National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3

Report Number: CCEVS-VR-VID11316-2023
Dated: January 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

Patrick Mallett, Ph.D.

Jerome Myers, Ph.D.

Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Eugene Polulyakh

Diana Polulyakh

Valeriy Polulyakh

Advanced Data Security

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of A10 Networks, Inc. Thunder Series Devices with ACOS 5.2.1-P3. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Advanced Data Security, LLC (ADSec) Common Criteria Testing Laboratory (CCTL) in San Jose, CA, United States of America, and was completed in January 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Advanced Data Security, LLC. 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, 23-March-2020 (NDcPP22e).

The Target of Evaluation (TOE) is the A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the A10 Networks, Inc. A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Security Target, Version 1.0, January 25, 2023 and analysis performed by the Validation Team.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

- 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 Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Name	Description
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3
Protection Profile	collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020
ST	A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Security Target, Version 1.0, January 25, 2023.
Evaluation Technical Report	Evaluation Technical Report for A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 , Version 1.1, January 26, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	A10 Networks, Inc.
Developer	A10 Networks, Inc.
Common Criteria Testing Lab (CCTL)	Advanced Data Security, LLC
CCEVS Validators	*Patrick Mallett, Jerome Myers, Mike Quintos*

3. ARCHITECTURAL INFORMATION

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

The Target of Evaluation (TOE) is A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3.

The TOE is composed of a hardware appliance with embedded software. The embedded software is a version of A10 Networks proprietary Advanced Core Operating System (ACOS) software. The software controls the provision of application delivery, converged networking, and application security services for network frames and packets among the connections available on the hardware appliances.

At the highest architectural level, the TOE consists of two (2) distinct planes, a management plane and a data plane. The management plane is responsible for summary control of the TOE device (startup, shutdown, etc), maintenance of the device configuration and stored information, and communications with external systems in the TOE's operational environment. The data plane processes traffic through the TOE.

The term ACOS (Advanced Core Operating System) is the name given to A10 distributed software installed and updated on the TOE. ACOS includes an underlying Linux-based operating system to support summary control and management services of the TOE.

ACOS management plane software and the Linux operating system operate on CPU cores separate from those used by the ACOS dataplane. Each plane operates with its own memory, along with memory shared to support cooperative access and processing needs within the system. The ACOS management plane employs the TOE's management port for communication with non-TOE elements in the TOE's operational environment. The TOE uses IPsec to protect communications with non-TOE systems in its operational environment, with cryptographic functionality provided by OpenSSL and the Linux Kernel Crytpo provider. Entropy and RNG needs of the ACOS management plane are supported by the Intel Secure Key capabilities of the underlying Intel Xeon processing devices.

The ACOS data plane software processes traffic through the TOE independent of the Linux OS/kernel using underlying A10 Flexible Traffic ASICs (FTAs), networking fabrics, and data plane processors included in the various TOE models. A10 Thunder models including those evaluated vary in terms of Xeon configuration (single vs dual), the underlying number of CPU cores supported, data plane port volumes/speeds, data plane FTAs, and data plane processors. Additional details for the various TOE models are included in the following subsection.

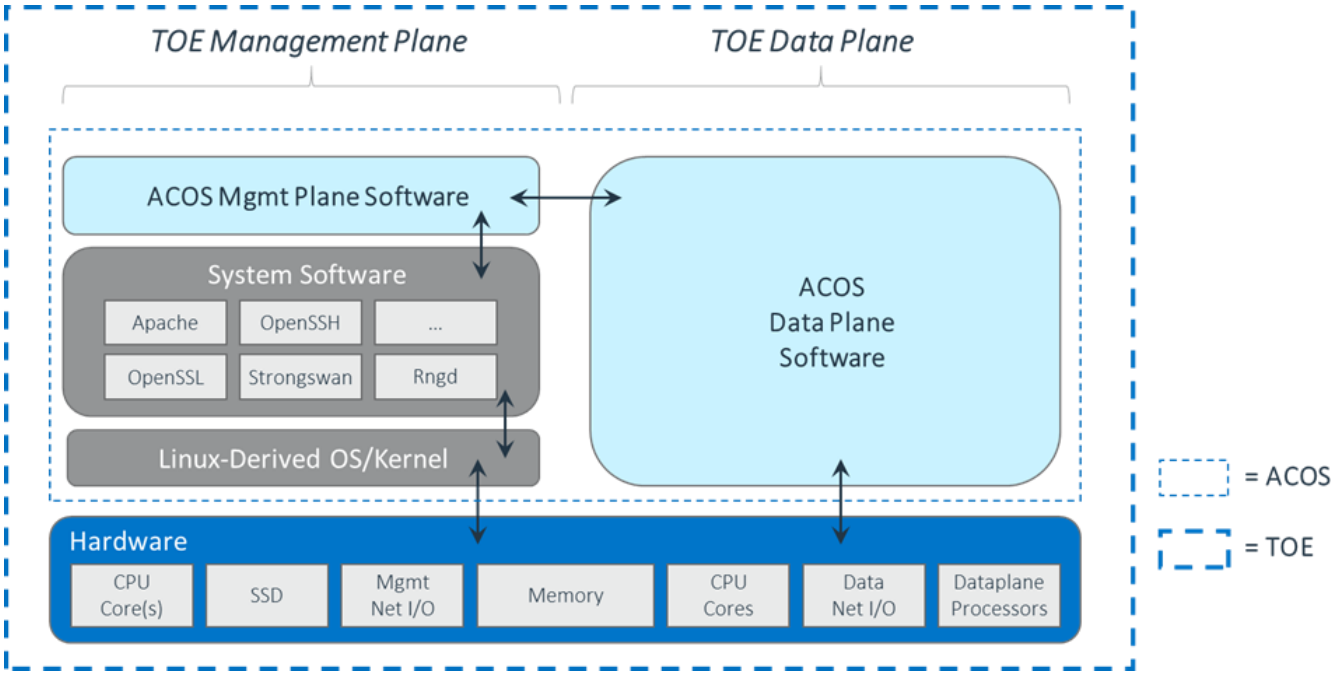

Figure 2: TOE Architecture for A10 Thunder-series Appliance

3.1 TOE DESCRIPTION

The TOE is a standalone network device. The hardware and software components of the TOE are enclosed in a metal enclosure which is the physical boundary of the TOE.

The scope of each TOE appliance begins with a hardware appliance having physical connections to the deployed network environment. Within the appliance, ACOS is designed to control and enable access to the available functions (e.g., program execution, device access, facilitate device functions and capabilities). ACOS enforces applicable capability and security policies on network information flowing through the appliance.

By their nature TOE appliances are administratively closed systems, providing access only through ACOS defined interfaces (e.g., CLI and Web GUI) to administrators configured in ACOS for this purpose. TOE appliances do not expose OS Shell access to administrators.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces. The appliance processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the data plane packets being forwarded out of the device over another interface. The TOE will process control and management plane packets destined for the TOE based on the requirements of the given protocol (e.g., IPSec, OSPF, etc).

3.2 TOE EVALUATED CONFIGURATION

The evaluated configuration consists of the hardware and software listed below, when configured in accordance with the documentation specified in section 6. The TOE is the A10 Networks Thunder Series devices running ACOS 5.2.1-P3 including the following models:

- A10 Thunder TH-4435
- A10 Thunder TH-5840-11
- A10 Thunder TH-7445
- A10 Thunder TH-7650-11
- A10 Thunder TH-7655

The TOE models differ primarily in physical form factor, number and types of connections, and relative performance. Though there are functional differences between these models, they all provide the same security characteristics claimed in this security target.

3.3 TOE PHYSICAL SCOPE

Each TOE appliance runs a version of the A10 Networks Advanced Core Operating System (ACOS) software and has physical network connections to its operational environment to facilitate application delivery, converged networking, and application security services for network traffic. The TOE appliance also provides interfaces necessary for the TOE system.

The TOE may be accessed and managed from a terminal directly connected to its local console or remotely from SSH terminals or web browsers.

The TOE has limited audit log storage space. Accordingly, the TOE can be configured to forward its audit records to an external syslog servers in the TOE's operational environment. In the evaluated configuration, ACOS supports authentication locally managed on the TOE.

4. SECURITY POLICY

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management

5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 SECURITY AUDIT

The TOE generates auditable events for actions on the TOE with the capability of selective audit record generation. The records of these events can be viewed within the Command Line Interface (CLI), web Graphic User Interface (GUI), or they can be exported to audit log servers in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. All administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

4.2 CRYPTOGRAPHIC SUPPORT

The TOE has CAVP-tested algorithms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec.

The TOE uses NIST SP 800-90 DRBG random bits generator and the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC to secure trusted channel and trusted path communication. The TOE zeroizes Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

4.3 IDENTIFICATION AND AUTHENTICATION

The TOE provides Identification and Authentication security functionality to ensure that all administrators are properly identified and authenticated before accessing TOE functionality. The TOE displays a configurable access banner and enforces a local password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login.

The TOE provides the ability to both assign attributes (administrator names, passwords, permitted interfaces, and privilege levels) and to authenticate users against these attributes. The TOE supports x509 certificates and Pre-Shared Keys to securely establish IPsec tunnels for management access to the TOE, and performs certificate status verification using Certificate Revocation Lists (CRLs) and the OCSP protocol.

4.4 SECURITY MANAGEMENT

The TOE provides Command Line Interface (CLI) commands and web Graphic User Interface (GUI) opreations to perform the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of read-only and read+write privileges assigned to TOE administrators. Read-only administrators can display information and perform basic tasks such as pings and traceroutes. Read+write administrators can add, modify, and delete configuration of the TOE. All read-write administrators are considered Security Administrators of the TOE

4.5 PROTECTION OF THE TSF

Internal testing of the TOE hardware, firmware, and firmware updates against tampering ensures that all security functions are running and available before the TOE accepts any communications. The TSF prevents reading of pre-shared keys, symmetric keys, private keys, and passwords. The TOE uses electronic signature verification before any firmware updates are installed.

4.6 TOE ACCESS

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.7 TRUSTED PATH/CHANNELS

The TOE protects interactive access with remote administrators using IPsec to support secure communications for to the TOE's CLI and web GUI Interfaces. The TOE also protects exchanges over trusted channels using IPsec to secure communications with Syslog audit, NTP, and file servers in the TOE's operational environment.

5. ASSUMPTIONS & CLARIFICATION OF SCOPE

5.1 ASSUMPTIONS

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

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.2 CLARIFICATION OF SCOPE

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

The following networking services, capabilities, and functions, while included in the product, were not tested during the TOE’s evaluation.

- Application Delivery Control (ADC),
- Carrier-Grade Networking (CGN),
- Convergent Firewall (CFW), and
- SSL Insight (SSLi)

The TOE also interfaces with the following non-TOE systems in its operational environment.

- Local and remote administrative interfaces,
- Syslog server interface for external audit log storage,
- Network Time Protocol (NTP) server interface for reliable time information in audit records,
- File server interface for trusted updates and configuration backups, and
- Certification Authority (CA) server

6. DOCUMENTATION

The following documents were available with the TOE for evaluation:

- A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Common Criteria Configuration Guide, January 25, 2023.

7. IT PRODUCT TESTING

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP22e) for A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3, Version 1.0, January 25, 2023 (AAR).

7.1 DEVELOPER TESTING

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

7.2 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team verified the product according to the Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in Section 5.5 of the AAR.

8. EVALUATED CONFIGURATION

The evaluated configuration is A10 Thunder Series Appliances with ACOS 5.2.1-P3. The Target of Evaluation (TOE) includes the following hardware models: TH-4435, TH-5840-11, TH-7445, TH-7650-11, and TH-7655. The models run the same firmware image.

To use the product in the evaluated configuration, the product must be configured as specified in the following documents.

- A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Common Criteria Configuration Guide, January 25, 2023

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 ETR.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5.

9.1 EVALUATION OF THE SECURITY TARGET (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the A10 Networks Thunder Series Appliances products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 THE DEVELOPMENT (ADV)

The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

The validator 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.

9.3 EVALUATION OF THE GUIDANCE DOCUMENTS (AGD)

The evaluation team applied each AGD CEM work units. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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.

9.4 EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE)

The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 VULNERABILITY ASSESSMENT ACTIVITY (VAN)

The evaluation team performed a public search for vulnerabilities at the following sites and did not discover any public issues with the TOE. The evaluator searched the following sources for vulnerabilities:

https://web.nvd.nist.gov/view/vuln/search

http://cve.mitre.org/cve/

https://www.cvedetails.com/vulnerability-search.php

http://www.kb.cert.org/vuls/html/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

The terms used for the search on 1/10/2023 were as follows:

Application Delivery Controller, Carrier Grade NAT, A10 Networks, A10 Thunder, TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655, ACOS, IPsec , IKE, NTP v.4, Xeon E5-2680v2, Xeon E5-2695v4, Xeon Gold 6258R, TCP, CentOS 7-9.2009, Apache HTTPD 2.4.46, OpenSSL 1.0.2k, Strongswan 5.0.4, NTP 4.2.6p5 and OpenSSH 7.4p1.

The validator 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.

9.7 SUMMARY OF EVALUATION RESULTS

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

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

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 A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Common Criteria Configuration Guide, January 25, 2023. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11. ANNEXES

Not applicable

12. SECURITY TARGET

The Security Target is identified as: *A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Security Target, Version 1.0, January 25, 2023*.

13 . GLOSSARY

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

BIBLIOGRAPHY

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

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

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

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 (CPP_ND_V2.1),

[5] A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3 Security Target, Version 1.0, January 25, 2023. (ST)

[6] Assurance Activity Report (NDcPP22e) for A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3, Version 1.0, January 25, 2023 (AAR)

[7] Detailed Report (NDcPP22e) for A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3, Version 1.1, January 26, 2023 (DTR)

[8] Evaluation Technical Report for A10 Networks Thunder Series Appliances TH-4435, TH-5840-11, TH-7445, TH-7650-11, TH-7655 with ACOS 5.2.1-P3, version 1.,1 January 26, 2023 (ETR)