AC with Base: NI-CER-2024F-AC and License: SW-CER-2024-ADVU

Figure 34 NI-CER-2024F-ADVPREM-AC backside with Power supply: RPS9 (AC Power supply)

Figure 35 NI-CER-2024F-ADVPREM-DC with Base: NI-CER-2024F-DC and License: SW-CER-2024-ADVU

Figure 36 NI-CER-2024F-ADVPREM-DC backside with Power supply: RPS9DC (DC Power supply)

Figure 37 NI-CER-2024F-ADVPREM-AC with Base: NI-CER-2024F-AC, Interface module: NI-CER-2024-2X10G and License: SW-CER-2024ADVU

Figure 38 NI-CER-2024F-ADVPREM-AC backside with Interface module: NI-CER-2024-2X10G with Power supply: RPS9 (AC Power Supply)

Figure 39 NI-CER-2024F-ADVPREM-DC with Base: NI-CER-2024F-DC, Interface module: NI-CER-2024-2X10G and License: SW- CER-2024-ADVU

Figure 40 NI-CER-2024F-ADVPREM-DC backside with Interface module: NI-CER-2024-2X10G with Power supply: RPS9DC (DC Power Supply)

Figure 41 NI-CER-2024C-ADVPREM-AC with Base: NI-CER-2024C-AC and License: SW-CER-2024-ADVU

Figure 42 NI-CER-2024C-ADVPREM-AC backside with Power supply: RPS9 (AC Power supply)

Figure 43 NI-CER-2024C-ADVPREM-DC with Base: NI-CER-2024C-DC and License: SW-CER-2024-ADVU

Figure 44 NI-CER-2024C-ADVPREM-DC backside with Power supply: RPS9DC (DC Power supply)

Figure 45 NI-CER-2024C-ADVPREM-AC with Base: NI-CER-2024C-AC, Interface module: NI-CER-2024-2X10G and License: SW-CER-2024-ADVU

Figure 46 NI-CER-2024C-ADVPREM-AC backside with Interface module: NI-CER-2024-2X10G with Power supply RPS9 (AC Power Supply)

Figure 47 NI-CER-2024C-ADVPREM-DC with Base: NI-CER-2024C-DC, Interface module: NI-CER-2024-2X10G and License: SW-CER-2024-ADVU

Figure 48 NI-CER-2024C-ADVPREM-DC backside with Interface module: NI-CER-2024-2X10G with Power supply RPS9DC (DC Power Supply)

Figure 49 NI-CER-2048C-ADVPREM-AC with Base: NI-CER-2048C-AC and License: SW-CER-2048-ADVU

Figure 50 NI-CER-2048C-ADVPREM-AC backside with Power supply: RPS9 (AC Power supply)

Figure 51 NI-CER-2048C-ADVPREM-DC with Base: NI-CER-2048-DC and License: SW-CER-2048-ADVU

Figure 52 NI-CER-2048C-ADVPREM-DC backside with Power supply: RPS9DC (DC Power Supply)

Figure 53 NI-CER-2048CX-ADVPREM-AC with Base: NI-CER-2048CX-AC and License: SW-CER-2048-ADVU

Figure 54 NI-CER-2048CX-ADVPREM-AC backside with Power supply: RPS9 (AC Power Supply)

Figure 55 NI-CER-2048CX-ADVPREM-DC with Base: NI-CER-2048CX-DC and License: SW-CER-2048-ADVU

Figure 56 NI-CER-2048CX-ADVPREM-DC backside with Power supply: RPS9DC (DC Power Supply)

Figure 57 BR-CER-2024F-4X-RT-DC with Base: BR-CER-2024F-4X-RT-DC and License:SW-CER-2024-RTUPG

Figure 58 BR-CER-2024F-4X-RT-DC backside with Power supply RPS9DC (DC Power Supply)

Figure 59 BR-CER-2024C-4X-RT-DC with Base: BR-CER-2024C-4X-RT-DC and License: SW-CER-2024-RTUPG

Figure 60 BR-CER-2024C-4X-RT-DC with Power supply RPS9DC (DC Power Supply)

Figure 61 BR-CER-2024F-4X-RT-AC with Base: BR-CER-2024F-4X-RT-AC and License:SW-CER-2024-RTUPG

Figure 62 BR-CER-2024F-4X-RT-AC backside with Power supply RPS9 (AC Power Supply)

Figure 63 BR-CER-2024C-4X-RT-AC with Base: BR-CER-2024C-4X-RT-AC and License: SW-CER-2024-RTUPG

Figure 64 BR-CER-2024C-4X-RT-AC with Power supply RPS9 (AC Power Supply)

4   Brocade CES 2000 series

Table 14 CES 2000 Series Firmware Version

Firmware
Multi-Service IronWare R05.5.00ca

Table 15 CES 2000 Series Part Numbers

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 CES 2024C-4X includes 24 RJ45 ports of 10/100/1000 Mbps Ethernet with 4combination 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 16 CES Power Supply Module 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 17 Validated CES 2000 Series Configurations

Validated CES 2000 Series Configurations	
CES Model	SKUs (Count)
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)

Figure 65 BR-CES-2024C-4X-AC with Base: BR-CES-2024C-4X-AC

Figure 66 BR-CES-2024C-4X-AC with Power supply: RPS9 (AC Power supply)

Figure 67 BR-CES-2024C-4X-DC with Base: BR-CES-2024C-4X-DC

Figure 68 BR-CES-2024C-4X-DC with Power supply: RPS9DC (DC Power supply)

Figure 69 BR-CES-2024F-4X-AC with Base: BR-CES-2024F-4X-AC

Figure 70 BR-CES-2024F-4X-AC backside with Power supply: RPS9 (AC Power supply)

Figure 71 BR-CES-2024F-4X-DC with Base: BR-CES-2024F-4X-DC

Figure 72 BR-CES-2024F-4X-DC backside with Power supply: RPS9DC (DC Power supply)

5   Ports and Interfaces

Each MLXe and CER 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.

5.1.1   Brocade MLXe Series

While not included in this validation, the Brocade MLXe series supports a variety of interface modules. The interface modules provide Ethernet ports with multiple connector types and transmission rates. Models in the series can provide up to:

- 256 10 Gigabit Ethernet ports per chassis

- 1536 Gigabit Ethernet ports per chassis

5.1.2   MLXe MR and MR2 Management Cards

The MR management module provides physical ports and status indicators. The MR's major features are listed below.

- 1 GB SDRAM

- Dual PCMCIA slots for external storage

- One Console port, EIA/TIA-232

- 10/100/1000 Mbps Ethernet port for out-of-band management

The MR2 management module provides physical ports and status indicators. The MR2's major features are listed below.

- GB SDRAM

- One internal 2GB compact flash drive

- One external compact flash slot

- Console port, EIA/TIA-232

- 10/100/1000 Mbps Ethernet port for out-of-band management

5.1.3   Brocade NetIron CER 2000 Series and CES 2000 Series

Models in the Brocade NetIron CER 2000 series provide either 24 or 48 Gigabit Ethernet ports. Models in the Brocade NetIron CES 2000 series provide 24 Ethernet ports and four fixed 10GbE ports. Each series supports both copper and fiber connectors with some models supporting combination ports. Some models support 10 Gigabit Ethernet uplink ports. All models have an out-of-band Ethernet management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

5.1.4   Interfaces

Table 18 shows the correspondence between the physical interfaces of NetIron devices and logical interfaces defined in FIPS 140-2.

Table 18 Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports	Data input
Console	
Networking ports	Data output
Console	
Networking ports	Control input
Console	
PCMCIA	
Networking ports	Status output
Console	
LED	
PCMCIA	
Power plugs	Power

5.1.4.1   Status LEDs

Table 19 Power and fan status LEDs for the CER 2024 and CES 2024 models

LED	Position	State	Meaning
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

LED	Position	State	Meaning
			faulty.
AC PS1 (labeled P1)	Right 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 PS2 (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.

Table 20 Power and fan status LEDs for the CER 2048 models[1]

LED	Position	State	Meaning
Fan (labeled Fn)	Left 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.
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.
PS2 (labeled P2)	Left 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
DC	Right side of front panel	Off	No DC Power
		Amber	The power supply has DC power, but the output is disabled or the power supply is over temperature or the fan failed
		Green	Power supply has DC power, is enabled and is operating normal.
		Green blinking	Power supply has input power, but the DC output is disabled

Table 21 Power and fan status LEDs for the MR Management Module

---

[1] The LEDs for the CER 2048CX, 2048F, and 2048FX models are just below the management Ethernet port on the left side of the front panel, labeled P1, P2, and Fn, left to right. The LEDs for the 2048C are just below the console connector on the left side of the front panel, labeled P1, P2, and Fn, left to right.

LED	State	Meaning
Port 1 and Port 2	On or blinking	The software is currently accessing the auxiliary flash card
	Off	The software is not currently accessing the axillary flash card
Active	On	The module is functioning as the active management module
	Off	The module is functioning as the standby management module.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
10/100/1000 Ethernet Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
10/100/1000 Ethernet Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

Table 22 Power and fan status LEDs for the MR2 Management Module

LED	State	Meaning
Slot 1(Internal) and Slot 2(External)	On or blinking	The software is currently accessing the compact flash card
	Off	The software is not currently accessing the compact flash card
Active	On	The module is functioning as the active management module
	Off	The module is functioning as the standby management module.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
10/100/1000 Ethernet Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
10/100/1000 Ethernet Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

5.2   Modes of Operation

The NetIron cryptographic module can operate as a validated cryptographic module or non-validated cryptographic module. The factory default is to run the module as a non-validated module. Firmware integrity checks are always performed for the validated cryptographic module. Firmware integrity checks are not performed for the non-validated cryptographic module.

When the FIPS Approved mode is invoked on a non-validated cryptographic module, the module starts operating as a validated cryptographic module. A validated cryptographic module cannot be transitioned to a non-validated cryptographic module.

The NetIron validated cryptographic module has two modes of operation: FIPS Approved mode and non-Approved mode. Section 7 describes services and cryptographic algorithms available in FIPS Approved mode.

In non-Approved mode, the module runs without the FIPS operational rules applied. Section 9.1.1 FIPS Approved Mode describes how to invoke FIPS Approved mode. The module does not support bypass.

5.3   Module Validation Level

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

Table 23 NetIron Security Levels

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

6   Roles

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

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).

4. Unauthenticated Role: The unauthenticated role on the device in FIPS Approved mode is possible while using serial console to access the device. Console is considered as a trusted channel. The scope of the role is same as the User Role without authentication. The enable command allows user to authenticate using a different role. Based on the authentication method mentioned in Section 7.1, the role would change to one of Crypto-officer, Port Configuration Administrator or User role.

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.

7   Services

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

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

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameter (CSP) associated with the service. Table 24 summarizes the available FIPS Approved cryptographic functions. Table 25 lists cryptographic functions that are allowed only in non-FIPS Approved mode of operation.

Table 24 FIPS Approved Cryptographic Functions

Label	Cryptographic Function
SHS	Secure Hash Standard
DSA	Digital Signature Algorithm

Table 25 Non-Approved Cryptographic Functions only allowed in non-FIPS Approved Mode

Label	Cryptographic Function
KW	RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength; non-compliant)
DH	Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
AES	Advanced Encryption Standard (non-compliant)
Triple-DES	Triple Data Encryption Standard (non-compliant)
DRBG	Deterministic Random Bit Generator (non-compliant)
HMAC	Keyed-Hash Message Authentication Code (non-compliant)
SNMP	SNMPv3 KDF
MD5	Message-Digest Algorithm 5
NDRNG	Non-Deterministic Random Number Generator used for generation of seeds for DRBG only
SP800-135 KDF	TLS 1.0/1.1 KDF (non-compliant) and SSHv2 KDF (non-compliant)
HMAC-MD5	Used to support RADIUS authentication
SHA -256	SHA -256 (non-compliant)
SHA-384	SHA -384(non-compliant)
SHA-512	SHA -512(non-compliant)
RSA	Rivest Shamir Adleman (non-compliant)
DSA	Signature generation (non-compliant)
HMAC-SHA1-96	Used for OSPFv3 authentication (non-compliant)

7.1 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 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.

