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

FIPS 140-2 Non-Proprietary Security Policy

Level 2

Document Version 1.0

June 17, 2014

Revision History

Revision Date	Revision	Summary of Changes
6/17/2014	1.0	Initial Draft

© 2014 Brocade Communications Systems, Inc. All Rights Reserved.

This Brocade Communications Systems, Inc. Security Policy for Brocade MLXe and Brocade NetIron CER 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.

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 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-port 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 line 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 crypto 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 R05.7.00

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 (P/N: 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: 80-1006872-01) 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: 80-1004809-04) 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) 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 (P/N: 80-1004811-04) 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)

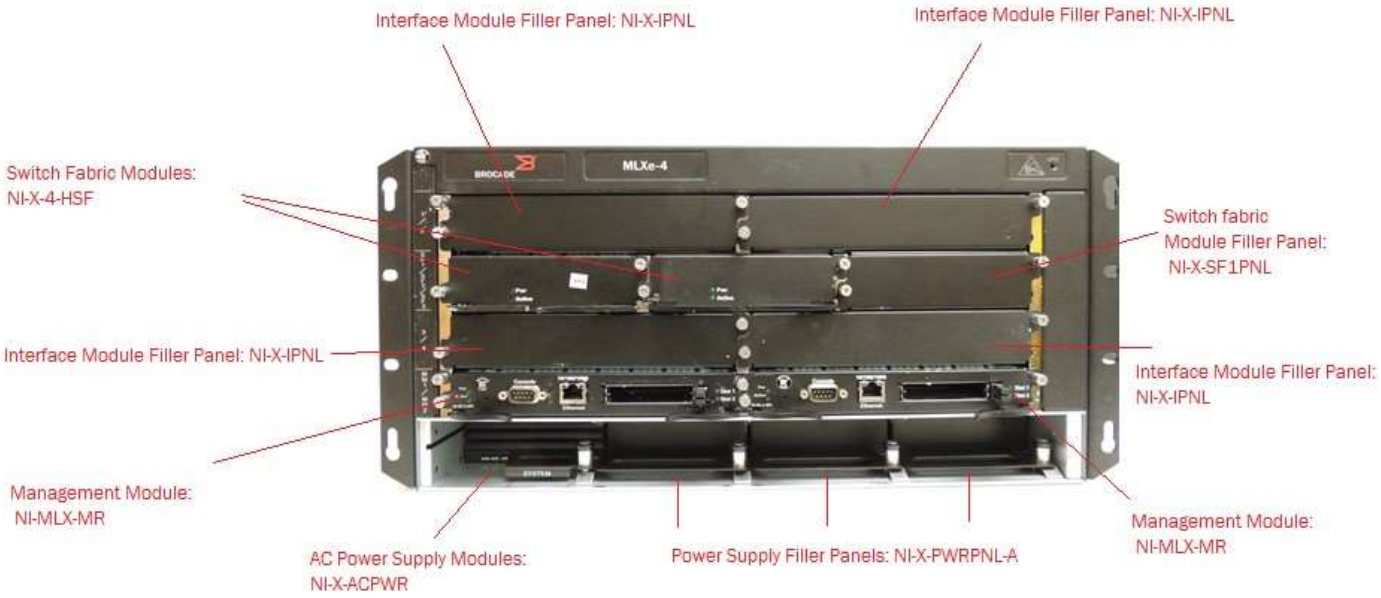


Figure 2 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-AC backside

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

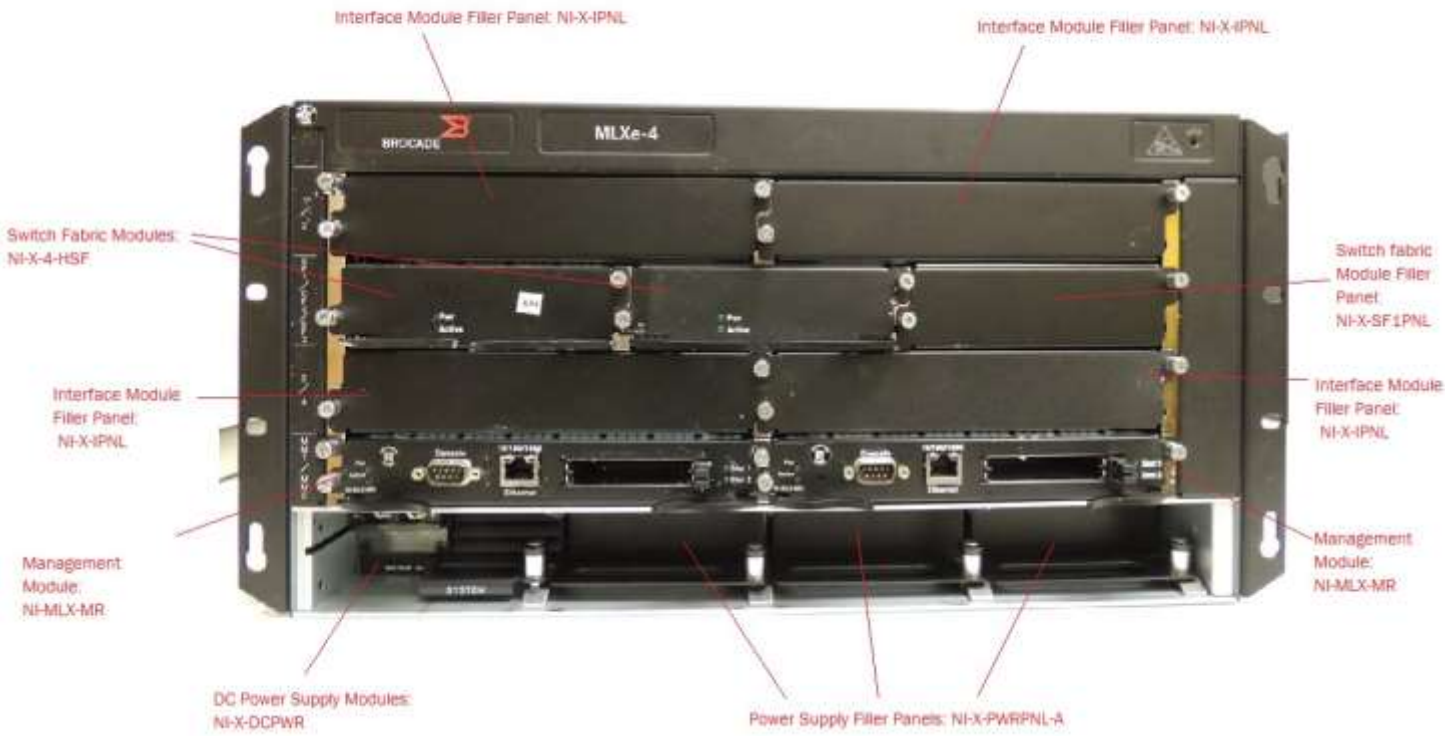


Figure 4 MLXe-4 Cryptographic Module with Chassis: BR-MLXE-4-MR-M-DC backside

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)

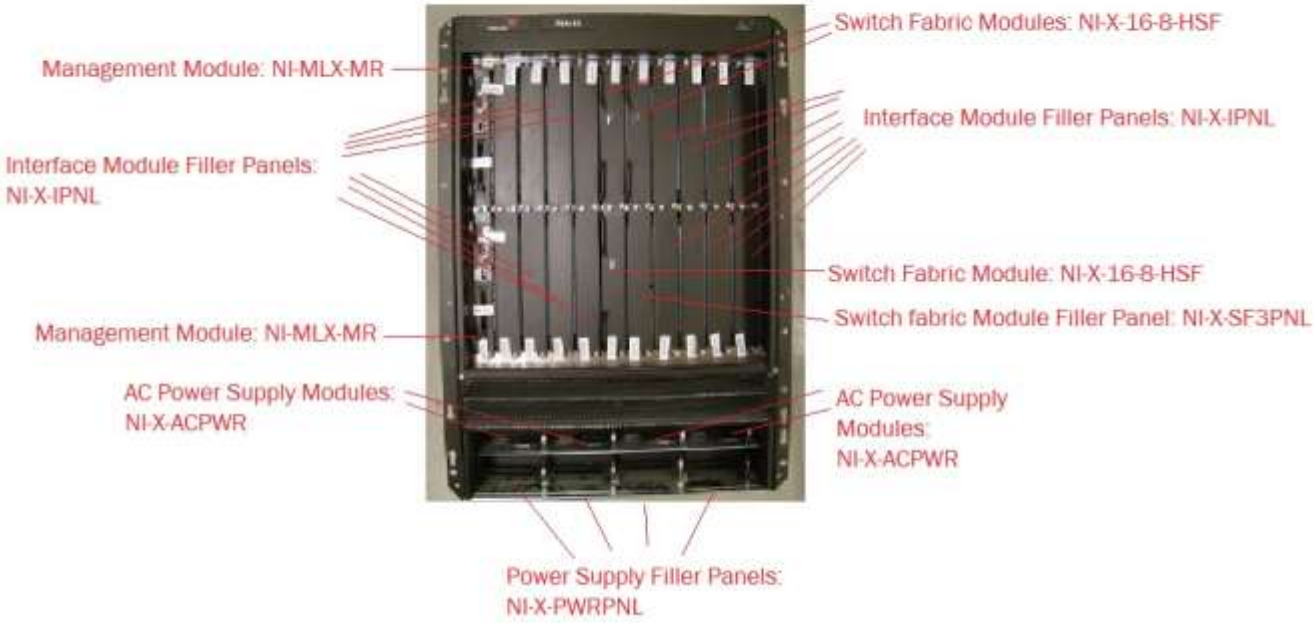


Figure 18 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-AC backside

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

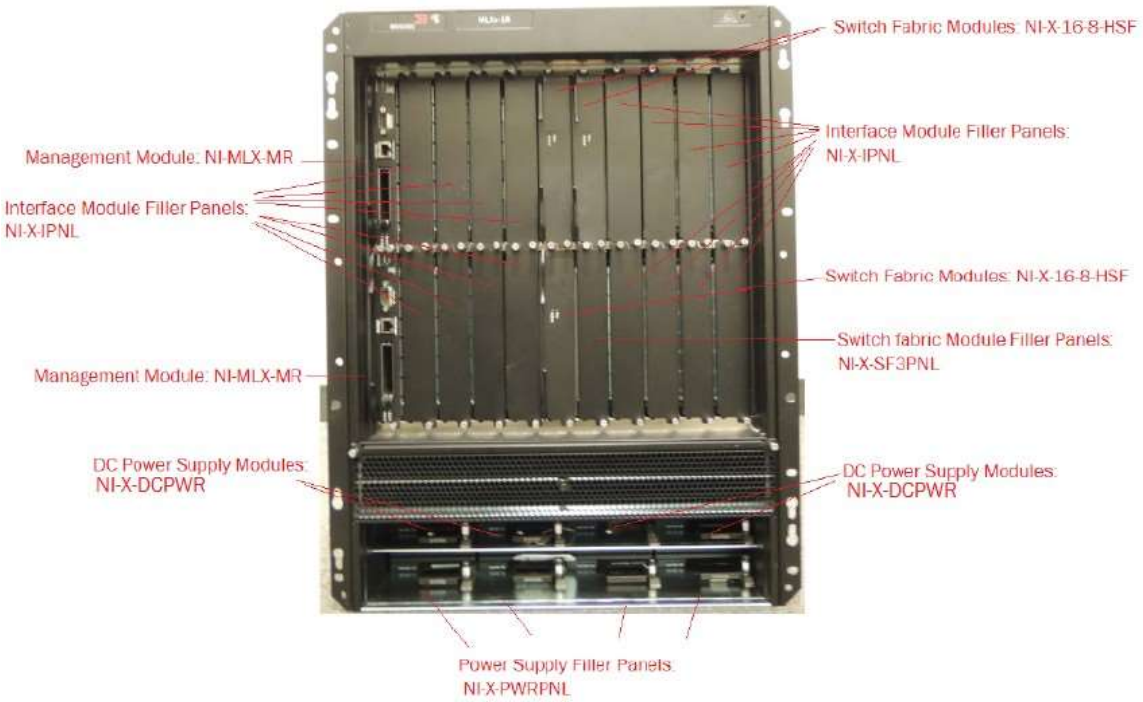


Figure 20 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR-M-DC backside

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

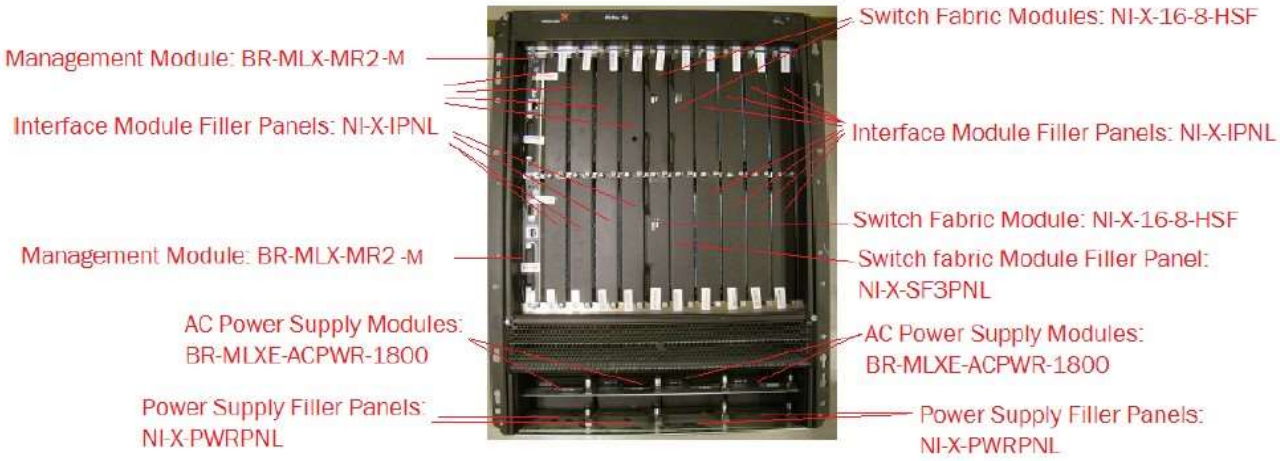


Figure 22 MLXe-16 Cryptographic Module with Chassis: BR-MLXE-16-MR2-M-AC backside

