National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Arista Networks 7280 Series Switches Running EOS 4.28

Report Number: CCEVS-VR-VID11356-2023

Dated: July 27, 2023

Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt
Russell Fink
Clare Parran
Michael Smeltzer
Chris Thorpe
Robert Wojcik

Common Criteria Testing Laboratory

Fathi Nasraoui

Nishan Singh

Brandon J. Solberg

Manohar Negi

Acumen Security, LLC

Table of Contents

1 Executive Summary 5

2 Identification 6

3 Architectural Information 7

4 Security Policy 9

4.1 Security Audit 9
4.2 Cryptographic Support 9
4.3 Identification and Authentication 9
4.4 Security Management 9
4.5 Protection of the TSF 9
4.6 TOE Access 10
4.7 Trusted Path/Channels 10

5 Assumptions, Threats & Clarification of Scope 11

5.1 Assumptions 11
5.2 Threats 12
5.3 Clarification of Scope 13

6 Documentation 15

7 TOE Evaluated Configuration 16

7.1 Evaluated Configuration 16
7.2 Excluded Functionality 17

8 IT Product Testing 18

8.1 Developer Testing 18
8.2 Evaluation Team Independent Testing 18

9 Results of the Evaluation 19

9.1 Evaluation of Security Target 19
9.2 Evaluation of Development Documentation 19
9.3 Evaluation of Guidance Documents 19
9.4 Evaluation of Life Cycle Support Activities 20
9.5 Evaluation of Test Documentation and the Test Activity 20
9.6 Vulnerability Assessment Activity 20
9.7 Summary of Evaluation Results 21

10 Validator Comments & Recommendations 22

11 Annexes 23

12 Security Target 24

13 Glossary 25

14 Bibliography 26

List of Tables

Table 1: Evaluation Identifiers 6
Table 2: Hardware Appliances 7
Table 3: Assumptions 12
Table 4: Threats 13
Table 5: Glossary 25

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 in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Arista Networks 7280 Series Switches Running EOS 4.28 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. 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 2.2e, March 23, 2020.

The TOE identified in this VR 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), as interpreted by the Assurance Activities contained in the Protection Profile (PP). 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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.

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). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Product Compliant List.

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

- TOE: the fully qualified identifier of the product as evaluated.
- ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Arista Networks 7280 Series Switches Running EOS 4.28
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
Security Target	Arista Networks 7280 Series Switches Running EOS 4.28 Security Target Version 0.5, July 19, 2023
Evaluation Technical Report	ETR Arista Networks 7280 Series Switches EOS 4.28 Version 0.4, July 3, 2023
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Arista Networks, Inc.
Developer	Arista Networks, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Lauren Brandt, Russell Fink, Clare Parran, Michael Smeltzer, Chris Thorpe, Robert Wojcik

Table 1: Evaluation Identifiers

3 Architectural Information

The Arista 7280 series switches are fixed form factor switches. The 7280 series switches range in size between 1 and 2 RU. Models vary in total throughput, port count, port speeds, route table scales etc.

Each switch model runs Arista's Linux-based network operating system called Extensible Operating System (EOS). The same EOS binary image runs on all TOE hardware models. All EOS code is compiled to the same i686 assembly, making it such that no processor runs anything different from any other processor. All processors implement the i686 assembly language. All SFRs in this ST are implemented by EOS. Hence, they behave identically on every switch model.

The table below provides the list of appliances across different series:

Series	Models	Interfaces	Host CPU
7280CR	● SKN-7280CR3-3C2	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-2	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-2-DEV	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-2G	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-3	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-3-DEV	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-3G	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-3C2-DEV	3x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C2	4x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C2-DEV	4x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C2G	4x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C6	3x100GbE (CFP2) + (9 or 10)x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C6-DEV	3x100GbE (CFP2) + (9 or 10)x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-4C6G	3x100GbE (CFP2) + (9 or 10)x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-5C2	5x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-5C2-DEV	5x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
	● SKN-7280CR3-5C2G	5x100GbE (CFP2) + 2x100GbE	Intel Broadwell-DE D1519
7280SR	● SKN-7280SR3-16YC8	4x CFP2 100G/200G + 4x 40/100G QSFP + 16x 25/10GbE SFP	Intel Broadwell-DE D1519

Table 2: Hardware Appliances

The TOE supports local administration via the local console port. Remote administration is performed over the Secure Shell v2 (SSHv2) protocol. Alternatively, management of the TSF can be automated and performed remotely over TLS connection via the eAPI automated remote management interface ("eAPI") using the eAPI JSON-RPC Client.