7.2   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.

Like the User role, the Port Configuration Administrator role operator is allowed to view all the web pages. In addition, the role operator is allowed to modify any configuration that is related to an interface. For example, the Configuration->Port page allows the operator to make changes to individual port properties within the page.

7.2.1   Console

Section 7.1.1, above, describes this service.

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.

7.3   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.

7.3.1   Console

This service is described in Section 7.1.1 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.

NOTICE: The cryptographic module "does not" support RSA key generation in FIPS mode.

7.4   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:

1. TFTP
   o 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.

2. Telnet
   o 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).

3. SNMP
   o Allows access to Critical Security Parameter (CSP) MIB objects

4. HTTP
   o This service provides a graphical user interface for managing a NetIron MLXe device over an unsecure communication channel. The HTTP service is not supported on CER 2000 Series devices.

8   Policies

8.1   Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the 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(CSP).

3) The cryptographic module performs the following tests:

   a) Power up Self-Tests:

      i) Cryptographic Known Answer Tests (KAT):

         (1) SHA-1
         (2) DSA 1024 bit key size, SHA-1 KAT (Signature/Verification)

      ii) Firmware Integrity Test[2] (DSA 1024 bit, SHA-1 Signature Verification)

      iii) 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) <u>Conditional Self-Tests:</u>

    i) Continuous Random Number Generator (RNG) test – N/A
    ii) Pairwise Consistency Test – N/A
    iii) Firmware Load Test – DSA 1024 SHA-1 (Signature Verification)
    iv) Manual Key Entry Test – N/A
    v) Bypass Test – N/A
    vi) Critical Functions – N/A

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

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

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

8.1.1 Cryptographic Module Operational Rules

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

External communication channels/ports are not available before initialization of an MLXe, CER 2000 series and CES 2000 series device.

8.2 Authentication

NetIron devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using:

1. Line password authentication

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.

8.2.2 Strength of Authentication

NetIron devices minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 7 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (26) letters, and punctuation marks (18) in passwords. Therefore the probability of a random attempted is $1/80^7$ which is less than $1/1,000,000$.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one minute period is $60/80^7$ which is less than $1/100,000$.

8.3   Access Control and Critical Security Parameter (CSP)

Table 26 Access Control Policy and Critical Security Parameter (CSP) summarize the access operators in each role have to critical security parameters. Grayed out table cells indicate that the intersection of the role and the CSP have not security relevance. 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 by executing a fips zeroize all command.

Table 26 Access Control Policy and Critical Security Parameter (CSP)

	User	Port Administrator	Crypto-officer
CSP / Services	Console	Console	Console
User Password	x		xrwd
Port Administrator Password		x	xrwd
Crypto-officer Password			xrwd
Firmware Integrity / Firmware Load DSA Public Key			xd

8.3.1   CSP Zeroization

The *crypto key zeroize* command removes CSPs.

Executing the *no fips enable* command zeroizes all CSPs.

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 module may be configured for FIPS mode by following the steps described in the security policy by an authorized human operator that is physically present at the cryptographic boundary when performing this activity; failure to adhere to the requirement of physical presence is an explicit violation of the security policy and as such deems the cryptographic module fully non-compliant and unfit for service in an Approved mode of operation.

The module is put in FIPS Approved mode of operation by following the following procedure:

MLXe Series Devices:

1. Log in as Crypto-officer.
2. Perform Zeroize service.
3.   Do not enable AAA authentication.
4.   Do not enable HTTPS.
5.   Do not enable TLS.
6.   Do not enable SNMP.
7.   Do not enable SSH and SCP.
8.   Do not use port 280.
9.   Do not use HTTPS SSL 3.0 access Command web-management and RC4 cipher.
10. Do not enable HTTP.
11. Do not use monitor mode.
12. Run "Fips Enable" command
13. Reload the module
14. Enable TFTP
15. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

CER Series and CES Series Devices:
1.   Log in as Crypto-officer.
2.   Perform Zeroize service.
3.   Do not enable AAA authentication.
4.   Do not enable TLS.
5. Do not enable SNMP.
6.   Do not enable SSH and SCP.
7.   Do not use port 280.
8.   Do not use monitor mode.
9.   Run "Fips Enable" command
10. Reload the module

11. Enable TFTP

12. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

NOTICE: This submission is impacted by SP800-131A. The only cryptographic service allowed in FIPS mode is to perform a firmware load via a directly attached console by an authorized human operator that is physically present at the cryptographic boundary.

Table 27 Algorithm Certificates for the MLXe Series with an MR Management Module

Algorithm	Supports	Certificate
Secure Hash Standard	SHA-1	#2221
Digital Signature Algorithm (DSA)	1024-bit keys	#798

Table 28 Algorithm Certificates for the MLXe Series with an MR2 Management Module

Algorithm	Supports	Certificate
Secure Hash Standard	SHA-1	#2222
Digital Signature Algorithm (DSA)	1024-bit keys	#799

Table 29 Algorithm Certificates for the CER 2000 Series/ CES

Algorithm	Supports	Certificate
Secure Hash Standard	SHA-1	#2223
Digital Signature Algorithm (DSA)	1024-bit keys	#800

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

NOTICE: This cryptographic module is impacted by SP800-131A transition rules effective January 1,2014. In FIPS mode the only FIPS Approved algorithm is DSA 1024 SHA-1 Signature Verification (Certs. #798, #799 and #800).

The following non-Approved and not allowed cryptographic methods are not allowed within limited scope in the FIPS Approved mode of operation:

1. DES
2. MD2
3. RC2
4. RC4

10 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
ECDSA	Elliptic Curve Digital Signature Algorithm
FI	FastIron platform
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
PRF	pseudo-random function
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
SSH	Secure Shell
TACACS	Terminal Access Control Access-Control System
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
XFP	10 Gigabit Small Form Factor Pluggable

11 References

[FIPS 186-2+]   Federal Information Processing Standards Publication 186-2 (+Change Notice), Digital
                       Signature Standard (DSS), 27 January 2000

[RSA PKCS #1]   PKCS #1: RSA Cryptography Specifications Version 2.1

[SP800-90]   National Institute of Standards and Technology Special Publication 800-90,
                       Recommendation for Random Number Generation Using Deterministic Random Bit
                       Generators (Revised), March 2007

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 remove to remove the seal residue. Then use additional alcohol to clean off any residual adhesive remover before applying a new seal.

Applying Tamper Evident Seals to a Brocade MLXe-4 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-4 device. Each Brocade MLXe-4 device requires the placement of nineteen (19) seals:

- **Front:** Fifteen (15) seals are required to complete the physical security requirements illustrated in Figure 73. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling.

- **Rear:** Four (4) seals are required to complete the physical security requirements illustrated in Figure 74. Affix one seal at each location designated in Figure 74. Each seal is applied from the top panel of the chassis to the flange of each of the four fan FRUs. You must bend each seal to place them correctly. See Figure 74 for correct seal orientation and positioning.

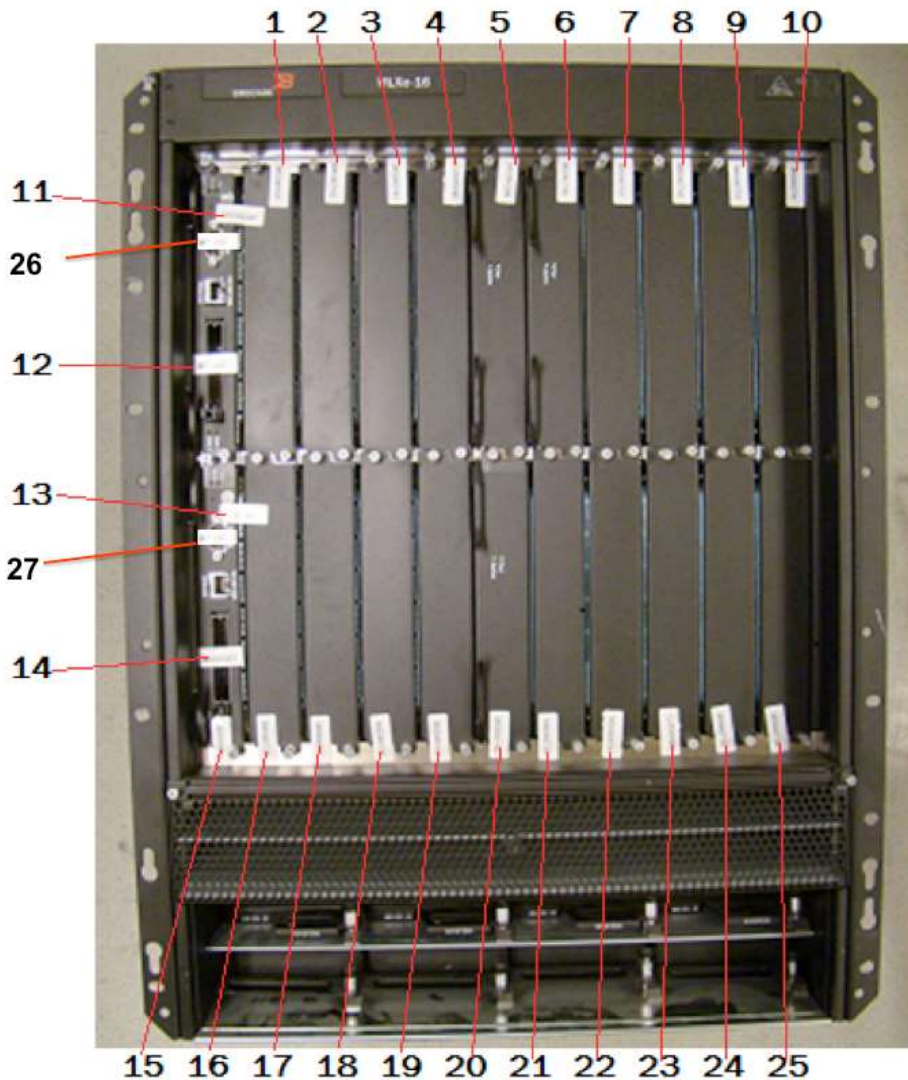**Figure 73 Front view of a Brocade MLXe-4 device with security seals**
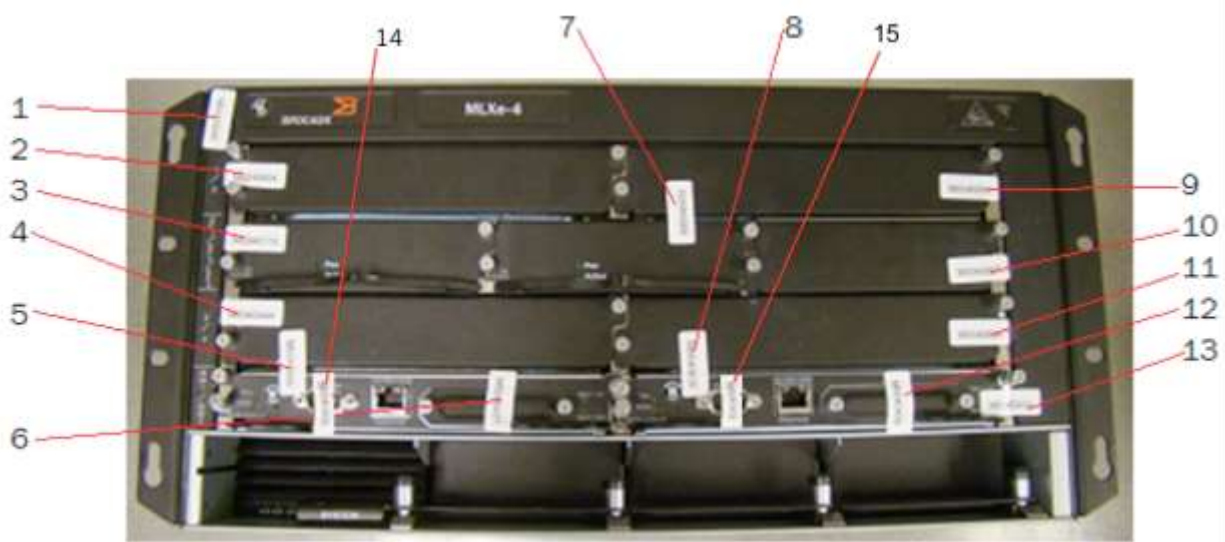
**Figure 74 Rear and side view of a Brocade MLXe-4 device with security seals**
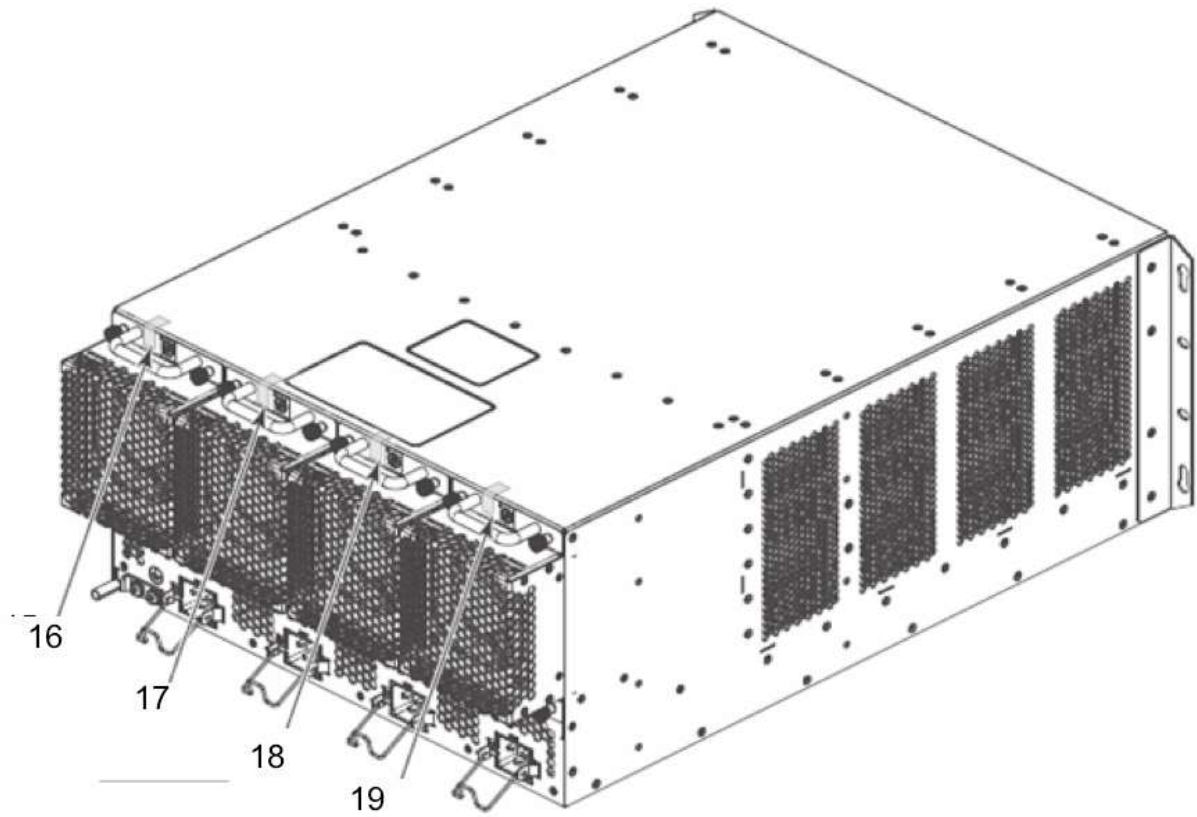
Applying Tamper Evident Seals to a Brocade MLXe-8 device

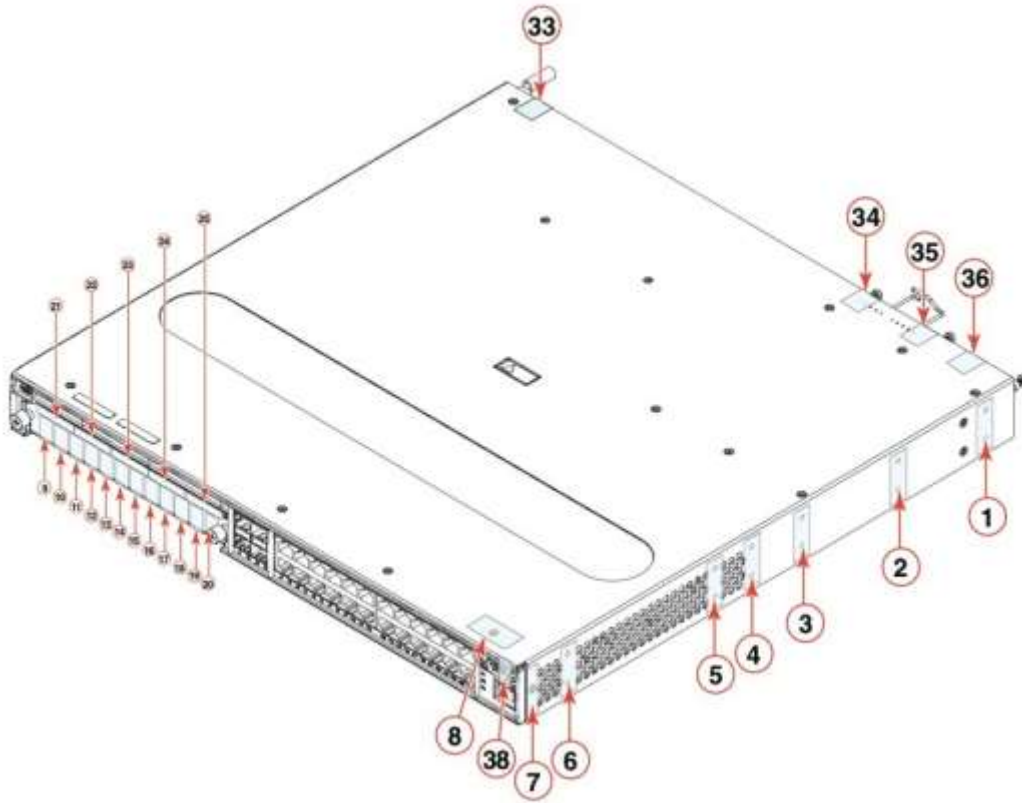Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-8 device. Each Brocade MLXe-8 device requires the placement of twenty-two (22) seals:

- Front: Twenty (20) seals are required to complete the physical security requirements illustrated in Figure 75. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling.

- Rear: Two (2) seals are required to complete the physical security requirements illustrated in Figure 75. Affix one (1) seal at each location designated in Figure 76. Each seal is applied from the top panel of the chassis to the flange of each of the two fan FRUs. You must bend each seal to place them correctly. See Figure 76 for correct seal orientation and positioning.

Figure 75 Front view of a Brocade MLXe-8 device with security seals
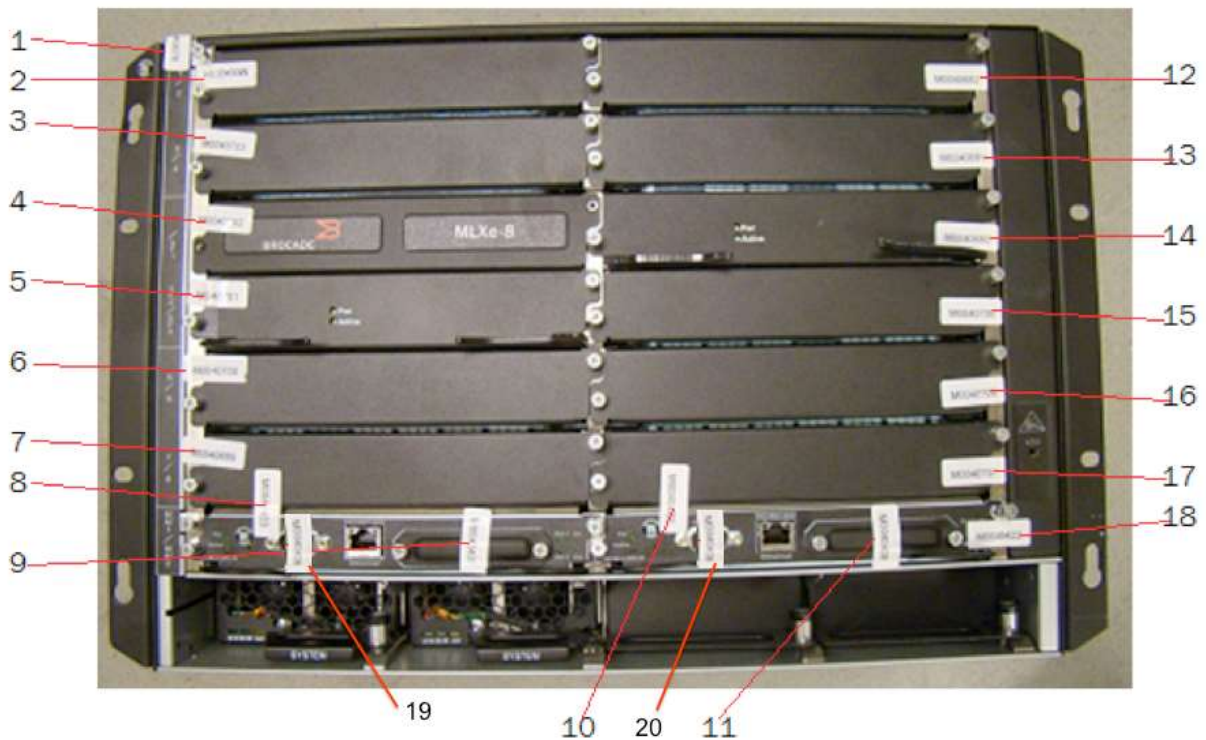
Figure 76 Rear and side view of a Brocade MLXe-8 device with security seals
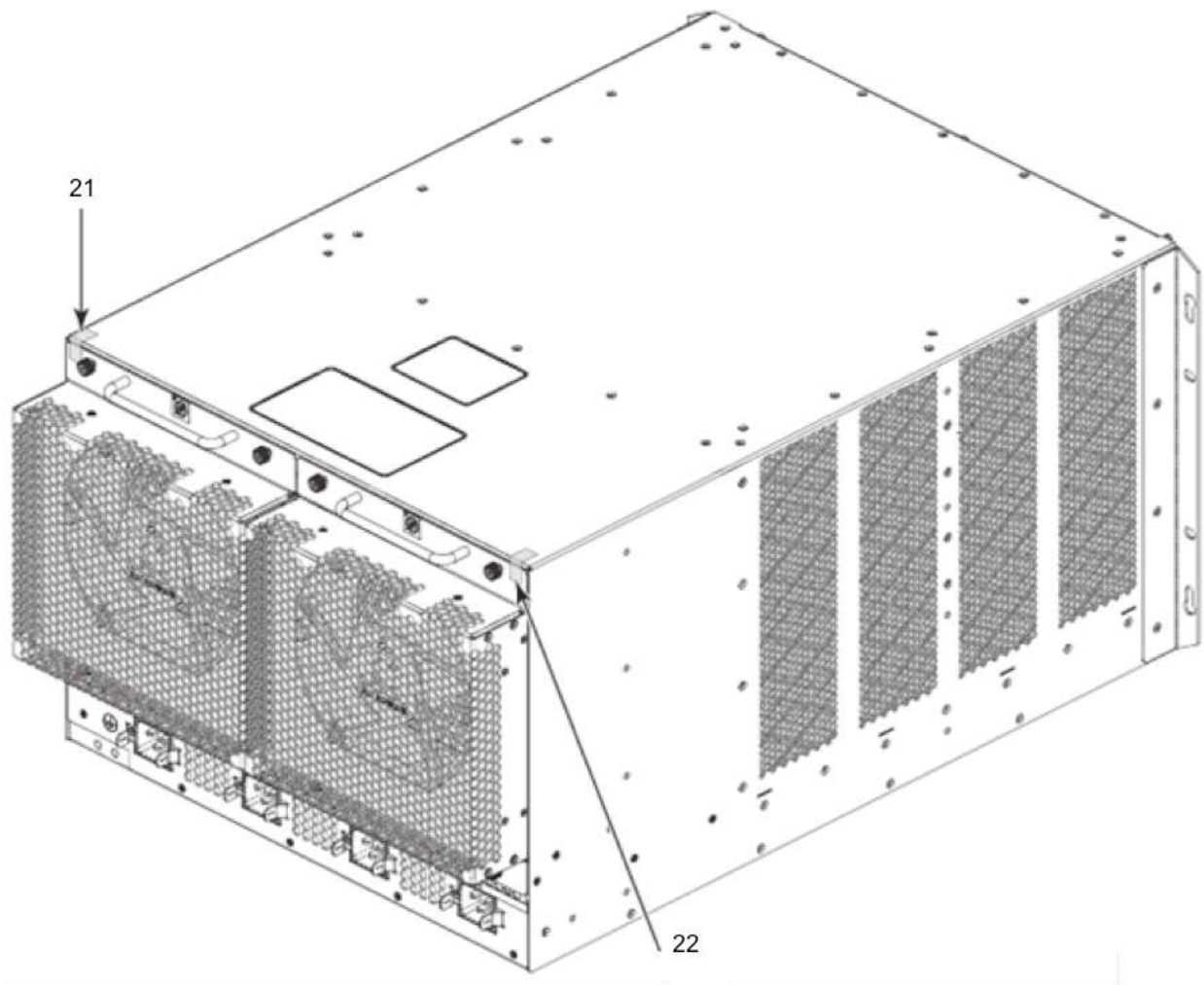
Applying Tamper Evident Seals to a Brocade MLXe-16 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-16 device. Each Brocade MLXe-16 device requires the placement of twenty-nine (29) seals:

- Front: Twenty-seven (27) seals are required to complete the physical security requirements illustrated in Figure 77. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling.

- Rear: Two (2) seals are required to complete the physical security requirements illustrated in Figure 78. Affix one (1) seal at each location designated in Figure 78. Each seal is applied from the back panel of the chassis to the flange of each of the two fan FRUs. See Figure 78 for correct seal orientation and positioning.

Figure 77 Front view of a Brocade MLXe-16 device with security seals

Figure 78 Rear and side view of a Brocade MLXe-16 device with security seals
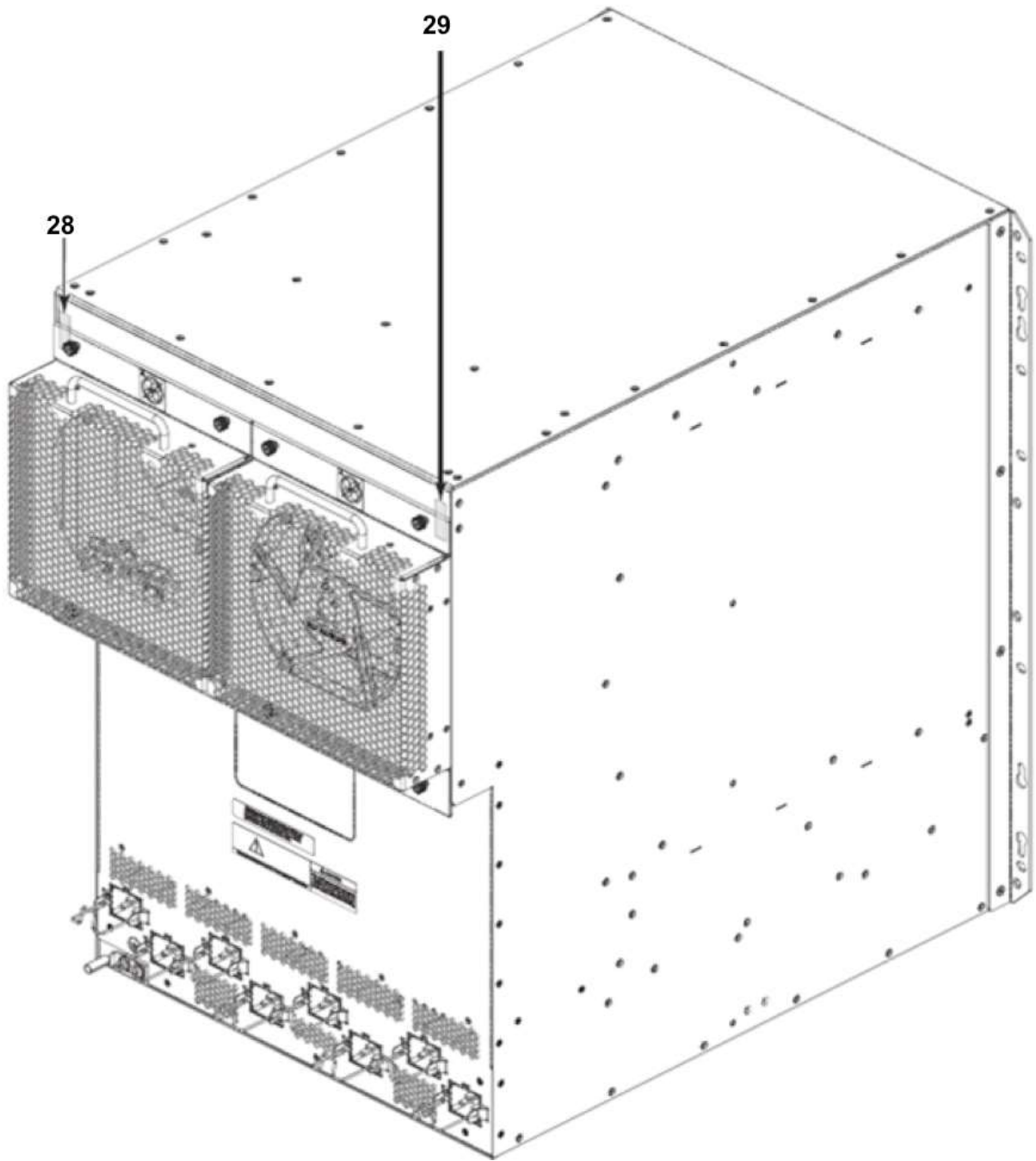
Applying Tamper Evident Seals to Brocade NetIron CER 2024C devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024C device. This configuration requires the placement of 38 seals.

- Top: Affix one (1) seal at seal location 8 lengthwise over the top rightmost screw that connects the faceplate to the device. See Figure 79 for correct seal orientation and positioning.

- Right and left sides: Affix seven (7) seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 80 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation placement of seals on the right side. See Figure 81 for correct seal orientation and placement of the seal on the left side of the switch.

- Front: Affix seventeen (17) seals in a vertical and horizontal layout so that every vent hole in the filler panel, installed on the left side of the front panel is obscured. Additionally, one seal is placed vertically over the console port.

- Rear: Affix four (4) seals from the top cover to the rear panel. Affix one (1) seal at seal location 37 from the rear panel to the bottom panel. See Figure 81 for correct seal orientation and placement.

Figure 79 Front view of a Brocade NetIron CER 2024C device without 2X10G Module with security seals
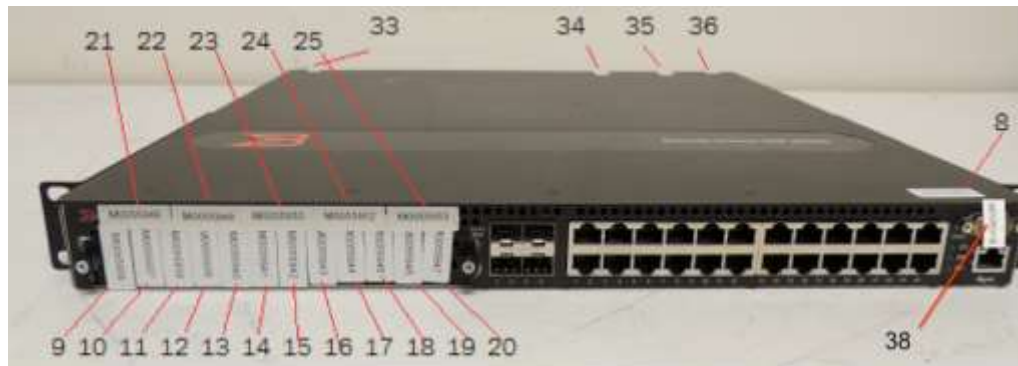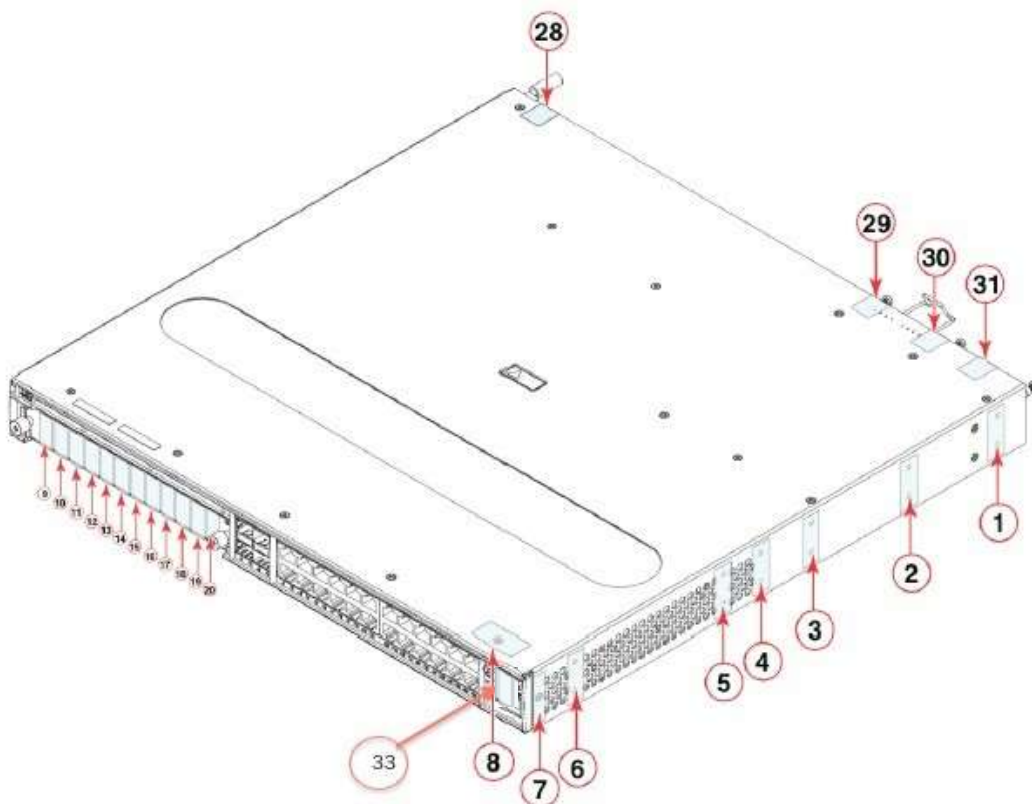
Figure 80 Front, top, and right side view of a Brocade NetIron CER 2024C device with security seals
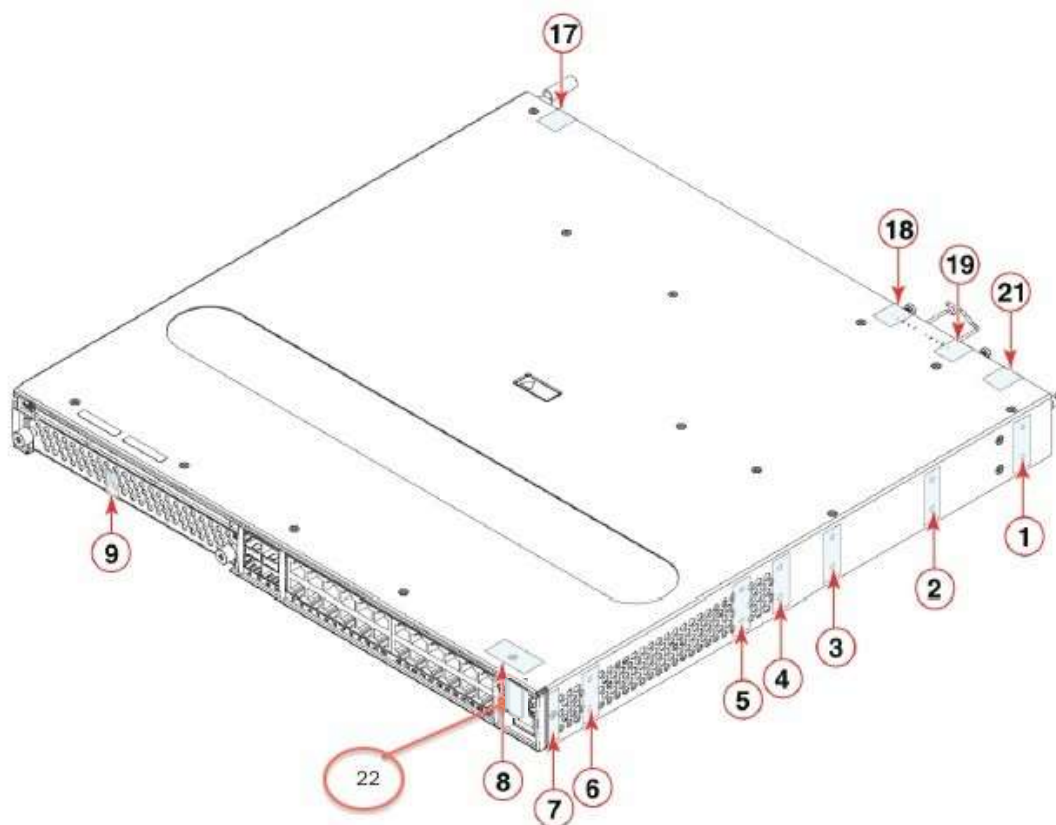
Figure 81 Rear, top and left side view of a Brocade NetIron CER 2024C device with security seals
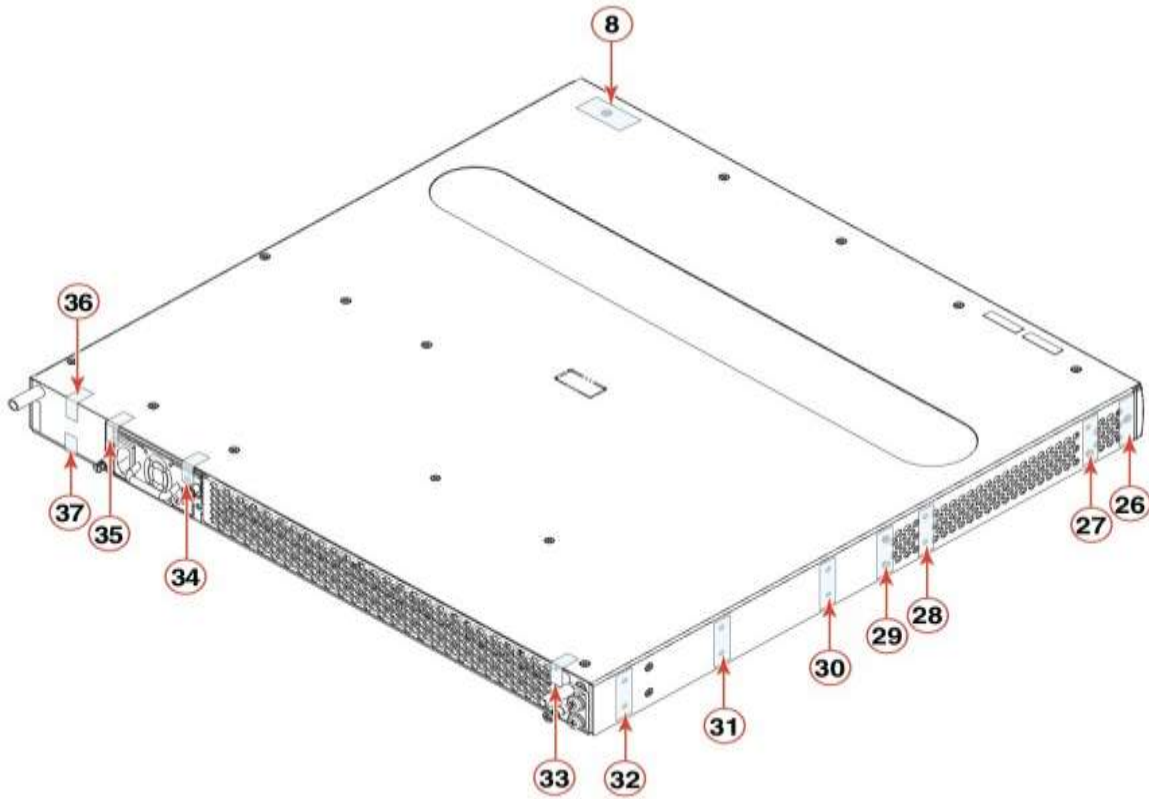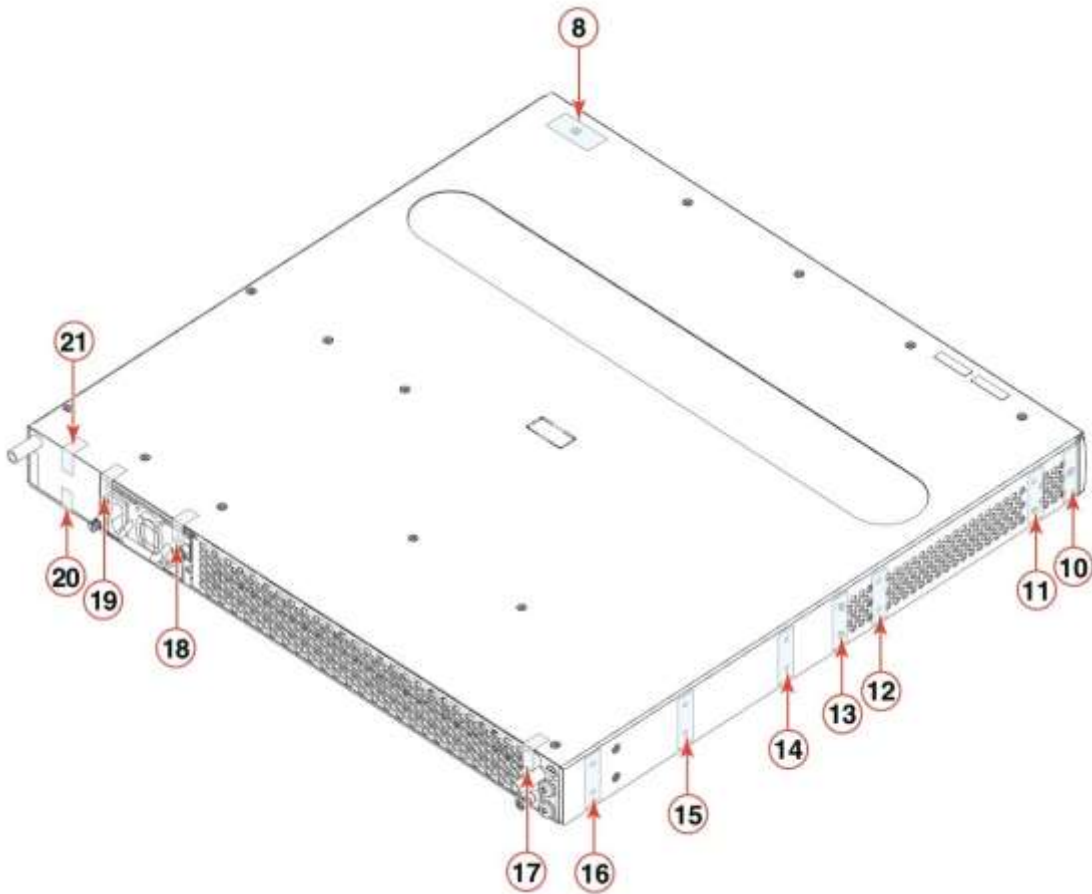
Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024C device configured with a 2x10G XFP uplink module (NI-CER-2024-2X10G). This configuration requires the placement of twenty-two (22) seals:

- **Top**: Affix one (1) seal at seal location 8 lengthwise completely covering the top rightmost screw that connects the faceplate to the device. See **Figure 82** for correct seal orientation and positioning.

- **Right and left sides**: Affix seven seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See **Figure 82** for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side. See **Figure 83** for correct seal orientation and positioning on the left side.

- **Front**: Affix a seal from the front panel to the bottom panel, and place one seal vertically over the console port. See **Figure 82** for correct seal orientation and placement.

- **Rear**: Affix four seals from the top panel to the rear panel. Affix one seal at seal location 20 from the rear panel to the bottom panel. See **Figure 83** for correct seal orientation and placement.

Figure 82 Front, top, and right side view of the security seals placement for a Brocade NetIron CER 2024C device with a 2x10G XFP uplink module
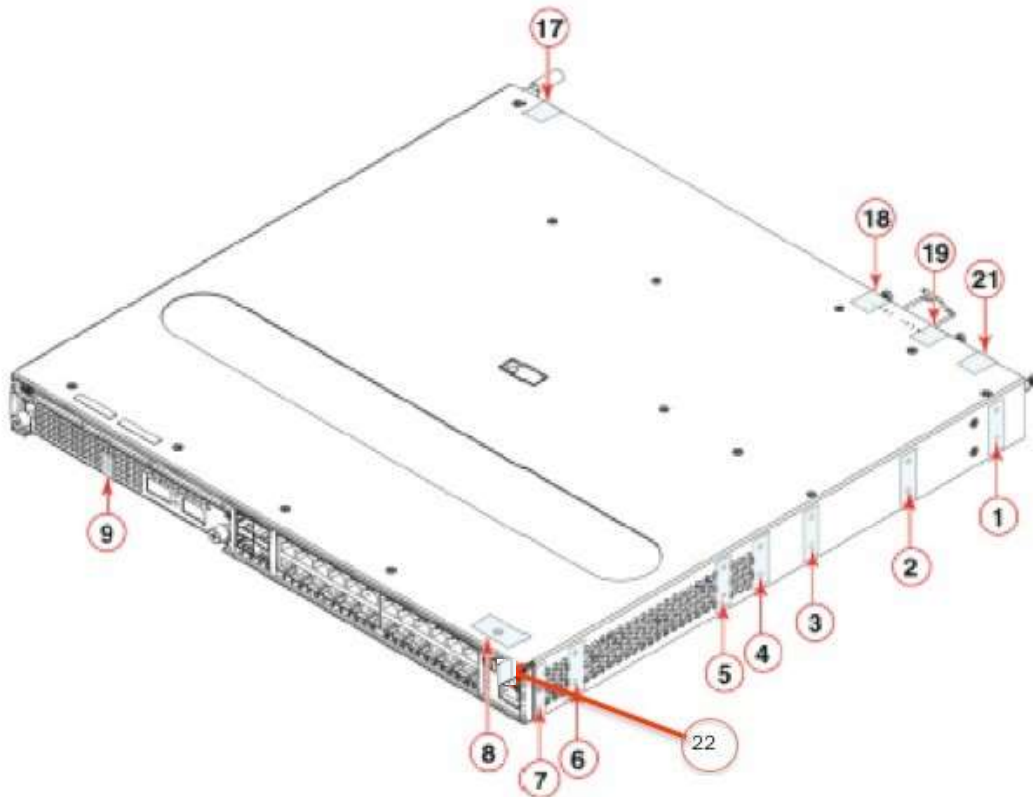
Figure 83 Rear, top and left side view of the security seals placement for a Brocade NetIron CER 2024C device with a 2x10G XFP uplink module
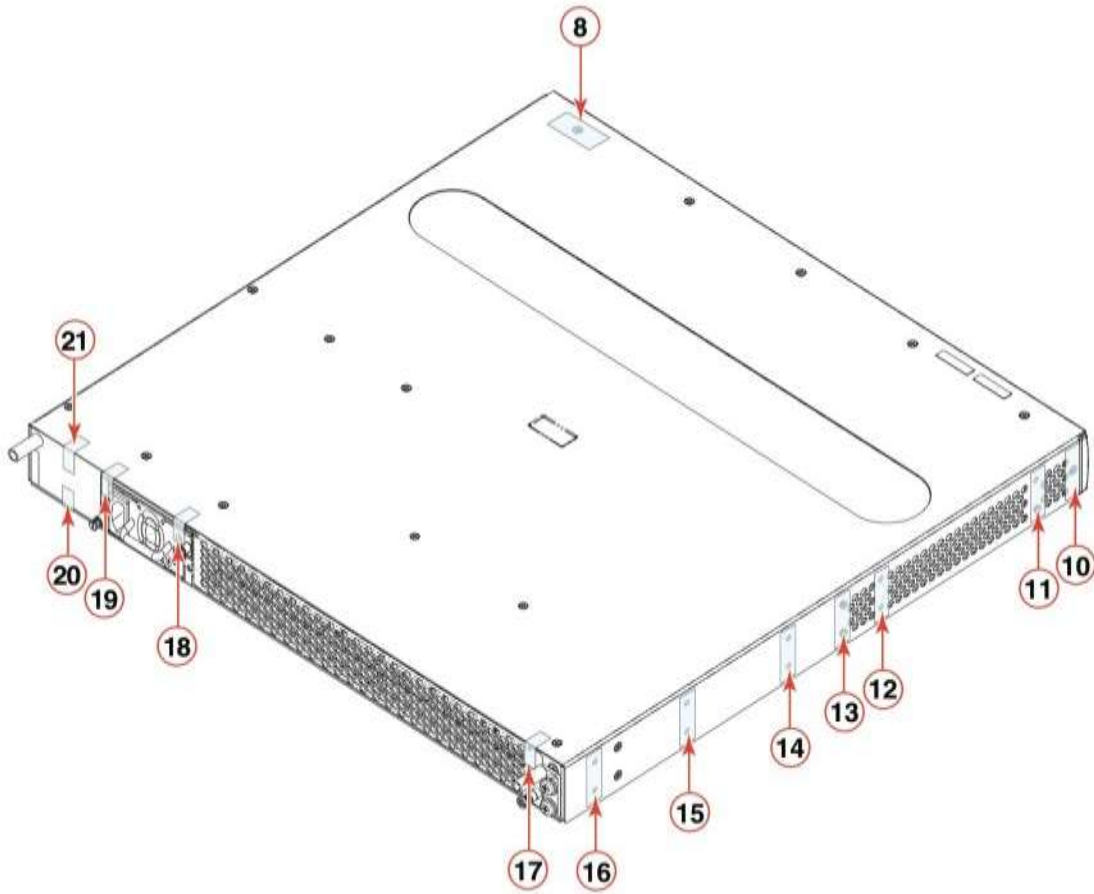
Applying Tamper Evident Seals to Brocade NetIron CER 2024F devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024F device. This configuration requires the placement of 33 seals:

- Top: Affix one (1) seal at seal location 8 lengthwise over the top rightmost screw that connects the faceplate to the device. See Figure 84 for correct seal orientation and positioning.

- Right and left sides: Affix seven (7) seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 84 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation placement of seals on the right side. See Figure 86 for the correct seal orientation and placement of the seal on the left side of the switch.

- Front: Affix twelve (12) seals in a vertical layout to the front, installed on the left side of the front panel is obscured. Additionally, one seal is placed vertically over the console port. See Figure 85 for correct seal orientation and placement.

- Rear: Affix four (4) seals from the top cover to the rear panel. Affix one (1) seal at seal location 32 from the rear panel to the bottom panel. See Figure 86 for correct seal orientation and placement.

Figure 84 Front, top, and right side view of a Brocade NetIron CER 2024F device with security seals

Figure 85 Front view of a Brocade NetIron CER 2024F device with security seals

Figure 86 Rear, top and left side view of a Brocade NetIron CER 2024F device with security seals
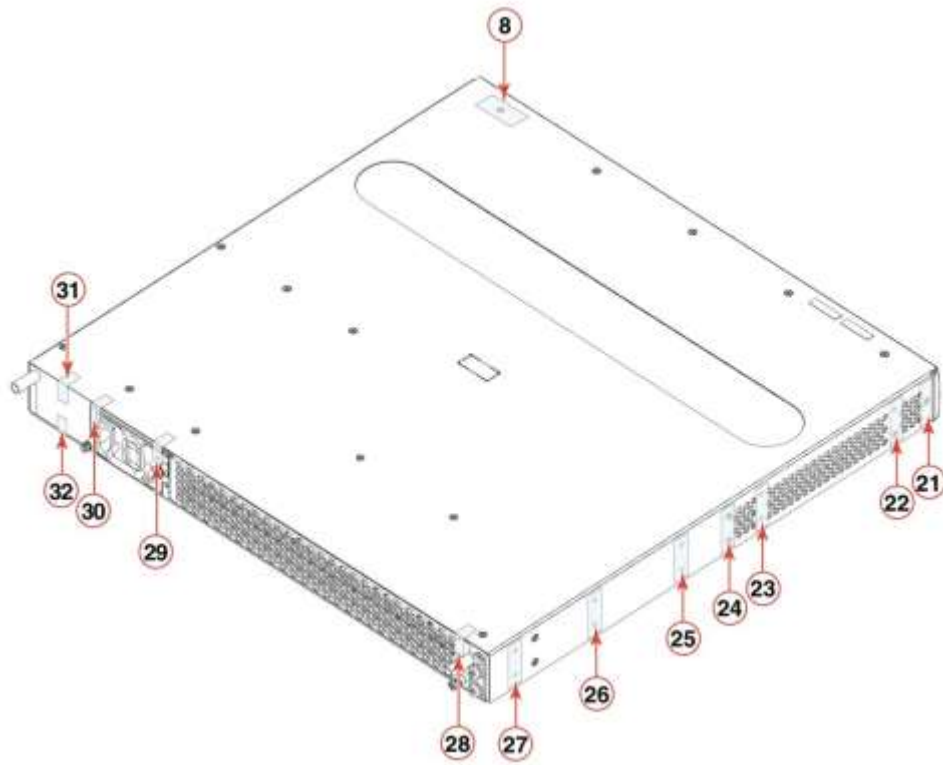
Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024F device configured with a 2x10G XFP uplink module (NI-CER-2024-2X10G). This configuration requires the placement of twenty-two (22) seals:

- Top: Affix one (1) seal at seal location 8 lengthwise completely covering the top rightmost screw that connects the faceplate to the device. See Figure 87 for correct seal orientation and positioning.

- Right and left sides: Affix seven seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 87 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side. See Figure 88 for the correct seal orientation and positioning on the left side.

- Front: Affix a seal from the front panel to the bottom panel, and place once seal vertically over the console port. See Figure 87 for correct seal orientation and placement.

- Rear: Affix four seals from the top panel to the rear panel. Affix one seal from the rear panel to the bottom panel. See Figure 88 and or correct seal orientation and placement.

Figure 87 Front, top, and right side view of the security seals placement for a Brocade NetIron CER 2024F device with a 2x10G XFP uplink module

Figure 88 Rear, top and left side view of the security seals placement for a Brocade NetIron CER 2024F device with a 2x10G XFP uplink module

Applying Tamper Evident Seals to a Brocade NetIron CER 2048 devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CER 2048C and CER 2048F series devices. The placement of the seals is the same for the CER 2048C, CER 2048CX, CER 2048F and CER 2048FX.

Brocade NetIron CER 2048C, Brocade NetIron CER 2048CX, Brocade NetIron CER 2048F and Brocade NetIron CER 2048FX devices require the placement of twenty-one (21) seals:

- Top: Affix one (1) seal lengthwise completely covering the top rightmost screw that connects the faceplate to the device at seal location number 8. See Figure 89 for correct seal orientation and positioning.

- Right and left sides: Affix seven (7) seals on each side of the device. The seals placed on the sides must each be vertically oriented and cover two open holes. See Figure 90 for correct seal orientation and positioning on the right side. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side. See Figure 91 for correct seal orientation and positioning on the left side.

- Front: Affix a seal over the console port on the front side of the module. See Figure 89 to view the location of the seal on the CER 2048C, CER 2048CX, CER 2048F and CER 2048FX.

- Rear: Affix four (4) seals from the top panel to the rear panel. Affix one (1) seal from the rear panel to the bottom panel. See Figure 91 for correct seal orientation and placement.

Figure 89 Front, top view of a Brocade NetIron CER 2048 device with security seals

