National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Brocade Communications Systems, Inc.

130 Holger Way

San Jose, CA 95134

Brocade VDX Product Series operating with NOS version 5.0.1b1

Report Number:	**CCEVS-VR-10577-2015**
Dated:	**May 8, 2015**
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

Paul Bicknell
Jay Vora
Jean Petty
Brad O'Neill
The MITRE Corporation
Mclean, VA

Common Criteria Testing Laboratory

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

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Brocade VDX Product Series 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 May 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) is the Brocade VDX Product Series operating with NOS version 5.0.1b1 provided by Brocade Communications Systems, Inc. The Brocade VDX Product Series are hardware network devices 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 Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

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

The technical information included in this report was obtained from the Brocade Communications Systems, Inc. VDX Product Series (NDPP11e3) 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 VDX Product Series operating with NOS version 5.0.1b1 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) (including the optional SSH and TLS requirements) with Errata #3
ST:	Brocade Communications Systems, Inc. VDX Product Series (NDPP11e3) Security Target, Version 0.7, May 11, 2015
Evaluation Technical Report	Evaluation Technical Report for Brocade VDX Product Series operating with NOS version 5.0.1b1, Version 0.1, April 23, 2015.
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.

Item	**Identifier**
CCEVS Validators	

3 Architectural Information

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

The Target of Evaluation (TOE) is the Brocade VDX Product Series. The VDX Product Series are hardware appliance with embedded software installed on a management processor. Optionally, a number of co-located appliances can be connected in order to work as a unit with a common security policy. The embedded software is a version of Brocades' proprietary Multiservice Network Operating System (NOS). The NOS controls the switching and routing of network frames and packets among the connections available on the hardware appliances. These switch/routers include virtual cluster switch (VCS), which allows users to create flatter, virtualized and converged data center networks. These VCS fabrics are scalable, permitting users to expand at their own pace, and simplified, allowing users to manage the fabric as a single entity. VCS-based Ethernet fabrics are convergence-capable, with technologies such as Fibre Channel over Ethernet (FCoE) for storage.

All TOE appliances are configured at the factory with default parameters and an admin and user account with default passwords. Users must login to access the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. The TOE uses SCP to download/compare software images. All of the remote management interfaces are protected using encryption as explained later in this ST.

The VDX 6710 switch is a fixed port switch with 48 1-Gigabit Ethernet copper interfaces and six 10 Gigabit Ethernet SFP+ interfaces. The VDX 6720 switches are also fixed port switches with either 24 10-Gigabit LAN ports or 60 10-Gigabit LAN ports, depending on the model. The VDX 6730 switch is a 10-Gigabit Ethernet fixed port switch with LAN and native Fibre Channel ports. Depending on the model, it either provides 24 10-Gigabit Ethernet LAN ports and eight 8-Gbps native Fibre Channel ports, or 60 10-Gigabit Ethernet LAN ports and 16 8-Gbps native Fibre Channel ports. The 6710, 6720 and 6730 hardware platforms that support the TOE have a number of common hardware characteristics:

- A system motherboard that features a Reduced Instruction Set Computer (RISC) CPU running at 1.3 GHz with integrated peripherals
- Extensive diagnostics and system-monitoring capabilities for enhanced high Reliability, Availability, and Serviceability (RAS)
- A USB port for firmware upgrades and system log downloads

- Support for long-range and short-range SFP+ 10-Gigabit Ethernet transceivers

The VDX 8770-4 switch provides up to 192 10-Gigabit Ethernet or 1 Gigabit Ethernet external ports or 48 40-Gigabit Ethernet external ports, while the VDX 8770-8 switch provides up to 384 10-Gigabit Ethernet or 1 Gigabit external ports or 96 40-Gigabit Ethernet external ports. The 8770 hardware platforms that support the TOE have a number of common hardware characteristics:

- Dual, redundant management modules
- Serial (console), Ethernet, and USB connections for management modules (though only Brocade-branded USB devices are supported)
- Support for short-range and long-range 1 Gbps SFP transceivers
- Support for short-range and long range 10 Gbps SFP+ transceivers
- Support for 40 Gbps QSFP transceivers

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the Brocade Communications Systems, Inc. VDX Product Series operating with NOS version 5.0.1a, including the following series and models

- VDX 6710-54
- VDX 6720-24
- VDX 6720-60
- VDX 6730-32
- VDX 6730-76
- VDX 6740
- VDX 6740T
- VDX 6740T-1G
- VDX 8770-4, and
- VDX 8770-8.

3.2 TOE Architecture

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

Given that this Security Target conforms to the NDPP, the security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as controlling the flow of network packets among the attached networks. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

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

3.3 Physical Boundaries

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

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

The TOE can be configured to forward its audit records to 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 MSG 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

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

4.4 Identification and authentication

The TOE 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 Server to perform the validation and the TOE enforces the decision. The administrator can configure the order in which order the external authentication provider and the local credentials are checked

4.5 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Authorized Administrator role can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

4.6 Protection of the TSF

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

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

Note that the TOE is a single appliance or a closely grouped (e.g., in the same rack) collection of appliances acting as a unit. As such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

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

4.7 TOE access

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

4.8 Trusted path/channels

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

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. SSH v2 is used to support SCP which the TOE uses for secure download of TOE updates.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP). That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- Brocade – Network OS Common Criteria Configuration Guide, Supporting Network OS v5.0.1b1, Publication # 53-1003789-01, 08 April 2015.
- Brocade – Network OS Administrator's Guide, Supporting Network OS v5.0.1, Publication #53-1003455-01, 30 September 2014.
- Brocade – Network OS Common Criteria Configuration Guide, Supporting Network OS v5.0.1b1, Publication # 53-1003789-01, 08 April 2015.
- Brocade – Network OS Command Reference, supporting Network OS v5.0.1, Publication # 53-1003456-01, 30 September 2014.
- Brocade – Network OS Message Reference Manual, Supporting Network OS v5.0.1, Publication # 53-1003460-01, 30 September 2014.
- Brocade – Network OS Security Configuration Guide, Supporting Network OS v5.0.1, Publication # 53-1003463-01, 30 September 2014.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for VDX Product Series operating with NOS version 5.0.1b, Revision 0.4, May 11, 2015.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDPP including the optional SSH and TLS tests.

8 Evaluated Configuration

The evaluated configuration consists of the Brocade Communications Systems, Inc. VDX Product Series operating with NOS version 5.0.1a, including the following series and models

- VDX 6710-54
- VDX 6720-24
- VDX 6720-60
- VDX 6730-32
- VDX 6730-76
- VDX 6740
- VDX 6740T
- VDX 6740T-1G
- VDX 8770-4, and
- VDX 8770-8.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VDX Product Series operating with NOS version 5.0.1b1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP related to the examination of the information contained in the TSS.

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

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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

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

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

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

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

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

9.7 Summary of Evaluation Results

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

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

9.8 Clarifications of Scope

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

1. 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities of the product were not covered by this evaluation.

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.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). In order to remain CC compliant, the device(s) must first be configured into FIPS mode, then into Common Criteria mode as specified in the Brocade

FIPS Configuration Manual. Note that the product includes FIPS validated cryptographic algorithms.

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

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

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Brocade Communications Systems, Inc. VDX Product Series (NDPP11e3) Security Target, Version 0.7, May 11, 2015.*

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.

- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

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

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

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