National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Brocade Communication Systems, Inc, 1745 Technology Dr., San Jose, CA 95110

Brocade Directors and Switches

Report Number: CCEVS-VR-10376-2012
Dated: September 2012
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

Jandria Alexander
Aerospace Corporation
Columbia, MD

Jean Hung
MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

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 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 Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in December 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

The Brocade Directors and Switches (Director Blade Models: FC10-6, FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48, CP8, CR8, CR4S-8, CR16-4, CR16-8, FCOE10-24, FS8-18, FX8-24; Director Models: DCX, DCX-4S, DCX 8510-4, DCX 8510-8; Switch Appliance Models: 300, 5100, 5300, 6510, 7800, 8000, BES; and Embedded Blades: 5410, 5424, 5450, 5460, 5470, 5480) provide 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 host bus adapters in the environment. Host bus adapters 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 host bus adapter is installed in as local (i.e. directly-attached) devices. More than one host bus adapter 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 host bus adapters and storage devices. Directors and switches both can be used by host bus adapters 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.

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 2) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 2). 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, observed evaluation testing activities, 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 SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Brocade Directors and Switches 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 Directors and Switches, as follows, running FabricOS version 7.0.0b1: Director Blade Models: FC10-6, FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48, CP8, CR8, CR4S-8, CR16-4, CR16-8, FCOE10-24, FS8-18, FX8-24 Director Models: DCX, DCX-4S, DCX 8510-4, DCX 8510-8 Switch Appliance Models: 300, 5100, 5300, 6510, 7800, 8000, BES Embedded Blades: 5410, 5424, 5450, 5460, 5470, 5480 Note that models FS8-18 and BES switch appliance support the user data encryption function.
Protection Profile	None
ST:	Brocade Directors and Switches Security Target, Version 2.91, August 30, 2012
Evaluation Technical Report	Evaluation Technical Report For the Brocade Directors and Switches (Proprietary), Version 2.0, December 7, 2011
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 2
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Brocade Communication Systems, Inc
Developer	Brocade Communication Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Jandria Alexander, Aerospace Corporation, Columbia, MD Jean Hung, MITRE Corporation, Bedford, MA

3 Architectural Information

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

3.1 TOE Architecture

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 (FOS) – 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.

In its most basic form, the TOE in its intended environment of the TOE is depicted in the figure below.