Figure 90 right view of a Brocade NetIron CER 2048 device with security seals
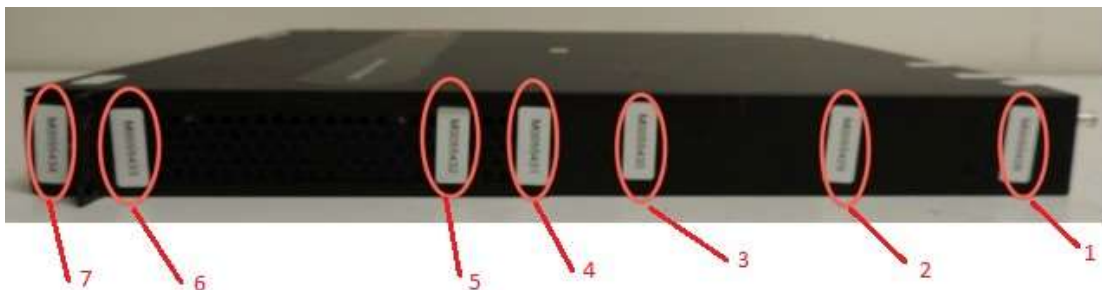
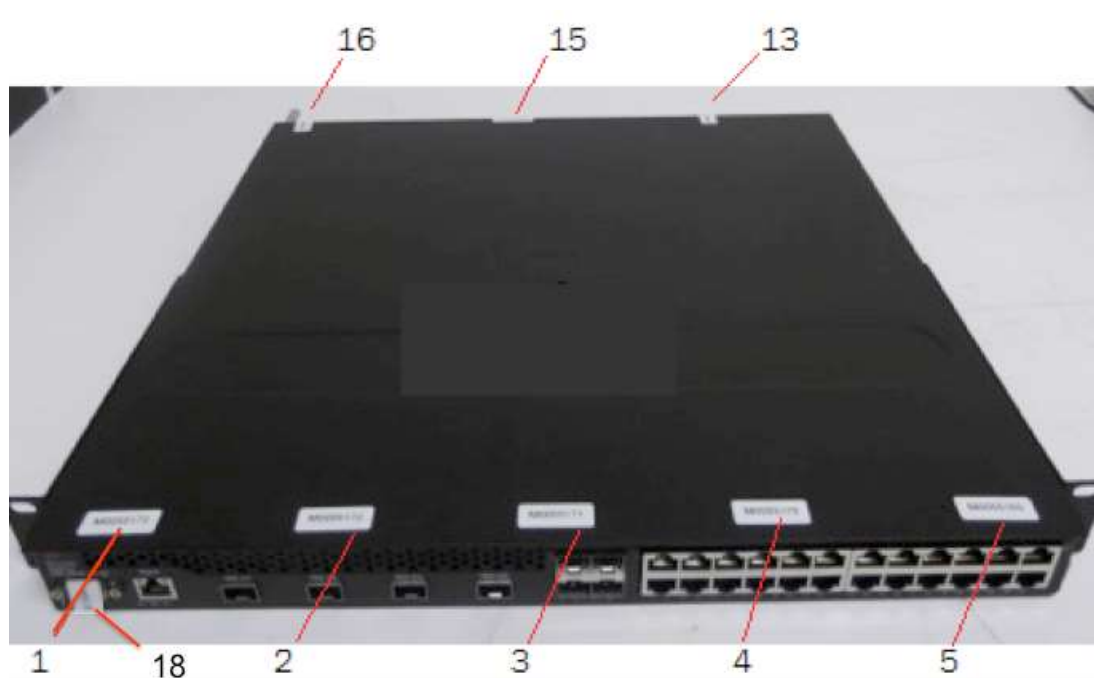**Figure 91 Rear, top and left side view of a Brocade NetIron CER 2048 device with security seals**
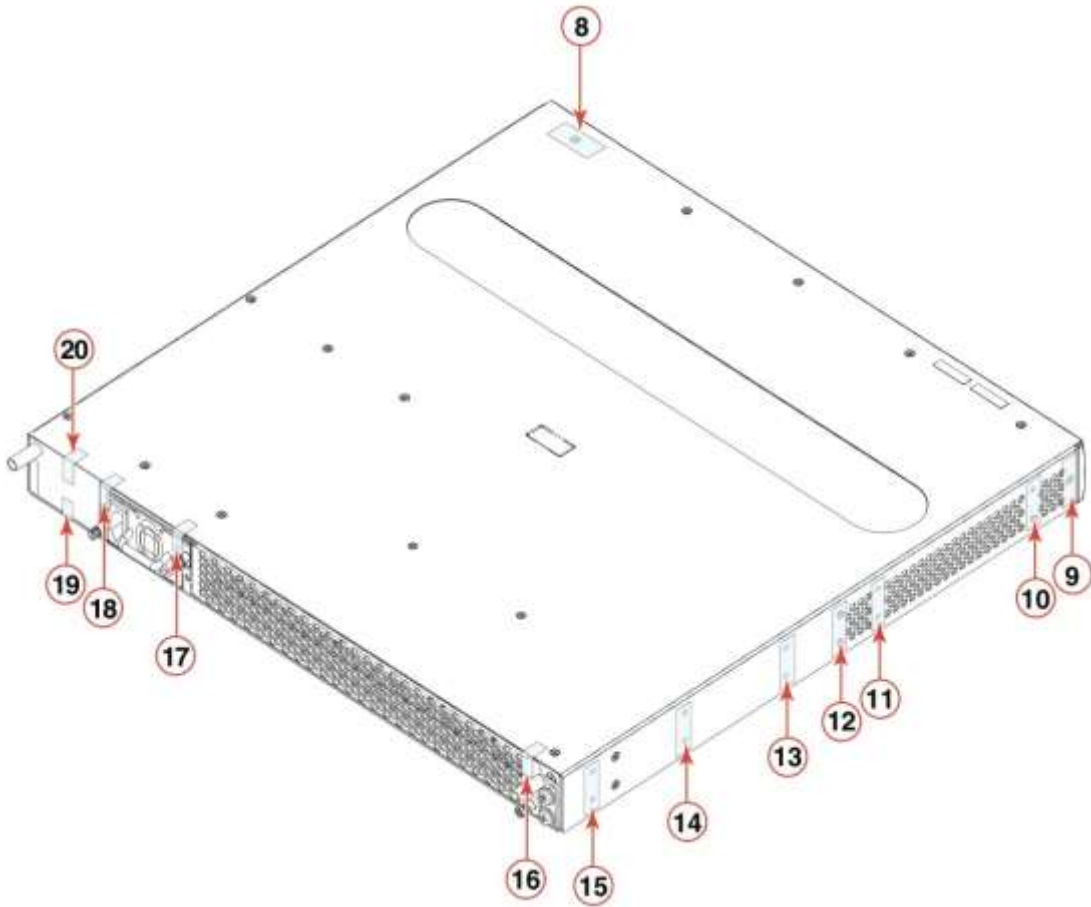
Applying Tamper Evident Seals to Brocade NetIron CER 2024C-4X-RT devices

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 seal over each flat head that connects the top cover to the base of the chassis. Five seals are needed to complete this step of the procedure. One seal is placed vertically over the console port. See Figure 92 for correct seal orientation and positioning.

- Right and left sides: Affix three 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 seals are needed to complete this step of the procedure. The orientation and placement of seals on the left and right sides mirrors each other. See Figure 93 and Figure 94 for correct seal orientation.

- Rear: Affix six seals across the back of the chassis to inhibit the removal of a power supply or fan module. Seals 15 and 16 wrap from the top cover to the fan module. Seal 12 touches both the power supply module and the bottom of the chassis. Seals 14 and 17 wrap from the fan module to the bottom of the chassis. See Figure 95 and Figure 96 for correct seal orientation and positioning.

Figure 92 Top front view of a Brocade CER 2024C-4X-RT device with security seals

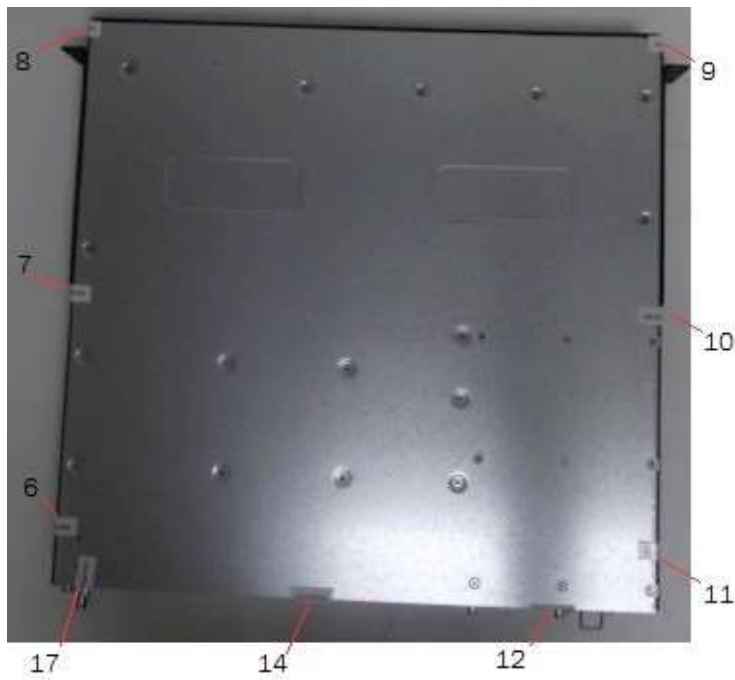Figure 93 Right view of a Brocade CER 2024C-4X-RT device with security seals

Figure 94 Left side view of a Brocade CER 2024C-4X-RT device with security seals

Figure 95 Rear view of a Brocade CER 2024C-4X-RT device with security seals
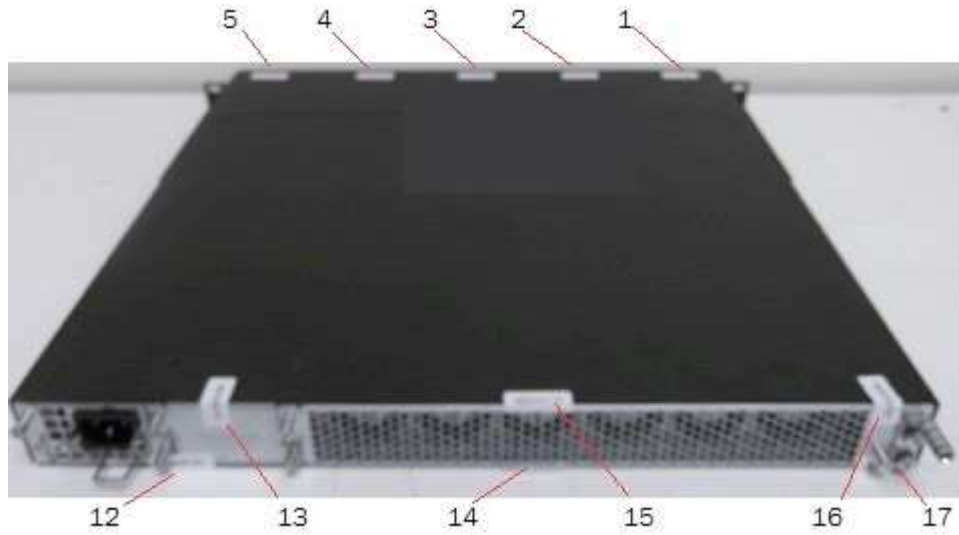
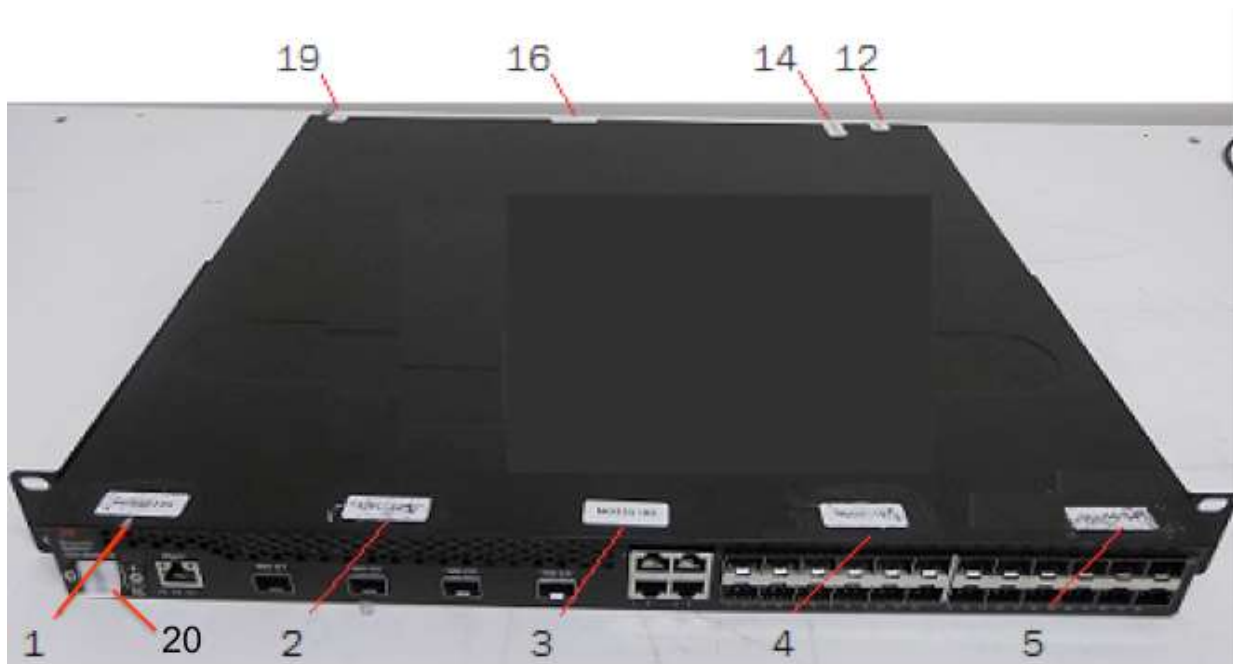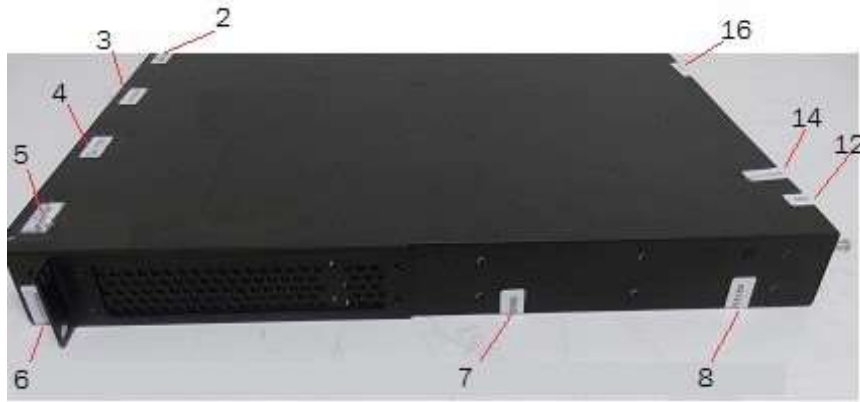**Figure 96 Bottom view of a Brocade CER 2024C-4X-RT device with security seals**

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 20 seals:

- **Top front:** Affix one seal over each flat head that connects the top cover to the base of the chassis. Five seals are needed to complete this step of the procedure. One seal is placed vertically over the console port. See Figure 97 for correct seal orientation and positioning.