The TOE also supports storage and forwarding of audit records, protected using SSHv2, to any syslog-compatible network entity.

The Physical boundary of the TOE is a switch appliance of one of the models described in Table 2, including all its hardware, firmware, software, local and remote management interfaces and Arista Extensible Operating System (EOS) version 4.28.

The TOE is delivered using a courier as a single device with the Arista EOS software installed. The TOE model number can be verified through the shipping label and device front panel.

The switch appliance contains host CPU, DRAM and flash to run EOS. There are a fixed number of copper or optical network ports on the appliance. The physical boundary of the TOE is the switch appliance as shown in Figure 1.

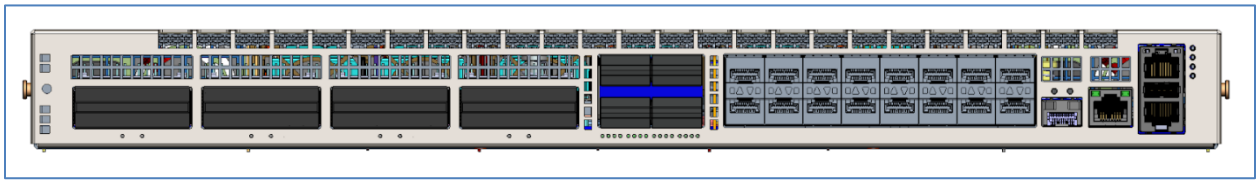

Figure 1: Physical Boundary of 7280 Series Switch

4 Security Policy

The logical boundary of the TOE includes the security functions implemented exclusively by the TOE. The TOE provides the security functions required by the collaborative Protection Profile for Network Devices Version 2.2e, March 23, 2020.

4.1 Security Audit

- The TOE will audit all events and information defined in Table 7 of the ST.
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion.
- The TOE prevents unauthorized modifications to the stored audit records.
- The TOE can transmit audit data to an external IT entity using the SSHv2 protocol.

4.2 Cryptographic Support

The TOE implements CAVP validated cryptographic algorithms for asymmetric key generation, encryption/decryption, digital signature, integrity protection/verification and random bit generation. These algorithms are used to provide security for the SSH and TLS connections of the Trusted Path and Trusted Channel. The TOE implements the Arista EOS Crypto Module v2.0 which uses the underlying OpenSSL FIPS Object Module 2.0.16 library for all cryptographic functions.

4.3 Identification and Authentication

- The TSF supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length and support passwords of 15 characters or greater.
- The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than:
    - Viewing the warning banner.

4.4 Security Management

- The TOE allows human users with the Security Administrator role to administer the TOE over a remote console (SSH Trusted Path) and local CLI (Local Console).
- The eAPI JSON-RPC trusted IT entity client allows machine users with the Security Administrator role to administer the TOE over a remote TLS Trusted Channel.

These interfaces do not allow the Security Administrator to execute arbitrary commands or executables on the TOE.

4.5 Protection of the TSF

- The TSF prevents the reading of secret keys, private keys, and passwords.

- The TOE runs a suite of self-tests, during the initial start-up (upon power on), and when programs which utilize the cryptographic libraries are initialized, to demonstrate the correct operation of the TSF.
- The TOE provides a means to verify firmware/software updates to the TOE using a published hash prior to installing those updates.
- The TOE provides reliable time stamps for itself.

4.6 TOE Access

- The TOE, for local interactive sessions, terminates the session after Security Administrator-specified period of session inactivity.
- The TOE terminates a remote interactive session after Security Administrator-configurable period of session inactivity.
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE is capable of displaying Security Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 Trusted Path/Channels

- The TOE uses SSH or TLS to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and modification.
- The TOE permits the TSF, or the authorized IT entities to initiate communication via the trusted channel.
- The TOE permits remote administrators to initiate communication via the trusted path.
- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

This section describes the assumptions on the operational environment in which the TOE is intended to be used. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following table defines specific conditions that are assumed to exist in an environment where the TOE is deployed.

Assumption	Description
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platform for general purpose Applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-modules for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g., offline

	verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g., offline verification).
A.REGULAR_UPDATES	The network device firmware and software are assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 3: Assumptions

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat	Description
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 4: Threats

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 collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020.