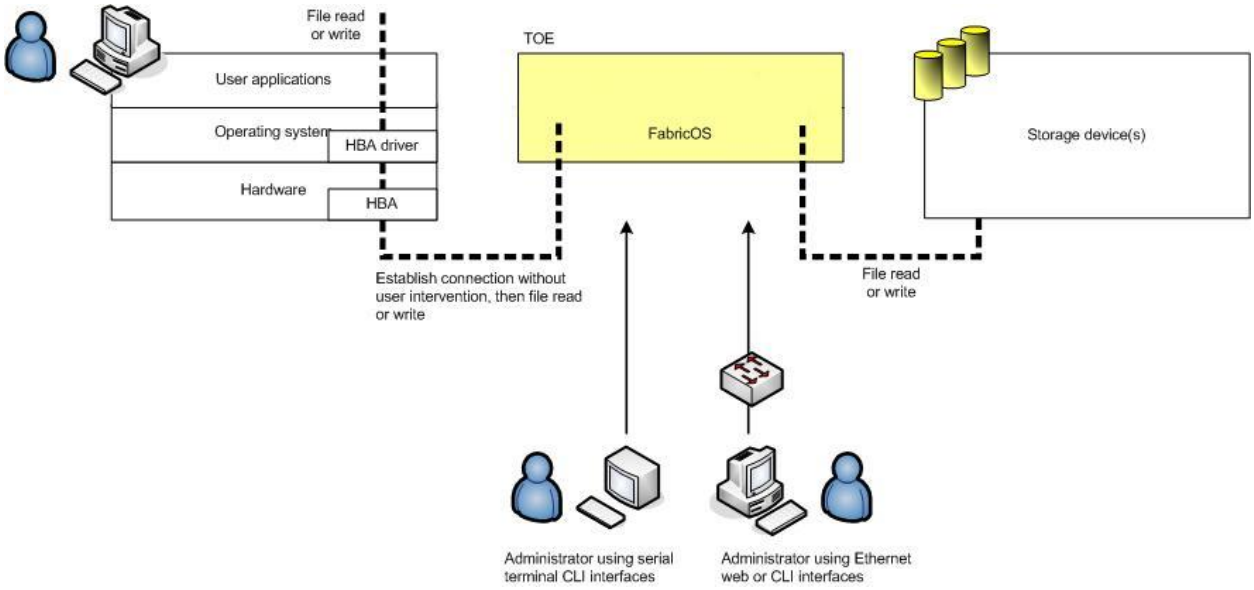

Figure 1: TOE and environment components.

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

- Host – A system in the environment that uses TOE 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.
- RADIUS/LDAP Server – An optional component that can perform authentication based on user credentials passed to it by the TOE. The TOE then enforces the authentication result returned by the RADIUS or LDAP Server.
- Certificate Authority (CA) – Provides digital certificates for SSH and 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 DEKs created by the encryption engine. Key management systems are provided by third party vendors.

3.1.1 Physical Boundaries

The TOE relies on a syslog server in the environment to store and protect audit records that are generated by the TOE. The TOE can be configured to use a RADIUS or LDAP Server also in the environment for authentication. The TOE does not rely on any other components in the environment to provide security-related services. The TOE is interoperable with any adapter or device that is interoperable with one or more of the following standards:

- FC-AL-2 INCITS 332: 1999
- FC-GS-5 ANSI INCITS 427:2006 (includes the following.)
    - FC-GS-4 ANSI INCITS 387: 2004
- FC-IFR revision 1
- FC-SW-4 INCITS 418:2006 (includes the following)
    - FC-SW-3 INCITS 384: 2004
- FC-VI INCITS 357: 2002
- FC-TAPE INCITS TR-24: 1999
- FC-DA INCITS TR-36: 2004 (includes the following)
    - FC-FLA INCITS TR-20: 1998
    - FC-PLDA INCIT S TR-19: 1998
- FC-MI-2 ANSI/INCITS TR-39-2005
- FC-PI INCITS 352: 2002
- FC-PI-2 INCITS 404: 2005

- FC-FS-2 ANSI/INCITS 424:2006 (includes the following)
    - FC-FS INCITS 373: 2003
- FC-LS revision 1.51 (under development)
- FC-BB-3 INCITS 414: 2006 (includes the following)
    - FC-BB-2 INCITS 372: 2003
- FC-SB-3 INCITS 374: 2003 (replaces FC-SB ANSI X3.271: 1996; FC-SB-2 INCITS 374: 2001)
- RFC 2625 IP and ARP Over FC
- RFC 2837 Fabric Element MIB
- MIB-FA INCITS TR-32: 2003
- FCP-2 INCITS 350: 2003 (replaces FCP ANSI X3.269: 1996)
- SNIA Storage Management Initiative Specification (SMI-S) Version 1.2 (includes the following)
    - SNIA Storage Management Initiative Specification (SMI-S) Version 1.02 (ANSI INCITS 388: 2004)
    - SNIA Storage Management Initiative Specification (SMI-S) Version 1.1.0

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. User data protection
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE Access
7. Trusted path

4.1.1 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 MSG contents into an encapsulating syslog record.

4.1.2 User data protection

Host bus adapters can only access storage devices that are members of the same zone. The TOE enforces an access control policy called the SAN Fabric SFP to accomplish this. The SAN Fabric SFP is implemented using hardware-enforced zoning (also called "hard zoning" or simply "zoning") that prevents a host bus adapter from accessing a device the host bus adapter is not authorized to access. A zone is a region within the fabric[1] where a specified group of fabric-connected devices (called zone members) have access to one another. Zone members do not have access to any devices outside the zone and devices outside the zone do not have access to devices inside the zone.

