National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa

Report Number: CCEVS-VR-11118-2020
Dated: November 30, 2020
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
Randy Heimann
Linda Morrison
Clare Olin

Common Criteria Testing Laboratory

Cornelius Haley
Bright Sun
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 SLX Product Series operating with version 20.1.1aa provided by Extreme Networks, 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 November 2020. 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 Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa family of products.

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, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 technical information included in this report was obtained from the Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa (NDcPP21) Security Target, Version 0.5, November 16, 2020 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 Common Criteria Testing Laboratories (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, Inc. SLX Product Series operating with version 20.1.1aa
Protection Profile	(Specific models identified in Section 3.1) collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)
ST	Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa (NDcPP21) Security Target, Version 0.5, November 16, 2020
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa, ETR Version 0.3, November 30, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
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.
CCEVS Validators	Paul Bicknell Randy Heimann Linda Morrison Clare Olin

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 SLX Product Series operating with Version 20.1.1aa. The SLX Product Series operating with Version 20.1.1aa are hardware appliances with embedded software installed on a management processor. The embedded software is a version of Extreme Network's proprietary Operating System. The OS controls the switching and routing of network frames and packets among the connections available on the hardware appliances.

3.1 TOE Evaluated Platforms

The Target of Evaluation (TOE) is the SLX Product Series operating with Version 20.1.1aa including the models shown in Table 3-1.

While there are different models in the SLX Product Series, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. While there are some functional differences among the models, they each provide the same security characteristics as claimed in the security target.

Model	CPU
SLX 9640	Intel Broadwell processor Intel(R) Xeon(R) CPU D-1527
SLX 9150/9250	Intel Denverton processor Intel(R) Atom(TM) CPU C3758

Table 3-1 Evaluated Models & Processors

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 TOE is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions).

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. All of the remote management interfaces are protected using encryption as explained later in the ST.

3.3 Physical Boundaries

Each TOE appliance runs a version of the Extreme proprietary OS 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 commands issued at the CLI interface or can use an NTP server.

The evaluation includes an audit server, management workstation, NTP server and certificate authority in the IT environment. The scope of the evaluation is limited to the requirements in the ST – all other functionality is outside the scope of the evaluation.

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 and also supports use of a RADIUS server.

4.4 Security management

The TOE provides Command Line Interface (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 and RADIUS 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 documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)

That information has not been reproduced here and the NDcPP21 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- 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 NDcPP21 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:

- Extreme SLX-OS Common Criteria Configuration Guide, 20.1.aa, 16 November 2020

Only this administrative guidance listed immediately above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration and use of this product in its evaluated configuration

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 Detailed Test Report (NDcPP21) for Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa, Version 0.3, November 30, 2020 (DTR).

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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements. Test activities were conducted at the Gossamer Security Solutions test facility in Catonsville, Maryland between March and October of 2020.

9 Evaluated Configuration

The evaluated configuration consists of the following hardware models supporting SLX version 20.1.1aa when configured in accordance with the instructions in the Guidance document specified in Section 7 of the VR.

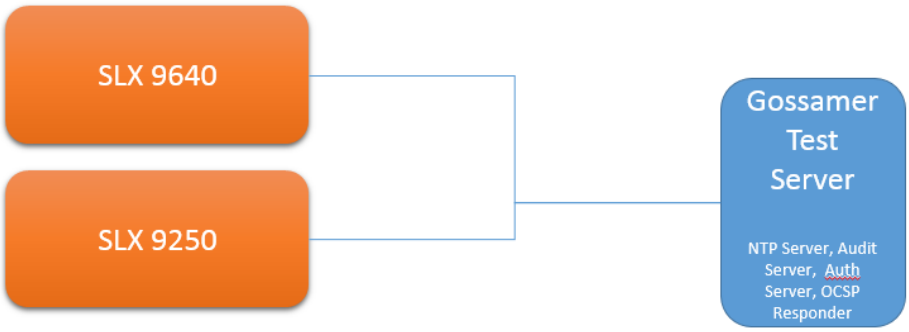
The Target of Evaluation (TOE) is the SLX Product Series operating with Version 20.1.1aa including the models shown in Table 9-1.

While there are different models in the SLX Product Series, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. While there are some functional differences among the models, they each provide the same security characteristics as claimed in the security target.

Model	CPU
SLX 9640	Intel Broadwell processor Intel(R) Xeon(R) CPU D-1527
SLX 9150/9250	Intel Denverton processor Intel(R) Atom(TM) CPU C3758

Table 9-1 Evaluated Models & Processors

9.1 Test Topology



9.2 Test Tools

The evaluator used the following supporting software for testing:

- Ubuntu Linux 16.04
- Openssl version 1.0.2g (create certificates and SSL peer)
- Rsyslog daemon version 8.16.0
- stunnnel4 version 5.30
- tcpdump version 4.9.3
- libpcap version 1.7.4
- PKIX-SSH 12.4.3
- OpenSSH 8.2p1
- Big Packet Putty version 6.8p1
- Microsoft Windows 10 (evaluator laptops)
    - Wireshark version 3.2.0

10 Results of the Evaluation

The results of exercising the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

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 5 and CEM version 3.1 rev 5. The evaluation determined the Extreme Networks, Inc. SLX Product Series operating with Version 20.1.1aa TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

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 Extreme Networks, Inc. SLX Product Series operating with Version 20.1.1aa products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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 Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP21 related to the examination of the information contained in the TSS.

The validators 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators 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 validators 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 NDcPP21 and recorded the results in a Test Report, summarized in the AAR.

The validators 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 on October 26, 2020 and did not discover any public issues with the TOE. The terms used for the search were as follows:

- “Extreme”,
- “SLX”,
- “openssl”,
- “ssh”,
- “tls”,
- “restapi”, and
- “radius”.

Using the following resources:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Exploit / Vulnerability Search Engin (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search),

- Offensive Security Exploit Database (https://www.exploit-db.com/)

The evaluated version of the product includes product updates to resolve some vulnerabilities found during this search; however neither the latest public search for vulnerabilities nor the fuzz testing uncovered any unresolved residual vulnerability.

The validators 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 notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Extreme SLX-OS Common Criteria Configuration Guide, 20.1.aa, 16 November 2020 document. No versions of the TOE and software, either earlier or later were evaluated.

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. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

12 Annexes

Not applicable

13 Security Target

Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa (NDcPP21) Security Target, Version 0.5, November 16, 2020.

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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21),

[5] Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa (NDcPP21) Security Target, Version 0.5, November 16, 2020 (ST)

[6] Assurance Activity Report (NDcPP21) for Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa, Version 0.3, November 30, 2020 (AAR)

[7] Detailed Test Report (NDcPP21) for Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa, Version 0.3, November 30, 2020 (DTR)

[8] Evaluation Technical Report for Extreme Networks, Inc. SLX Product Series operating with version 20.1.1aa, ETR Version 0.3, November 30, 2020 (ETR)

[9] Extreme SLX-OS Common Criteria Configuration Guide, 20.1.aa, 16 November 2020