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 R05.7.00

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 includes24 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)
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 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

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-AC 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

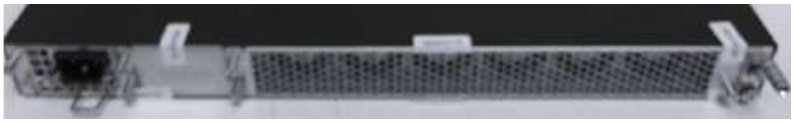
Figure 60 BR-CER-2024C-4X-RT-DC backside with Power supply RPS9DC (DC Power Supply)

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 backside with Power supply RPS9 (AC Power Supply)



4 Brocade CES 2000 Series

Table 14 CES 2000 Series Firmware Version

Firmware
Multi-Service IronWare R05.7.00

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 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 16 CES 2000 Series 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 backside 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 backside 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.

4.1.1 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

4.1.2 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

4.1.3 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 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 and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

4.1.4 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

[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.

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

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 the 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.

NetIron devices provide services for remote communication (SSH, SCP, HTTPS, and Console) for management and configuration of cryptographic functions.

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 while not FIPS Approved are allowed in FIPS Approved mode of operation.

Table 24 FIPS Approved Cryptographic Functions

Label	Cryptographic Function
AES	Advanced Encryption Standard
SHS	Secure Hash Standard
HMAC	Keyed-Hash Message Authentication Code
DRBG	Deterministic Random Bit Generator
RSA	Rivest Shamir Adleman
CVL	SSH and TLS Key Derivation Function
TDEA	Triple Data Encryption Algorithm
DSA	Digital Signature Algorithm

Table 25 Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

Label	Cryptographic Function
KW	RSA Key Wrapping
DH	Diffie-Hellman Key Agreement
MD5	Message-Digest Algorithm
NDRNG	Nondeterministic Random Number Generator used for generation of seeds for DRBG only
HMAC-MD5	Used to support RADIUS authentication
HMAC-SHA1-96	Used for OSPFv3 authentication

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 SSH

This service provides a secure session between a NetIron device and an SSH client. The NetIron device authenticates an SSH client and provides an encrypted communication channel. An operator may use an SSH session for managing the device via the command line interface.

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

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

The keyboard interactive (KI) authentication goes one-step ahead. It allows multiple challenges to be issued by the NetIron device, using the backend RADIUS or TACACS+ server, to the SSH client. Only after the SSH client responds correctly to the challenges, will the SSH 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 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 SSH 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 reauthenticate 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 SSH client in addition to show commands.

7.1.2 HTTPS

This service provides a graphical user interface for managing a NetIron MLXe device over a secure communication channel. The HTTPS service is not supported on CER 2000 Series devices. Using a web browser, an operator connects to a designated TCP port on a NetIron device. The device negotiates a TLS connection with the browser and authenticates the operator. The device uses HTTP over TLS with cipher suites TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA

In the User role, after a successful login, the default HTML page is same for any role. The operator can surf to any page after clicking on any URL. However, this operator is not allowed to make any modifications. If the user presses the 'Modify' button within any page, the user will be challenged to reenter the Crypto-officer's credentials. The challenge dialog box does not close unless the operator provides the Crypto-officer's access credentials. After three failed attempts, the page 'Protected Object' is displayed, in effect disallowing any changes from the web.

7.1.3 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 same as the list mentioned in the SSH service.

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.

7.2.1 SSH

Section 7.1.1, above, describes this service.

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 reauthenticate as described in Section 7.1.1. 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. This operator however, can review the configuration.

7.2.2 HTTPS

Section 7.1.2, above, describes this service.

Like the User role, the Port Configuration Administrator role operator is allowed to view all the web pages. In addition, this role the 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.

7.2.3 Console

Section 7.1.4, 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. The commands available to operator within the Port Configuration Administrator role are same as those mentioned in the SSH service Section 7.2.1.

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. The Crypto-officer role is able to perform firmware loading for the device as it has complete access to the system.

7.3.1 SSH

Section 7.1.1, above, describes this service.

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

7.3.2 SCP

This is a secure copy service that works over SSH protocol. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary files can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and data compression level configured for SSH. For example, if password authentication is enabled for SSH, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on NetIron devices is to copy user digital certificates and host public-private key pairs to the cryptographic module in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

7.3.3 HTTPS

Section 7.1.2, above, describes this service.

In addition to Port Configuration Administrator-role capabilities, the Crypto-officer has complete access to all the web pages and is allowed to make configuration updates through the web pages that support configuration changes.

7.3.4 Console

This service is described in Section 7.1.4 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 SSH service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSH access; afterwards the operator may securely import additional pairs of RSA host keys over a secured SSH connection. To enable

the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSH connection), and enable the HTTPS server.

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
   - 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
   - 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. HTTP
   - 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.
4. SNMP
   - SNMPv3 KDF (non-compliant) can only be used in the non-Approved mode of operation.

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 (CSP).
3) The cryptographic module performs the following tests:
   a) Power up Self-Tests:
      i) Cryptographic Known Answer Tests (KAT):
         (1) Triple-DES-168-bit key size KAT (encrypt/decrypt)
         (2) AES-128,192,256-bit key sizes KAT (encrypt/decrypt)
         (3) SHA-1,224,256,384,512 KAT (Hashing)
         (4) HMAC-SHA-1,256 KAT (Hashing)
         (5) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature/ verification)
         (6) DSA 1024 bit key size, SHA-1 KAT (signature/verification)
         (7) DRBG KAT
         (8) SP800-135 TLS KDF KAT

(9) SP800-135 SSH KDF KAT

ii) Firmware Integrity Test (CRC 32)

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 Random Number Generator (RNG) Test: performed on non-Approved RNG.

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

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

iv) 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

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 key generation, 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 be available before initialization of an MLXe, CER 2000 series and CES 2000 series device.

MLXe, CER 2000 series and CES 2000 series devices use a FIPS Approved random number generator implementing Algorithm CTR_DRBG based on hash functions.

MLXe, 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.

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

- RSA public and private keys
    - NOTICE: The cryptographic module “does not” support DSA key generation in FIPS mode.

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

NOTICE: The cryptographic module “does not” support DSA key generation in FIPS mode.

MLXe, CER 2000 series and CES 2000 series devices use NIST Approved key establishment techniques:

- Diffie-Hellman
- RSA Key Wrapping

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

MLXe, CER 2000 series and CES 2000 series devices do not display plaintext secret or private keys. The device displays "..." in place of plaintext keys.

MLXe, CER 2000 series and CES 2000 series devices use automated methods to realize session keys for SSHv2 and HTTPS.

MLXe, CER 2000 series and CES 2000 series devices perform Get, GetNext, and GetBulk operations.

8.2 Authentication

NetIron devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS/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 (e.g. SSH, Web) 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/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 SSH 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/TACACS+ Authentication Method

The TACACS and TACACS+ methods use one or more TACACS/TACACS+ servers to verify user names and passwords. For TACACS, the NetIron device prompts an operator for user name and password. The device sends the user name and password to the TACACS server. Upon successful authentication, the NetIron device selects the operator's role implicitly based on the action requested (for example, User role for a login request or Crypto-officer role for a configure terminal command). 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/TACACS+ authentication, a Crypto-officer must configure TACACS/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 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.

RADIUS and TACACS+ require that passwords be a minimum of 7 characters, and selected from the character sets noted above in this section. The probability of a random attempt succeeding is 1/80^7, which is less than 1/1,000,000. An operator is allowed a maximum of (Qty. 3) attempts in a one-minute period for RADIUS/TACACS+. Therefore, the probability of success in a one-minute period is 3/80^7, 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 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 (zeroize) by executing a fips zeroize all command. See item 4a in Section 9.1.1.1 and Section 9.1.1.2 for further details.

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

	User				Port Administrator			Crypto Officer				
CSP / Services	**SSH**	**HTTPS**	**SNMP**	**Console**	**SSH**	**HTTPS**	**Console**	**SSH**	**SCP**	**HTTPS**	**SNMP**	**Console**
SSH Host RSA Private Key (2048 bit)	x				x			xwd	x			wd
SSH DH Private Key (2048 bit modulus)	x				x			xwd	x			wd
SSH DH Shared Secret Key (2048 bit)	x				x			x	x			xd
SSH/SCP Session Keys (128 and 256 bit AES CBC)	x				x			x	x			xd
SSH/SCP Authentication Key (HMAC-SHA-1)	x				x			x	x			xd
SSH KDF Internal State	x				x			x	x			xd
TLS Host RSA Private Key (RSA 2048 bit)		x				x		rwd		x		rwd
TLS Pre-Master Secret		x				x				x		xd
TLS Master Secret		x				x				x		xd
TLS PRF Internal State		x				x		xd		x		xd
TLS Session Key		x				x				x		xd
TLS Authentication Key		x				x				xd		xd
DRBG Seed	x	x			x	x		x	x	x		xd
DRBG Value V	x	x			x	x		x	x	x		xd
DRBG Key	x	x			x	x		x	x	x		xd
DRBG Internal State	x	x			x	x		xd	x	x		xd
User Password	x	x	x	x				xrwd	xrwd	xrwd	x	xrwd
Port Administrator Password					x	x	x	xrwd	xrwd	rwd		xrwd
Crypto-officer Password								xrwd	xrwd	xrwd		xrwd
RADIUS Secret	x	x		x	x	x	x	xrwd	xrwd	xrwd		xrwd
TACACS+ Secret	x	x		x	x	x	x	xrwd	xrwd	xrwd		xrwd
Firmware Integrity / Firmware Load RSA Public Key								x		x		xd
SSH Host RSA Public key	x				x			xrwd	xrw			rwd
SSH Client RSA Public Key	x				x			xrwd	xrwd			xrwd
SSH DH Public Key	x				x			x	x			xd
SSH DH Peer Public Key	x				x			x	x			xd
TLS Host Public Key (RSA 2048 bit)		x				x		rwd		x		rwd
TLS Peer Public Key (RSA 2048 bit)		x				x		rwd		x		rwd

8.3.1 CSP Zeroization

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

The TLS pre-master secret is generated during the TLS handshake. It is destroyed after it is used.

The TLS session key is generated for every HTTPS session. The TLS session key is deleted after the session is closed.

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 SSH, 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

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).

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 mode: Administrative Status: ON, Operational Status: OFF

Some shared secrets inherited from non-Approved mode may not be FIPS 140-2 compliant and have to be zeroized separately by the Crypto-officer before the system is rebooted. This ensures that the data path of the system is not immediately impacted after FIPS Approved mode is enabled administratively. A separate command needs to be executed by the Crypto-officer in order to zeroize all the configured shared secrets and keys.

The system needs to be reloaded to operationally enter FIPS Approved mode.

System Specific:

OS monitor mode access:	Disabled
Management Protocol Specific:	
Telnet server:	Disabled
TFTP Client:	Disabled
HTTPS SSL 3.0:	Disabled
SNMP Access to security objects:	Disabled
Critical Security Parameter Updates across FIPS Boundary:	
Protocol shared secret and host passwords:	Clear
SSH RSA Host and Client Keys:	Clear
HTTPS RSA Host Keys and Signature:	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 mode: Administrative Status: ON, Operational Status: ON

System Specific:

OS monitor mode access:	Disabled
Management Protocol Specific:	
Telnet server:	Disabled
TFTP Client:	Disabled
HTTPS SSL 3.0:	Disabled

SNMP Access to security objects:	Disabled
Critical Security Parameter Updates across FIPS Boundary:	
Protocol shared secret and host passwords:	Clear
SSH RSA Host and Client Keys:	Clear
HTTPS RSA Host Keys and Signature:	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 disables the following:

1. Telnet access including the telnet server command
2. AAA authentication for the console including the enable aaa console command
3. Command ip ssh scp disable
4. TFTP access
5. SNMP access to CSP MIB objects
6. Access to all commands that allows debugging memory content within the monitor mode
7. HTTP access including the web-management http command (applies to Brocade MLXe series only)
8. HTTPS SSL 3.0 access and RC4 cipher (applies to Brocade MLXe series only)
9. Command web-management allow-no-password (applies to Brocade MLXe series only)

Entering FIPS Approved mode also clears:

1. Protocol shared secret and host passwords
2. SSH DSA host keys
3. HTTPS RSA host keys and certificate (applies Brocade MLXe series only)

FIPS Approved mode enables:

1. SCP
2. HTTPS TLS version 1.0 and greater (applies to Brocade MLXe series only)

In FIPS Approved mode, NetIron devices provide FIPS Approved cryptographic algorithms as well as non-Approved security functions.

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

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES) NOTICE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation	128, 192, and 256-bit keys, ECB and CBC mode	#2716
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	#1633
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	#2281
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256	#1695
Deterministic Random Bit Generator (DRBG)	SP 800-90 CTR_DRBG	#453

Algorithm	Supports	Certificate
Digital Signature Algorithm (DSA) NOTICE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys	#833
Rivest Shamir Adleman Signature Algorithm (RSA) NOTICE: The module does not support 1024-bit keys in FIPS Mode	1024-bit and 2048-bit keys	#1412
Component Test Key Derivation Function (CVL)	TLS and SSH	#174

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

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES) NOTICE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation	128, 192, and 256-bit keys, ECB and CBC mode CTR (int only; 128, 192, 256-bits)	#2717
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	#1634
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	#2282
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256	#1696
Deterministic Random Bit Generator (DRBG)	SP 800-90 CTR_DRBG	#454
Digital Signature Algorithm (DSA) NOTICE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys	#834
Rivest Shamir Adleman Signature Algorithm (RSA) NOTICE: The module does not support 1024-bit keys in FIPS Mode	1024-bit and 2048-bit keys	#1413
Component Test Key Derivation Function (CVL)	TLS and SSH	#175

Table 29 Algorithm Certificates for the CER and CES 2000 Series

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES) NOTICE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation	128-, 192, and 256-bit keys, ECB and CBC mode CTR (int only; 128, 192, 256-bits)	#2715
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	#1632
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	#2280

Algorithm	Supports	Certificate
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256	#1694
Deterministic Random Bit Generator (DRBG)	SP 800-90 CTR_DRBG	#452
Digital Signature Algorithm (DSA) NOTICE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys	#832
Rivest Shamir Adleman Signature Algorithm (RSA) NOTICE: The module does not support 1024-bit keys in FIPS Mode	1024-bit and 2048-bit keys	#1411
Component Test Key Derivation Function (CVL)	TLS and SSH	#173

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: 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.

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

1. RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
2. Diffie-Hellman (key agreement; key establishment provides 112 bits of encryption strength)
3. MD5-- Used in the TLS v1.0 pseudo-random function (PRF) in FIPS mode (MD5 not exposed to the operator). Also used in TACACS+ packets for message integrity verification (MD5 not exposed to the operator).
4. HMAC-MD5 – Used to support RADIUS authentication
5. HMAC-SHA1-96-- Used for IPSec AH Authentication header, which is used for OSPFv3 authentication (Notice: The module provides a service to configure OSPFv3 authentication, however, use of OSPFv3 requires hardware that is not included within the scope of the validated configuration. Furthermore, the latent OSPFv3 authentication implemented by the module does not provide cryptographic protection, and is considered plaintext.).
6. NDRNG-- Non-deterministic random number generator used for generation of seeds for DRBG only.

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

9.1.1.1 Invoking FIPS Approved Mode for Brocade MLXe Series Devices

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

1. Assume Crypto-officer role
   a. The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in section 8.2 Authentication. Both the Enable Authentication Method and Local Authentication Method can be used to assume the 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 zeros out the shared secrets use by various networking protocols including host access passwords, SSH Host keys, and HTTPS host keys with the digital signature.
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 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 zeros out the shared secrets used by various networking protocols including host access passwords, SSH Host keys, and HTTPS host keys with the digital signature.
5. Save the running configuration: write memory
6. The device saves the running configuration as the startup configuration
7. Reload the device
    a. The device resets, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
8. Enter command: fips show
    a. The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
9. Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

9.1.1.3 Negating FIPS Approved Mode for Brocade MLXe 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,

HTTP, 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 zeroes out the shared secrets used by various networking protocols including host access passwords, SSH Host keys, and HTTPS host keys with the digital signature.

c. Reload the device to begin non-Approved mode of operation.

9.1.1.4 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 zeroes out the shared secrets used by various networking protocols including host access passwords, SSH Host keys, and HTTPS host keys with the digital signature.
    c. Reload the device to begin non-Approved mode of operation.

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

[ANSI X9.31] ANSI X9.31:1998 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry

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

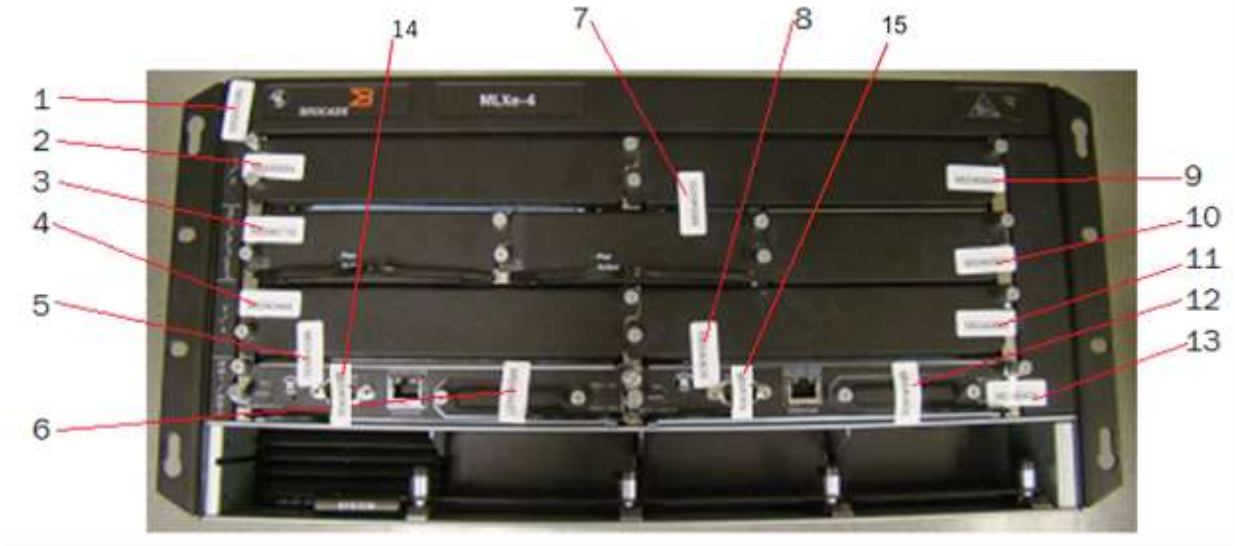
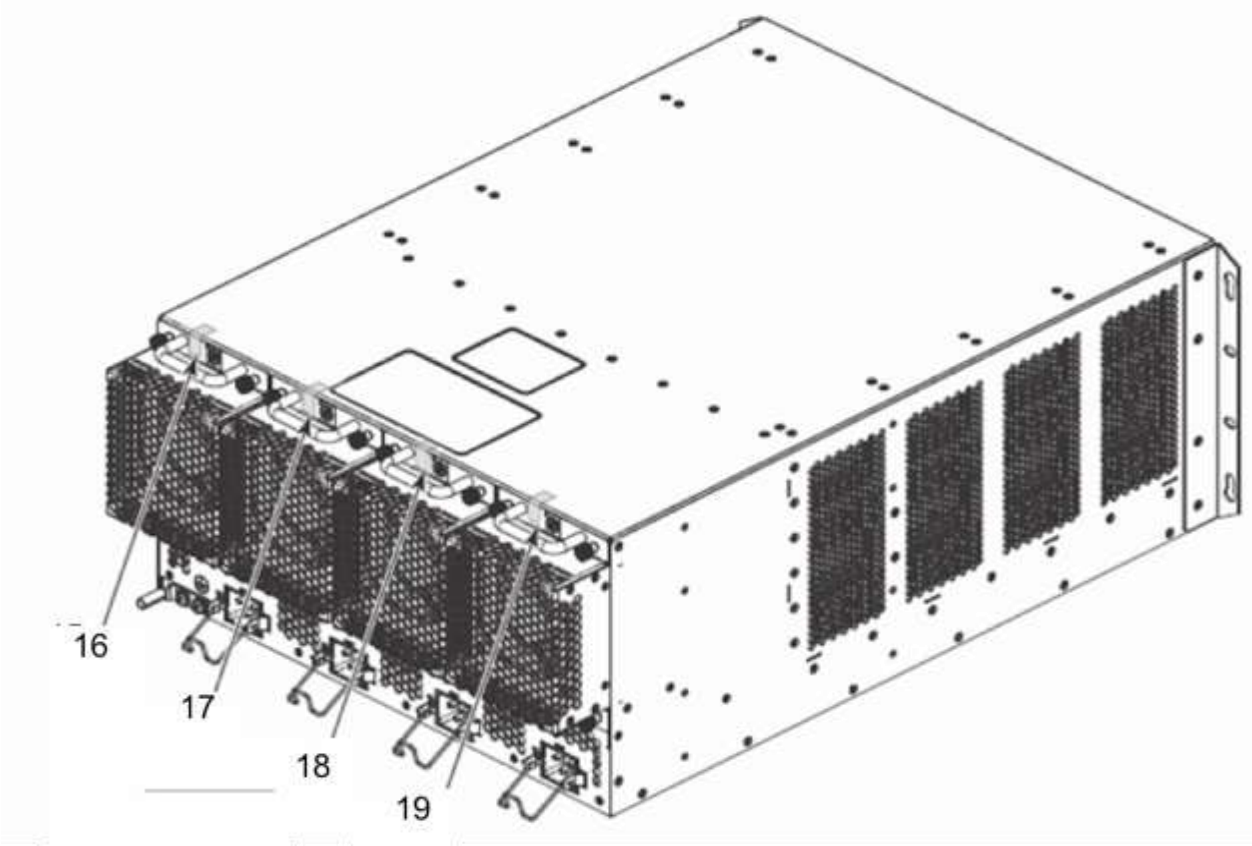


Figure 74 Rear and side view of a Brocade MLXe-4 device with security seals



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 76. 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

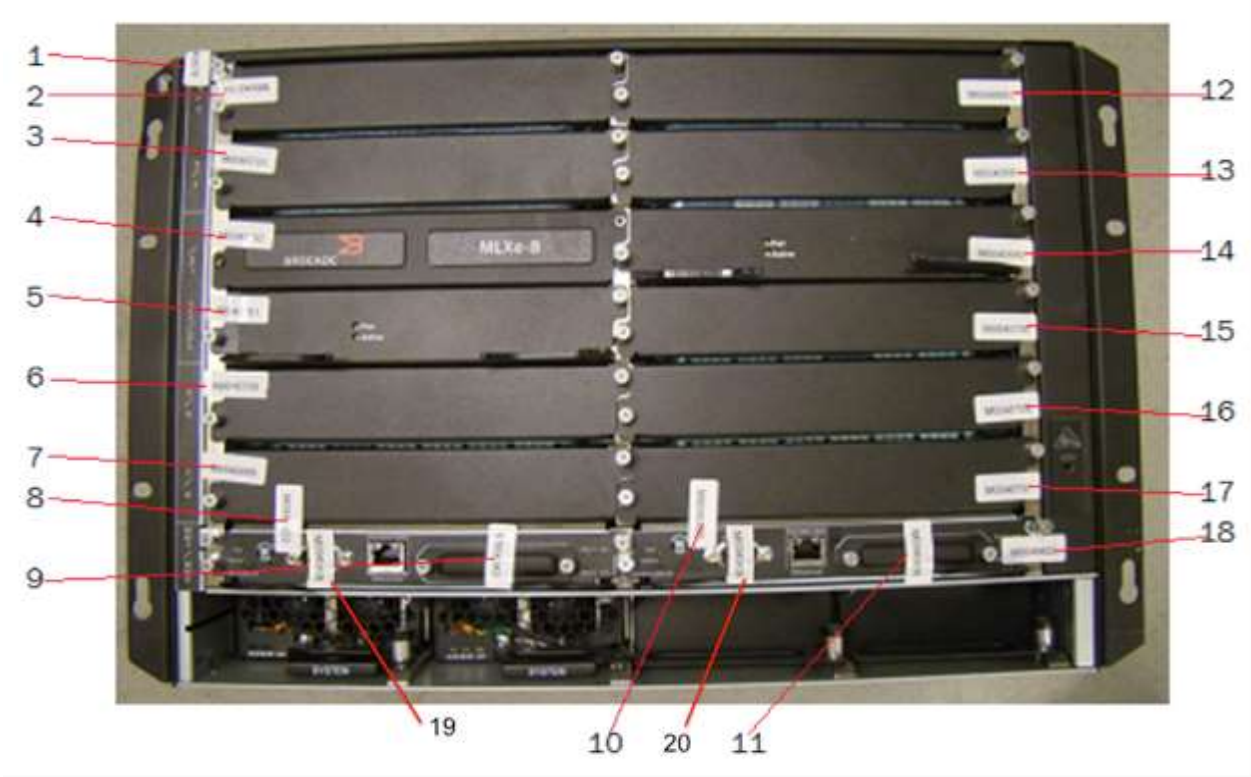
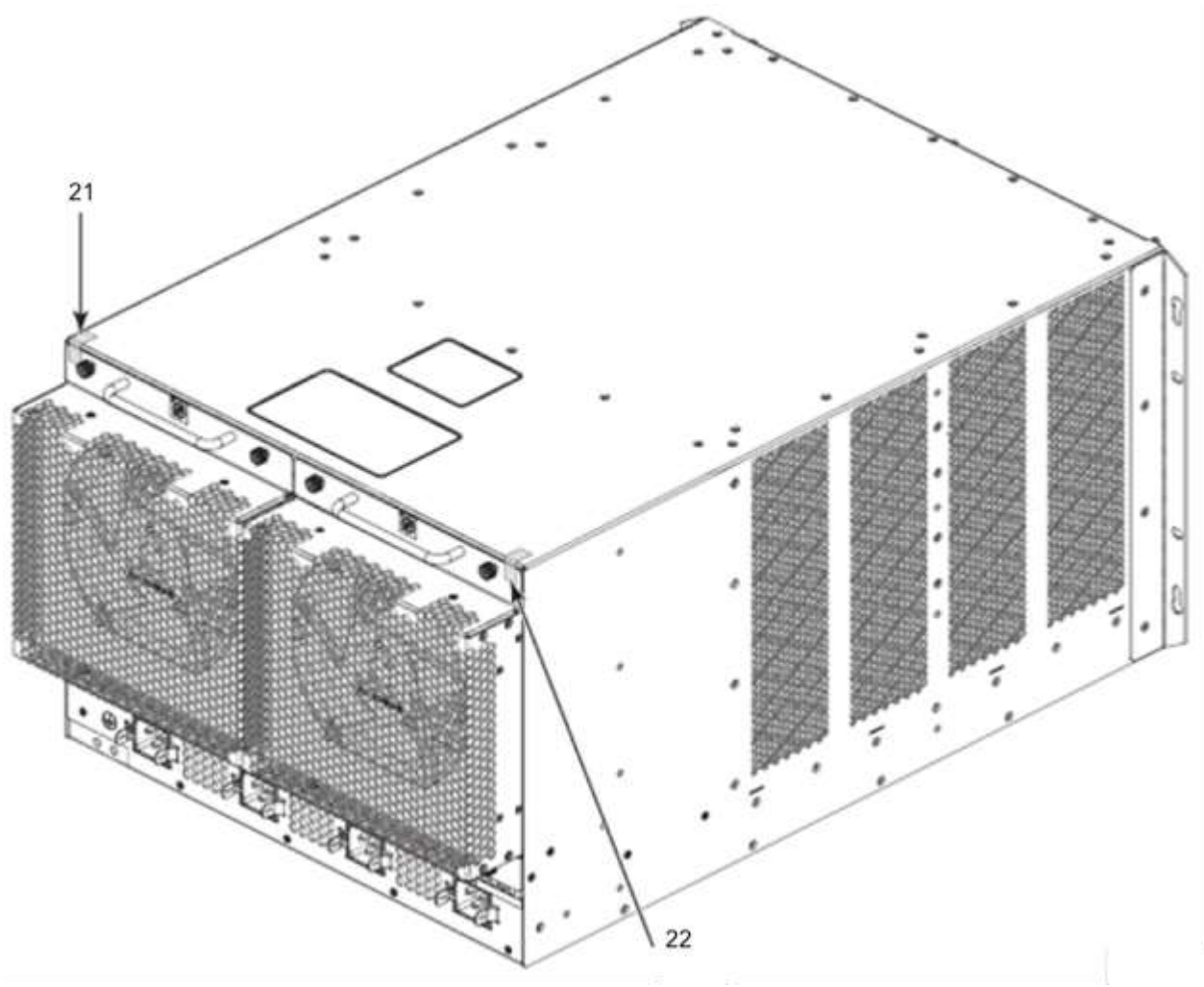


Figure 76 Rear and side view of a Brocade MLXe-8 device with security seals



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

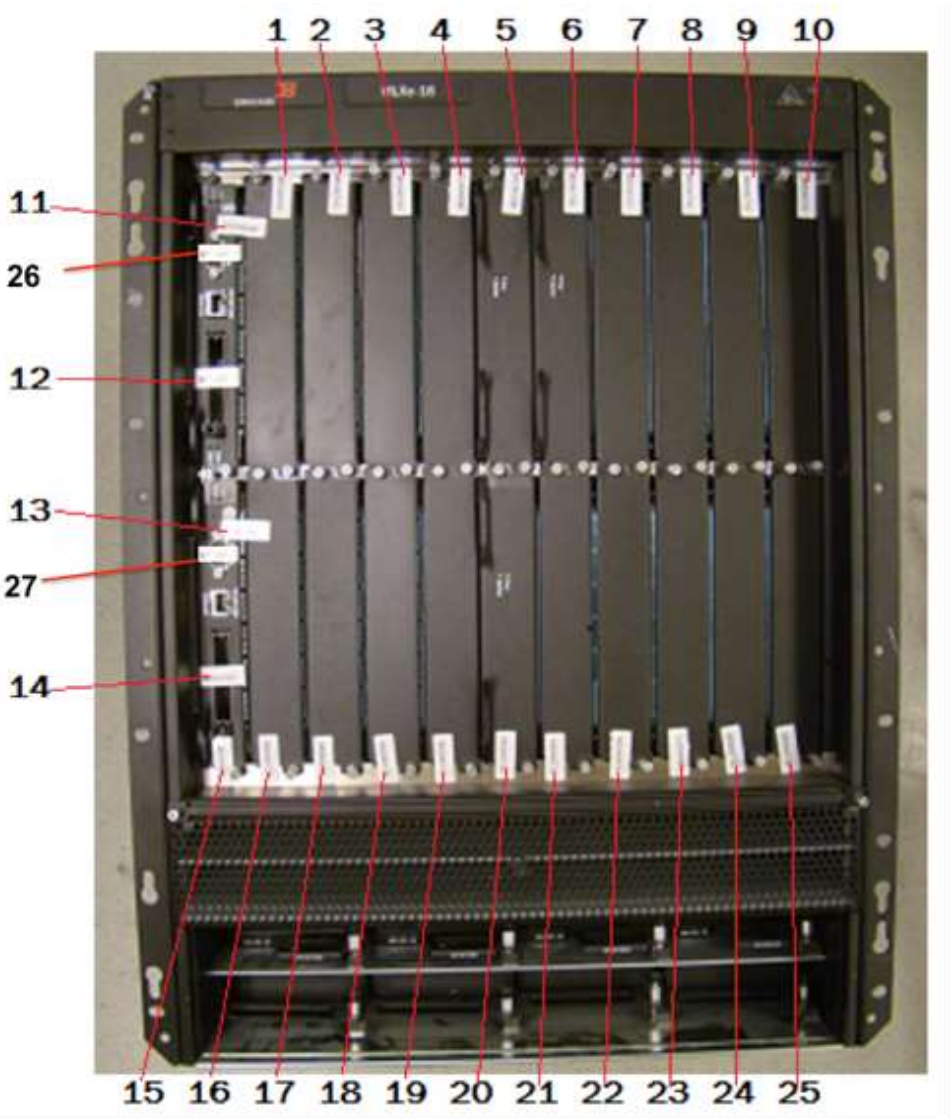
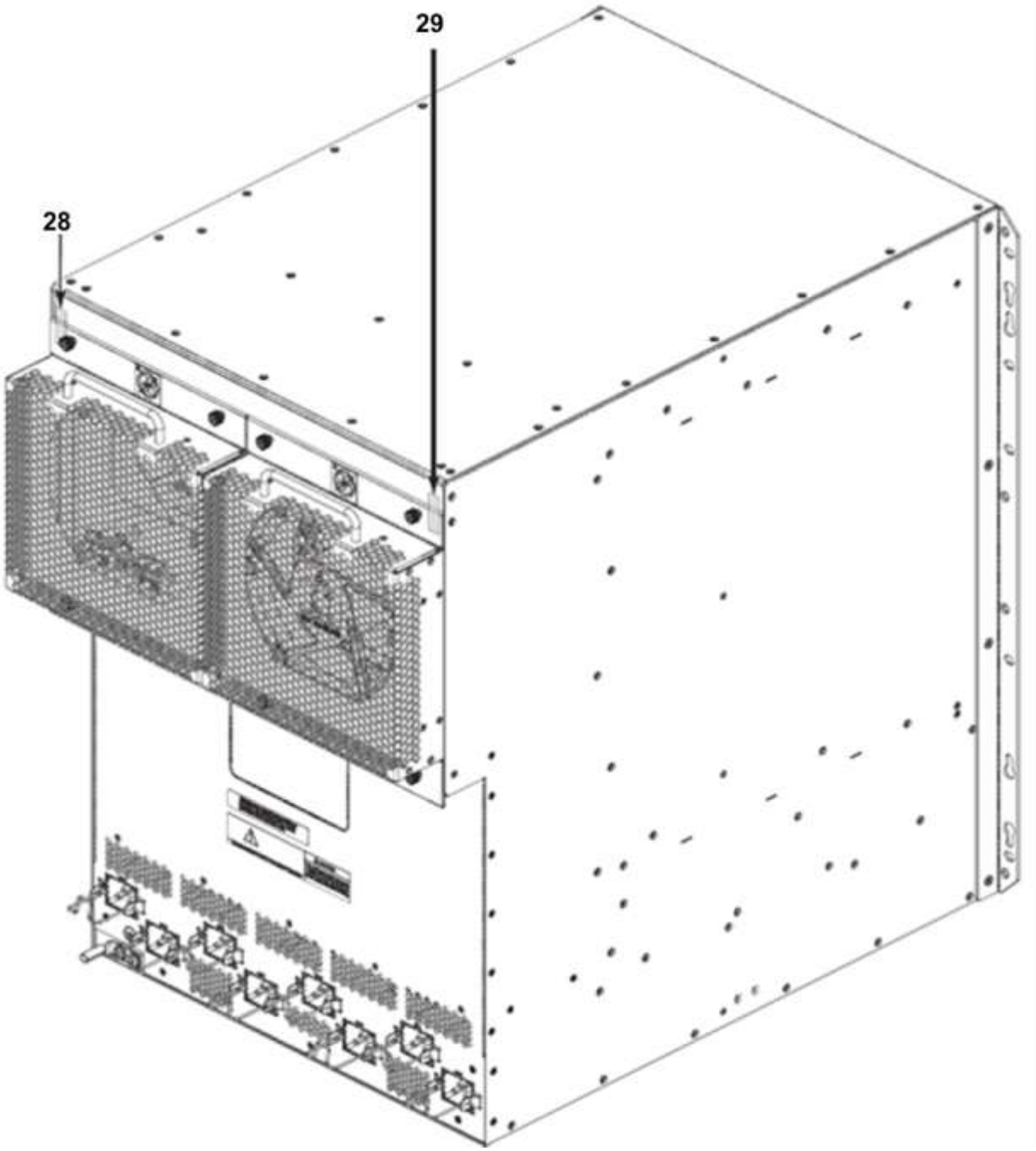


Figure 78 Rear and side view of a Brocade MLXe-16 device with security seals



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 thirty- eight (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 and 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 the left side of the front panel is obscured. Additionally, one seal is placed vertically over the console port. See Figure 79 Front view of a Brocade NetIron CER 2024C device with security seals
- 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 with security seals

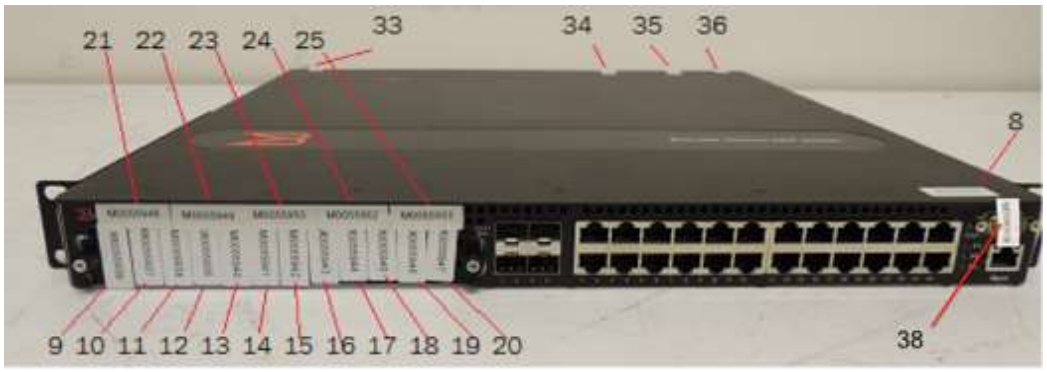


Figure 80 Front, top, and right side view of a Brocade NetIron CER 2024C device with security seals

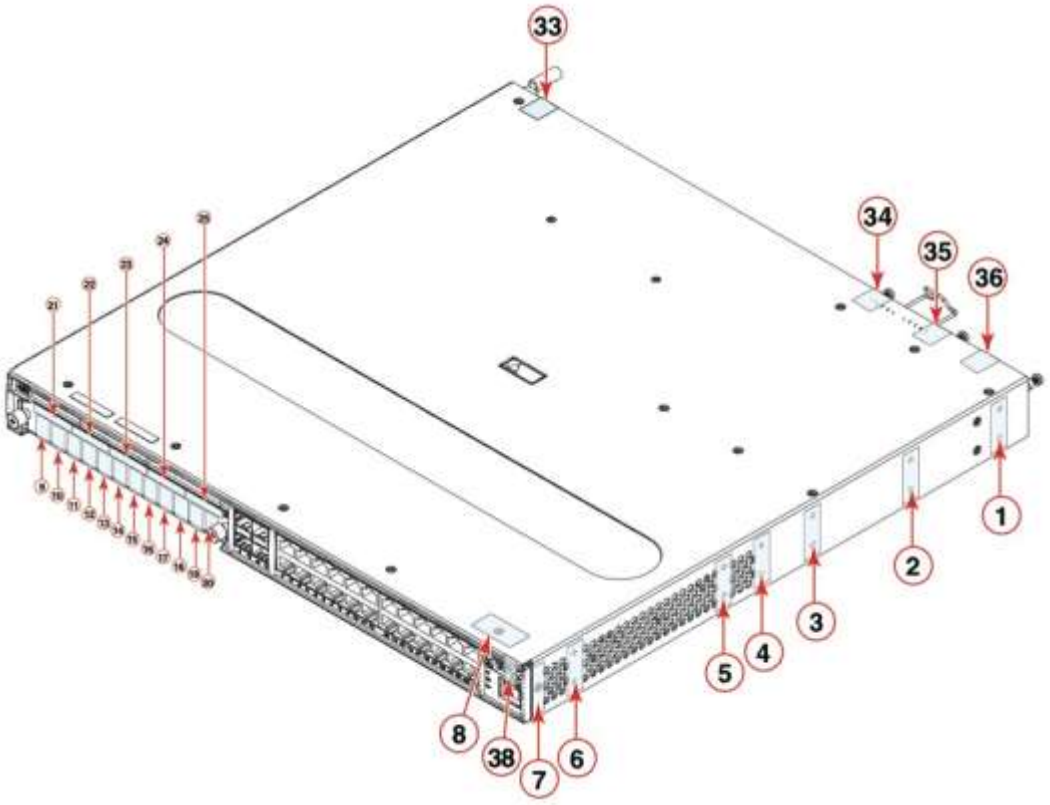
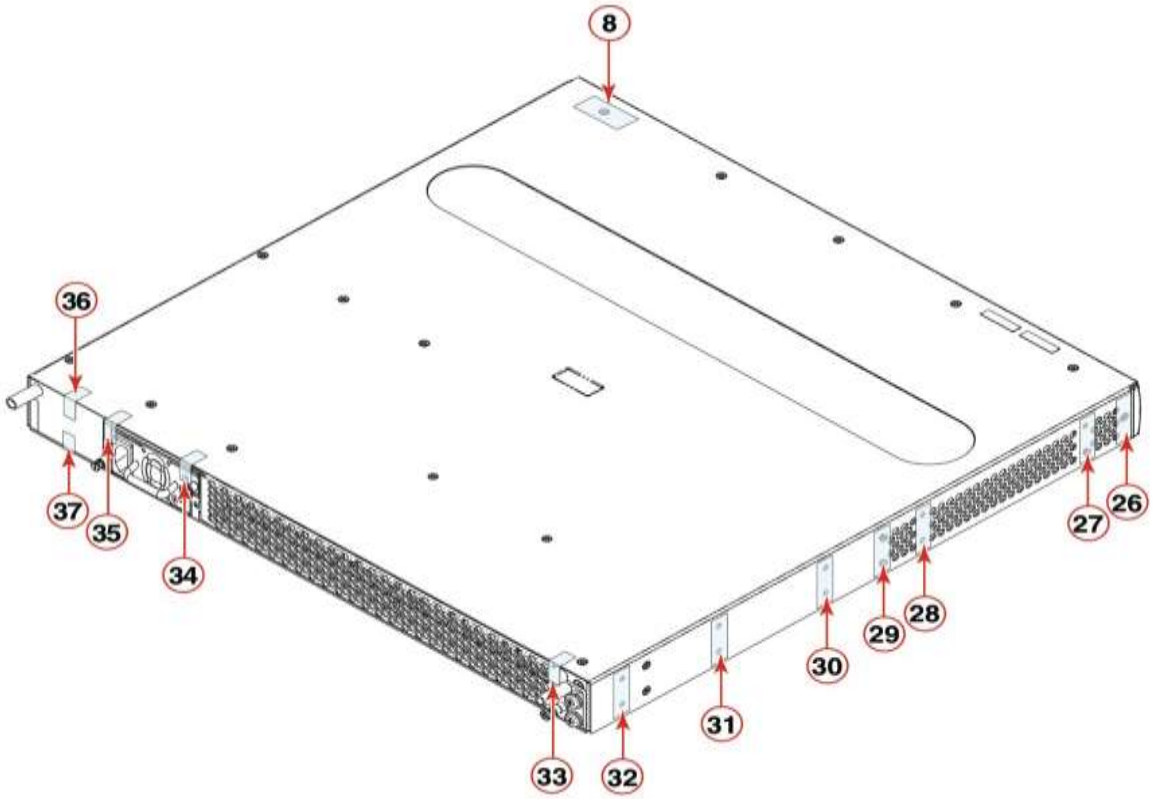


Figure 81 Rear, top and left side view of a Brocade NetIron CER 2024C device with security seals



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 (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 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 (4) seals from the top panel to the rear panel. Affix one (1) 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

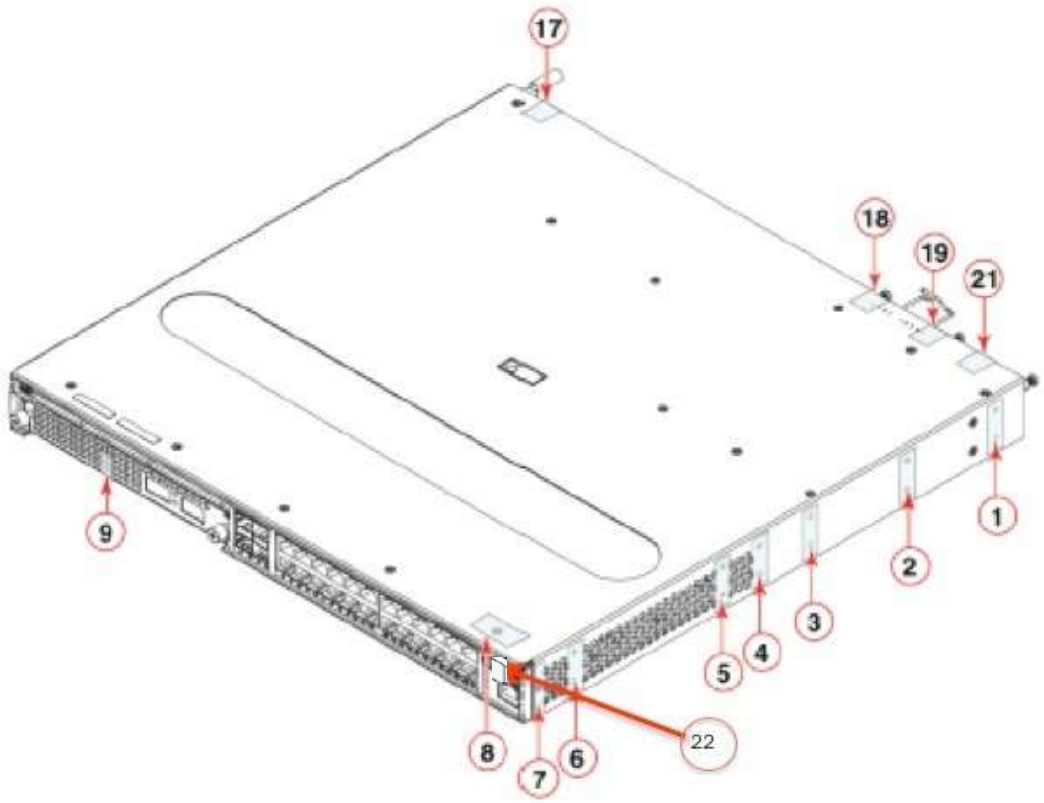
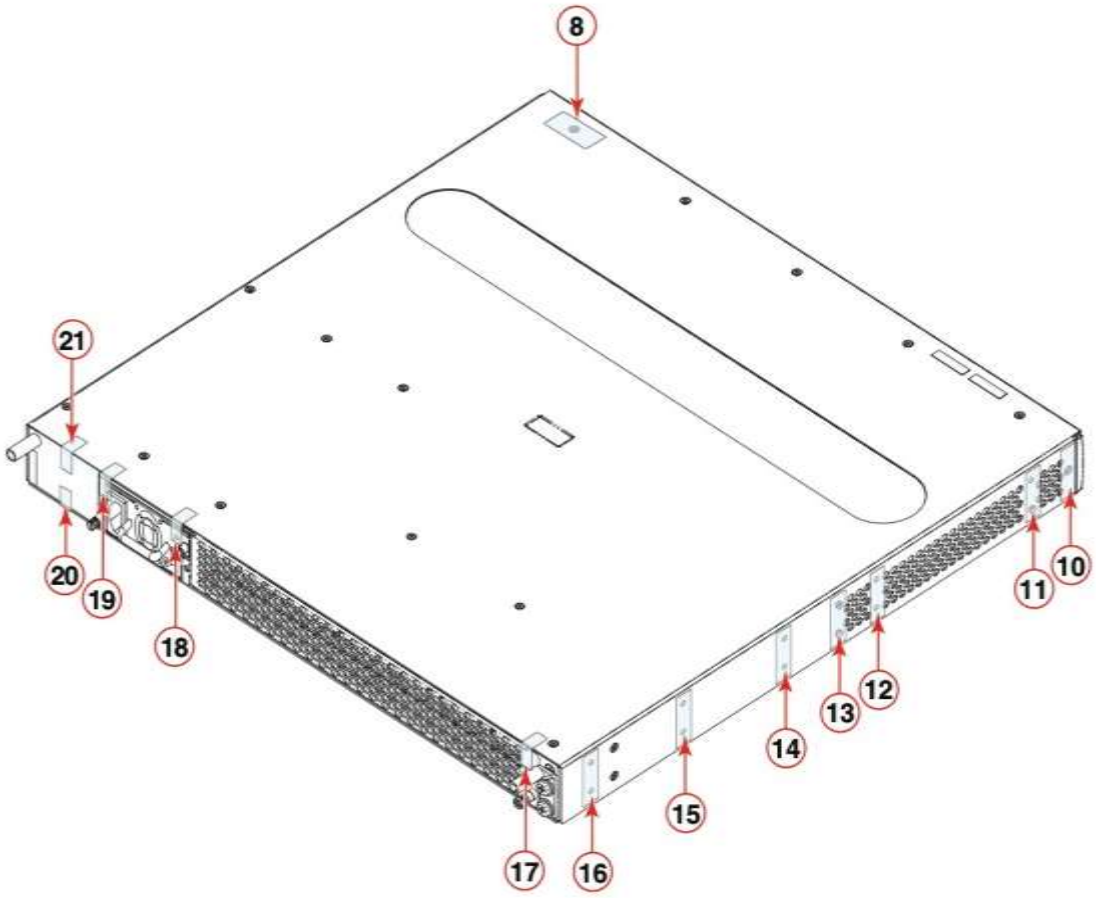


Figure 83 Rear, top and left side view of the security seals placement for a Brocade NetIron CER 2024C device with a 2X10G XFP uplink module



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 thirty- three (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 and 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 so that the left side of the front panel is obscured. Additionally, one seal is placed vertically over the console port. See Figure 84 and 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

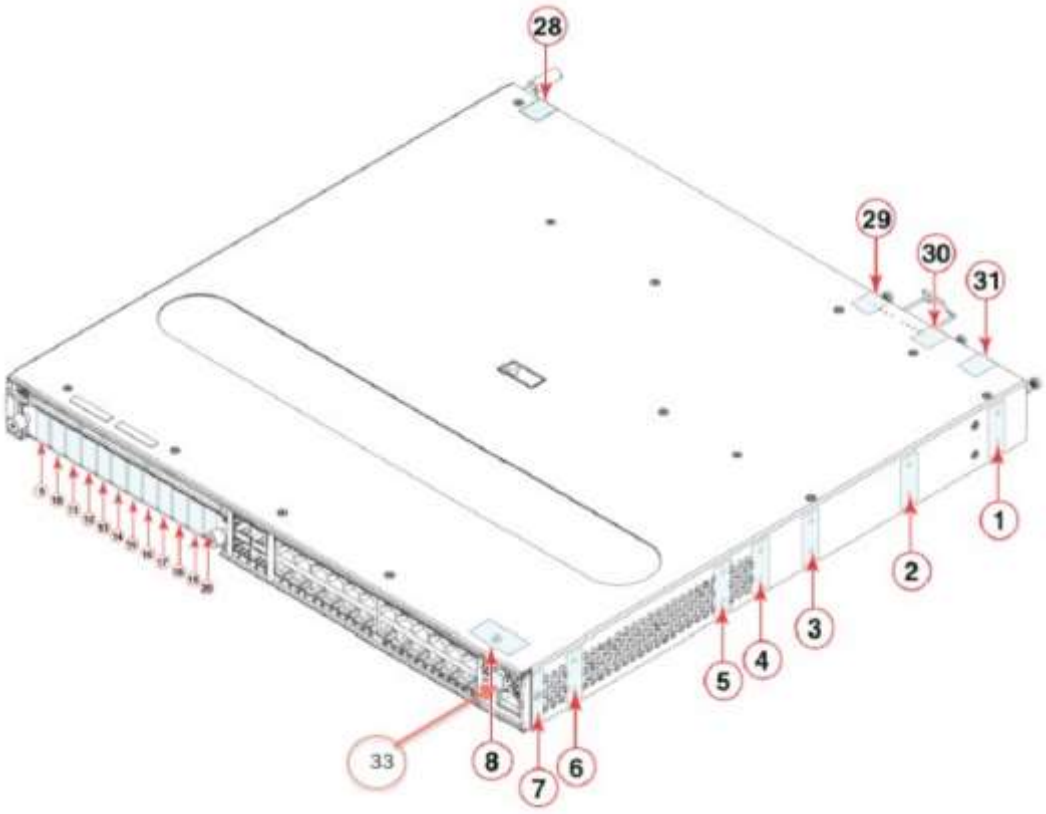
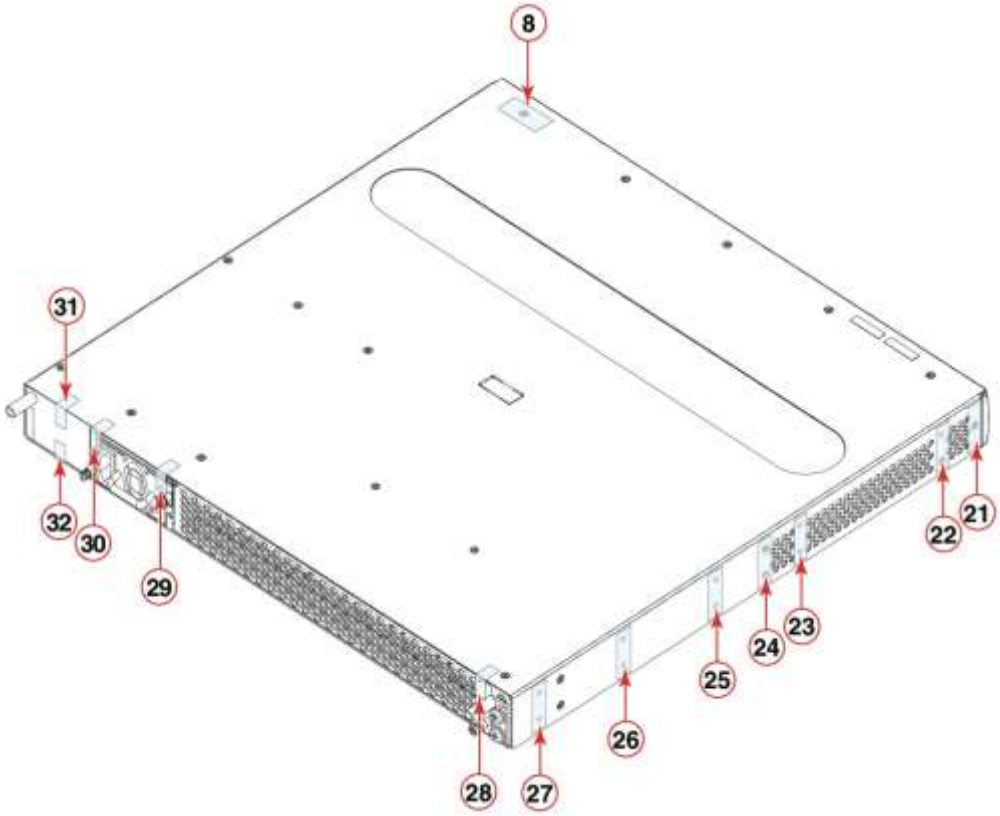


Figure 85 Front view of a Brocade NetIron CER 2024F devicewith security seals

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 (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 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 for 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

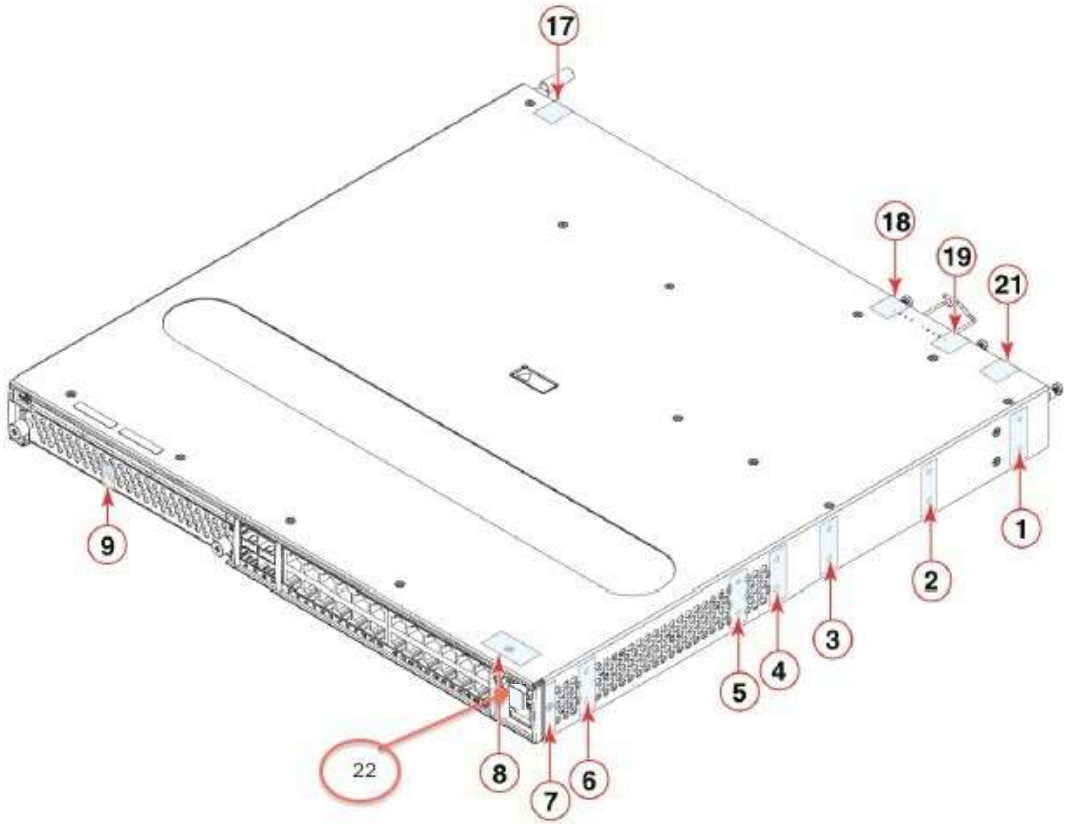
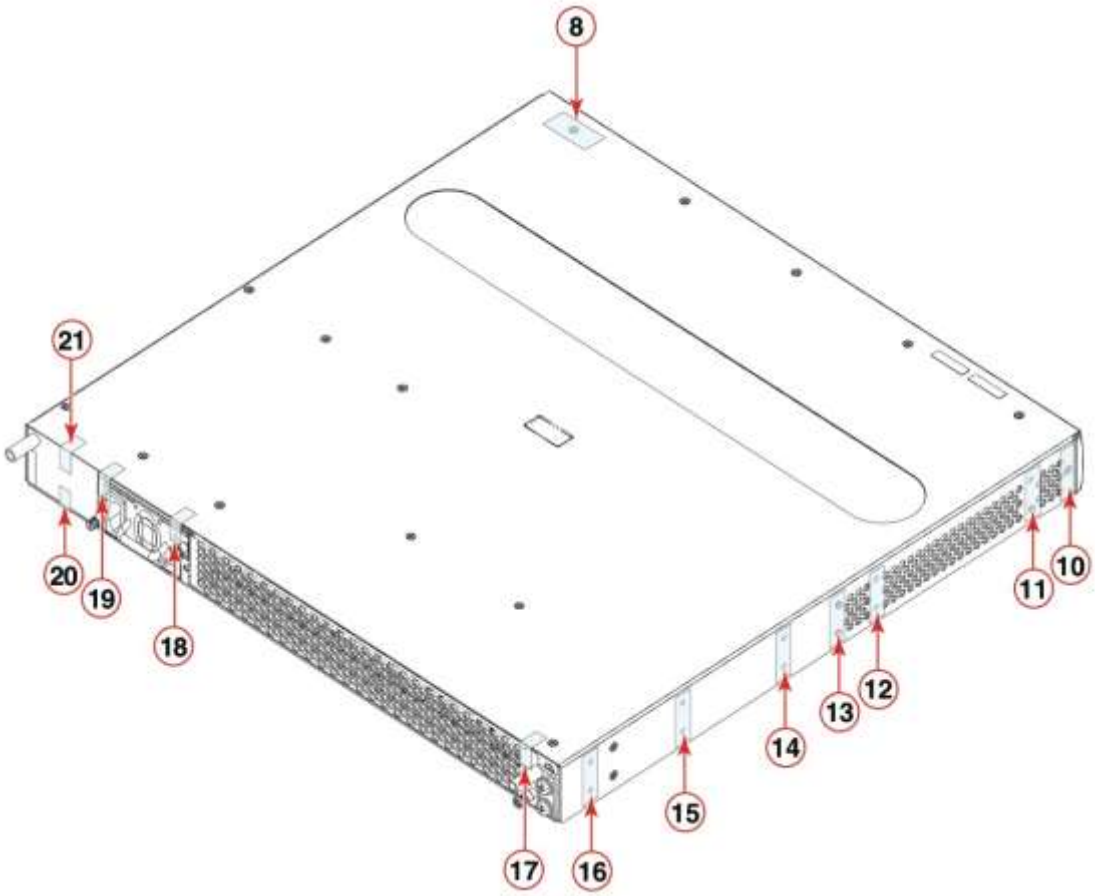


Figure 88 Rear, top and left side view of the security seals placement for a Brocade NetIron CER 2024F device with a 2x10G XFP uplink module



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

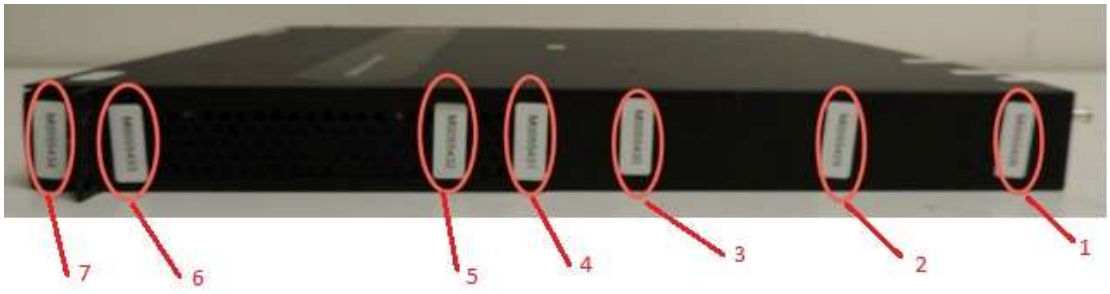
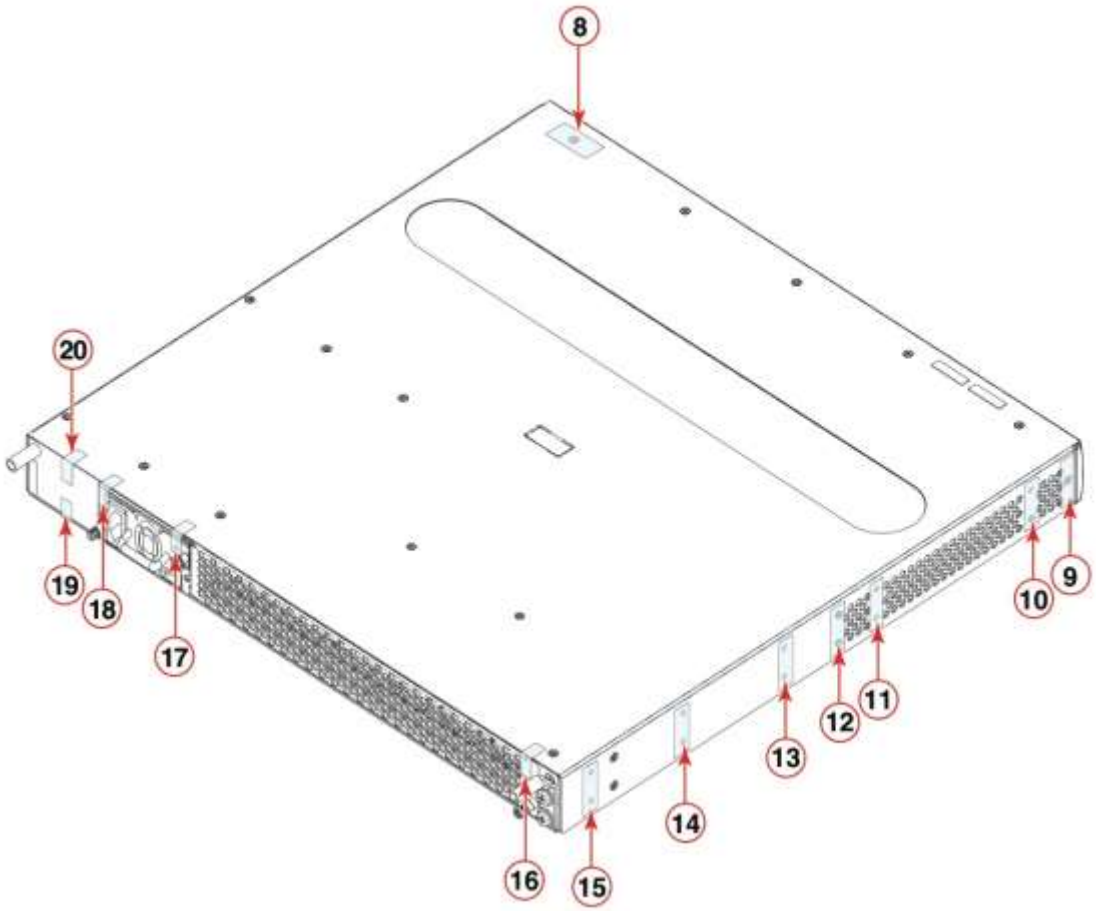


Figure 91 Rear, top and left side view of a Brocade NetIron CER 2048 device with security seals



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, 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. 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 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

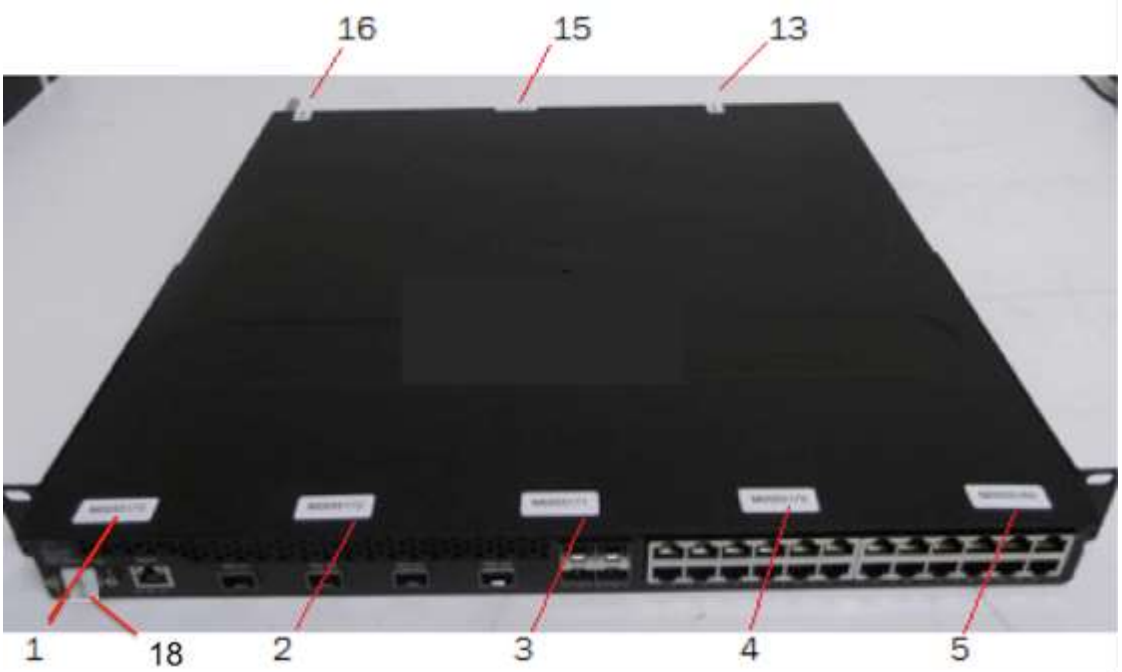


Figure 93 Right view of a Brocade CER 2024C-4X-RT device with security seals

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

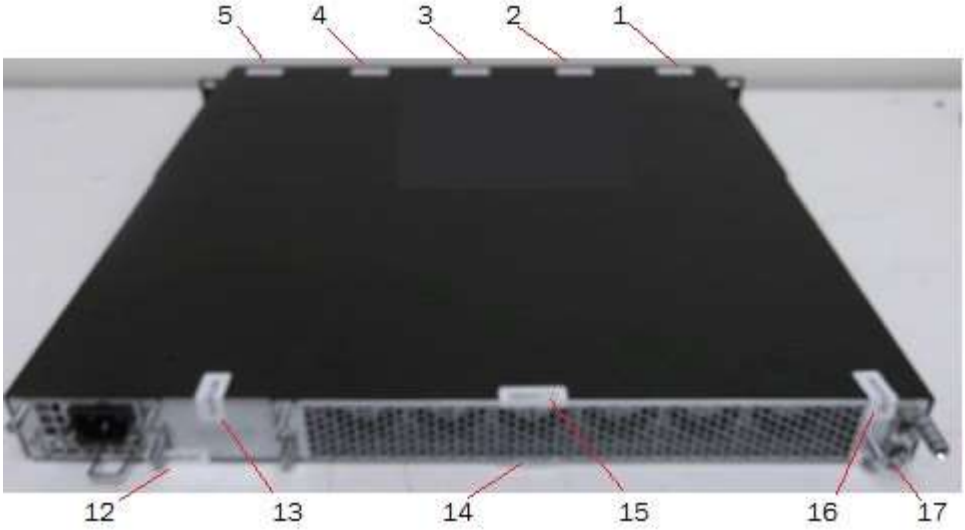
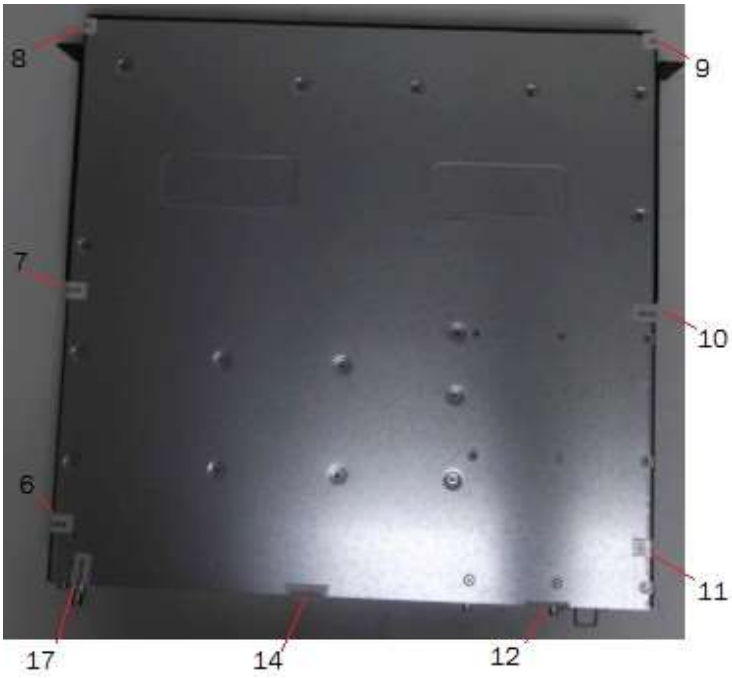


Figure 96 Bottom view of a Brocade CER 2024C-4X-RT device with security seals



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 twenty (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 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 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, 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. 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 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

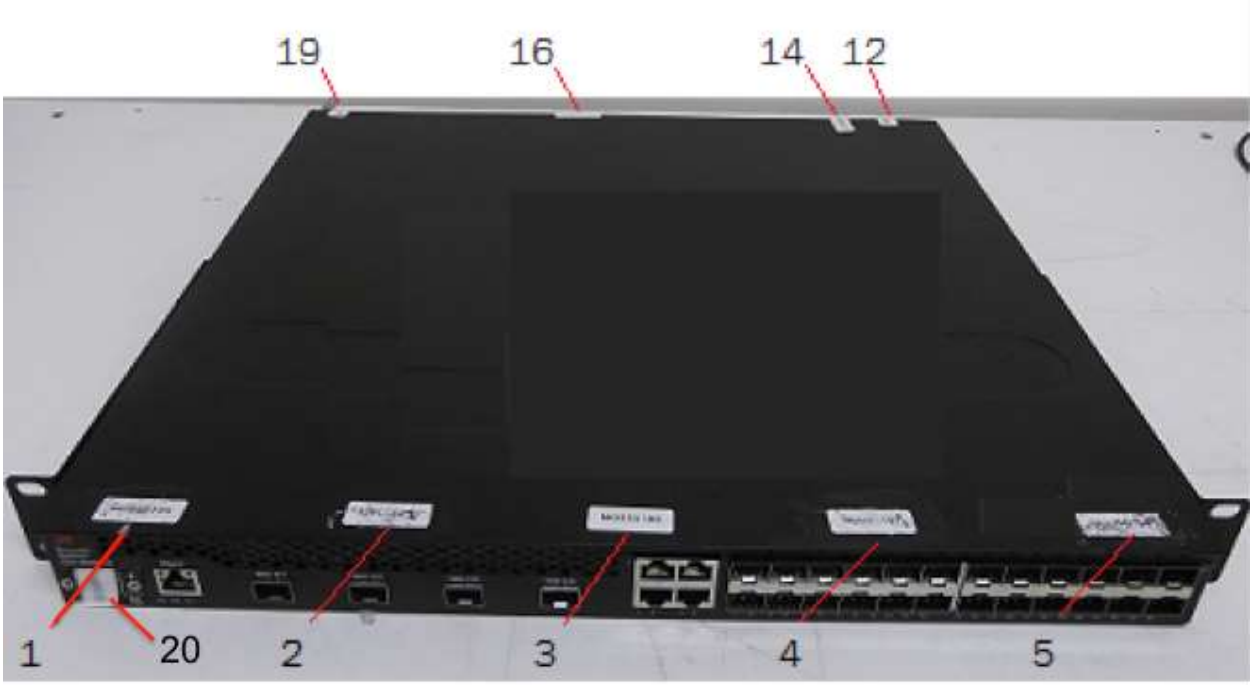


Figure 98 Right side view of a Brocade CER 2024F-4X-RT device with security seals

