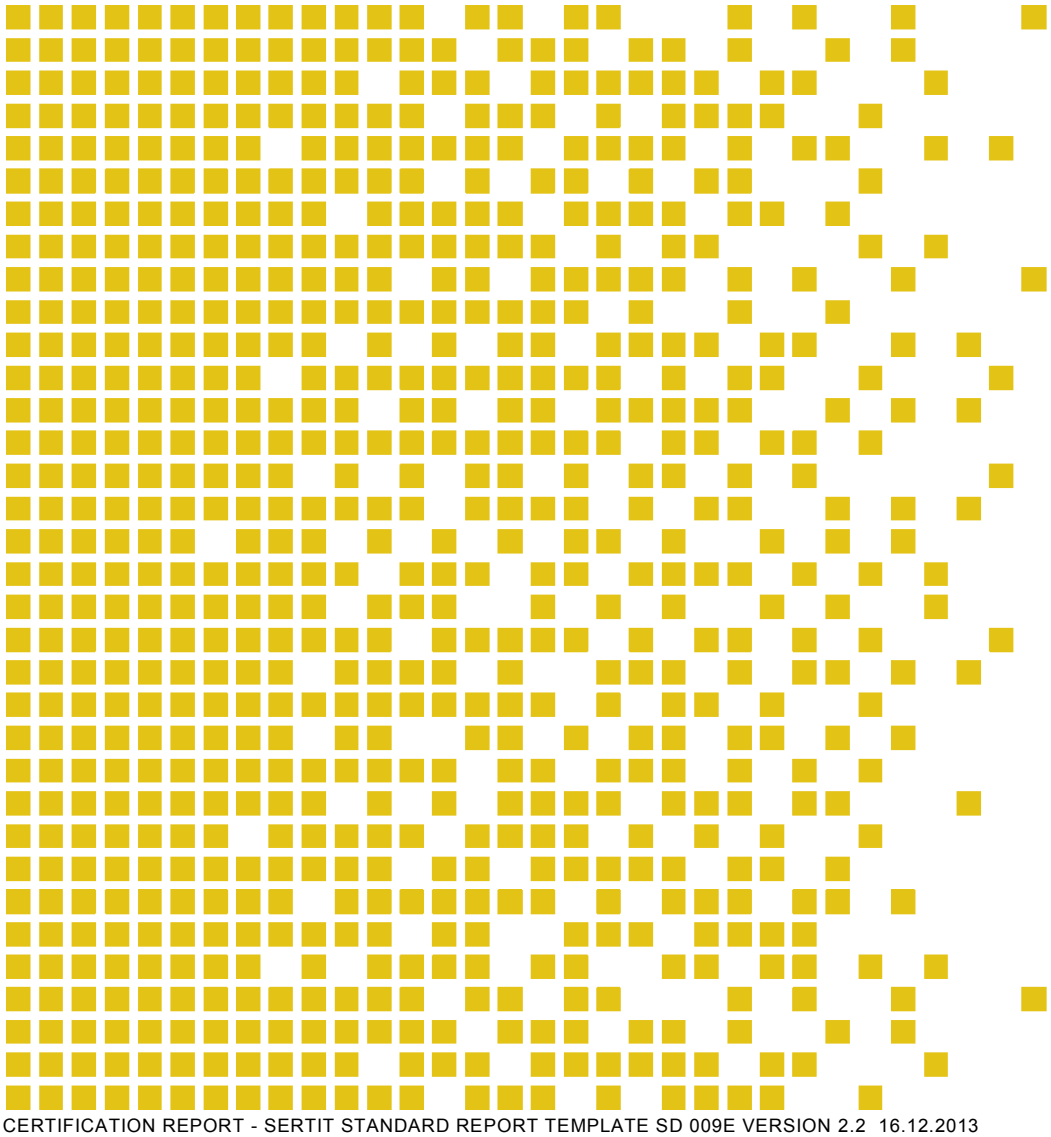
SERTIT-062 CR Certification Report

Issue 1.0 29 June 2017

A10 Networks Thunder TPS 4435S, 5435S and 6435S



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

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 Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

Contents

1 Certification Statement

A10 Networks Thunder TPS 4435S, 5435S and 6435S with firmware version 3.2.2-P1 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant 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.

