Certification Report

EAL 4+ (ALC_FLR.1) Evaluation of

EPATİ BİLİŞİM TEK. SAN. TİC. LTD. ŞTİ.

Antikor Next Generation Firewall Management v2

2.0.1188

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00/TSE-CCCS-85

TABLE OF CONTENTS

TABLE OF CONTENTS 2
DOCUMENT INFORMATION....3
DOCUMENT CHANGE LOG 3
DISCLAIMER 3
FOREWORD 4
RECOGNITION OF THE CERTIFICATE....5
1 EXECUTIVE SUMMARY 6
2 CERTIFICATION RESULTS....8
2.1 IDENTIFICATION OF TARGET OF EVALUATION 8
2.2 SECURITY POLICY 9
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 9
2.4 ARCHITECTURAL INFORMATION 10
2.5 DOCUMENTATION 10
2.6 IT PRODUCT TESTING 10
2.7 EVALUATED CONFIGURATION....11
2.8 RESULTS OF THE EVALUATION 12
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS 12
3 SECURITY TARGET....14
4 GLOSSARY 14
5 BIBLIOGRAPHY....15
6 ANNEXES....15

Document Information

Date of Issue	10.04.2023
Approval Date	17.04.2023
Certification Report Number	21.0.03/23-002
Sponsor and Developer	*Epati Bilişim Tek. San. Tic. Ltd. Şti.*
Evaluation Facility	*Beam Teknoloji A.Ş.*
TOE Name	*Antikor Next Generation Firewall Management v2 2.0.1188*
Pages	15

Prepared by *(Common Criteria Expert)*	*Mehmet Kürşad ÜNAL, Barış UÇAR(Candidate Expert)*
Reviewed by *(Reviewer)*	*Merve Hatice KARATAŞ*

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	**10.04.2023**	**All**	**First Release**

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product/PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product/PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCTL is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by *BEAM TEKNOLOJİ A.Ş.*, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product/PP means that such product/PP meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target/PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product/PP should also review the security target/PP document in order to understand any assumptions made in the course of evaluations, the environment where the IT product/PP will run, security requirements of the IT product/PP and the level of assurance provided by the product/PP.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for *Antikor Next Generation Firewall Management v2 2.0.1188* whose evaluation was completed on 17.03.2023 and whose evaluation technical report was drawn up by 17.03.2023 (as CCTL), and with the Security Target with version no 0.25 of the relevant product.

The certification report, certificate of product/PP evaluation and security target/PP document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including *EAL2*. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: *Antikor Next Generation Firewall Management v2*

IT Product version: *2.0.1188*

Developer's Name: *Epati Bilişim Tek. San. Tic. Ltd. Şti.*

Name of CCTL: *Beam Teknoloji A.Ş.*

Assurance Package: *EAL 4+ (ALC_FLR.1)*

Completion date of evaluation: *17.03.2023*

1.1. Brief Description

TOE is a Next-Generation Unified Threat Management (UTM) firewall management software solution. By offering a simplified interface and workflow to the security capabilities of its environment, the program creates a security suite on top of the operating system facilities and networking applications.

1.2. Major Security Features

The TOE provides the following security services;

- Security Audit,
- Identification and Authentication,
- User Data Protection,
- Security Management,
- TOE Access,
- Trusted Path/Channels

1.3. Threats

The threats are;

- T.UNAUTH: Gain unauthorized access to the TOE data.
- T.DOS: Make the service provided by the TOE or the TOE itself unusable or inaccessible for a period of time to a specific user or all users.
- T.CHANNEL: Gain the valuable information (passwords and enterprise data) of authorized administrators.
- T.BRUTE: Repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
- T.WEAKNESS: Exploit a weakness of the protocol used and gain access to the TOE in order to read, modify or destroy TSF data.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00/TSE-CCCS-85
TOE Name and Version	*Antikor Next Generation Firewall Management v2 2.0.1188*
Security Target Title	*Antikor Next Generation Firewall Management v2 Security Target*
Security Target Version	*0.25*
Security Target Date	*17.03.2023*
Assurance Level	*EAL 4+(ALC_FLR.1)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017*
Protection Profile Conformance	None
Sponsor and Developer	*Epati Bilişim Tek. San. Tic. Ltd. Şti.*
Evaluation Facility	*Beam Teknoloji A.Ş.*
Certification Scheme	TSE CCCS

