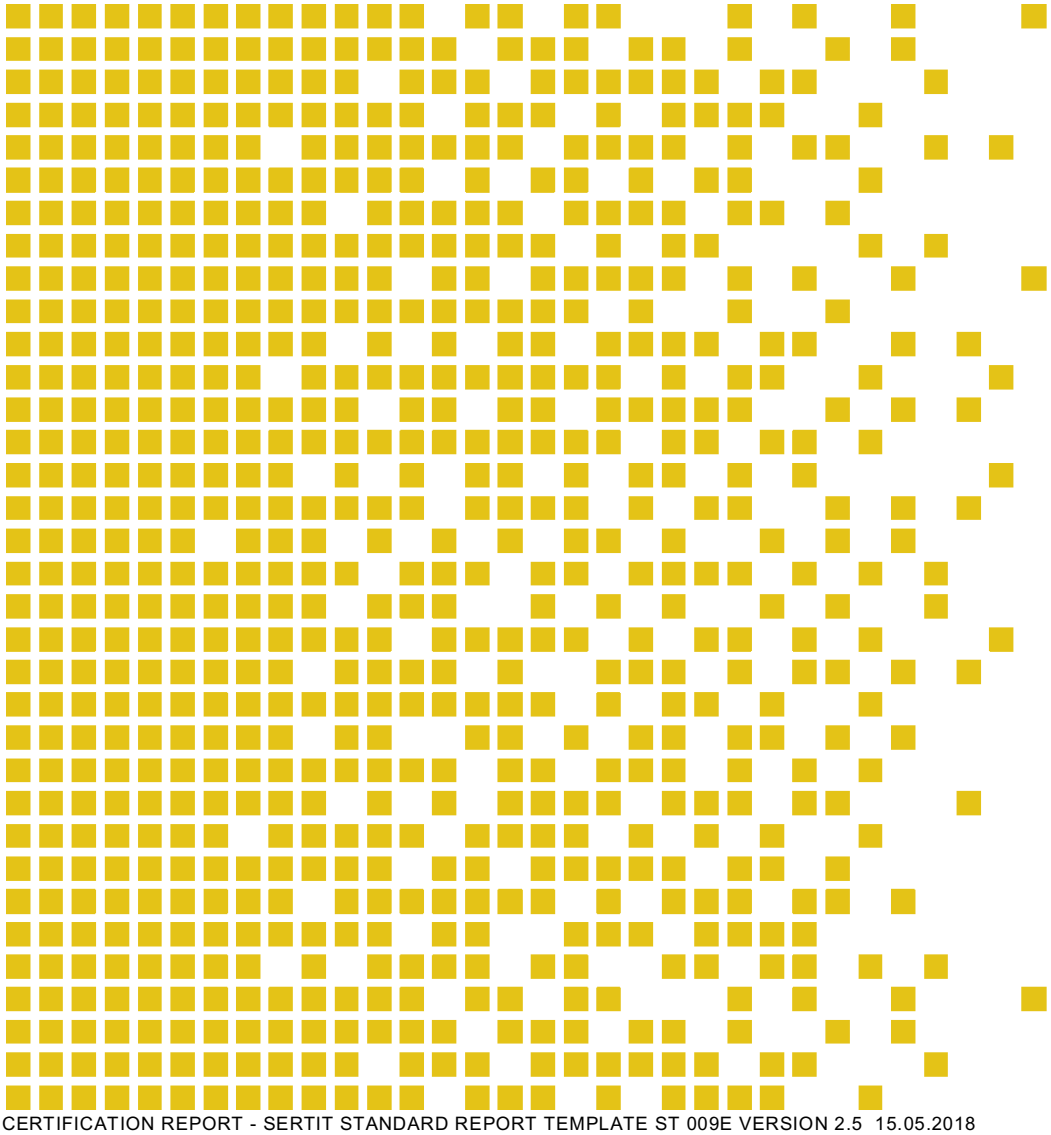
SERTIT-107 CR Certification Report

Issue 1.0 02 July 2018

Expiry date 02 July 2023

A10 Networks Thunder TPS 14045



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

Contents

1 Certification Statement

A10 Networks Thunder TPS is a line of Threat Protection Systems that provides high-performance, network-wide protection against distributed denial of service (DDoS) attacks, and enables service availability against a variety of volumetric, protocol, resource and other sophisticated application attacks. The Thunder TPS product line is built upon A10's Advanced Core Operating System (ACOS) platform, with A10's Symmetric Scalable Multi-Core Processing (SSMP) software architecture that delivers high performance and leverages a shared memory architecture to provide efficient tracking of network flows, as well as accurate DDoS protection enforcement for service providers, Web site operators and enterprises.

A10 Networks Thunder TPS 14045 with firmware version 3.2.2-P5 has been evaluated under the terms of the Norwegian Certification Authority for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Certification team	Arne Høye Rage, SERTIT Kjartan Jæger Kvassnes, SERTIT
Date approved	02 July 2018
Expiry date	02 July 2023

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[2] CCRA (2017), *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[7] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[8] A10 Thunder TPS Security Target Version 1.5, 26 June 2018.

[9] Evaluation Technical Report for the evaluation project SERTIT-107 Common Criteria Evaluation of A10 Thunder TPS issue 1.3, 20 June 2018.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of A10 Networks Thunder TPS 14045 to the developer, A10 Networks, Inc. and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the ST[8] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated was A10 Networks Thunder TPS 14045. Firmware version 3.2.2-P5.