- Consistent with the expectations of the PP, 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 PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Arista Networks 7280 Series Switches Running EOS 4.28 Security Target Version 0.5, July 19, 2023
- Arista Networks 7280 Switches Running EOS 4.28 Common Criteria Guidance Supplement Version 2.0, July 18, 2023

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

EOS includes subsystems designed to implement operational, security, management and networking functions. EOS contains management interface subsystem comprising of applications that implement Serial Console, eAPI and SSH. This subsystem utilizes APIs provided by the Crypto Module to implement cryptographic algorithms. The keys and certificates database supports operation of cryptographic algorithms. The AAA subsystem maintains administrative user credentials, which the management subsystem relies on to identify and authenticate the users. The Audit Agent creates audit logs on relevant events, sends them to remote audit server utilizing the services of SSH, and stores them on local storage. The Config Database stores switch configuration. The Switching and Routing Engine performs core function of the switch, which is to implement traffic forwarding logic. The rules generated by this engine are programmed into line cards, which perform actual traffic forwarding function.

The TOE architecture and subsystem interactions are shown in Figure 2.

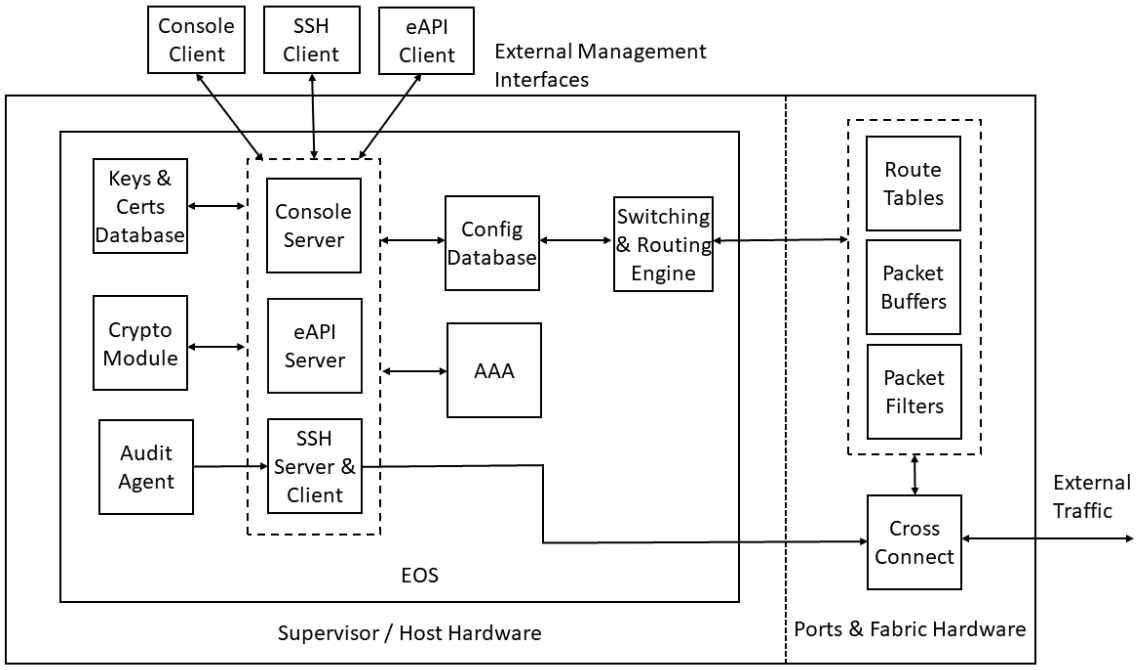

Figure 2: TOE Architecture

The switch appliance contains host CPU, DRAM and flash to run EOS. There are a fixed number of copper or optical network ports on the appliance. The physical boundary of the TOE is the switch appliance as shown in Figure 3.

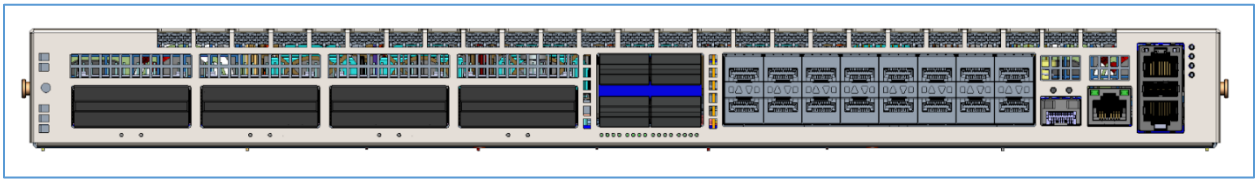

Figure 3: Physical Boundary of 7280 Series Switch

7.2 Excluded Functionality

The following features should not be used in the CC evaluated configuration. They are disabled by default (e.g., telnet) or require explicit additional configuration to make them work (e.g., integration with remote authentication server). These have not been evaluated.

