National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Brocade Communications Systems, Inc.

130 Holger Way

San Jose, CA 95134 USA

Brocade Directors and Switches using Fabric OS v8.1.0

Report Number: CCEVS-VR-10797-2017
Dated: June 30, 2017
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 Senior Validator
Dr. Patrick Mallett PhD Lead Validator

Common Criteria Testing Laboratory

Cornelius Haley
Catherine Sykes
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 Directors and Switches 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 June 2017. 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 the collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015.

The Target of Evaluation (TOE) is the Brocade Directors and Switches 8.1.0.

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 Communications Systems, Inc. Directors and Switches (NDcPP10) Security Target, version 0.3, June 1, 2017 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) 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 Directors and Switches 8.1.0 (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015
ST	Brocade Directors and Switches Security Target, version 0.3, June 1, 2017
Evaluation Technical Report	Evaluation Technical Report for Brocade Directors and Switches 8.1.0, version 0.1, June 5, 2017
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.
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 **Error! Reference source not found.** running Fabric OS v8.1.0. The various models of the TOE identified below differ in performance, form factor and number of ports, but all run the same Fabric OS version 8.1.0 software. The TOE is available in two form factors:

1. a rack-mount Director chassis with a variable number of replaceable modules or 'blades', and
2. a self-contained network switching appliance device

The Target of Evaluation (TOE) is the Brocade Director and Switch family of products using Fabric OS v8.1 provided by **Error! Reference source not found. Error! Reference source not found.** are hardware network devices that create what is called a 'Storage Area Network' or 'SAN'. SANs provide switched connections between servers connected to the SAN and storage devices such as disk storage systems and tape libraries that are also connected to the SAN.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

- Gen 5 Directors and Switches
  - Director Blade Models: FC16-32, FC16-48, FC16-64, CP8, CR16-4, CR16-8, FX8-24
  - Director Models: DCX 8510-4 and DCX 8510-8
  - Switch Appliance Models: 6510, 6520 and 7840
- Gen 6 Directors and Switches
  - Director Blade Models: FC32-48, CPX6, CR32-4, CR32-8 and SX6
  - Director Models: X6-4 and X6-8
  - Switch Appliance Model: G620

3.2 TOE Architecture

The TOE provides the ability to centralize the location of storage devices in a network in the environment. Instead of attaching disks or tapes to individual hosts in the environment, or for example attaching a disk or tape directly to the network, storage devices can be physically attached to the TOE, which can then be physically attached to HBAs in the environment. HBAs that are connected to the TOE can then read from and write to storage devices that are attached to the TOE according to TOE configuration. Storage devices in the environment appear to the operating system running on the machine that the HBA is installed in as local (i.e. directly-attached) devices.

More than one HBA can share one or more storage devices that are attached to the TOE according to TOE configuration. Scalability is achieved by interconnecting multiple instances of TOE directors and switches to form a fabric that supports different numbers of HBAs and storage devices.

Directors and switches both can be used by HBAs to access storage devices using the TOE. Switch appliances provide a fixed number of physical interfaces to hosts and storage devices in the environment. Directors provide a configurable number of physical interfaces using a chassis architecture that supports the use of blades that can be installed in and removed from the director chassis according to administrator configuration.

There are administrative interfaces to manage TOE services that can be accessed using an Ethernet network, as well as interfaces that can be accessed using a directly-attached console as follows:

- Ethernet network-based web-based administrator console interfaces – Provides web-based administrator console interfaces called the "Brocade Advanced Web Tools."
- Ethernet network-based command-line administrator console interfaces – Provides command-line administrator console interfaces called the "FabricOS Command Line Interface."
- Serial terminal-based command-line administrator console interfaces – Provides command-line administrator console interfaces called the "FabricOS Command Line Interface."

There also exists administrative Ethernet network-based programmatic API interfaces that can be protected using SSL. The API interface is not supported in the evaluated configuration. Similarly, there exists a modem hardware component that is optional to the product that can be used in a similar manner as a serial console port, but it is disabled by virtue of not being physically installed during initial installation and configuration in the evaluated configuration.

The TOE can operate in either "Native Mode" or "Access Gateway Mode". Only Native mode is supported in the evaluated configuration. Access Gateway mode makes the switch function more like a "port aggregator" and in Access Gateway mode the product does not support the primary access control security functions (mainly zoning) claimed when operating in Native mode.

While actual implementations may interconnect multiple instances of TOE models, each TOE device (i.e., instance of the TOE) is administered individually.

Separate appliance ports are relied on to physically separate connected HBAs. The appliance's physical location between HBAs and storage devices is relied on to ensure TOE interfaces cannot be bypassed. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface and HTTPS for the Advanced Web Tools GUI interface. The TOE requires administrators to login before an SSH or HTTPS session is established.

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

The TOE can be described in terms of the following components:

- Brocade Switch and Director Appliances – One or more of each type are supported in the evaluated configuration. The evaluated configuration also supports one or more blades per director, depending on the number supported by a given director model.
- Brocade FabricOS operating system – Linux-based operating system that runs on Brocade switches and directors. FabricOS is comprised of user-space programs, kernel daemons and kernel modules loaded as proprietary components into LINUX. The base features of LINUX, including the file system, memory management, processor and I/O support infrastructure for FOS user-space programs, daemons, and kernel modules. Interprocess communication is handled through commonly mapped memory or shared PCI memory and semaphores as well as IOCTL parameter passing. LINUX provides access to memory or to make a standard IOCTL call, and all the contents of the buffers and IOCTL message blocks or other message blocks are proprietary to the FOS user-space programs, kernel modules and daemons. The FabricOS operating system is considered to include the OpenSSL crypto engine as internal functionality supporting TOE operation.

The intended environment of the TOE can be described in terms of the following components:

- Host – A system in the environment that uses TOE Storage Area Network (SAN) services.
- Host Bus Adapters (HBAs) – Provides physical network interfaces from host machines in the environment to the TOE. HBA drivers provide operating system interfaces on host machines in the environment to storage devices in the environment. Storage devices in the environment appear to the host operating system as local (i.e. directly-attached) devices.
- Storage device – A device used to store data (e.g. a disk or tape) that is connected to the TOE using a FC/FCIP connection and is accessed by a host using the TOE.
- Terminal application – Provides a runtime environment for console-based (i.e. SSH) client administrator console interfaces.
- Web browser – Provides a runtime environment for web-based (i.e. HTTPS) client administrator console interfaces.
- Syslog server – Provides logging to record auditable event information generated by the TOE. The syslog server is expected to protect audit information sent to it by the TOE and make that data available to administrators of the TOE.
- Certificate Authority (CA) – Provides digital certificates HTTPS-based interfaces that are installed during initial TOE configuration. After installation, the CA no longer needs to be on the network for operation.

- Key management systems – Provide life cycle management for all data encryption keys (DEKs) created by the encryption engine. Key management systems are provided by third-party vendors and are not included in the scope of this evaluation.

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE does not rely on any other components in the environment to provide security-related services.

Each TOE appliance runs a version of the FOS 8.1.0 and has physical network connections to its environment to facilitate a routing Storage Area Network traffic. The TOE appliance is a destination of network traffic, where it provides an interface 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 a syslog server in the 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 TOE includes the ability to communicate with SYSLOG servers in its environment to export audit data. The TOE is designed to interact with SYSLOG servers in accordance with their respective protocols, including security capabilities where applicable.

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 generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message contents into an encapsulating syslog record.

4.2 Cryptographic support

The TOE contains FIPS-certified cryptographic implementations that provide 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

While implementing SAN and HBA protocols, the TOE is carefully designed to ensure that it doesn't inadvertently release or leak residual data. When the TOE allocates a new buffer for either an incoming or outgoing network packet, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, and additional space will be overwritten (padded) with zeros before the packet is forwarded (either to an external network of HBA or written to a storage device) on both Ethernet and FC connections.

4.4 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. The TOE performs the validation of the login credentials and the TOE enforces the decision. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

4.5 Security management

The TOE provides serial terminal (command line) and Ethernet network-based (command-line and web) management interfaces. Each of the three types of interfaces provides equivalent management functionality. The TOE provides administrative interfaces to configure hard zoning, as well as to set and reset administrator passwords. By default, HBAs do not have access to storage devices.

4.6 Protection of the TSF

The TOE implements a number of features designed 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.

4.7 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 enforces a trusted path between the TOE administrators and the TOE using SSH and TLS/HTTPS connections for Ethernet connections from the Administrator terminal to the TOE. The TOE encrypts commands sent from terminal applications by administrators using SSH for the command line interface and TLS/HTTPS for the Advanced Web Tools GUI interface.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *collaborative Protection Profile for Network Devices*, Version 1.0, 27 February 2015 (NDcPP10). That information has not been reproduced here and the NDcPP10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The

CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Configuration Guide Fabric OS Common Criteria Supporting Fabric OS 8.1.0b, June 7, 2017

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP10) for Directors and Switches 8.1.0, Version 0.3, June 22, 2017 (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP10 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Director Model	Blades
DCX 8510-4	CP8, CR16-4, FC16-32, FC16-48, FC16-64, FX8-24
DCX 8510-8	CP8, CR16-8, FC16-32, FC16-48, FC16-64, FX8-24
X6-4	CPX6, CR32-4, , FC32-48, SX6
X6-8	CPX6, CR32-8, FC32-48, SX6

10 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 assurance activities and 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 Directors and Switches TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP10.

10.1 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 Directors and Switches 8.1.0 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.

10.2 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 NDcPP10 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.

10.3 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.

10.4 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.

10.5 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 NDcPP10 and recorded the results in a Test Report, summarized in the AAR.

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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “SAN”, “Brocade”, “FabricOS”, “OpenSSH” and “OpenSSL”.

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.

10.7 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.

11 Validator Comments/Recommendations

The validators have no further comments.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Brocade Directors and Switches (NDcPP10) Security Target, Version 0.3, June 1, 2017*.

14 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.

15 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] collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015

[5] Brocade Directors and Switches using Fabric OS v8.1.0 (NDcPP10) Security Target, Version 0.3, June 1, 2017 (ST)

[6] Assurance Activity Report (NDcPP10) for Directors and Switches 8.1.0, Version 0.3, June 22, 2017 (AAR)

[7] Evaluation Technical Report for Brocade Directors and Switches, Version 0.3, June 22, 2017 (ETR)