National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Arista Networks

7050X, 7250X, 7300X, and 7500E Series with EOS 4.13.3.4

Report Number: CCEVS-VR-VID10559-2014
Dated: July 29, 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

Acknowledgements

Validation Panel

Jerome F. Myers

Kenneth B. Stutterheim

The Aerospace Corporation, 6940 Columbia Gateway Drive, Suite 400, Columbia, MD

Common Criteria Testing Laboratory

Kenji Yoshino

Ryan Day

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) validation team's assessment of the CCEVS evaluation of the Arista Networks 7050X, 7250X, 7300X and 7500E Series with EOS 4.13.3.4. 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 InfoGard Laboratories, Inc. in San Luis Obispo, California. The evaluation completed in June 2014. The evaluation team determined that the Arista Networks 7050X, 7250X, 7300X and 7500E Series meets the assurance requirements specified by the Network Device Protection Profile, June 8, 2012, Version 1.1 with the Security Requirements for Network Devices Errata #1, Version 1.0, December 19, 2013.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE, the Arista Networks 7050X, 7250X, 7300X, and 7500E Series with EOS V4.13.3.4, is a Network Device that provides layer 2, 3, and 4 Ethernet network management and interconnectivity. The Ethernet management layers refer to the Open Systems Interconnection (OSI) model layers. They refer to the data link, network, and transport layers respectively. It also contains a modern Linux-based operating system that allows for complex management solutions. It is designed with high performance electronics to meet the requirements of latency-critical applications such as financial Electronic Communication Networks (ECNs) or High Performance Computing (HPC) clusters.

The TOE supports remote administration over the Secure Shell v2 (SSHv2) protocol that supports cryptographic encryption and authentication using CAVP Validated algorithms.

The TOE also supports storage and forwarding of detailed audit logs. The process that manages audit messages is capable of forwarding audit messages, encrypted using SSHv2, to any syslog-compatible network entity.

2 Identification of the TOE

This section contains the following:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation;
- The User Guidance, user facing documentation that is within the scope of the evaluation;

- The Operational Environment, IT devices required to support the secure operation of the TOE.

Table 1 provides information needed to completely identify the TOE.

<table>
<tr><td>Evaluation Scheme</td><td colspan="2">United States Common Criteria Evaluation Validation Scheme</td></tr>
<tr><td rowspan="13">Evaluated Target of Evaluation</td><td colspan="2">Arista Networks 7050X, 7250X, 7300X, and 7500E Series</td></tr>
<tr><td colspan="2">Hardware Models</td></tr>
<tr><td>Part Number</td><td>Description</td></tr>
<tr><td>DCS-7050SX-128-F</td><td>Arista 7050, 96xSFP+ & 8xQSFP+ switch, front-to-rear airflow and dual 750W AC power supplies</td></tr>
<tr><td>DCS-7050SX-128-R</td><td>Arista 7050, 96xSFP+ & 8xQSFP+ switch, rear-to-front airflow and dual 750W AC power supplies</td></tr>
<tr><td>DCS-7250QX-64-F</td><td>Arista 7250, 64xQSFP+ switch, front-to-rear airflow and dual 1100W AC power supplies</td></tr>
<tr><td>DCS-7250QX-64-R</td><td>Arista 7250, 64xQSFP+ switch, rear-to-front airflow and dual 1100W AC power supplies</td></tr>
<tr><td>DCS-7316X-BND-F</td><td>Arista 7316X chassis bundle. Includes 7316 chassis, 6 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (F-R)</td></tr>
<tr><td>DCS-7316X-BND-D-F</td><td>Arista 7316X chassis bundle. Includes 7316 chassis, 6 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (F-R)</td></tr>
<tr><td>DCS-7316X-BND-R</td><td>Arista 7316X chassis bundle. Includes 7316 chassis, 6 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (R-F)</td></tr>
<tr><td>DCS-7316X-BND-D-R</td><td>Arista 7316X chassis bundle. Includes 7316 chassis, 6 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (R-F)</td></tr>
<tr><td>DCS-7308X-BND-F</td><td>Arista 7308X chassis bundle. Includes 7308 chassis, 4 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (F-R)</td></tr>
<tr><td>DCS-7308X-BND-D-F</td><td>Arista 7308X chassis bundle. Includes 7308 chassis, 4 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (F-R)</td></tr>
</table>

