National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Brocade Communications Systems, Inc.

130 Holger Way

San Jose, CA 95134

Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20

Report Number:	**CCEVS-VR-VID10604-2014**
Dated:	**December 16, 2014**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jean Petty, *The MITRE Corporation*
Jerome Myers, *The Aerospace Corporation*

Common Criteria Testing Laboratory

Tammy Compton
Chris Keenan
Gossamer Security Solutions, Inc.
Catonsville, MD

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 FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 solution provided by Brocade Communications 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 Month Year. 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, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) is the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 family of products. The TOE is composed of a hardware appliance with embedded software installed on a management processor.

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 Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the Brocade Communications Systems, Inc. Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 (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
ST:	Brocade Communications Systems, Inc. Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 Security Target, Version 0.3, November 25, 2014
Evaluation Technical Report	Evaluation Technical Report for Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20), Version 1.0, November 21, 2014
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 Communications Systems, Inc.
Developer	Brocade Communications Systems, Inc.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	

3 Architectural Information

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

The Target of Evaluation (TOE) is the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. Optionally, a number of co-located appliances can be connected in order to work as a unit with a common security policy. The embedded software is a version of Brocades' proprietary Multiservice IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware 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 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 SSH.

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
- Flash memory, used to store the operating system image
- Non-volatile memory, which stores configuration parameters used to initialize the system at system startup
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

3.1 TOE Evaluated Platforms

The Target of Evaluation (TOE) is the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 including the following series and models:

- SX Series Hardware Platforms (FI-SX-800 and FI-SX-1600),

- ICX Series Hardware Platforms (
    - ICX 6610-24, 6610-24F, 6610-24P, 6610-48, 6610-48P,
    - ICX 6450-24, 6450-24P, 6450-48, 6450-48P, 6450-C12-PD
    - ICX 7450,
    - ICX 7750), and
- FCX Series Hardware Platforms (FCX 624S, FCX 624S-HPOE-ADV, FCX 624-F-ADV, FCX 648S, and FCX 648S-HPOE-ADV).

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 IOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). IOS 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, or dropped in accordance with a configured policy.

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 NTP server in the operational environment.

The use of external authentication services such as RADIUS or TACACS/TACACS+ is excluded from the evaluated configuration.

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. Protection of the TSF
7. TOE access
8. 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 TLS to protect the logs while in transit on the network.

4.2 Cryptographic support

The TOE includes a FIPS-certified 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 SSH and TLS.

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 doesn’t 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.

The TOE also provides the authorized administrators with the ability to configure Authentication Method lists. These lists are used to specify the order in which the authentication methods are employed whenever there are one or more authentication methods available.

4.5 Security management

The TOE provides Command Line Interface (CLI) commands 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 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 or a closely grouped (e.g., in the same rack) collection of appliances acting as a unit. 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.

4.7 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.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

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

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP). 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 FastIron FIPS Configuration Guide Supporting FastIron Software Release 08.0.20, 53-1003418-01, 25 August 2014
- Brocade FastIron Ethernet Switch Security Configuration Guide Supporting FastIron Software Release 08.0.20, 53-1003405-01, 30 September 2014
- Brocade FastIron Ethernet Switch Administration Guide Supporting FastIron Software Release 08.0.20, 53-1003388-01, 30 September 2014

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 Evaluation Team Test Report for the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20, Version 1.0, November 21, 2014.

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 the Brocade FastIron FIPS Configuration Guide Supporting FastIron Software Release 08.0.20, 53-1003418-01, 25 August 2014 document and ran the tests specified in the NDPP including the optional SSH and TLS tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 including the following series and models

- SX Series Hardware Platforms (FI-SX-800 and FI-SX-1600),
- ICX Series Hardware Platforms (
  a. ICX 6610-24, 6610-24F, 6610-24P, 6610-48, 6610-48P,
  b. ICX 6450-24, 6450-24P, 6450-48, 6450-48P, 6450-C12-PD,
  c. ICX 7450,
  d. ICX 7750) and
- FCX Series Hardware Platforms (FCX 624S, FCX 624S-HPOE-ADV, FCX 624-F-ADV, FCX 648S, and FCX 648S-HPOE-ADV).

To use the product in the evaluated configuration, the product must be configured as specified in the Brocade FastIron FIPS Configuration Guide Supporting FastIron Software Release 08.0.20, 53-1003418-01, 25 August 2014.

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 EAL1 work units 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. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

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 Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20 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 EAL 1 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 NDPP 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 EAL 1 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 EAL 1 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP 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 EAL 1 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 particular attention to the evaluated configuration of the device(s). In order to remain CC compliant, the device(s) must first be configured into FIPS mode, then into Common Criteria mode as specified in the FastIron FIPS and Common Criteria Configuration Manual. Note that the product includes FIPS validated cryptographic algorithms.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Please note further that certain network related functionality is excluded from the approved configuration and that some networking functions relative to the devices were not tested, nor are any claims made relative to their security.

The product contains more functionality than was covered by the evaluation. Only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Brocade Communications Systems, Inc. Brocade FastIron SX, ICX, and FCX Series Switch/Router 08.0.20, Version 0.3, November 25, 2014*.

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 2102.

[4] Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP).