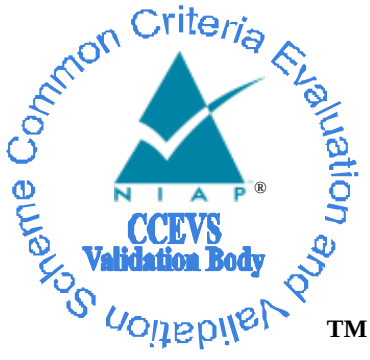
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Brocade Directors and Switches Validation Report

Report Number: CCEVS-VR-VID10233-2009
Dated: 31 March 2009
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander, Senior Validator
The Aerospace Corporation

Jean Hung, Validator
Meg Weinberg, Lead Validator
The Mitre Corporation

Common Criteria Testing Laboratory

Jean Petty, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Validation Report

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 with Fabric OS version 6.1.1. 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 February 2009. 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 3 augmented with ALC_FLR.2.

The Target of Evaluation (TOE) is the Brocade Directors and Switches provided by Brocade Communications Systems, Inc. Brocade Directors and Switches are hardware appliances that implement what is called a "Storage Area Network" or "SAN". SANs provide physical connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment.

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 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 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.

The Brocade Directors and Switches hardware appliances can operate in one of two modes: a fabric switch mode or an "Access Gateway" mode. The evaluated configuration supports only interconnected TOE instances operated in a fabric switch mode.

All TOE models may be operated in the default fabric switch mode. Only selected models including the Brocade 200E, 300, and embedded blades 4012, 4016, 4020 and 4024 platforms may also be operated in Access Gateway mode. In Access Gateway mode the appliance acts as a transparent "port expander" between the fabric edge and multiple FC devices (typically host HBA), multiplexing HBA ports over multiple N_Ports which are in turn connected to multiple FC ports on the fabric edge. Access Gateway mode allows the attached HBA to send and receive FC traffic through the appliance, but the appliance does not enforce the TOE access control policy. User guidance specifically warns the user that Access Gateway mode is not allowed in the CC evaluated configuration.

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.

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."

  The Brocade Advanced Web Tools login interface distinguishes between the correct entry of a userID and password. This feedback would allow an attacker to systematically guess userIDs until a correct userID is found and then switch to guessing passwords. The vendor plans to remove this feedback in the next release. If this is a concern for the target environment, then only the Command Line Interface should be used.

- 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, however these interfaces are disabled during initial installation and configuration 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 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, Revision 2) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 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 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 3 (EAL 3) 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 including: • Director Blade[1] Models: FC2-16, FC4-16, FC4-32, FC4-48, FC4-16, FC4-32, FC4-48, FR4-18i, FC8-16, FC8-32, FC8-48, CP4, CP8, CR8 • Director Models: 48000, DCX • Switch Appliance Models: 200E, 300, 4100, 4900, 5000, 5100, 5300, 7500 and 7500E • Embedded Blades[2]: 4012, 4016, 4018, 4020, and 4024 • All models running FabricOS version 6.1.1
Protection Profile	Not applicable
Security Target	Brocade Directors and Switches Security Target version 1.6, March 18, 2009
Evaluation Technical Report	Brocade Directors and Switches Final Non-Proprietary ETR – Part I, version 1.0 Brocade Directors and Switches Final Proprietary ETR – Part II, version 1.0
CC Version	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, September 2006 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007 Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	Brocade Communications Systems, Inc.

[1] A blade refers to a purpose-built component that is installed in a Brocade director.
[2] An embedded blade is a Brocade switch in a blade form factor that may be installed in a blade server product.

Item	Identifier
Developer	Brocade Communications Systems, Inc.
Common Criteria Test Lab	SAIC, Columbia, MD
CCEVS Validators	Jandria Alexander, Jean Hung, Meg Weinberg

3. Architectural Information

The TOE architecture can be described in terms of the following subsystems:

- Runtime Subsystem, which includes the following :
  - blade or switch hardware
- Fabric Subsystem, which includes the following:
  - user-mode software (FOS services and server applications, excluding the Management Subsystem)
  - kernel-mode software (FOS kernel)
- Management Subsystem, which includes the following:
  - user-mode software (FOS WebTools and command line interfaces)

Individual subsystems are described below.