	DCS-7308X-BND-R	Arista 7308X chassis bundle. Includes 7308 chassis, 4 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (R-F)
	DCS-7308X-BND-D-R	Arista 7308X chassis bundle. Includes 7308 chassis, 4 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (R-F)
	DCS-7304X-BND-F	Arista 7304X chassis bundle. Includes 7304 chassis, 2 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (F-R)
	DCS-7304X-BND-D-F	Arista 7304X chassis bundle. Includes 7304 chassis, 2 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (F-R)
	DCS-7304X-BND-R	Arista 7304X chassis bundle. Includes 7304 chassis, 2 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor (R-F)
	DCS-7304X-BND-D-R	Arista 7304X chassis bundle. Includes 7304 chassis, 2 x 3000W PS, 4 Fabric modules with fans, 1x Supervisor with SSD (R-F)
	DCS-7300X-64S-LC	Arista 7300X-64S linecard for 7300X Series, 48 port 10GbE SFP+ and 4 port 40GbE QSFP+ (spare)
	DCS-7300X-64T-LC	Arista 7300X-64T linecard for 7300X Series, 48 port RJ45 10GBASE-T and 4 port 40GbE QSFP+ (spare)
	DCS-7300X-32Q-LC	Arista 7300X-32Q linecard for 7300X Series, 32 port 40GbE QSFP+ (spare)
	DCS-7508E-BND	Arista 7508E chassis bundle. Includes 7508 chassis, 4x2900PS, 6xFabric-E modules, 1xSupervisor-E
	DCS-7504E-BND	Arista 7504E chassis bundle. Includes 7504 chassis, 4x2900PS, 6xFabric-E modules, 1xSupervisor-E
	DCS-7508E-BND-D	Arista 7508E chassis bundle. Includes 7508 chassis, 4x2900PS, 6xFabric-E modules, 1xSupervisor-E-SSD
	DCS-7504E-BND-D	Arista 7504E chassis bundle. Includes 7504 chassis, 4x2900PS, 6xFabric-E modules, 1xSupervisor-E-SSD

	DCS-7500E-36Q-LC	36 port 40GbE QSFP+ wire-speed line card for 7500E Series ⍰
	DCS-7500E-72S-LC	48 port 10GbE SFP+ & 2 x 100GbE SR10 Embedded MXP wire-speed line card for 7500E Series
	DCS-7500E-48S-LC	48 port 1/10GbE SFP+ wire-speed line card for 7500E Series
	DCS-7500E-12CM-LC	12 port 100GbE SR10 Embedded MXP wire-speed line card for 7500E Series
	Hardware Version	
	Arista 7050SX CPU Model: Intel(R) Pentium(R) CPU @ 1.50GHz, Security Chip: R5H30211, Forwarding ASIC: Linecard0/0: Chip: BCM56850	Security hardware built into all Arista 7050SX models.
	Arista 7250X Series Intel(R) Pentium(R) CPU @ 1.50GHz, Security Chip: R5H30211, Forwarding ASIC: Linecard *x*/*y*[1]: Chip: BCM56850	Security hardware built into all Arista 7250X models.
	Arista 7300X Series CPU Model: Intel(R) Xeon(R) CPU @ 2.60GHz, Security Chip: R5H30211, Forwarding ASIC: Linecard *x*/*y*[1]: Chip: BCM56850	Security hardware built into all Arista 7300X models.
	Arista 7500E Series CPU Model: Intel(R) Xeon(R) CPU @ 2.60GHz, Security Chip: R5H30211, Forwarding ASIC: Arad*x*/*y*[1]	Security hardware built into all Arista 7500E models.

[1] Note: The output of "Forwarding ASIC" will vary in the number of linecards, and depend on how many and which linecards are populating the chassis. *X* and *Y* will be integers denoting each linecard in the configuration. All ASIC types for a specific TOE will always display the same chip or model type..

	Model: Arad	
	Software (identical for all models)	
	Arista EOS Version 4.13.3.4	Modular switch OS that separates switch state from protocol processing and application logic.
Protection Profile	Network Device Protection Profile, June 8, 2012, Version 1.1 Security Requirements for Network Devices Errata #1, Versions 1.0, December 19, 2013	
Security Target	Arista Networks 7050X, 7250X, 7300X and 7500E Series Security Target, Version 1.6, July 22, 2014	
Dates of Evaluation	February 2014 – July 2014	
Conformance Result	Pass	
Common Criteria Version	v3.1 Revision 3	
Common Evaluation Methodology (CEM) Version	v3.1 Revision 3	
Assurance Activities Report (AAR)	14-3140-R-0033 V1.0	
Sponsor/Developer	Arista Networks, Inc.	
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.	
CCTL Evaluators	Kenji Yoshino	
CCEVS Validators	Jerome F. Myers	