2.2 Security Policy

Organizational Security Policies presented at the Security Target are;

- P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.
- P.PW_CONFIDENTIALITY: The TOE shouldn't store any plain-text passwords, but only the hashes, and must use the hashes of the passwords to authenticate, which are not available to the TOE users by any means.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

- A.ADMIN: It is assumed that authorized administrator who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experienced, trained and meet the security conditions.
- A.PROTECT: Each appliance configuration is securely managed by authorized people to provide protection of secured data in terms of its confidentiality and integrity.
- A.CONFW: The management interface can be accessed through a browser or console port. Physical access to the console port should be restricted.
- A.TSP: The IT environment provides reliable time stamps.
- A.PROT: The connections between the network components (*) around the TOE are protected by cryptographic transforms. (Mostly asymmetric encryption is used.)The IT environment provides a hashing function algorithm, whose vulnerability is unknown, for passwords.
- A.AUDIT: The IT environment provides a logging server where logs are kept and a means to present a readable view of the audit data.

2.4 Architectural Information

The TOE runs on a NanoBSD distribution of FreeBSD. The operating system, hardware and connected network devices (switch, hub, access point) are not part of the TOE. License Manager and ACL providers are operated by the vendor and are also not part of the TOE.

2.5 Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
Antikor Next Generation Firewall Management v2 Security Target	*V0.25*	*17.03.2023*
Antikor v2 Kullanma Kılavuzu	*V0.5*	*12.12.2022*
Antikor v2 Kurulum Kılavuzu	*V0.3*	*12.12.2022*

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of Antikor Next Generation Firewall Management v2 2.0.1188.

It is concluded that the TOE supports EAL 4+ (ALC_FLR.1). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

2.6.1.Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 12 functional tests in total.

2.6.2 Evaluator Testing

- Independent Testing: Evaluator has chosen 9 developer tests to conduct by itself. Additionally, evaluator has prepared 13 independent tests. TOE has passed all 22 functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 19 penetration tests have been conducted.

2.7 Evaluated Configuration

The evaluated TOE configuration is composed of;

- Antikor Next Generation Firewall Management v2 2.0.1188,
- Guidance Documents

Also Firmware/Hardware/Software requirements for the TOE are;

- 8 Core Xeon CPU,
- 32 GB DDR4 2133 Mhz RAM,
- Multi-queue Ethernet card,
- 256GB SSD disk,
- A typical workstation with a modern web browser and an local console client installed,
- Operating System: FreeBSD 13.1
- Database: PostgreSQL 14.5

2.8 Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.1

Assurance Class	Component	Component Title
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
	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_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent testing - sample
Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_FLR.1) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “Antikor Next Generation Firewall Management v2 2.0.1188”, the results of the assessment of all evaluation tasks are “Pass”.

2.9 Evaluator Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: *Antikor Next Generation Firewall Management v2 Security Target*

Version: *v0.25*

Date of Document: *17.03.2023*

4 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

DOS: Denial of Service

ITCD: Information Technologies Test and Certification Department

EAL : Evaluation Assurance Level

NTP: Network Time Protocol

OSP : Organisational Security Policy

PP : Protection Profile

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

UTM: Unified Threat Management

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017,

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017,

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017,

[4] Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017,

[6] BTTM-CCE-072 ETR v.3.2 Antikor Next Generation Firewall Management v2 2.0.1188, March 17th 2023

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.