Figure 99 Left side 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

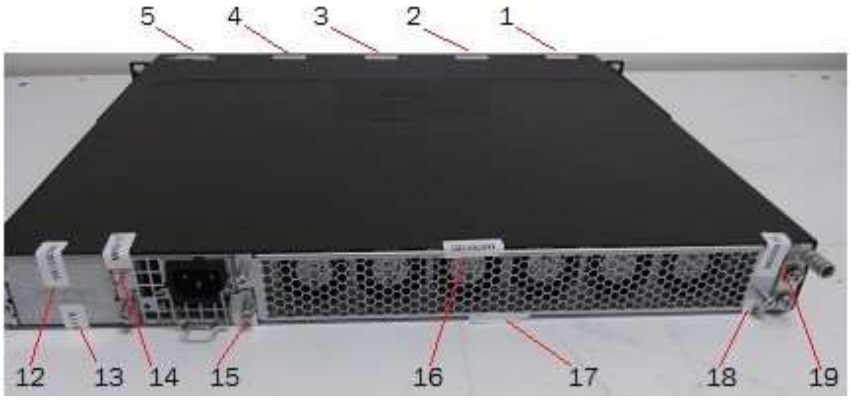
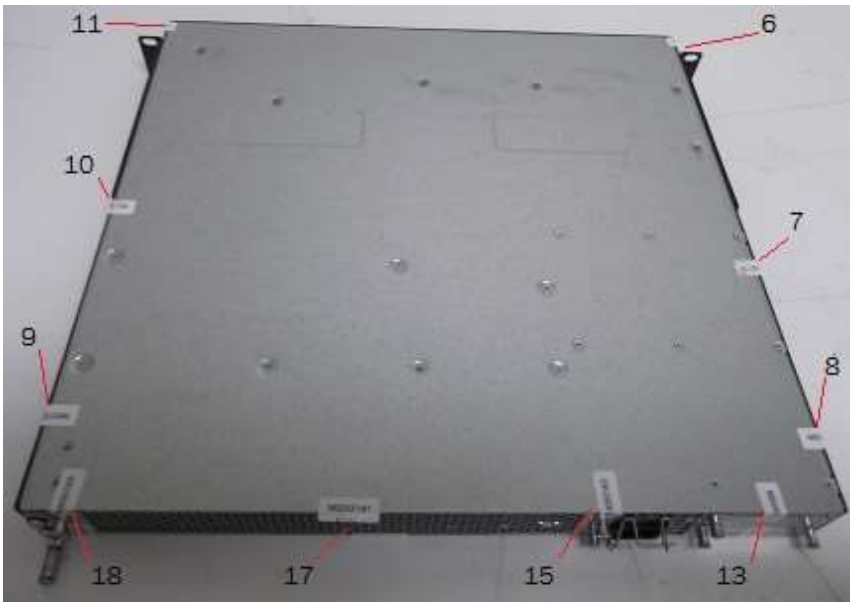


Figure 101 Bottom view of a Brocade CER 2024F-4X-RT device with security seals



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 twenty (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 placement of seals on the left and right sides mirrors each other.
- Rear: Affix eight 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. 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

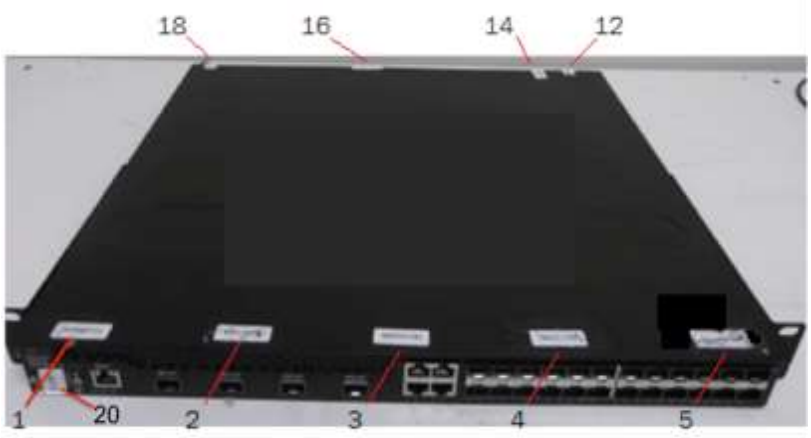


Figure 103 Right side view of a Brocade CES 2024C-4X device with security seals

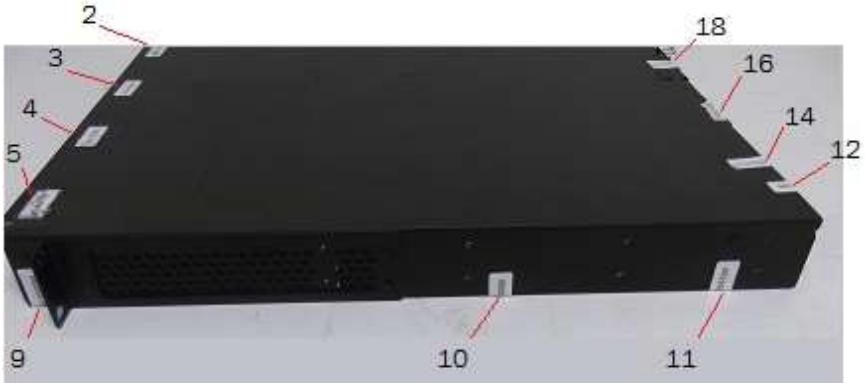


Figure 104 Left side view of a Brocade CES 2024C-4X device with security seals

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

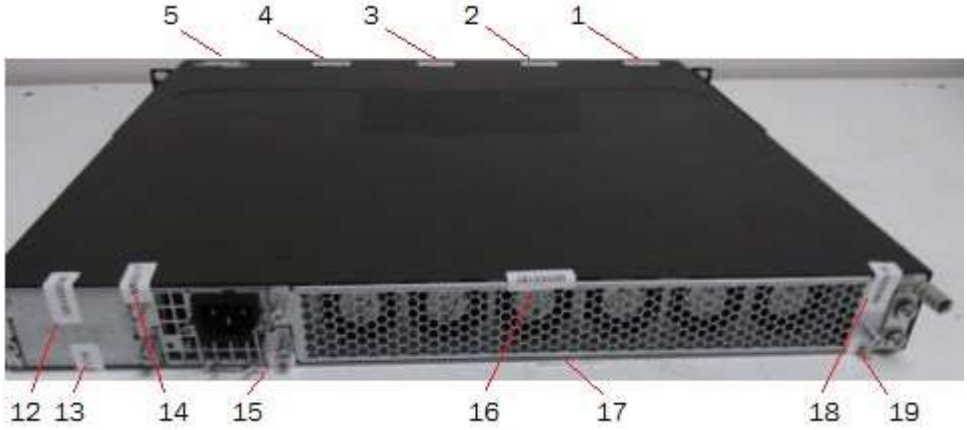
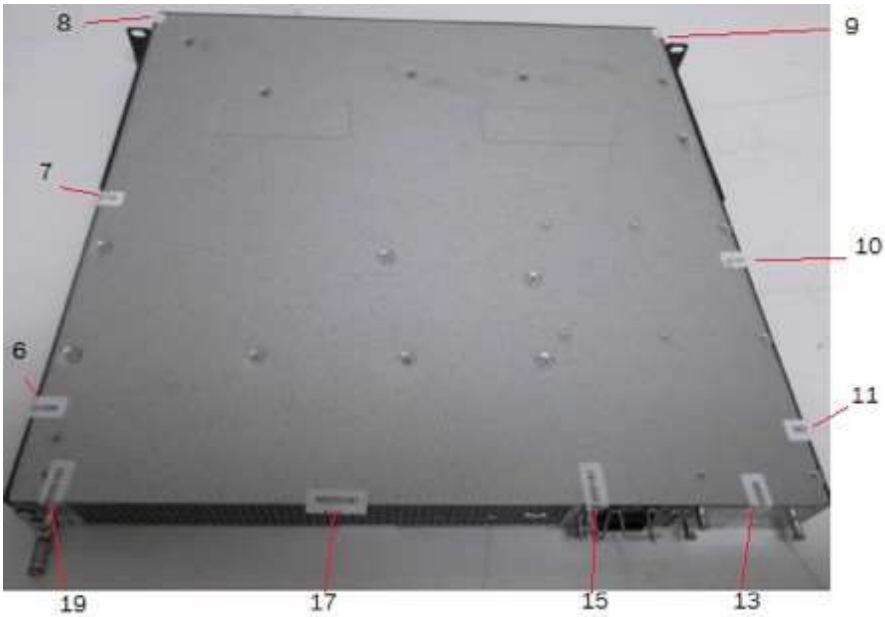


Figure 106 Bottom view of a Brocade CES 2024C-4X device with security seals



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 twenty (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 mirrors each other.
- Rear: Affix eight 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. 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

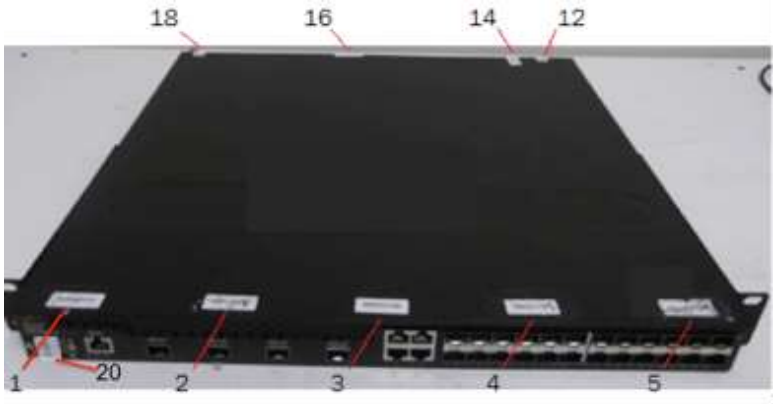


Figure 108 Right side view of a Brocade CES 2024F-4X device with security seals

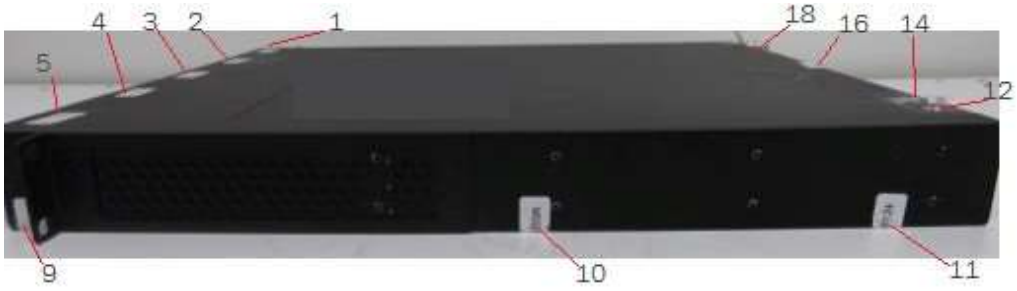


Figure 109 Left side view of a Brocade CES 2024F-4X device with security seals

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

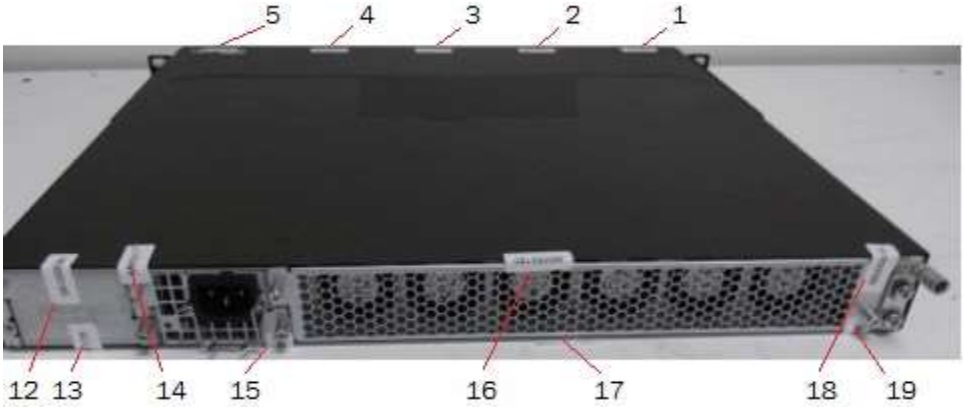


Figure 111 Bottom view of a Brocade CES 2024F-4X device with security seals