Table 1: Evaluation Identification

The following User Guidance is considered part of the TOE, delivered via electronic download, and within the scope of the evaluation:

- Common Criteria Guidance Supplement Arista 7150, 7050X, 7250X, 7300X and 7500E Series Switches Guidance Document AGD_OPE.1, AGD_PRE.1, Version 1.4, June 10, 2014
- Arista User Manual, Arista EOS version 4.13.3.4, June 9, 2014
- Arista EOS System Message Guide Software Release 4.13.3.4, April 18, 2014
- Arista Quick Start Guide 7000 Series 2 RU Data Center Switches, PDOC-00039-05
- Arista Quick Start Guide 7300 Series Module Data Center Switches, PDOC-00040-02
- Arista Quick Start Guide 7500 Series Module Data Center Switches, PDOC-00015-05

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Syslog Server	Syslog server conforming to RFC 5424 SSH server allowing port forwarding and supporting RSA 2048, AES-128/256 CBC, HMAC-SHA1, and diffie-hellman-group14-sha1
NTP Server	NTP server conforming to RFC 5095
SSH Client	SSHv2 client supporting RSA 2048, AES-128/256 CBC, HMAC-SHA1, and diffie-hellman-group14-sha1
RS-232 Terminal	Serial console supporting 9600 baud, no flow control, 1 stop bit, no parity bits, and 8 data bits

Table 2: Operational Environment Components

The following SFP and QSFP interfaces are supported by each series:

SFP Interface	SFP Type	Speed (gigabit)	7500E	7300X	7050SX-128	7250QX-64
40GBASE-CR4	QSFP+	40	✓	✓	✓	✓
40GBASE-SR4	QSFP+	40	✓	✓	✓	✓
AOC-40G-Q-Q	QSFP+	40	✓	✓	✓	✓
40GBASE-XSR4	QSFP+	40	✓	✓	✓	✓
40G-PLRL4	QSFP+	40	✓	✓	✓	✓
40G-LRL4	QSFP+	40	✓	✓	✓	✓
40GBASE-LR4	QSFP+	40	✓	✓	✓	✓
10GBASE-CR	QSFP+ / SFP+	10	✓	✓	✓	✓
10GBASE-SRL	SFP+	10	✓	✓	✓	
10GBASE-SR	SFP+	10	✓	✓	✓	
10GBASE-LR	SFP+	10	✓	✓	✓	
10GBASE-LRL	SFP+	10	✓	✓	✓	
10GBASE-ER	SFP+	10	✓	✓	✓	
10GBASE-ZR	SFP+	10	✓	✓	✓	
10GBASE-DWDM	SFP+	10	✓	✓	✓	
1GbE-SX	SFP+	1	✓	✓	✓	
1GbE-LX	SFP+	1	✓	✓	✓	
1GbE-TX	SFP+	1	✓	✓	✓	
100Mb-TX	SFP+	0.1		✓		

Table 3: SFP Interfaces

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before February 25, 2014.

3.1 Clarification of Scope

The TOE claims exact compliance to the Network Device Protection Profile, June 8, 2012, Version 1.1 with Security Requirements for Network Devices Errata #1, Version 1.0, December 19, 2013. Exact compliance indicates that the TOE implements the security functions exactly as specified by the PP and Errata; however, functions not described in the Security Target may be used but were not tested as part of this evaluation.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptography
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.1 Audit

The Arista EOS uses an internal syslog process that receives, stores, and forwards auditable events from all system processes. When a user or system process triggers applicable TSF functionality an audit message is generated, and sent to the internal syslog process. These events are then sent to an external audit server for storage and review by an administrator. The communication between the TOE and external audit server is protected by tunneling the syslog protocol through an encrypted SSH tunnel.

4.2 Cryptography

The TSF performs the following cryptographic operations:

- SSH with the following algorithms:
    - RSA-2048 for public-key authentication
        - Signature Verification (FIPS algorithm Cert. #1315)
        - Signature Generation tested with CAVS v15.2[2]
    - AES-128/256 CBC for data encryption (FIPS algorithm Cert. #2567)

[2] SP 800-131A disallowed issuance of new algorithm certificates for SHA-1 based signature generation.