Runtime Subsystem

The Runtime Subsystem provides a runtime environment for Brocade software and is comprised of a range of hardware platforms including both directors and switches. Director platforms are characterized by a bladed architecture in which a chassis may be configured to include a range of different blades. Switches are self-contained, purpose-built systems. The specific hardware appliances included in the TOE are identified in Security Target.

Brocade director and switch appliances are designed and developed with Brocade proprietary ASIC components, general commercially available components, and Brocade FOS software modules. The hardware is assembled by a Contract Manufacturer and the FOS modules are loaded onto blades and switches by OEM/channel hubs. Director appliances accept a family of blades that support a range of functions and network throughput capability. The Fibre Channel capabilities of each switch appliance model functionality is identical, differing only in network throughput capability. The Brocade blades and switches include the following externally-visible hardware interfaces:

- Fibre Channel port(s)
- Ethernet port(s)
- serial port

More than one host bus adapter can share one or more storage devices that are attached to the TOE according to TOE configuration. More than one instance of TOE directors and switches can be interconnected in the evaluated configuration to support different numbers of host bus adapters and storage devices, to provide scalability. 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 IT environment. Directors provide a configurable number of physical interfaces using an appliance architecture that supports the use of blades that can be installed in and removed from the director appliance chassis according to administrator configuration.

The runtime subsystem accepts input from its externally-visible hardware interfaces and provides that input to the Fabric Subsystem and Management Subsystem for interpretation as network protocols and operations upon devices. The Runtime subsystem performs no security checking on the data that is read or written to these hardware interfaces. All security checks are performed upon the data interpreted as protocols by the Fabric subsystem and the Management subsystem. Data obtained from the serial port is provided to the management subsystem to be interpreted as a terminal session.

The runtime subsystem also includes a hardware clock that can be read by other subsystems to obtain accurate time information. This hardware clock is not externally visible.

Fabric Subsystem

The Fabric Subsystem interprets inputs from the Runtime Subsystem into block read/write operations. The Fabric Subsystem mediates block read and write operations by hosts (subjects) to storage devices (objects) using supported FC protocols.
The Fabric Subsystem consists of the Linux operating system and additional components that together are called Fabric OS (FOS). The FOS implementation is separated into kernel space and user space. While these separate spaces create distinct environments for execution, they are both completely internal to the Fabric Subsystem. The separation provided between kernel space and user space provides internal system structure, not a separation between trusted and untrusted domains. Because both kernel and user space are entirely within the Fabric subsystem, both are parts of the TOE security architecture. For example, for an application to check the state of the switch, or of a port, in order to talk to the kernel, a FOS internal application needs to get a file descriptor by opening a Fabric OS kernel driver, and perform Fabric OS system calls on the file descriptor. The boundary of kernel and user space is transparent to FOS internal applications. Both the Fabric OS and the Fabric OS internal application are trusted parts of the TOE.
Fabric Subsystem FOS kernel consists of modules that include two called Switch and FC drivers. These modules are implemented as character device drivers and provide the interfaces between the FOS kernel and FOS internal applications.
FOS kernel modules and drivers are run under an upper level application context if they are part of system calls, whereas, if they are part of interrupt handlers, they are run in the interrupt thread (top-half or bottom-half, in Linux terminology) or the scheduler thread (Linux kernel task) without a user context.
FOS is an embedded environment that uses Linux as an underlying platform to host fixed, special-purpose applications. While the term "application" is used in the context of an application running on the Linux kernel, these "applications" are embedded FOS components. The underlying Linux platform is not exposed to allow hosting of general-purpose user applications.
FOS applications include all Fibre Channel Fabric services, management agents and servers, as well as Brocade value-added features. FOS applications include:

- ***Fabric***: Switch interconnection using FC-SW.
- ***Fabric watch:*** Performance and threshold monitoring
- ***FCP probing:*** Auto device registration.
- ***FSPF:*** FC standard – Fabric Shortest Path First routing
- ***Manager server:*** Provide management information to management clients
- ***Name Server:*** Fibre Channel directory services - provides a means to discover information about Nodes and Ports attached to a fabric.
- ***Zoning:*** Access control and boundary protection - allows the administrator to partition the Storage Area Network into logical groups of devices that can access each other.
- ***System diagnostics:*** A set of HW diagnostics and board sanity test.
- ***Security:*** Provide security features included in the base Fabric OS platform.
- **Authentication:** Provide password and SNMP community string distribution in a secure fabric environment
- ***RASlog:*** Centralized logging mechanism for software running on Brocade products. RASLOG covers error reporting, handling, and presentation of data into a format consumable by management tools and the user.

Fabric Subsystem FOS internal applications are run as individual processes, with each having its own context and communicating with one another through the IPC (inter-process communication) server. They also interoperate with the FOS kernel using library functions and system calls.
The following are the libraries provided for FOS internal applications:

- Configuration library: this library contains the functions to retrieve and update a switch's optional parameters. The configuration parameters are stored in a text file.
- FOS kernel library: this library contains the functions to control and manage a switch, as well as to transmit and receive sequences over Fibre Channel interfaces.

These library functions are typically implemented using ioctl, read or write system calls. These libraries are accessible to FOS internal applications and thus are strictly internal to the Fabric Subsystem.

Management Subsystem

The Management Subsystem interprets inputs from the Runtime Subsystem into network protocols. The Management Subsystem provides both web- and CLI-based interfaces that can be used to manage TOE functions in general. The web-based interfaces are accessed using a web browser in the IT Environment. The CLI-based interfaces are accessed using either a SSH terminal client in the IT Environment, or using a terminal that is connected directly to the TOE appliance by a serial port.

The Management Subsystem is comprised of individual processes, each having its own context and communicating with other FOS internal applications through IPC services. It also interoperates with the FOS kernel using library functions and system calls.

The administrative interfaces to manage TOE services can be accessed using an Ethernet network (i.e., HTTPS protocol, SSH protocol), or can be accessed using a terminal directly-attached through a serial port (i.e., a command-line interface, CLI).

HTTPS Protocol Interface

Ethernet network-based web-based administrator console interfaces provide web-based administrator console interfaces. This interface is called the "Brocade Advanced Web Tools".

SSH Protocol Interface

Ethernet network-based command-line administrator console interfaces provide a command-line administrator console. This interface is called the "Fabric OS Command Line Interface".

Terminal sessions

Data from a serial port is provided by the runtime subsystem to the management subsystem. This data is interpreted as a terminal session. Terminal-based command-line administrator console interfaces provide a command-line administrator console. This interface is called the "Fabric OS Command Line Interface".

Other Interfaces

There also exists administrative Ethernet network-based programmatic API interfaces, however these interfaces are disabled during initial installation and configuration 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 was tested on a subset of the platforms by the Evaluation Team. Evaluators performed testing on the following TOE models:

- Director Blade Models: FR4-18i, CP8, CR8, FC8-16, FC8-32, FC8-48
- Director Model: DCX
- Switch Appliance Models: 200E, 300, 4100, 7500

An equivalency argument was provided by the vendor demonstrating that these models represent one model from each "class" of TOE models, which vary by the number of ports and capacity included on the appliance. The equivalency argument was acceptable to the evaluation and validation teams.

4. Security Policy

Brocade Directors and Switches provide the following security functions:

- Security audit
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path

There is no distinction between the product and the TOE.

5. Assumptions

The following are assumptions made for the Environment of the TOE:

- 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.

The Brocade Directors and Switches must be configured in the "FIPS Mode" configuration as defined in the Brocade FabricOS Administrator's Guide. FIPS Mode ensures that HTTPS and SSH are the only means of accessing the TOE via Ethernet. The following capabilities of Brocade Directors and Switches are optional or are separately licensed (and purchased) features that are not included in the evaluated configuration:

- Ethernet network-based programmatic API interfaces (disabled during installation)
- Modem hardware component that is optional to the product that can be used in a similar manner as a serial console port (not installed)
- Separately licensed feature not included in the evaluated configuration (see pages 16 – 17 Brocade FabricOS Administrator's Guide)
- Interoperability features, e.g., FICON, remote switch, iSCSI not tested as part of the evaluated configuration, since these require hardware and software from other vendors and are provided by Brocade only to ensure interoperability with other vendor products.

6. Documentation

Brocade Directors and Switches guidance documents that were evaluated and should be considered as evaluator verified include the following:

- Fabric OS Administrator's Guide, Supporting Fabric OS v6.1.1, Publication Number: 53-1000598-04, Publication Date: 18 July 2008
- Fabric OS Command Reference Manual, Supporting Fabric OS 6.1.1, Publication Number: 53-1000599-03, Publication Date: 18 July 2008
- WebTools Administrator Guide Supporting Fabric OS Version 6.1.1, 53-1001080-01, July 18 2008
- Brocade Fabric OS v6.1.1 Release Notes v4.0, February 17, 2009

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

CC Assurance	CI Unique Identifier and description
Authorization Controls (ALC_CMC)	Brocade Systems Security Process, Revision 1.2
Implementation representation CM Coverage (ALC_CMS)	Brocade Configuration Management Plan, Version 2.0, July 13, 2007
Delivery and Operation (ALC_DEL)	Brocade Directors and Switches Delivery Procedures, Version 1.0, May 29, 2007
Flaw reporting procedures (ALC_FLR.2)	Brocade Configuration Management Plan, Version 2.0, July 13, 2007

CC Assurance	CI Unique Identifier and description
Functional Specification (ADV_FSP)	Brocade TOE Design Document, Version 1.7, February 9, 2009
Operational User Guidance (AGD_OPE)	Fabric OS Administrator's Guide, Supporting Fabric OS v6.1.1, Publication Number: 53-1000598-04, Publication Date: 18 July 2008
	Fabric OS Command Reference Manual, Supporting Fabric OS 6.1.1, Publication Number: 53-1000599-03, Publication Date: 18 July 2008
	WebTools Administrator Guide Supporting Fabric OS Version 6.1.1, 53-1001080-01, July 18 2008
Preparative Procedures (AGD_PRE)	Fabric OS Administrator's Guide, Supporting Fabric OS v6.1.1, Publication Number: 53-1000598-04, Publication Date: 18 July 2008
	Brocade Fabric OS v6.1.1 Release Notes v4.0, February 17, 2009
Architectural Design (ADV_TDS)	Brocade TOE Design Document, Version 1.7, February 9, 2009
Developer Life-Cycle Model (ALC_LCD)	Brocade Communications Systems Life Cycle document, July 20, 2007
Security Architecture Description (ARC)	Brocade TOE Design Document, Version 1.7, February 9, 2009
Identification of Security Measures (ALC_DVS)	Brocade Security Manual, April 16, 2007
Security Target (ST)	Brocade Directors and Switches Security Target, Version 1.6, March 18, 2009
Test Documentation (ATE)	Brocade Common Criteria Test Specification, Version 7.2, Release Date: 4 December 2008 Brocade V6.1.1 Common Criteria Integration Test Hardware Configuration, Version 1.2, Date: 12/4/2008 Brocade Common Criteria Test Plan, Version 2.0, September 12, 2008 Test Script, Error, and Results files in fvt_611.zip

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 Plan.

The developer provided a suite of automated tests that tested all TOE functionality. The evaluation team executed all developer tests on the following TOE hardware platforms:

- Director Blade Models: FR4-18i, CP8, CR8, FC8-16, FC8-32, FC8-48
- Director Model: DCX
- Switch Appliance Models: 200E, 300, 4100, 7500

In addition, the evaluation team ran team and vulnerability tests to address the following:

- Placing the TOE in the evaluated configuration is dependent on use of the Evaluated Configuration information in the release notes. This information was to ensure that it is sufficient

to place the system in the evaluated configuration and that the specifications are complete and correct.

- The TOE must be configured in FIPS mode in order to ensure that HTTPS and SSH are the only means of accessing the TOE via Ethernet. The evaluation tested that the instructions in the Admin Guide are sufficient to put the TOE in FIPS mode for all of the models tested and
- Once the TOE is in FIPS mode, no access via Ethernet is allowed other than through HTTPS and SSH. A test was run to see if telnet or HTTP access is possible via the Ethernet connections.
- Fibre Channel frame integrity was and the reaction of the TOE to malformed Frames was tested for vulnerabilities (such as denial of service). The TOE identified and dropped malformed Frames and it did not crash during this testing, indicating that it handles this type of attack.
- Authorization vulnerabilities between HBAs and the TOE and storage devices and the TOE may be present that allow man-in-the-middle, session hijacking, and spoofing attacks. These were tried to ensure that there are no authorization vulnerabilities. No vulnerabilities were identified.
- Strength of Zoning was tested to ensure that "Zone Hopping" is not allowed based on knowledge of the user behind the HBA to access an unauthorized zone. Zone hopping was not allowed.
- Performed a port scan to ensure that all open ports are known and managed
- Attempt access to the OS; OS access is allowed through the root account and the vendor recommends that the customer disable this account after install.
- Attempted to use commands to produce an unsecure state and check for auditing; audit records were generated.
- Vulnerability was identified in Account Harvesting attack:
    - The WebTools interface allows attackers to gather user accounts. This is because it returns different error message for invalid username and correct (or incorrect) password, and valid username and incorrect password.
    - If the username is valid but the password is incorrect, the web tool returns "Error: Invalid Password".
    - If the username is invalid and password is incorrect or correct, the web tool returns "Error: Invalid User".
    - Attackers can write a script that goes through a list of usernames. If the error message is "Error: Invalid Password", then the username is a valid username. Note that the password still needs to be guessed or brute forced.
    - This vulnerability does not violate any ST claim; the vendor was advised that this should be fixed in the next release.