Some models of the TOE support encryption of user data for specified storage devices. A storage device configured to host encrypted data receives only encrypted data from the TOE and the TOE decrypts data received from the storage device. The encryption of the data exchanged between the TOE and an encrypted storage device is called "user data encryption". A CryptoTarget container is a configuration of "virtual devices" that is created for each storage device hosted on the TOE. A LUN is simply a number assigned to an addressable logical unit within a storage device. A CryptoTarget container identifies individual LUNs within a storage device as either encrypted or cleartext.

4.1.3 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. Either the TOE performs the validation of the login credentials or the information is passed to a RADIUS or LDAP, in the environment, Server to perform the validation and the TOE enforces the decision. The administrator can configure the order in which the external authentication provider and the local credentials are checked.

4.1.4 Security management

The TOE provides both serial terminal- and Ethernet network-based 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, host bus adapters do not have access to storage devices.

4.1.5 Protection of the TSF

Protection of the TSF is provided primarily by virtue of the fact that the TOE is a hardware appliance that is physically protected in the environment. On most models, the TOE does not encrypt data written to or read from storage devices by host bus adapters. Encryption

[1] When more than one instance of the TOE is interconnected (i.e. installed and configured to work together), they are referred to collectively as a "SAN fabric" or simply a "fabric."

of this data is called "user data encryption" and is available only on a subset of the models of the TOE being evaluated. The TOE relies instead on the environment to physically protect the network between the HBA and the TOE, and between the TOE and the storage device. 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 or HTTPS. Further, TOE requires administrators to login after a SSH or HTTPS connection has been established. The TOE provides a reliable time stamp for audit records.

4.1.6 TOE Access

The TOE provides an IP Filter policy that is a set of rules applied to the IP management interfaces. These rules provide the ability to control how and to whom the TOE exposes the management services hosted on a switch. They cannot affect the management traffic that is initiated from a switch.[2]

The TOE limits the number of concurrent login sessions for users, such that the number of simultaneous login sessions for each role is limited.

4.1.7 Trusted Path

The TOE enforces a trusted path between the TOE administrators and the TOE using SSH and 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 HTTPS for the Advanced Web Tools GUI interface.

5 Assumptions

The following assumptions were made during the evaluation of Brocade Directors and Switches:

- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The environment will protect network communication to and from the TOE from unauthorized disclosure or modification.
- The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

[2] While the mechanism is built from a general purpose firewall capability of the underlying FabricOS, limitations on functionality provided to the end user limit its use to providing restrictions on administrative connectivity.

6 Documentation

The following documentation was used as evidence for the evaluation of the Brocade Directors and Switches:

6.1 Design Documentation

1. Brocade Directors and Switches Security Architecture Document, Revision 0.3, August 5, 2011
2. Brocade Directors and Switches Functional Specification, Revision 0.3, August 5, 2011
3. Brocade Directors and Switches TOE Design Specification, Revision 0.3, August 5, 2011

6.2 Guidance Documentation

1. Brocade Fabric OS v7.0.0b1 Release Notes v1.0
2. Brocade Fabric OS Administrator's Guide, 53-1002148-02, 3 June 2011
3. Brocade Fabric OS Command Reference Manual, 53-1002147-01, 29 April 2011
4. Brocade Fabric OS Message Reference, 53-1002149-01, 29 April 2011
5. Brocade Fabric OS Encryption Administrator's Guide, 53-1001341-02, 7 August 2009
6. Brocade Web Tools Administrator's Guide, 53-1002152-01, 29 April 2011
7. Brocade Access Gateway Administrator's Guide, 53-1002156-01, 29 April 2011
8. Brocade Converged Enhanced Ethernet Administrator's Guide, 53-1002163-01, 29 April 2011
9. Brocade Converged Enhanced Ethernet Command Reference, 53-1002164-01, 29 April 2011
10. Brocade Fabric OS FCIP Administrator's Guide, 53-1002155-01, 29 April 2011
11. Brocade Fabric OS Documentation Updates, 53-1002165-04, 01 September 2011