Author	Arne Høye Rage Certifier
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance
Approved	Kristian Steinfeldt Bae Head of SERTIT
Date approved	29 June 2017

2 Abbreviations

ACOS	Advanced Core Operating System
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
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FIPS 140-2	Federal Information Processing Standards
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ISO/IEC 15408	Information technology – Security techniques - Evaluation criteria for IT security
IP	Internet Protocol
ISP	Internet Service Provider
OSP	Organisational Security Policy
SERTIT	Norwegian Certification Authority for IT Security
SFP	Security Function Policy
SLB	Server Load Balancing
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TPS	Threat Protection System
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

3 References

[1] Security Target for A10 Networks Thunder TPS, v.1.5, 01 June 2017.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] ETR for the evaluation project SERTIT-062, v.1.1, 01 June 2017.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of A10 Networks Thunder TPS 4435S, 5435S and 6435S 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 Security Target[1] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The versions of the product evaluated were A10 Networks Thunder TPS 4435S, 5435S and 6435S.The firmware version is 3.2.2-P1.

These products are also described in this report as the Target of Evaluation (TOE). The developer was A10 Networks, Inc.

A10 Networks' Thunder TPS provides high-speed monitoring and scrubbing of client-server traffic. The TOE provides network-wide protection against distributed denial of service (DDoS) attacks to prevent services from being unavailable. The TOE is a hardware device. The hardware and firmware components of the TOE are enclosed in a metal enclosure which is the physical boundary of the TOE.

The TOE are devices with the same security functionality, but with different performance parameters.

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 the Section 7.1 of the Security Target[1] for Thunder TPS.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] 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 Organisational Security Policies

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 Security Target[1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter and security functional components and security functions to elaborate the objectives. 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.BYPASS 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 Security Objectives for the TOE

O.ID_AUTH The administrator roles must identify and authenticate to the TOE prior to getting access to the functions and data.

O.ACCESS The TOE must allow only authorized administrators to access the system.

O.AUDIT The TOE shall record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data

O.DATA_PROTECTION The TOE shall protect TSF data stored in the TOE from unauthorized exposure, modification and deletion.

O.INTEGRITY The TOE must ensure the integrity of all system data.

O.MANAGEMENT The TOE shall provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.

O.SELF_TEST DDoS Mitigation configurable rate interval shall be tested.

4.12 Security Objectives for the operational environment

OE.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.

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

OE.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.

OE.TIME_STAMP The TOE shall accurately record the security related events by using the reliable time stamps provided by the TOE operational environment.

4.13 Security Functional Components

- FAU_GEN.1 Audit data generation
- FAU_SAR.1 Audit review
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access
- FDP_IFC.2 Complete information flow control
- FDP_IFF.1 Simple security attributes

- FIA_ATD.1 User attribute definition
- FIA_UAU.1 Timing of authentication
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps
- FPT_TST.1 TSF Testing

4.14 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[5]. 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), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] 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)[6].

SERTIT monitored the evaluation which was carried out by the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 01 June 2017. SERTIT then produced this Certification Report.

4.15 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. 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

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR 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 all documents that comprise the administrator guidance, user guidance and installation guide provided by the developer.

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. Developers should 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. The evaluators have searched for potential vulnerabilities and penetration tests have been devised and performed based on this search.

After the completion of the penetration test the evaluators have not found any exploitable vulnerabilities or residual vulnerabilities in the TOE and the conclusion is that the TOE is resistant to attackers possessing Basic attack potential.

5.6 Developer's Tests

The evaluators have examined the developers 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.

5.7 Evaluators' Tests

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 evaluator´s sample represent 30% of the developer´s test,

For independent testing the evaluators devised a set of tests based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. They 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.

To devise a test subset, they used augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that A10 Networks Thunder TPS 4435S, 5435S and 6435S with firmware version 3.2.2-P1 meet the 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 4435S, 5435S and 6435S should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with several environmental considerations as specified in the Security Target.

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.

The above “Evaluation Findings” include several recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

A10 Networks Thunder TPS 4435S, 5435S and 6435S with firmware version 3.2.2-P1.

TOE Documentation

The supporting guidance documents evaluated were:

a) Security Target for A10 Networks Thunder TPS, v.1.5, 01 June 2017
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: