National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2

Report Number: **CCEVS-VR-VID10827**

Dated: **December 20, 2017**

Version: **0.5**

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

Mr. Paul A. Bicknell

Mr. Chris Thorpe

Ms. Linda Morrison

The MITRE Corporation

Bedford, MA

Common Criteria Testing Laboratory

Mr. Kirill Sinitski

Mr. Fathi Nasraoui

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Extreme Networks Summit Series Switches Security Target.

Table of Contents

List of Figures and Tables

1. Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope and the Validator Comments, where any restrictions on the evaluated configuration are highlighted.

The Target of Evaluation (TOE) is the Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2 and consists of the Summit x870, Summit x690, Summit x620, Summit x440-G2, Summit x450-G2, Summit x460-G2, and Summit x670-G2 series platforms.

The TOE provides high density layer 2/3 switching with low latency cut-through switching and IPv4 and IPv6 unicast and multicast routing to enable enterprise aggregation and core backbone deployments. TOE consists of a hardware appliance with embedded software components.

The TOE is a Network Device as defined by the collaborative Protection Profile for Network Devices v2.0: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".*

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in December 2017. The information in this report is derived from the Evaluation Technical Report (ETR), Assurance Activity Report (AAR), and Test Report (TR), all written by the CygnaCom CCTL. The evaluation team determined that the product:

- Is Common Criteria version 3.1 R5 Part 2 extended and Part 3 conformant
- Demonstrates exact compliance to c*ollaborative Protection Profile for Network Devices, Version 2.0, May 2017* as changed/clarified by *Supporting Document Mandatory Technical Document* and all applicable technical decisions.

The following CCEVS technical decisions were applied to this evaluation:

- TD0228: NIT Technical Decision for CA certificates - basicConstraints validation

The evaluation and validation were 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.

2. Identification

Target of Evaluation: Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2

Series	Platform	Specifications
Summit x870 Series	Summit x870-32c	32 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports
	Summit x870-96x-8c	96 10Gb ports on 24 QSFP28 ports, 8 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports
Summit x690 Series	Summit x690-48x-2q-4c	48 1Gb/10Gb SFP+ ports, 2 10Gb/40Gb QSFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports
	Summit x690-48t-2q-4c	48 1Gb/10Gb 10GBASE-T ports, 2 10Gb/40Gb QSFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports
Summit x620 Series	Summit x620–16x	16 100Mb/1Gb/10GBASE-X SFP+ ports
	Summit x620–16t	12 100Mb/1Gb/10GBASE-T ports with EEE, 4 100Mb/1Gb/10GBASE-T with EEE shared with 4 1Gb/10GBASE-X SFP+ ports
	Summit x620–10x	10 100Mb/1Gb/10GBASE-X SFP+ ports
	Summit x620–8t-2x	8 100Mb/1Gb/10GBASE-T with EEE, and 2 100Mb/1Gb/10GBASE-X SFP+ ports
Summit x440-G2 Series	Summit x440-G2-12t-10GE4	12 10/100/1000BASE-T, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-12p-10GE4	12 10/100/1000BASE-T POE+, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-24t-10GE4	24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-24p-10GE4	24 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-48t-10GE4	48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradable to 10GbE
	Summit x440-G2-48p-10GE4	48 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradable to 10GbE
	Summit x440-G2-24t-10GE4-DC	24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-48t-10GE4-DC	48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+
	Summit x440-G2-24x-10GE4	24 unpopulated 1000BASE-X SFP (4 combo), 4 10/100/1000 combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+