No issues were identified and only the account harvesting vulnerability was identified.

8. Evaluated Configuration

The TOE evaluated configuration consists of the TOE appliance running in Brocade defined "FIPS mode." Note that this does not mean that the TOE is FIPS 140-2 certified; it is not. FIPS mode is the name of a mode where access to the switch is limited to secure access methods. The Brocade Directors and Switches must be configured in the "FIPS Mode" configuration as defined in the Brocade FabricOS Administrator's Guide. FIPS Mode ensures that HTTPS and SSH are the only means of accessing the TOE via Ethernet. The following capabilities of Brocade Directors and Switches are optional or are separately licensed (and purchased) features that are not included in the evaluated configuration:

- Ethernet network-based programmatic API interfaces (disabled during installation)
- Modem hardware component that is optional to the product that can be used in a similar manner as a serial console port (not installed)

- Separately licensed feature not included in the evaluated configuration (see pages 16 – 17 Brocade FabricOS Administrator's Guide)
- Interoperability features, e.g., FICON, remote switch, iSCSI not tested as part of the evaluated configuration, since these require hardware and software from other vendors and are provided by Brocade only to ensure interoperability with other vendor products.

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, Volume II. 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 [1], [2], [3] and CEM version 3.1 [4]. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level 3 (EAL3) requirements augmented with ALC_FLR.2. The rationale supporting each CEM work unit verdict is recorded in volume II of this ETR, which is considered proprietary.

Evaluation of the Security Target (ST) (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 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 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 one document that included a functional specification, a high-level design document, architecture description, and correspondence demonstration.

Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 3 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to install and use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to perform configuration management, 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.

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

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE security functional requirements are enforced by the TOE. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

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 on a representative number of models of the TOE, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST. Evaluators performed testing on the following TOE models:

Director Blade Models: FR4-18i, CP8, CR8, FC8-16, FC8-32, FC8-48

Director Model: DCX

Switch Appliance Models: 200E, 300, 4100, 7500

These models represent one model from each "class" of TOE models, which vary by the number of ports and capacity included on the appliance.

The assurance requirements for the TOE evaluation are those required by EAL3 augmented with ALC_FLR.2.

The CEM work units associated with EAL3 augmented with ALC_FLR.2 are distributed amongst the ETR sections in volume II of this ETR. Collectively, the ETR sections in volume II encompass all CEM work units for EAL3 augmented with ALC_FLR.2. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

- Verdict
- Verdict Rationale
- Analysis Approach

The rationale justifies the verdict using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The Analysis Approach contains a description of the action performed or the method used to apply the work unit.

The evaluators applied the measures described in Chapter 2 of the CEM regarding evaluation conduct and the content of the ETRs.

10. Validator Comments / Recommendations

The *Brocade Advanced Web Tools* login interface distinguishes between the correct entry of a userID and password. This feedback would allow an attacker to systematically guess userIDs until a correct userID is found and then switch to guessing passwords.

The OS "root" account is required for installation of the *Brocade and Switches appliance*, and the "root" account allows direct command line access to the *Fabric OS*. The **Brocade Fabric OS v6.1.1 Release Notes v4.0** strongly cautions the system administrator to disable the "root" account after installation and configuration of the appliance to ensure that access to the OS is not allowed.

11. Annexes

Not applicable

12. Security Target

The security target is the Brocade Directors and Switches Security Target, version 1.6, March 18, 2009.

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, September 2006.

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007.

[5] Final Evaluation Technical Report for Brocade Directors and Switches, version 1.0, February 27, 2009, Final Proprietary ETR – Part II.

[6] Brocade Directors and Switches Security Target, Version 1.6, March 18 2009.

[7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories. Version 1.0, March 20, 2001.

[8] SAIC CCTL Evaluation Procedures Annex, Version .20, January 31 2004.