6.3 Life Cycle

1. Life Cycle Support Evidence Questionnaire, July 12, 2010
2. Brocade Configuration Management Plan, July 9, 2010
3. Brocade Directors and Switches Delivery Procedures, July 9, 2010
4. Software Development at Brocade Using ClearCase, 2007
5. Data Center Management, 09/22/2010
6. Brocade Software Engineering Environment, September 22, 2010
7. Life Cycle Overview, 09-07-2010
8. Security Manual –Section 1 4 07.doc
9. Security Policy.doc
10. Systems Security Processes_071107.doc
11. User Account Managemen_2.doc

6.4 Testing

1. Brocade Common Criteria Test Plan, Revision 3.6, October 3, 2011
2. Brocade Common Criteria Test Specification, Version 7.5, September 28, 2011
3. Brocade V7.0.0b Common Criteria Integration Test Hardware Configuration, Version 1.3, September 15, 2011
4. Test_Coverage.xlsx
5. Post Matador Initiative SQA C+H- Security.docx
6. LSWAT Result.msg
7. Brocade Encryption CAT – Test Spec 0.1, September 30, 2011
8. Brocade Encryption LSWAT – Test Spec 0.1, July 22, 2011
9. Brocade Encryption Manual Testing – Test Spec 0.1, August 18, 2011
10. User Defined RBAC Test Specification (v0.2), October 4, 2011
11. LSWAT Security II and III Test Specification, September 15, 2011
12. Brocade Gemini SWAT Test Specification (v0.2), October 20, 2008
13. Quantum Security SWAT Test Specification (v0.9), October 2, 2011

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 Directors and Switches, Version 2.0, December 7, 2011.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. Security audit
2. User data protection
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE Access
7. Trusted Path

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Common Criteria Guide, ran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing audit generation, cryptographic support, proper authentication data handling, and concurrent session limits, not tested by Brocade.

For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, are the following Brocade Directors and Switches running FabricOS version 7.0.0b1:

- Director Blade Models: FC10-6, FC8-16, FC8-32, FC8-48, FC8-64, FC16-32, FC16-48, CP8, CR8, CR4S-8, CR16-4, CR16-8, FCOE10-24, FS8-18, FX8-24
- Director Models: DCX, DCX-4S, DCX 8510-4, DCX 8510-8
- Switch Appliance Models: 300, 5100, 5300, 6510, 7800, 8000, BES
- Embedded Blades: 5410, 5424, 5450, 5460, 5470, 5480

To use the product in the evaluated configuration, the product must be configured as specified in the Brocade Fabric OS v7.0.0b1 Release Notes v1.0 document.

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 EAL4 augmented with ALC_FLR.2 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 2 and CEM version 3.1 rev 2. The evaluation determined the Brocade Directors and Switches TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 Directors and Switches product 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 4 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 and a detailed design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

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 4 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. Both of these 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 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in 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.

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

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

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 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

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 performance of the entire vendor tests suite, the independent tests, and the penetration test 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 validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

The evaluation team observed that the vendor's security tests were taken directly from their testing suite, which is predominantly automated tests but does contain some manual tests. These tests, used routinely as a part of product development, were able to be integrated to

satisfy Common Criteria requirements and were supplemented as needed to provide for extensive test coverage. Therefore, both the evaluation and validation teams were pleased with the test coverage provided by Brocade, since the tests were more detailed than standard Common Criteria testing in the cryptographic area.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Brocade Directors and Switches Security Target, Version 2.91, August 30, 2012*.

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 Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Brocade Directors and Switches Part 2 (Proprietary)*, Version 3.0, March 16, 2012.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Brocade Directors and Switches, ETR Part 2 Supplement (SAIC and Brocade Proprietary)*, Version 4.0, March 16, 2012.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Brocade Directors and Switches Security Target, Version 2.91, August 30, 2012.