- Telnet management interface.
- HTTP and HTTPS web GUI management interface.
- Integration with external authentication server over RADIUS, TACACS+, and LDAP.
- Management interfaces for XMPP, Openconfig, CloudVision eXchange (CVX) and CloudVision Portal (CVP).
- SNMP for management and notification.
- SMTP to post email notifications.
- Real-time streaming of switch state to remote server using `TerminAttr' service.
- Remote configuration backup with CLI command.
- FTP server.
- Integration with orchestration services such as Puppet, Ansible, Chef, Prometheus etc. by installing their agents on the switch.

The following features have also not been evaluated as their RFC-compliant implementations are unable to satisfy cryptographic requirements outlined in the PP:

- 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)
- In the evaluated configuration, the switch supports eAPI JSON-RPC interface over TLS for remote automation scripts to perform management functions on the switch. This interface supports only JSON request/response format. This is a machine-to-machine interface and not to be used as human interactive interface.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Arista Networks 7280 Series Switches Running EOS 4.28, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

All testing was conducted on the TOE model SKN-7280SR3-16YC8 running software version 4.28.0FX-CC, situated at the Acumen Security offices, specifically at 2400 Research Blvd Suite #395, Rockville, MD 20850. The testing took place between March 2022 and June 2023.

The TOE was located in a physically protected and access-controlled designated test lab, where unattended entry or exit was not permitted. Prior to the start of each testing day, the test bed underwent verification to ensure its integrity and security. All evaluation documentation was consistently stored in a secure folder accessible only to authorized evaluators.

A regressing testing was also conducted on the TOE model SKN-7280SR3-16YC8 using the TOE's version 4.28.0FX-CC.1, situated at the Acumen Security offices, specifically at 2400 Research Blvd Suite #395, Rockville, MD 20850. The regression testing took place between May 30, and June 2, 2023, on all SSHC SFR, 2 TLS and 2 x509 test cases.

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 the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and 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.5 and CEM version 3.1 Rev.5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

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 Arista Networks 7280 Series Switches Running EOS 4.28 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020.

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.

9.2 Evaluation of Development Documentation

The Evaluation team applied each ADV CEM work unit. 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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of Guidance Documents

The Evaluation team applied each AGD CEM work unit. 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 guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. 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.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The Evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The following vulnerability databases were searched:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories

- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities
- https://www.arista.com/

The following search terms were used.

- Arista
- Arista networks
- Arista networks 7280
- EOS 4.28
- 7280CR
- 7280SR
- Intel Pentium D1519
- nginx 1.21.4
- rsyslog 8.2001.0
- linux kernel 4.19.142
- jitterentropy-rngd-1.0.6
- openssl 1.0.2k
- openssl-fips 2.0.16
- openssh 7.8p1
- eAPI
- TLS 1.2
- TCP

The vulnerability public searches were performed on March 15, 2023 and on July 05, 2023.

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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, and that the conclusion reached by the Evaluation team was justified.

9.7 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 test activities 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 performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020, and correctly verified that the product meets the claims in the ST.

10 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 7. Arista Networks 7280 Switches Running EOS 4.28 Common Criteria Guidance Supplement Version 2.0, July 18, 2023. No versions of the TOE and software, either earlier or later were evaluated.

The Validation team suggests that the consumer pay particular attention to the installation guidance to ensure the product is placed into the evaluated configuration and that the consumer reads section 7.2 of this document to determine what functionality is excluded from the TOE.

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. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Arista Networks 7280 Series Switches Running EOS 4.28 Security Target Version 0.5, July 19, 2023.

13 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 5: Glossary

14 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.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020.
6. Evaluation Technical Report for Arista Networks 7280 Series Switches Running EOS 4.28 Version 1.4, July 3, 2023.
7. Arista Networks 7280 Switches Running EOS 4.28 Common Criteria Guidance Supplement Version 2.0, July 18, 2023.
8. Arista Networks 7280 Series Switches Running EOS 4.28 Security Target Version 0.5, July 19, 2023.
9. Assurance Activity Report for Arista Networks 7280 Series Switches Running EOS 4.28 Version 1.8, July 24, 2023.