- **Right and left sides:** Affix three 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 wraparound to the bottom of the chassis. Six seals are needed to complete this step of the procedure. The orientation and placement of seals on the left and right sides mirrors each other. See Figure 98 and Figure 99 for correct seal orientation.

- **Rear:** Affix six seals across the back of the chassis to inhibit the removal of a power supply or fan module. Seal 13 wraps from the top cover. Seals 15 and 16 wrap 16 wrap from the top cover to the fan module. Seal 12 touches both the power supply module and the bottom of the chassis. Seals 14 and 17 wrap from the fan module to the module to the bottom of the chassis. See Figure 100 and Figure 101 for correct seal orientation and positioning.

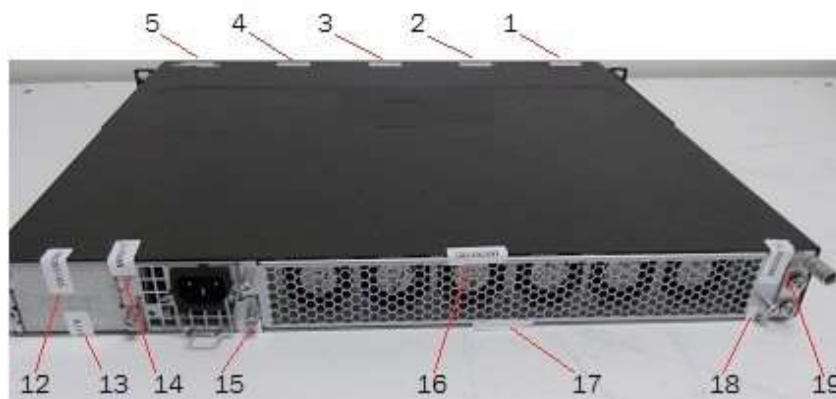**Figure 97 Top front view of a Brocade CER 2024F-4X-RT device with security seals**

Figure 98 Right side view of a Brocade CER 2024F-4X-RT device with security seals

Figure 99 Left view of a Brocade CER 2024F-4X-RT device with security seals

Figure 100 Rear view of a Brocade CER 2024F-4X-RT device with security seals

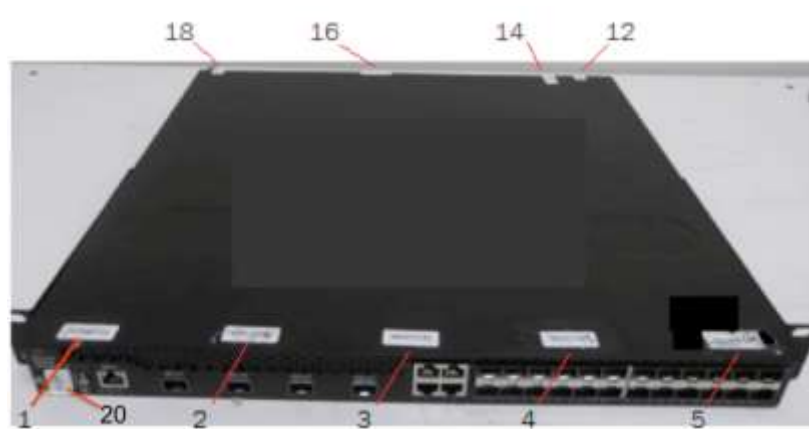**Figure 101 Bottom view of a Brocade CER 2024F-4X-RT device with security seals**

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 20 seals:

- Top front: Affix one seal over each flat head that connects the top cover to the base of the chassis. Five seals are needed to complete this step of the procedure. One seal is placed vertically over the console port. See Figure 102 for the correct seal orientation and positioning.

- Right and left sides: Affix three 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 seals are needed to complete this step of the procedure. See Figure 103 and Figure 104 for correct seal orientation. The orientation and placements of seals on the left and right side mirror each other.

- Rear: Affix eight seals across the back of the chassis to inhibit the removal of a power supply or fan 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 105 and Figure 106 for correct seal orientation and positioning.

Figure 102 Top front view of a Brocade CES 2024C-4X device with security seals

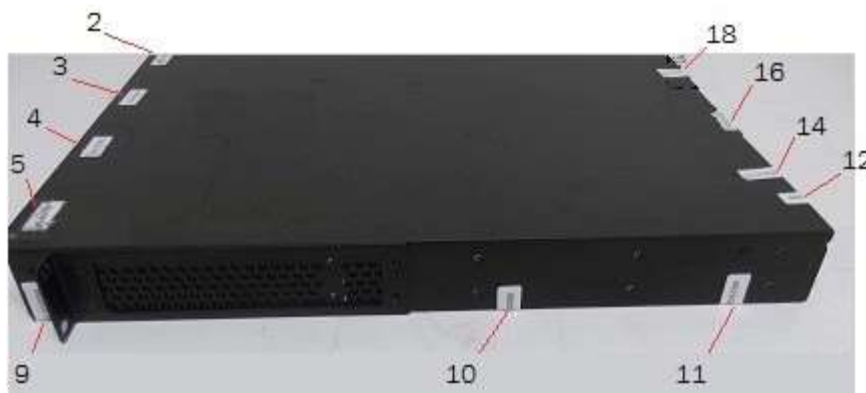Figure 103 Right view of a Brocade CES 2024C-4X device with security seals

Figure 104 Left side view of a Brocade CES 2024C-4X device with security seals

Figure 105 Rear view of a Brocade CES 2024C-4X device with security seals
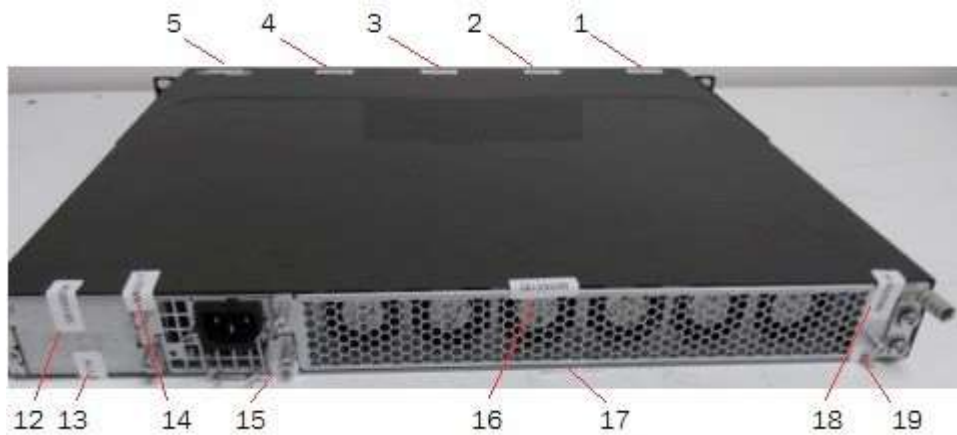

Figure 106 Bottom view of a Brocade CES 2024C-4X device with security seals

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 20 seals:

- Top front: Affix one seal over each flat head that connects the top cover to the base of the chassis. Five seals are needed to complete this step of the procedure. One seal is placed vertically over the console port. See Figure 107 for the correct seal orientation and positioning.

- Right and left sides: Affix three 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 seals are needed to complete this step of the procedure. See Figure 108 and Figure 109 for correct seal orientation. The orientation and placement of seals on the left and right sides mirror each other.

- Rear: Affix eight seals across the back of the chassis to inhibit the removal of a power supply or fan 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 110 and Figure 111 for correct seal orientation and positioning.

Figure 107 Top front view of a Brocade CES 2024F-4X device with security seals
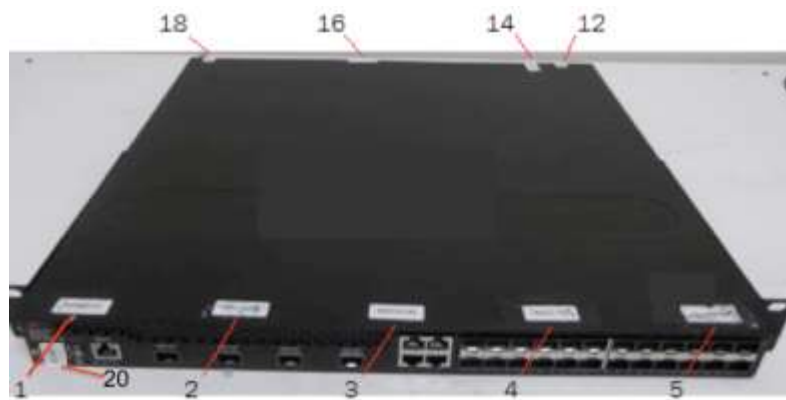

Figure 108 Right view of a Brocade CES 2024F-4X device with security seals

Figure 109 Left side view of a Brocade CES 2024F-4X device with security seals

Figure 110 Rear view of a Brocade CES 2024F-4X device with security seals
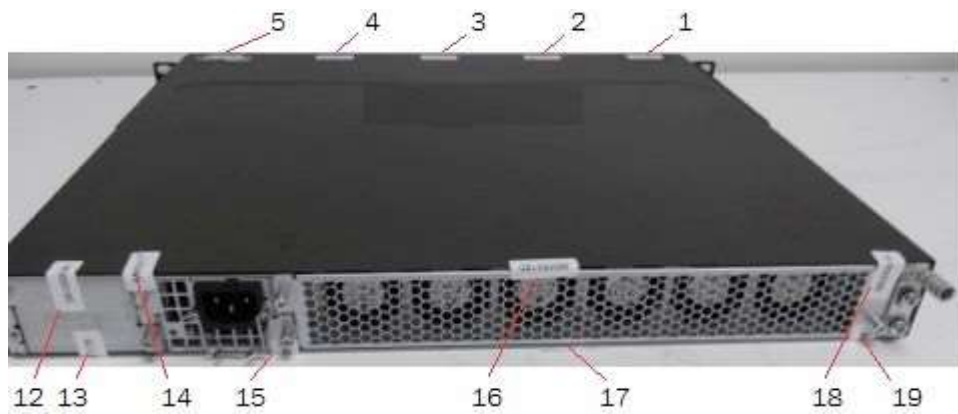

Figure 111 Bottom view of a Brocade CES 2024F-4X device with security seals