National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Brocade Communication Systems, Inc

130 Holger Way

San Jose, CA 95134

Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00

Report Number:	**CCEVS-VR-10657-2016**
Dated:	**January 27, 2016**
Version:	**0.4**

ACKNOWLEDGEMENTS

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Brocade MLXe Family Devices with Multi-Service IronWare solution provided by Brocade Communication Systems, Inc It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in January 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is the Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 internet router and VPN gateway.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 (NDPP11E3/VPNGEP11) Security Target, Version 0.7, 1/13/16 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in

accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.

- The Security Target (ST), describing the security features, claims, and assurances of the product.

- The conformance result of the evaluation.

- The Protection Profile to which the product is conformant.

- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) (including the optional SSH and TLS requirements) with Errata #3 Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 12 April 2013(VPNGWEP11).
ST:	Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 (NDPP11E3/VPNGEP11) Security Target, Version 0.7, 1/13/16
Evaluation Technical Report	Evaluation Technical Report for Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00, Version 0.3, January 22, 2016.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Brocade Communication Systems, Inc
Developer	Brocade Communication Systems, Inc
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Stelios Melachrinoudis, The MITRE Corporation Jean Petty, The MITRE Corporation

Item	Identifier
	Chris Thorpe, The MITRE Corporation

3   Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocades' proprietary Multi-Service IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances. The TOE includes a card (BR-MLX-10GX4-IPSEC-M) that supports IPsec processing on the appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration (using the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide) prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using IPsec. Once configured following the Common Criteria specific guidance, the TOE also offers an encrypted Web Management Interface using IPsec. All of the remote management interfaces are protected using encryption as explained later in this ST.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations
- Non-volatile flash memory, used to store the operating system image, startup configuration and other relevant files.
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

3.1   TOE Evaluated Platforms

The evaluated configuration consists of the following models …

Brocade Communication Systems, Inc Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00, including the following series and models

- Brocade NetIron MLXe Series Hardware Platforms with the BR-MLX-10GX4-IPSEC-M Card

- BR-MLXe-4-MR2-M-AC, BR-MLXe-4-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXe-4-MR2-X-AC, BR-MLXe-4-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXe-8-MR2-M-AC, BR-MLXe-8-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXe-8-MR2-X-AC, BR-MLXe-8-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXe-16-MR2-M-AC, BR-MLXe-16-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXe-16-MR2-X-AC, BR-MLXe-16-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- BR-MLXE-32-MR2-M-AC, BR-MLXE-32-MR2-M-DC
    - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X
- BR-MLXE-32-MR2-X-AC, BR-MLXE-32-MR2-X-DC
    - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X

3.2 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the Brocade IronWare OS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing functions). IronWare OS enforces applicable security policies on network information flowing through the hardware appliance.

The basic start-up operation of the TOE is as follows:

1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them

according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface. The TOE will process other packets destined for itself (control path packets) based on the requirements of the given protocol (IPsec).

Given that this Security Target conforms to the NDPP11e3 and VPNGWEP11, the security claims focus on the TOE as a secure network infrastructure device with VPN Gateway functionality and do not focus on other key functions provided by the TOE. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

Each TOE appliance runs a version of the Brocades software and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an external NTP server in the operational environment.

The TOE can be configured to use external RADIUS and TACACS+ authentication servers.

4 Security Policy

This section summaries the security functionality of the TOE:
1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Packet Filtering
7. Protection of the TSF
8. TOE access
9. Trusted path/channels

4.1   Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using IPsec to protect the logs while in transit on the network

4.2   Cryptographic support

The TOE is a cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec.

4.3   User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various network connections. While implementing applicable network protocols associated with network traffic routing, the TOE is carefully designed to ensure that it does not inadvertently reuse data found in network traffic. This is accomplished primarily by controlling the size of all buffers, fully overwriting buffer contents, and zero-padding of memory structures and buffers when necessary

4.4   Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes.

4.5   Security management

The TOE provides Command Line Interface (CLI) commands and an HTTPS over IPsec Graphical User Interface (Web GUI) to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system

4.6 Packet Filtering

The TOE provides extensive packet filtering capabilities for IPv4, IPv6, TCP, and UDP. The authorized administrator can define packet filtering rules that apply to most every field within the identified packet types. The authorized administrator can define each rule to permit, deny, and log each decision.

4.7 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance, and as such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.8 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.9 Trusted path/channels

The TOE protects interactive communication with administrators using IPsec for CLI access or for Web graphical user interface access (HTTPS over IPsec). In each case, the both integrity and disclosure protection is ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, the attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using IPsec connections to prevent unintended disclosure or modification of logs

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3) with the following two extended packages:

- Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall, Version 1.0, 19 December 2011 (FW)

- Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 15 April 2013(VPN)

That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- Brocade NetIron FIPS and Common Criteria Configuration Guide Supporting Multi-Service Ironware R05.9.00a, 53-1003826-01, 22 January 2016.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (NDPP11e3/VPNGWEP11) for Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00, version 0.3, 1/22/2016.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDPP11e3 and VPNGWEP11 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the following series and models

- Brocade NetIron MLXe Series Hardware Platforms with the BR-MLX-10GX4-IPSEC-M Card

- o BR-MLXe-4-MR2-M-AC, BR-MLXe-4-MR2-M-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXe-4-MR2-X-AC, BR-MLXe-4-MR2-X-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXe-8-MR2-M-AC, BR-MLXe-8-MR2-M-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXe-8-MR2-X-AC, BR-MLXe-8-MR2-X-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXe-16-MR2-M-AC, BR-MLXe-16-MR2-M-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXe-16-MR2-X-AC, BR-MLXe-16-MR2-X-DC
  - ▪ With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
- o BR-MLXE-32-MR2-M-AC, BR-MLXE-32-MR2-M-DC
  - ▪ With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X
- o BR-MLXE-32-MR2-X-AC, BR-MLXE-32-MR2-X-DC
  - ▪ With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X

9   Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all work units described in the ND PP and CEM v3.1 rev 4 received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4.

9.1   Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the MLXe Family Devices with Multi-Service IronWare R05.9.00 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP11e3 and VPNGWEP11 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP11e3 and VPNGWEP11 and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay special attention to the evaluated configuration of the device(s) and the specific functionality defined within the Security Target. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the security functional requirements within the Security Target was evaluated. Other functionality included in the product was not assessed as part of this evaluation.

The product contains more functionality than was covered by the evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

It is important for sponsors and customers to understand that as of the close of this evaluation, the TOE does not carry an up-to-date FIPS CMVP certificate; as such, all references to CMVP certification in documentation and prompts generated by the device itself, including references to a FIPS validated cryptographic module, must be disregarded until a valid CMVP certificate is issued.

11 Annexes

Not applicable

12 **Security Target**

The Security Target is identified as: *Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 (NDPP11E3/VPNGEP11)* Security Target, Version 0.7, 1/13/16.

13 **Glossary**

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 **Bibliography**

The Validation Team used the following documents to produce this Validation Report:

[1]   Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2]   Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3]   Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4]   Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3)

[5]   Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 15 April 2013(VPNGWEP11)

[6]   Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00 (NDPP11E3/VPNGEP11) Security Target, Version 0.7, 1/13/16 (ST)

[7]   Assurance Activity Report (NDPP11e3/VPNGWEP11) for Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00, Version 0.1, 01/15/2016 (AAR)

[8]   Detailed Test Report (NDPP11e3/VPNGWEP11) for Brocade MLXe Family Devices with Multi-Service IronWare R05.9.00, version 0.3, 1/22/2016 (DTR)