Series	Platform	Specifications
	Summit x440-G2-24fx-GE4	24 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP
	Summit x440-G2-12t8fx-GE4	12 10/100/1000BASE-T plus 8 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP
	Summit x440-G2-24t-GE4	24 fixed 10/100/1000BASE-TX , 4 1GBASE-X unpopulated SFP
Summit x450-G2 Series	Summit x450-G2-24t-GE4	24 10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports
	Summit x450-G2-24p-GE4	24 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports
	Summit x450-G2-48t-GE4	48 10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP)
	Summit x450-G2-48p-GE4	48 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports
	Summit x450-G2-24t-10GE4	24 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports
	Summit x450-G2-24p-10GE4	48 10/100/1000BASE-T, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports
	Summit x450-G2-48t-10GE4	48 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports
	Summit X450-G2-48p-10GE4	48 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports, 2 unpopulated power supply slots, fan module slot (unpopulated)
	Summit x450-G2-24p-10GE4-FB-715-TAA	24 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports (QSFP)
	Summit x450-G2-48p-10GE4-FB-1100-TAA	48 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports (QSFP)
	Summit x450-G2-24t-GE4-FB-TAA	24 10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP)
	Summit x450-G2-24p-GE4-FB-715-TAA	24 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP)
Summit x460-G2 Series	Summit x460-G2-24t-10GE4	24 10/100/1000BASE-T, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1000/10GBaseX unpopulated SFP+ ports
	Summit x460-G2-48t-10GE4	48 10/100/1000BASE-T, 4 1000/10GBaseX unpopulated SFP+ ports
	Summit x460-G2-24p-10GE4	24 10/100/1000BASE-T PoE-plus, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1000/10GBaseX unpopulated SFP+ ports

Series	Platform	Specifications
	Summit x460-G2-48p-10GE4	48 10/100/1000BASE-T PoE-plus, 4 1000/10GBaseX unpopulated SFP+ ports
	Summit x460-G2-24x-10GE4	24 100/1000BASE-X unpopulated SFP, 8 10/100/1000BASE-T (4 10/100/1000BASE-T ports shared with SFP ports), 4 1000/10GBaseX unpopulated SFP+ ports
	Summit x460-G2-48x-10GE4	48 100/1000BASE-X unpopulated SFP, 4 1000/10GBaseX unpopulated SFP+ ports
	Summit x460-G2-24t-GE4	24 10/100/1000BASE-T, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1GBase-X unpopulated SFP ports
	Summit x460-G2-48t-GE4	48 10/100/1000BASE-T, 4 1GBaseX unpopulated SFP ports, Rear VIM Slot (unpopulated)
	Summit x460-G2-24p-GE4	24 10/100/1000BASE-T PoE-plus, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1GBaseX unpopulated SFP ports
	Summit x460-G2-48p-GE4	48 10/100/1000BASE-T PoE-plus, 4 1GBaseX
Summit x670-G2 Series	Summit x670-G2-72x	72 10GBASE-X SFP+
	Summit x670-G2-48x-4q	48 10GBASE-X SFP+ and 4 40GBASE-X QSFP+
	Summit x670-G2-48x-4q-FB-AC-TAA	48 10GBASE-X SFP+ and 4 40GBASE-X QSFP+

Developer: Extreme Networks Inc.

TOE : Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2

CCTL: CygnaCom Solutions
7925 Jones Branch Dr, Suite 5200
McLean, VA 22102

Evaluators: Kirill Sinitski, Fathi Nasraoui

Validation Scheme: National Information Assurance Partnership CCEVS

Validators: Paul A. Bicknell, Chris Thorpe, Linda Morrison

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1 R5, April 2017

CEM Identification: Common Methodology for Information Technology Security Evaluation, Version 3.1 R5, April 2017

3. Security Functionality

The TOE implements the following security functionality as described in the Security Target (ST):

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- TOE Access
- Trusted Path/Channels

3.1. Security Audit

The TOE generates audit records for all security-relevant events. For each audited events, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The resulting records are stored locally and can be sent securely to a designated audit server for archiving. Security Administrators, using the appropriate CLI commands, can also view audit records locally. The TOE provides a reliable timestamp relying on the appliance's to built-in clock.

3.2. Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSHv2 for remote administration
  - TLS v1.2 for communication with authorized IT entities
- Randomness is collected and processed to support seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X.509v3 certificate authentication integrated with TLS protocol

The TOE uses a dedicated cryptographic module to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

3.3. Identification and Authentication

The TOE supports Role-Based Access Control (RBAC) managed by an Authentication, Authorization, and Accounting (AAA) module that stores and manages permissions of all users and their roles. The TOE requires users to provide their assigned unique username and password before any administrative access to the system is granted. Each authorized user is associated with an assigned role and role-specific permissions that determine their access to TOE features. The AAA module stores the assigned role of each user along with all other information required for that user to access the TOE.

3.4. Security Management

The TOE allows remote administration using an SSHv2 session over an out of band RJ-45 LAN management port, and local administration using a console via a separate RJ-45 port running RS-232 signaling for a serial connection. Both remote and local administration are conducted over a Command Line Interface (CLI) terminal that facilitates access to all of the management functions used to administer the TOE.

There are two types of administrative users within the system: Security Administrator and User. All of the management functions are restricted to Security Administrators, including: managing user accounts and roles, rebooting and applying software updates, administering the system configuration, and reviewing audit records. The term "Security Administrator" is used to refer to any administrative user with the appropriate role to perform the relevant functions.

3.5. Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

- The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable or accessible in plaintext.
- The TOE ensures that reliable time information is available for both log accountability and synchronization with the operating environment.
- The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

3.6. TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which any inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

3.7. Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path secured using SSH between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel using TLS between itself and the audit server.

3.8. Secure Usage Assumptions

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

1. 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. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
2. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the operational environment.
3. TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
4. It is assumed that there is no protection of traffic that traverses the TOE. Only traffic that originates on or is destined to the device itself is protected.
5. It is assumed that the TOE is regularly updated when in use.
6. It is assumed that the TOE will be securely decommissioned when removed from its operational environment.

4. Architectural Information

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the EXOS is shared across all platforms.

EXOS is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. The dedicated cryptographic module is integrated with protocol libraries that implement the secure channel functionality. The control plane subsystem, that includes the Internet Protocol (IP) host stack (which can be further subdivided into protocol and control layers), implements the switching and routing functions. The system management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements the administrative interface and maintains configuration information.

The physical boundary of the TOE is the Extreme Networks Summit Series Switches running EXOS v22.3, which includes:

- The appliance hardware
- RJ-45/RS-232 management ports
- A USB port
- A dedicated Ethernet management port
- Embedded software installed on the appliance
- The CLI management interface

The Operational Environment of the TOE includes:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- An Audit server for external storage of audit records
- A NTP server for synchronizing system time
- OCSP servers to support revocation checking
- A DNS server

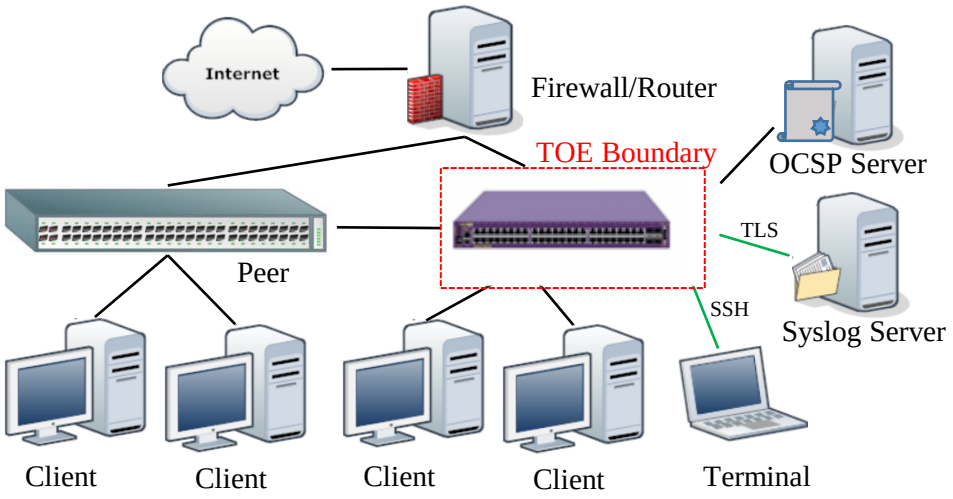

Figure 1: TOE Boundary

The TOE supports a number of features that are not part of the core functionality. This excluded functionality was not included in the scope of the evaluation:

- Any integration and/or communication with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control Systems (TACACS) is not evaluated.
- Any use of HTTP and HTTPS (web interface) is excluded, and the TOE's web interface is disabled by default.
- Routing protocols that integrate authentication or encryption, such as Routing Information Protocol (RIPv1, RIPv2), Open Shortest Path First (OSPFv2), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) are not evaluated. RFC-compliant implementations are unable to satisfy cryptographic requirements outlined in the PP.
- Use of the FTP server is excluded and it is disabled by default.
- Telnet is disabled in the evaluated configuration.
- The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- Virtualized EXOS is not evaluated.
- Synchronization with an external NTP server is not restricted; however, this functionality is not evaluated.
- The TOE's debug mode is not intended for normal use and is not evaluated.
- Python support is disabled in the evaluated configuration.

5. Assumptions, Threats & Clarification of Scope

5.1. Assumptions

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

- Collaborative Protection Profile for Network Devices, Version 2.0, 5 February 2017 (NDcPPv2)

That information has not been reproduced here and the NDcPPv2 should be consulted if there is interest in that material.

5.2. Threats

The Security Problem Definition, including the threats, may also be found in the NDcPPv2. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

5.3. 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPPv2. All NIAP Technical Decisions related to the protection profile security functional requirements were considered and applied as necessary.
- This evaluation covers only the specific device models and software as identified in Security Target, and not any earlier or later versions released or in process.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by Extreme Networks and delivered to the end user of the TOE:

6.1. Security Target

Extreme Networks Summit Series Switches Security Target, Version 2.4, December 19, 2017

6.2. User Documentation

Reference Title
ExtremeXOS User Guide for Version 22.3, published July 2017
ExtremeXOS Command Reference Guide for Version 22.3, published July 2017
Extreme Networks Summit Series Switches Common Criteria Admin Guide, December, 2017

7. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Extreme Networks Summit Series Switches Test Report* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

7.1. Developer Testing

cPP evaluations do not require developer testing evidence for assurance activities.

7.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDcPPv2.0.

Testing was conducted in parallel at two different sites. At both sites the testing topology included a hardware appliance and a virtualized operational environment containing servers utilized in testing. Each test setup was isolated to a dedicated and isolated LAN. Where possible, local LAN addresses were duplicated across setups to simplify test evidence processing.

The Evaluators successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the NDcPP Assurance-defined tests including the optional SSH and TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined, after examining the Test Report and the full set of test results provided by the evaluators, that the testing requirements for the NDcPP v2.0 are fulfilled.

8. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5.

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 version 3.1 R5 of the CC and the CEM. Additionally, the evaluators performed the assurance activities specified in the Protection Profile *collaborative Protection Profile for Network Devices Version 2.0.*

The evaluation determined that the TOE meets the SARs contained in the NDcPP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the CygnaCom CCTL (proprietary).

Below lists the assurance requirements for which the TOE was required to be evaluated, as specified in the PP. All assurance activities and work units received a Pass verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9. Validators Comments/Recommendations

The validators suggest that consumers pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed above to ensure the evaluated configuration is established and maintained.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality, including the excluded functionality discussed above, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated version of the products utilizes the *Intel Atom C series and Cavium Octeon II* processors and no earlier or later versions were evaluated and therefore cannot be considered as compliant.

The TOE stores a limited amount of audit records in its internal persistent storage. It is recommended that the administrator configure the TOE to export audit logs to a remote audit storage server.

10. Glossary

10.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

BGP	Border Gateway Protocol
CLI	Command Line Interface
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSPFv2	Open Shortest Path First
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell Network Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

11. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017 Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017, Version 3.1 Revision 5 Final, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017, Version 3.1 Revision 5 Final, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, April 2017, Version 3.1 Revision 5 Final, CCMB-2017-04-004.