This product is also described in this report as the Target of Evaluation (TOE). The developer was A10 Networks, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The scope of the evaluation includes firmware and hardware that form the TOE and the TOE security functions that are stated in Section 7.1 of the Security Target [8].

4.4 Protection Profile Conformance

The ST[8] did not claim conformance to any protection profile/cPP.

4.5 Assurance Level

The ST[8] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 2 augmented with ALC_FLR.1 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

P.PATCH The patch policy for the TOE environment must be sufficient for stopping all known, publicly available vulnerabilities in the TOE environment software.

P .AUDIT To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained and reviewed.

P .SECURE_MANAGEMENT The TOE shall provide management means for the authorised administrator to manage the TOE in a secure manner.

4.7 Security Claims

The ST[8] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

TT.TAMPERING The TOE may be subject to physical attack that may compromise information and data processing.

TT.MALFUNCTION The TOE may malfunction which may compromise information and data processing.

TT.BYPASSING Bypassing of a security mechanism may compromise information and data processing in the TOE.

TT.MISCONFIG Misconfiguration of TOE, making the TOE inoperable.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

A.PHYSICAL_SECURITY The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.

A.SECURITY_MAINTENANCE When the internal network environment changes due to change in the network configuration, host increase/ decrease and service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.

A.TRUSTED_ADMIN The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

4.11 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[1]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information

Technology Security, CCRA[7], and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[8], which prospective consumers are advised to read. To ensure that the ST[8] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[5].

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[9] to SERTIT in 20 June 2018. SERTIT then produced this Certification Report.

4.12 General Points

The evaluation addressed the security functionality claimed in the ST[8] with reference to the assumed operating environment specified by the ST[8]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.1.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the ST[8]. The results of this work were reported in the ETR[9] under the CC Part 3[4] headings. The following sections note considerations that are of particular

relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The developer ships products using Shipping boxes with sealed tape.

HTTPS cryptographic signatures are used to verify the integrity of the firmware upon electronic transfer of firmware.

The access to the firmware downloads is controlled, and the corresponding mechanism uses user name and password. Users registered to Support Web Portal and selected user id and password.

The firmware downloads are encrypted by an HTTPS session. Self-Signed Certificate is used for software distribution

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the guidance documents provided by the developer. See Annex A.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE’s security functions.

5.5 Vulnerability Analysis

The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. They conducted a search of ST, guidance documents, functional specification, TOE design and security architecture description to identify possible vulnerabilities.

Potential vulnerabilities have been identified and analyzed.

Penetration tests have been created and performed by the evaluators.

The conclusion is that the TOE is not vulnerable and the TOE is resistant to attackers possessing Basic attack potential per requirements of EAL2.

5.6 Developer's Tests

The evaluators have examined the test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE and on any test equipment being used, as well as information about how to execute the tests. This information is detailed enough to ensure that the test configuration is reproducible

5.7 Evaluators' Tests

For sampling of the developers test the evaluators have employed a combination of a random sampling method and a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible.

The evaluators checked that the actual test results are consistent with the expeted test results that were specified by the developer.

For independent testing the evaluators have employed a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. We took into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests.

The evaluators conducted testing and recorded the results. All results were consistent with expected result and of passing grade.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[9], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that A10 Networks Thunder TPS version 14045 with firmware version 3.2.2-P5 meet the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of A10 Networks Thunder TPS version 14045 should understand the specific scope of the certification by reading this report in conjunction with the ST[8]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST[8].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

A10 Networks Thunder TPS 14045. Firmware version 3.2.2-P5.

TOE Documentation

The supporting guidance documents evaluated were:

[a] A10 Thunder TPS Security Target, Version: 1.4

[b] DDoS Mitigation Guide, Thunder Series TPS ACOS 3.2.1, 26 July 2016

[c] System Configuration and Administration Guide A10, Thunder Series TPS ACOS 3.2.1, 25 July 2016

[d] Graphical User Interface Guide, A10 Thunder Series TPS ACOS 3.1.1, 28 January 2015

[e] ACOS 3.2.1 aXAPIv3 Reference Document

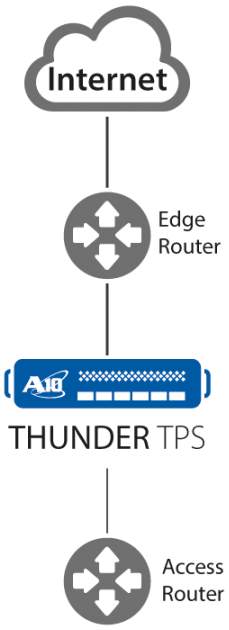
[f] Network Configuration Guide, A10 Thunder Series TPS ACOS 3.2.1, 25 July 2016

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

The following configuration was used for testing:

Symmetric mode:



Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Certificate Identifier: SERTIT-107 C

Product Name: A10 Networks Thunder TPS 14045

Version and Release Numbers: HW:14045-TPS, FW: 3.2.2-P5

Type of Product: Network Device

Product Manufacturer: A10 Networks, Inc.

Assurance Type: EAL 2 augmented with ALC_FLR.1

Evaluation Criteria: Common Criteria Version 3.1 Revision 5

Name of IT Security Evaluation Facility: Advanced Data Security

Name of Validation Body and Certification Authority: SERTIT

Certification Report Identifier: SERTIT-107 CR, issue 1.0, 02 July 2018

Certificate Issued Date: 02. July 2018 Certificate Expiry Date: 02. July 2023

Arne Høye Rage
Certifier

Kjartan Kvassnes
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CC Recognition Arrangement
for cPPs or components up to
EAL 2 and ALC_FLR