National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Extreme Networks, Inc.

6480 Via Del Oro

San Jose, CA 95119

Extreme Networks, Inc. VDX Product Series with NOS Version 7.3.0aa

Report Number: CCEVS-VR-10928-2019
Dated: January 11, 2019
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, Senior
Jenn Dotson
Sheldon Durrant
Linda Morrison
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Cornelius Haley
Wasif Sikder
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 Extreme Networks VDX Product Series with NOS) solution provided by Extreme Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) 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 January 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E*).

The TOE is the Extreme Networks VDX Product Series with NOS Version 7.3.0aa. VDX switches, featuring embedded automation capabilities of Extreme data center fabrics, deliver high performance, capacity, and reliability in data center spine and leaf deployments.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 VR 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 ETR are consistent with the evidence provided.

The Validation Team monitored the activities of the Evaluation Team, provided guidance on technical issues and evaluation processes. 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Extreme Networks, Inc.VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target, Version 0.5, 1/4/2019* and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing

laboratories called CCTLs using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The 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:	Extreme Networks VDX Product Series with NOS Version 7.3.0aa (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E)
ST:	Extreme Networks, Inc.VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target, Version 0.5, 1/4/2019.
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks, Inc. VDX Product Series with NOS Version 7.3.0aa, Version 0.2, January 4, 2019
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	Extreme Networks, Inc.
Developer	Extreme Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.

3 Architectural Information

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

The TOE is VDX Product Series operating with NOS version 7.3.0aa. The VDX Product Series operating with NOS version 7.3.0aa are hardware appliances with embedded software installed on a management processor. VDX switches, featuring embedded automation capabilities of Extreme data center fabrics, deliver high performance, capacity, and reliability in data center spine and leaf deployments. 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 Extreme Network's proprietary Multiservice 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.

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. Administrator can also use REST APIs (over HTTPS) or NetConf (over SSH) for configuring the TOE. The TOE uses SCP to download/compare software images.

The TOE includes the following models with accompanying CPUs:

Model	CPU
VDX- 6740, 6740-T, 6740T-1G, VDX-6940-36Q	Freescale P3041 four e500mc core processors at 1.5 Ghz
VDX6940-144S, VDX8770-4 and VDX8770-8 (including 8770-MM-1)	Freescale P4080 four e500mc core processors at 1.5 Ghz

The VDX 6740 switch is a fixed port switch with 48 10-Gigabit Ethernet (GbE) SFP+ interfaces and four 40 GbE independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports. The Extreme Networks VDX 6740T offers 48 10 GbE 10BASE-T ports and four 40 GbE QSFP+ ports. Each can be broken out into four independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports. The Extreme Networks VDX 6740T-1G offers 48 1000BASE-T ports and two 40 GbE QSFP+ ports. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional eight 10 GbE SFP+ ports for uplink.

The VDX 6940-36Q base system has thirty-six 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, or 36 ports can be configured as 144 10Gbe QSFP+ ports in breakout mode.

The VDX 6940-144S base system has Ninety six (96) 10 Gbe SFP+ ports and eight (8) 40Gbe QSFP + Ports enabled and Four (4) 100Gbe/40Gbe QSFP ports enabled

- One-hundred forty-four (144) 10 Gigabit Ethernet (GbE) QSFP+ ports using breakout cables, or
- Ninety-six fixed 10 Gigabit Ethernet (Gbe) QSFP+ ports and additional forty-eight 10 Gbe QSFP+ ports with breakout cables on twelve (12) 40 Gbe ports or
- Ninety-six fixed 10 Gigabit Ethernet (Gbe) QSFP+ ports and additional Thirty-Two (32) 10 Gbe QSFP+ ports with breakout cables on eight (8) 40Gbe ports and Four (4) fixed 100 Gbe QSFP+

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 following models:

- VDX 6740
- VDX 6740-T
- VDX 6740T-1G
- VDX 6940-36Q
- VDX 6940-144S
- VDX 8770-4 w/ 8770-MM-1 management module
- VDX 8770-8 w/ 8770-MM-1 management module

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 Extreme Networks 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 the ST conforms to the NDCPP20E, 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.

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 Extreme Networks 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 sets its internal clock using administrative command issued at the CLI interface.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. 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.

4.2 Cryptographic support

The TOE contains CAVP-tested 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 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. The TOE performs the validation of the login credentials

4.4 Security management

The TOE provides CLI commands to access the wide range of security management functions to manage its security policies. The TOE also provides REST APIs (protected by TLS) and NetConf (protected by SSH) to configure the TOE. 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.

4.5 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.

4.6 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.

4.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI and NetConf 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 also provides a REST API interface for security management that is protected with TLS.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. SSHv2 is used to support SCP which the TOE uses for download of TOE updates.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following document:

- collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E)

That information has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.

- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Configuration Guide, Network OS Common Criteria, Supporting Network OS v7.3.0aa, January 2019.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activities Report (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The Evaluation Team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP20E including the tests associated with all applicable optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the following series and models

- VDX 6740
- VDX 6740-T
- VDX 6740T-1G
- VDX 6940-36Q
- VDX 6940-144S
- VDX 8770-4 w/ 8770-MM-1 management module
- VDX 8770-8 w/ 8770-MM-1 management module

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all 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 all applicable assurance requirements outlined by the Protection Profile.

10.1 Evaluation of the Security Target (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VDX Product Series with NOS Version 7.3.0aa products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

10.2 Evaluation of the Development (ADV)

The Evaluation Team 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 ST and Guidance document. Additionally, the Evaluation Team performed the assurance activities specified in the NDcPP20E related to the examination of the information contained in the TSS.

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

10.3 Evaluation of the Guidance Documents (AGD)

The Evaluation Team 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. The guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the

evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team found that the TOE was identified.

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

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

The Evaluation Team ran the set of tests specified by the assurance activities in the NDCPP20E and recorded the results in a Detailed Test Report (DTR), summarized in the AAR.

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

10.6 Vulnerability Assessment Activity (VAN)

The Evaluation Team performed a public search for vulnerabilities and did not discover any public issues with the TOE. See the AAR for an identification of search terms.

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

10.7 Summary of Evaluation Results

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

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

11 Validator Comments/Recommendations

The Validation Team suggests that the consumer pay particular attention to the evaluated configuration of the products(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST, and only the functionality implemented

by the SFR's within the ST was evaluated. All other functionality provided by the product(s), to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about the effectiveness of the additional functionality.

Consumers employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed in Section 7 to ensure the evaluated configuration is established and maintained.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Extreme Networks, Inc.VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target*, Version 0.5, 1/4/2019.

14 Glossary

The following definitions are used throughout this document:

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

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

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

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

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E)

[5] Extreme Networks, Inc.VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target, Version 0.5, 1/4/2019 (ST)

[6] Assurance Activity Report (PP/EP) for VDX Product Series operating with NOS version 7.3.0aa, Version 0.2, 01/04/2019 (AAR)

[7] Detailed Test Report (PP/EP) for Extreme Networks, Inc. VDX Product Series operating with NOS version 7.3.0aa, Version 0.2, 01/04/2019 (DTR)