    - HMAC-SHA1 for data integrity (FIPS algorithm Cert. #1584)
    - diffie-hellman-group14-sha1 for key exchange
- SHA-512 for the following purposes: (FIPS algorithm Cert. #2163)
    - Local administrator password storage and authentication
    - CLI “verify” function which allows the SHA-512 hash calculation of any file
- SHA-1 for the following purposes: (FIPS algorithm Cert. #2163)
    - Used within HMAC-SHA1 and diffie-hellman-group14-sha1
- HMAC-SHA1 for the following purposes: (FIPS algorithm Cert. #1584)
    - SSH data verification
- Random bit generation using FIPS 140-2 X9.31-AES (FIPS algorithm Cert. #1218)

4.3 User Data Protection

The TOE uses various software and hardware mechanisms to ensure that network packets traveling through the TOE are not re-used or accessible once they have finished being used by the TOE. The hardware packet-routing architecture is built without the use of padding to ensure that all data is passed between components exactly as-is. Therefore, when an Ethernet packet is received by the switch, the exact size of the packet is known and allocated for in global memory. When a packet is stored within global memory it is stored along with metadata to ensure packet integrity.

The Linux kernel API, which handles padding in a safe manner, is leveraged to generate packets internally. If the kernel is given a payload that does not meet the minimum payload size requirement it will pad the payload with zeros. In addition, the kernel will not accept payloads with a bit length non-divisible by eight. Therefore, each individual system process is responsible for creating a payload that does not require padding past the minimum length requirement. These features together protect user data from being disclosed.

4.4 Identification and Authentication

The TOE supports password authentication for administrative users over console and SSH. The TOE also supports RSA key-based authentication for administrative users over SSH. The TOE stores the local system administrator password locally using SHA-512 hashing and allows special characters and passwords in excess of 15 characters. The remote authentication server stores the privilege level of each user along with all other information required to access the TOE. The TOE enforces that administrative users authenticate through this mechanism before performing any administrative actions. Communications between the TOE and the external authentication server are protected by an encrypted SSH TCP tunnel between both systems.

4.5 Security Management

The TOE enforces protection of TSF data with encrypted and authenticated network communications. The TOE also performs self-tests on boot to verify that each of these cryptographic algorithms are functioning correctly.

4.6 Protection of the TSF

The TOE protects TSF data from disclosure using different cryptographic methods and security-functionality. The TOE provides administrative access to users through a CLI that enforces user and group profiles. The administrator configures user profiles on the authentication server that specify varying degrees of access to the system. The limited CLI, user account system, and underlying file system permissions serve to restrict access to TSF data such as private keys. Plaintext private keys used for SSH authentication are stored on internal flash which is only accessible through CLI commands performed by the local administrator. The local administrator password stored by the TOE is kept in a hashed form so that it cannot be read in plaintext format.

The TOE derives a reliable time source for logging and other system processes through the local NTP service. The exact time can be provided by setting the value locally, or through synchronizing the time from an external server via NTP.

When updating TSF functionality, a published cryptographic hash of the updated software is provided to the user to ensure the integrity of the software.

The TOE is also able to verify that TSF protection is functioning properly by running a memory test at boot-time and several diagnostic tools throughout the operation of the TOE. During the EOS boot sequence the TOE also initializes FIPS self-tests which utilize known-answer tests against each cryptographic algorithm supported by the TOE.

4.7 TOE Access

In order to prevent unauthorized access to the TOE, administrative sessions can be terminated manually or automatically. If an administrator accesses the TOE the session may be terminated by the administrator’s own actions or automatically after a specified time of inactivity. These termination features apply to both local and remote connections to the TOE.

The TOE will also display a customizable warning message that is displayed to the user during each administrative logon. The message can serve as an advisory notice and consent warning regarding use of the TOE.

4.8 Trusted Path/Channels

The TOE implements and requires a secured method of communication between itself, external devices, and remote administrators. In order to accomplish a secure connection to external devices, the TOE uses an SSHv2 connection with RSA based authentication and AES-based encryption. A private/public key pair can either be generated by the TOE or imported from another device and imported into the TOE. After an SSHv2 connection is authenticated via RSA key pairs, AES encryption keys are exchanged via diffie-hellman-group14-sha1 key exchange algorithm. After these steps, all further traffic between the TOE and the external device is encrypted via AES-128/256-CBC encryption. This method provides assured identification of the external device and prevents disclosure or undetected modification of data across the communication channel. Communications between the TOE and external devices may be initiated from either the TOE or the external device.

Remote administrators may also create a secured connection to the TOE that provides cryptographic authentication and protection of data. Remote administrators connecting to the TOE via SSHv2 have the option of using password-based authentication or RSA key-based authentication.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

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

6 Architectural Information

The TOE is classified as a Network Device for Common Criteria purposes. The TOE is made up of hardware and software components.

The TOE is an ultra-low latency and feature rich network switch that is intended to connect many Ethernet-based network devices together in an enterprise environment while maintaining security, reliability, and wire-speed network connections.

6.1 Architecture Overview

Each non-administrative network interface uses a small form-factor pluggable (SFP) transceiver to provide connectivity between the network device motherboard and a fiber optic or copper cable. This allows the customer to use several different types of network cables with the network device. The list of compatible SFPs is provided in Table 3 and the user guidance.

Each model of the TOE under evaluation varies by the amount and type of SFPs supported by the hardware.

The Arista Extensible Operating System, or Arista EOS, is built upon the mainline Linux kernel (www.kernel.org) and an x86 dual-core CPU.

Table 1: Evaluation Identification lists the hardware and software components that comprise the TOE.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Arista 7150 Series. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is shipped to the customer using a standard parcel service. The guidance documents are provided via electronic download and apply to the CC Evaluated configuration:

7.1 Guidance Documentation

Document	Revision	Date
Common Criteria Guidance Supplement Arista 7150, 7050X, 7250X, 7300X and 7500E Series Switches Guidance Document AGD_OPE.1, AGD_PRE.1	1.4	June 10, 2014
Arista User Manual, Arista EOS version 4.13.3.4	N/A	June 9, 2014
Arista EOS System Message Guide Software Release 4.13.3.4	N/A	April 18, 2014
Arista Quick Start Guide 7000 Series 2 RU Data Center Switches	PDOC-00039-05	N/A
Arista Quick Start Guide 7300 Series Module Data Center Switches	PDOC-00040-02	N/A
Arista Quick Start Guide 7500 Series Module Data Center Switches	PDOC-00015-05	N/A

7.2 Security Target

Document	Revision	Date
Arista Networks 7050X, 7250X, 7300X and 7500E Series Security Target	1.6	July 22, 2014

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Evaluation Team Independent Testing

The evaluation team performed all of the test activities specified in the Network Device Protection Profile, June 8, 2012, Version 1.1 and Security Requirements for Network Devices Errata #1, Version 1.0, December 19, 2013. The test environment consisted of:

- centos 6.2 final
  - rsyslog 5.8.12
  - OpenSSH 5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
- debian-7.0.0-amd64
  - ntpd 4.2.6p5
  - OpenSSH 6.0p1, OpenSSL 1.0.1e 11 Feb 2013
  - nmap 6.00

The TOE passed all required test activities.

8.2 Vulnerability Analysis

On May 21, 2014, the evaluation team searched http://www.cvedetails.com for known vulnerabilities in:

- Linux version 2.6.38.8.Ar-1398415
- OpenSSH_5.5p1
- OpenSSL 1.0.0e-fips 6 Sep 2011
- ntpd version 4.2.6p3-RC10
- Arista EOS 4.13.3

The evaluation team determined that suitable vulnerabilities would have Low CVSSv2 Access Complexity, because a Medium Access complexity as defined by http://www.first.org/cvss/cvss-guide.html#i2.1.2 requires additional access, social engineering, and/or a non-default configuration.

The evaluation team found three potential vulnerabilities. Of the three potential vulnerabilities, a public exploit has only been released for one of the vulnerabilities. The evaluation team ran the one exploit against the TOE and determined the TOE was not vulnerable.

9 Results of the 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, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard determined that the TOE meets the security criteria in the Security Target, which specifies an assurance requirements specified in Network Device Protection Profile, June 8, 2012, Version 1.1 with Security Requirements for Network Devices Errata #1, Version 1.0, December 19, 2013. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in June 2014.

10 Validator Comments/Recommendations

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

The evaluation team worked closely with the validation team to resolve issues that arose during the consistency review – to include retesting.

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.

11 Security Target

Arista Networks 7050X, 7250X, 7300X and 7500E Series Security Target, Version 1.6, July 22, 2014.

12 Terms

12.1 Acronyms

AAA	Authentication Authorization and Accounting
AAR	Assurance Activity Report
CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
FIPS	Federal Information Processing Standards Publication 140-2
I/O	Input/Output
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
QSFP	Quad Small Form-factor Pluggable
SF	Security Functions
SFR	Security Functional Requirements

SFP	Small Form-factor Pluggable
SSH	Secure Shell
ST	Security Target
STP	Spanning Tree Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[5] Network Device Protection Profile, June 8, 2012, Version 1.1.

[6] Security Requirements for Network Devices Errata #1, Version 1.0, December 19, 2013