

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Brocade Communications Systems, Inc. VDX Product Series

Report Number: CCEVS-VR-VID10579-2014
Dated: 11 July 2014
Version: 1.0

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

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

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
The Aerospace Corporation

Jean Petty
The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc. (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

1	Executive Summary	1
1.1	Evaluation Details	1
1.2	Interpretations	2
1.3	Threats.....	2
1.4	Organizational Security Policies.....	3
2	Identification	3
3	Security Policy	3
3.1	Security Audit	3
3.2	Cryptographic Support.....	3
3.3	User Data Protection	3
3.4	Identification & Authentication	3
3.5	Security Management	4
3.6	Protection of the TOE’s Security Functions	4
3.7	TOE Access	4
3.8	Trusted Path/Channels	4
4	Assumptions.....	4
4.1	Clarification of Scope	4
5	Architectural Information	5
6	Documentation.....	6
7	Product Testing	6
7.1	Developer Testing.....	6
7.2	Evaluation Team Independent Testing	7
7.3	Penetration Testing	8
8	Evaluated Configuration	8
9	Results of the Evaluation	9
10	Validator Comments/Recommendations	9
11	Annexes.....	10
12	Security Target.....	10
13	Bibliography	10

List of Tables

Table 1 – Evaluation Details.....	1
-----------------------------------	---

1 Executive Summary

The evaluation of the Brocade Communications Systems, Inc. VDX Product Series with Network OS 3.0.1a5 was performed by Leidos Inc. (formerly Science Applications International Corporation) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in July 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is conformant to *Protection Profile for Network Devices*, Version 1.1, 8 June 2012. The information in this Validation Report is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team. 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 VDX Product Series comprises the VDX 6710-54, VDX 6720-24, VDX 6720-60, VDX 6730-32, VDX 6730-76, VDX 8770-4 and VDX 8770-8 switch/router devices, each running Brocade's Network Operating System (NOS)—v3.0.1a5 in the evaluated configuration.

The VDX switch/routers, in the context of the evaluation, are network devices that provide a secure base (comprising auditing, cryptographic support for network communications and update integrity, user identification and authentication, and secure management) for operational functions related to switching and routing IP network traffic.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Brocade Communications Systems, Inc. VDX Product Series Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	VDX Product Series with NOS 3.0.1a5, including the following series Hardware Platforms: VDX 6710-54, VDX 6720-24, VDX 6720-60, VDX 6730-32, VDX 6730-76, VDX 8770-4 and VDX 8770-8.
Sponsor:	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134
Developer:	Brocade Communications Systems, Inc. 130 Holger Way San Jose, CA 95134
CCTL:	Leidos Inc. (formerly Science Applications International Corporation) 6841 Benjamin Franklin Drive Columbia, MD 21046

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

Kickoff Date:	6 June 2014
Completion Date:	11 July 2014
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	None
Description:	The TOE provides a secure base, comprising auditing, cryptographic support for network communications and update integrity, user identification and authentication, and secure management, for operational functions related to switching and routing IP network traffic.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Brocade Communications Systems, Inc. VDX Product Series by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	Protection Profile for Network Devices, Version 1.1, 8 June 2012
Evaluation Personnel:	Leidos Inc. Anthony J. Apted Dawn Campbell
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

1.4 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

2 Identification

The evaluated product is **Brocade Communications Systems, Inc. VDX Product Series with NOS 3.0.1a5**.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the Brocade Communications System, Inc. VDX Product Series Security Target and Final ETR.

3.1 Security Audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an authorized TOE User and also to send the logs to a designated log server using TLS to protect the logs on the network.

3.2 Cryptographic Support

The TOE includes a FIPS-certified cryptographic module that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols (SSH and TLS).

3.3 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.

3.4 Identification & Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules.

3.5 Security Management

The TOE provides a Command Line Interface (CLI) to access the security management functions used to configure and manage its security functionality. Security management commands are limited to authorized users and available only after they have provided acceptable user identification and authentication data to the TOE.

3.6 Protection of the TOE's Security Functions

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

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

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.

3.7 TOE Access

The TOE can be configured to display an informative 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.

3.8 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 external audit servers 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.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.1 Clarification 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:

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

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 *Protection Profile for Network Devices* 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. 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.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

The TOE consists of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocade’s 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 appliance.

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 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)

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

- 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.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Network OS Administrator's Guide—Supporting Network OS v3.0.1a5, 28 March 2013
- Network OS Command Reference—Supporting Network OS v3.0.1a5, 28 March 2013
- Network OS Message Reference—Supporting Network OS v3.0.1a5, 17 December 2012
- Brocade VDX 6710-54 Hardware Reference Manual, 10 August 2012
- Brocade VDX 6710-54 QuickStart Guide, 10 August 2012
- Brocade VDX 6720 Hardware Reference Manual, 16 May 2012
- Brocade VDX 6720 QuickStart Guide, 15 December 2011
- Brocade VDX 6730 Hardware Reference Manual, 16 May 2012
- Brocade VDX 6730 QuickStart Guide, 30 September 2011
- Brocade VDX 8770-4 Hardware Reference Manual, 21 September 2012
- Brocade VDX 8770-4 QuickStart Guide, 22 August 2012
- Brocade VDX 8770-8 Hardware Reference Manual, 21 September 2012
- Brocade VDX 8770-8 Hardware Reference Manual, 22 August 2012.

