Certification Report

EAL 4+ (ALC_FLR.2) Evaluation of

Comodo Yazılım A.Ş.

Korugan UTM v1.10

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-38

TABLE OF CONTENTS

Document Information

Date of Issue	***19.04.2017***
Approval Date	***20.04.2017***
Certification Report Number	***21.0.03/17-001***
Sponsor and Developer	***Comodo Yazılım A.Ş.***
Evaluation Lab	***BEAM Teknoloji A.Ş.***
TOE	***Korugan UTM v1.10***
Pages	***15***

Prepared by	***Halime Eda BİTLİSLİ***
Reviewed by	***İbrahim Halil KIRMIZI***

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
1.0	***19.04.2017***	***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 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. 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 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 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.

CCEF 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 CCEF 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 Teknoloji A.Ş. which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target 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 should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Korugan UTM v1.10 whose evaluation was completed on 19.04.2017 and whose evaluation technical report was drawn up by BEAM Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 1.2 of the relevant product.

The certification report, certificate of product evaluation and security target 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 EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org

1. *EXECUTIVE SUMMARY*

Evaluated IT product name: Korugan UTM
IT Product version: v1.10
Developer's Name: Comodo Yazılım A.Ş.
Name of CCTL: BEAM Teknoloji A.Ş.
Assurance Package: EAL 4+ (ALC_FLR.2)
Completion date of evaluation: 19.04.2017

TOE is a management software collection over a web interface that provides mechanisms for management and monitoring of packet filtering, authentication, authorization, access control management, data flow control and policy, web and shell based management user interface, and audit records generation and collection.

1.1 Required non-TOE hardware/software/firmware

Software, hardware environment of the TOE are described below.

- Software environment of TOE

TOE runs on a customized operating system. Operating system is a customized version of open source Linux distribution Cent OS 6 or higher.

- Hardware Environment of TOE

TOE runs on all versions of KORUGAN compliant hardware and on virtual appliances, with the following minimum requirements and equivalent/more performant hardware.

- Intel® AtomTM processor E3815 (Codenamed "Bay Trail")
- 4GB CF Type 2 Storage
- 2 GB RAM
- 4 x Intel GbE LAN ports without Bypass

The hardware must be compatible with the Linux distribution used for deployment

- 2 x USB 2.0 Port
- 1 x CF socket
- 1 x RJ-45 Port
- 100-240AC Power supply

1.2 Main Security Features

- **ACCESS CONTROL MANAGEMENT**
  The Korugan provides a role-based access control capability to ensure that only authorized administrators are able to administer the Korugan UTM unit.

- **AUTHENTICATION**
  Korugan enables configuration and management over username and password mechanism for identification and authentication and authorization.

- **DATA FLOW CONTROL AND POLICY**
  Korugan enables configuration of stateful traffic inspection firewall, i.e. inbound and outbound data flow is adherent to a arbitrarily set of rules defined by an authorized administrator over management interface. The default policy is default-deny unless configured to act else and can be configured.

- **LOGGING**
  Korugan enables management of log generation and collection operations on both TOE and non-TOE components.

- **POLICY VIOLATION LOGS**
  TOE collects and sends data for further processing in order to identify policy violation issues.

- **AUTHORIZATION**
  The TOE verifies the identification information of an administrator provided by the environment (application) before any management function can be performed.

1.3 Threats

- **T.REPLAY**
  An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.

- **T.REPEAT**
  An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

- **T.WEAKNESS**
  A user might gain access to the TOE in order to read, modify or destroy TSF data by sending IP packets to the TOE and exploiting a weakness of the protocol used. This attack may happen from outside and inside the protected network. A user might also try to access sensitive data of the TOE via web management interface.

- **T.AUDACC**
  Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

- **T.NOAUTH**
  An unauthorized person may attempt to bypass the security of the TOE so as to access and use security function and/or non-security functions provided by the TOE.

- **T.SELPRO**
  An unauthorized person may read, modify, or destroy security critical TOE configuration data.

- **T.BYPASS**
  A user might attempt to bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected networks. e. g., a user might send non-permissible data through the TOE in order to gain access to resources in protected networks by sending IP packets to circumvent filters. This attack may happen from outside the protected network.

- **T.USAGE**
  The TOE may be inadvertently delivered, configured, used and administered in an insecure manner by authorized persons.

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-38
TOE Name and Version	Korugan UTM v1.10
Security Target Title	Korugan UTM Security Target
Security Target Version	v1.2
Security Target Date	18.04.2017
Assurance Level	EAL 4+ (ALC_FLR.2)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012, conformant
Sponsor and Developer	Comodo Yazılım A.Ş.
Evaluation Facility	BEAM Teknoloji A.Ş.
Certification Scheme	TSE-CCCS

2.2 Security Policy

Organizational Security Policies are;

❖ **P.GENPUR**

There shall be no use of general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on platforms where TOE runs.

❖ **P.PUBLIC**

The platforms where TOE runs shall not host public data. Databases or other company related information that may be accessed from internal or external network, which is publicly available to remote applications, shall not be stored on platforms where TOE runs.

❖ **P.SINGEN**

Network infrastructure shall be configured such that all the information between internal networks, external networks and DMZ pass through the gateway configured by the TOE.

2.3 Assumptions and Clarification of Scope

❖ **A.CORRECT**

The platform, where management interface runs, correctly transmits the information to the administrator’s web browser and receives the information correctly, which is sent to it by the server.

❖ **A.NOEVIL**

All authorized administrators are non-hostile, well trained and knows and follow the existing documentation of the TOE. However administrators are capable of error.
The administrator is responsible for the secure operation of the TOE.

❖ **A.PHYSEC**

TOE is physically secure and controlled environment.
It is assumed that:

- There are no physical attacks on platforms
- Physical access right is granted only to authorized administrators.
- TOE shall only be accessed and managed from a Secure Environment using a computer system without known malware infection.
- The administrator handles the authentication secrets with care, specifically that he will keep them secret and can use it in a way that nobody else can read it.

❖ **A.SECINIT**

The TOE is securely initialized, i.e. that the initialization is done according the procedure described in the documentation.

❖ **A.INFLOW**

No information can flow between internal, DMZ and external networks unless it passes through the TOE.

❖ **A.CONFW**

The network components (TOE and application) are configured in a secure manner. Specifically it is assumed that no incoming connections are accepted except protected data (e. g. SSL) from the management interface.

- **A.TSP**
  The IT environment provides reliable timestamps (NTP server).

- **A.PROT**
  The data flow between the management machine and the network components is protected by cryptographic transforms (e. g. SSL authorization and SSL transport protection).

- **A.AUDIT**
  The IT environment provides a Syslog server and a means to present a readable view of the audit data or an external log application is available as a means to present human readable view of audit data

2.4 Architectural Information

TOE is used for monitoring and managing the network traffic policies between two different networks. TOE functions by configuring the information flow policy, network address translation and routing mechanisms of the security gateway of the network. According to policy specified by TOE, packet filter component of TOE denies or accepts the transmitted data to guard internal network.

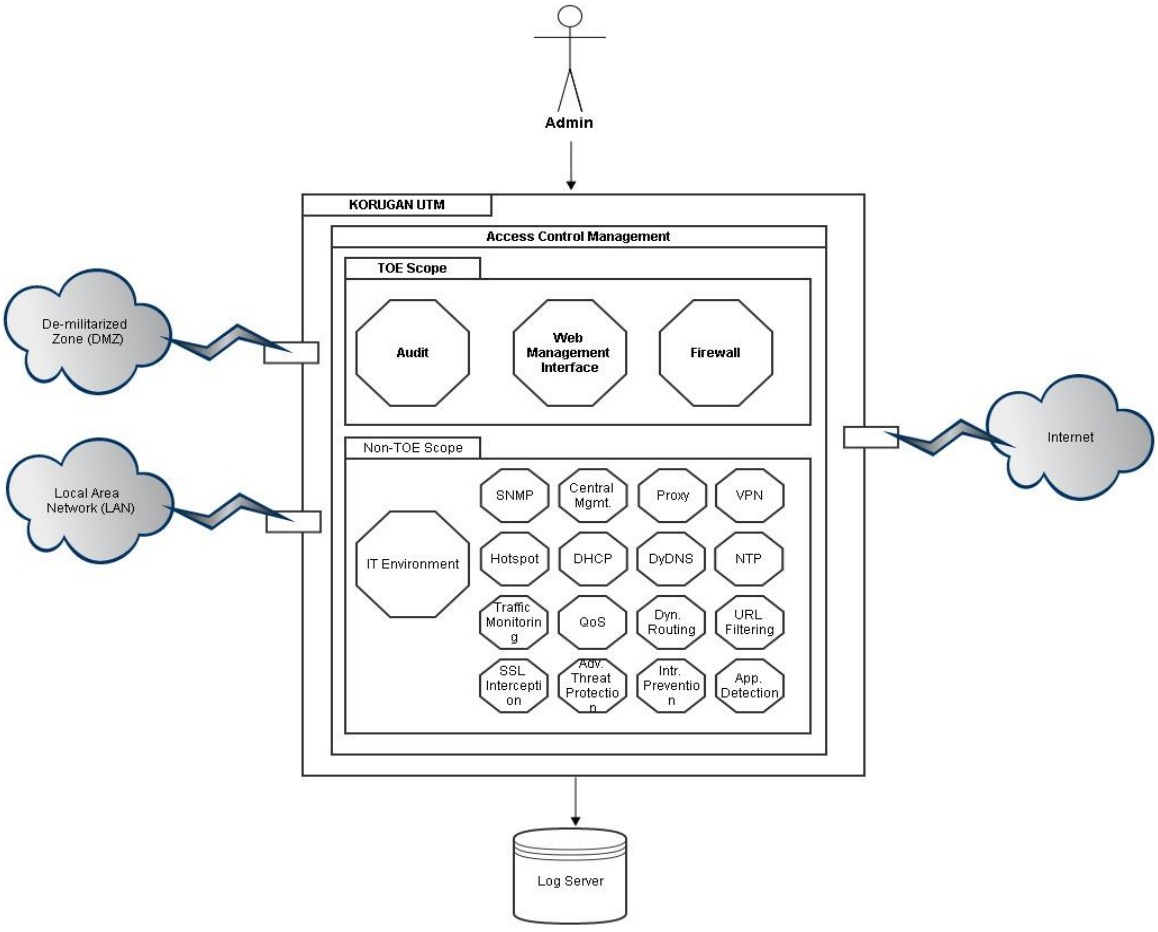

Figure 1: Physical and Logical scope of the TOE

Korugan UTM consists of three main subsystems which are Firewall (Netfilter), Web Management Interface and Audit / System Logging (syslog-ng). Physical and Logical scope of the TOE is shown in Figure 1.

2.5 Documentation

Name of Document	Version Number	Date
COMODO KORUGAN UTM Security Target	v.1.2	18.04.2017
Comodo Korugan UTM Admin Guide	v1.10	18.04.2017

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 Korugan UTM v1.10

It is concluded that the TOE supports EAL 4+ (ALC_FLR.2). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly described in two parts:

2.6.1 Developer Testing

Developer has done total of 147 functional tests via Testrail test scenario management software tool. Test scenarios provided by developer covers all TSFI's of the TOE. Also Korugan Test Plan document includes required information about developer's testing strategy, test environment, used testing tools, etc

2.6.2 Evaluator Testing

Independent Testing: Evaluator has done total of 29 test. 12 of them were selected from developer's tests. The other 17 of them were evaluator's independent tests.

Penetration Testing: Evaluator has done 38 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes. Potential vulnerabilities and penetration tests are defined in "Vulnerability Analysis Report".

2.7 Evaluated Configuration

Name of Document	Version Number	Publication Date
COMODO KORUGAN Security Target	1.2	18.04.2017
GL423-COMODO-ANK-DEV-Functional Specifications	1.8	13.02.2017
GL427-COMODO-ANK-DEV-Security Architecture-	1.5	08.09.2016
GL425-COMODO-ANK-DEV-Low Level Design	1.5	28.12.2016
CUTM_Admin_Guide	1.10	18.04.2017
GL003-COMODO-ANK - CMP@Comodo TR - Configuration Management Process	1.1	07.10.2013
Comodo Korugan Test Planı	1.4	18.04.2017
Comodo Korugan Test Dokümantasyonu	1.9	26.12.2016
BTTM-CCE-002 ZAR	1.2	03.03.2017

2.8 Results of the Evaluation

Table 2 above 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.2

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	Sufficiency of Security Measures

	ALC_FLR.2	Flaw Reporting Procedures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-defined Development Tools
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: Security Enforcing Modules
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.3	Focused vulnerability analysis

Table 2 – Security Assurance Requirements of TOE

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 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 “Korugan UTM v1.10” the results of the assessment of all evaluation tasks are “Pass”.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “Korugan UTM v1.10” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

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

Title: Korugan UTM Security Target
Version: 1.2
Date of Document: 18.04.2017

A public version has been created and verified according to ST-Santizing:

Title: Korugan UTM Security Target Lite
Version: 1.2L2F
Date of Document: 18.04.2017

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTTM-CCE-002 DTR v.2.0.3

[4] COMODO KORUGAN Security Target v.1.2

6 ANNEXES

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