7 Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the following:

- Evaluation Team Test Report for Brocade Communications Systems, Inc. VDX 6730
- Evaluation Team Test Report for Brocade Communications Systems, Inc. VDX 8770.

7.1 Developer Testing

The assurance activities in the Protection Profile for Network Devices do not specify any requirement for developer testing of the TOE.

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

7.2 Evaluation Team Independent Testing

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Network Devices. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the Team Test Report for Brocade Communications Systems, Inc. VDX 6730 and Team Test Report for Brocade Communications Systems, Inc. VDX 8770. Tests were executed on the following sample of platforms claimed in the ST:

- VDX 6730-76—the other VDX 67xx platforms included in the TOE are functionally equivalent. They share a common underlying processor architecture and run the same firmware image. The only differences are related to the number and type of external network connectors.
- VDX 8770-8—the VDX 8770-4 device included in the TOE is functionally equivalent. The same firmware image is executed on both platforms and the only differences are in the number of ports.

Testing was conducted the week of May 20, 2013 at the vendor's facility in San Jose, CA. The developer assisted during the testing phase. The testing demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for Network Devices.

The testing performed by the evaluation team is summarized as follows:

- The evaluation team confirmed the TOE's ability to generate the audit events specified in the ST
- The evaluation team confirmed the TOE's ability to establish a trusted channel with an external audit server and transfer audit records to the audit server via the trusted channel
- The evaluation team confirmed the TOE supports RSA for public key authentication and password-based authentication over SSH
- The evaluation confirmed the TOE drops an SSH connection if it receives a packet over 256K bytes in length
- The evaluation team confirmed the TOE supports SSH connections using AES-CBC-128 and AES-CBC-256
- The evaluation team confirmed the TOE does not support DH Group 1 and that it does support DH Group 14
- The evaluation team confirmed the TOE supports each of the TLSv1.0 ciphersuites specified in the ST
- The evaluation team confirmed the TOE supports the specified password composition requirements, including the specified minimum length
- The evaluation team confirmed the TOE provides only obscured feedback when authentication information is entered at the local console
- The evaluation team confirmed, for all supported methods of administrator access, the TOE allows access to the CLI when the correct authentication credentials are provided, and denies access when incorrect credentials are provided, and that the services available without authentication are as specified in the ST
- The evaluation team confirmed the time could be set by the administrator and synchronized using an external NTP server. Note, the ST does not make any claims about using cryptographic protocols to protect the connection to the NTP server, so testing with the NTP server occurred only over TCP/IP

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

- The evaluation team confirmed a legitimate update could be installed successfully on the TOE and that an illegitimate update was rejected
- The evaluation team confirmed the TOE terminated a remote interactive session after the configured period of inactivity had elapsed. The evaluation team used values of 2, 5, and 8 minutes
- The evaluation team confirmed the user was able to terminate both an interactive local session at the TOE console and a remote interactive session over the SSH-provided trusted path
- The evaluation team confirmed the TOE terminated a local interactive session after the configured period of inactivity had elapsed. The evaluation team used values of 2, 5, and 8 minutes. Note that the TOE terminates a local interactive session after the inactivity time period has elapsed, rather than locking the session. This is consistent with the selection made in FTA_SSL_EXT.1.1 in the ST
- The evaluation team confirmed the TOE displayed a configured notice and consent warning message for each method of access supported by the TOE, i.e., local interactive console, remote interactive SSH using password authentication, and remote interactive SSH using public-key authentication
- The evaluation team confirmed the TOE was able to establish a trusted channel with an external syslog server using TLSv1.0. Testing additionally demonstrated the trusted channel was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE. A test was also performed to physically interrupt the connection between the TOE and the external syslog server and to verify that communications remained protected when connectivity was restored
- The evaluation team confirmed the only method of remote administration for the TOE is via SSH—the evaluation team did not identify any interface that could be used to establish a remote administrative session without invoking the trusted path. Testing additionally demonstrated the trusted path was established with the appropriate cryptographic protocol and algorithms to ensure channel data was not sent in plaintext and modification of channel data would be detected by the TOE.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerabilities applicable to the TOE in its evaluated configuration, but did identify a vulnerability related to another Brocade product (BigIron). The evaluation team outlined a test for determining if the TOE was susceptible, but analysis of the vulnerability (bypassing ACL rules by using 179 as the source port of a packet) determined it was not relevant as it represents a vulnerability in a TOE capability (packet filtering) that was not subject to evaluation.

8 Evaluated Configuration

The evaluated version of the TOE is Brocade Communication Systems, Inc. VDX Product Series with NOS 3.0.1a5, including the following series Hardware Platforms:

- VDX 6710-54
- VDX 6720-24
- VDX 6720-60

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

- VDX 6730-32
- VDX 6730-76
- VDX 8770-4
- VDX 8770-8.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP), in conjunction with version 3.1, revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the NDPP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

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

VALIDATION REPORT
Brocade Communications Systems, Inc. VDX Product Series

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 ST for this product's evaluation is Brocade Communications Systems, Inc. VDX Product Series Security Target, Version 1.0, 3 April 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004.
5. Protection Profile for Network Devices, Version 1.1, 8 June 2012.
6. Brocade Communications Systems, Inc. VDX Product Series Security Target, Version 1.0, 3 April 2014.