# Comodo Yazılım A.Ş.

## Comodo Korugan UTM 1.10
## Security Target Lite

**COMODO YAZILIM A.Ş.**

# List of Tables


.

## List of Figures

# Table of Contents

# 1. SECURITY TARGET INTRODUCTION

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Specifies the ST conventions,
- Defines the terminology and acronyms used in the ST,
- Defines TOE overview and TOE description.

## 1.1 ST Reference and TOE Reference

| | |
|---|---|
| **ST Title:** | Comodo Korugan UTM 1.10 Security Target Lite |
| **ST Version:** | v1.2L2F (GL-000-COMODO-ANK -Güvenlik Hedefi-Internet-v1.2L2F) |
| **TOE Identification:** | Korugan UTM v1.10 |
| **CC Identification:** | Common Criteria for Information Technology Security Evaluations, version 3.1R4 |
| **Technical References** | |
| **Keywords:** | |

**Table 1 ST and TOE References**

## 1.2 Document Conventions, Terminology & Acronyms

This section specifies the formatting information used in the ST.

### 1.2.1 Conventions

In this Security Target some notations and conventions which are taken from the Common Criteria v3.1R4 have been used in order to guide to the reader.

During the specification of the functional requirements under the Section 6, the functional components are interpreted according to the “assignment” and “selection” operations.

The outcome of the assignment operations are shown with underlined identified between “[brackets]”.

The outcome of the selection operations are shown with **bold** and **italic** and identified between “***[brackets]***”.

Iterated functional requirement components are shown with a “**/IDENTIFIER”** for the components which used more than once with varying operations.

Refinements on requirements are indicated by underlined text for additions or strikethrough text for deleted items, e.g. ~~deletion~~ addition

Under the term “**Application Note**”, an informal explanation added under some of the functional requirements in order to highlight or to describe the component in detail.

### 1.2.2 Terminology

The following terminology is used in this Security Target:

### 1.2.3 Acronyms

CC : Common Criteria
CCMB : Common Criteria Management Board
CCMC : Common Criteria Management Committee
CLI : Command Line Interface

| | |
|---|---|
| DMZ | : De-Militarized Zone |
| EAL | : Evaluation Assurance Level (defined in CC) |
| LAN | : Local Area Network |
| IT | : Information Technology |
| NTP | : Network Time Protocol |
| NIC | : Network Interface Card |
| OSP | : Organizational Security Policy |
| PP | : Protection Profile |
| SAR | : Security Assurance Requirements |
| SFP | : Security Function Policy |
| SFR | : Security Functional Requirements |
| SSH | : Secure Shell |
| ST | : Security Target |
| TOE | : Target of Evaluation |
| TSF | : TOE Security Functionality (defined in CC) |
| TSE | : Turkish Standards Institution (Türk Standartları Enstitüsü) |
| UTM | : Unified Threat Management |
| VPN | : Virtual Private Network |

## 1.3 TOE Overview

### 1.3.1 General overview of the TOE and related components

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.

### 1.3.2 Required non-TOE hardware/software/firmware

Software, hardware environment of the TOE are described below.

#### 1.3.2.1 Software environment of TOE

TOE runs on a customized operating system. Operating system is a customized version of open source Linux distribution.

#### 1.3.2.2 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® processor
- 4GB 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 RJ-45 Port
- 100-240AC Power supply

### 1.3.3 Major security and functional features

The functional and major security features of the TOE are described below.

#### 1.3.3.1 TOE functional features

| Feature | Description |
|---|---|
| **Network Console** | Korugan enables configuration and management capabilities via a text-based Network CLI interface. |
| **WebGUI** | Korugan enables configuration and management capability of multiple functions including management of filter rules and related configuration data over network Web-Based GUI, accessed via HTTPS, for system management and configuration. |

**Table 2 Functional features of TOE**

#### 1.3.3.2 TOE major security features

| Feature | Description |
|---|---|
| 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 |

**Table 3 Major Security Features of TOE**

### 1.3.4 TOE Type

TOE is a packet filter functionality bundled with a management software collection serving over a web interface. Web interface of TOE provides mechanisms for management and monitoring of authentication, authorization, access control management, network console, data flow control and policy by packet filtering and policy violation logs

### 1.3.5 TOE Description

#### 1.3.5.1 Physical Scope

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. Internal network carries the data to be protected from the external network. External network may have malicious users or software as its users.

Two internal networks are represented with DMZ and Internal Network. In addition there is an external network. As an example, TOE protects Internal and DMZ from threats originating from external network by properly configuring the gateway between them.

- Internet
- Local Area Network (LAN)
- Demilitarized Zone (DMZ)

Physical and Logical scope of the TOE is shown in Figure 1.

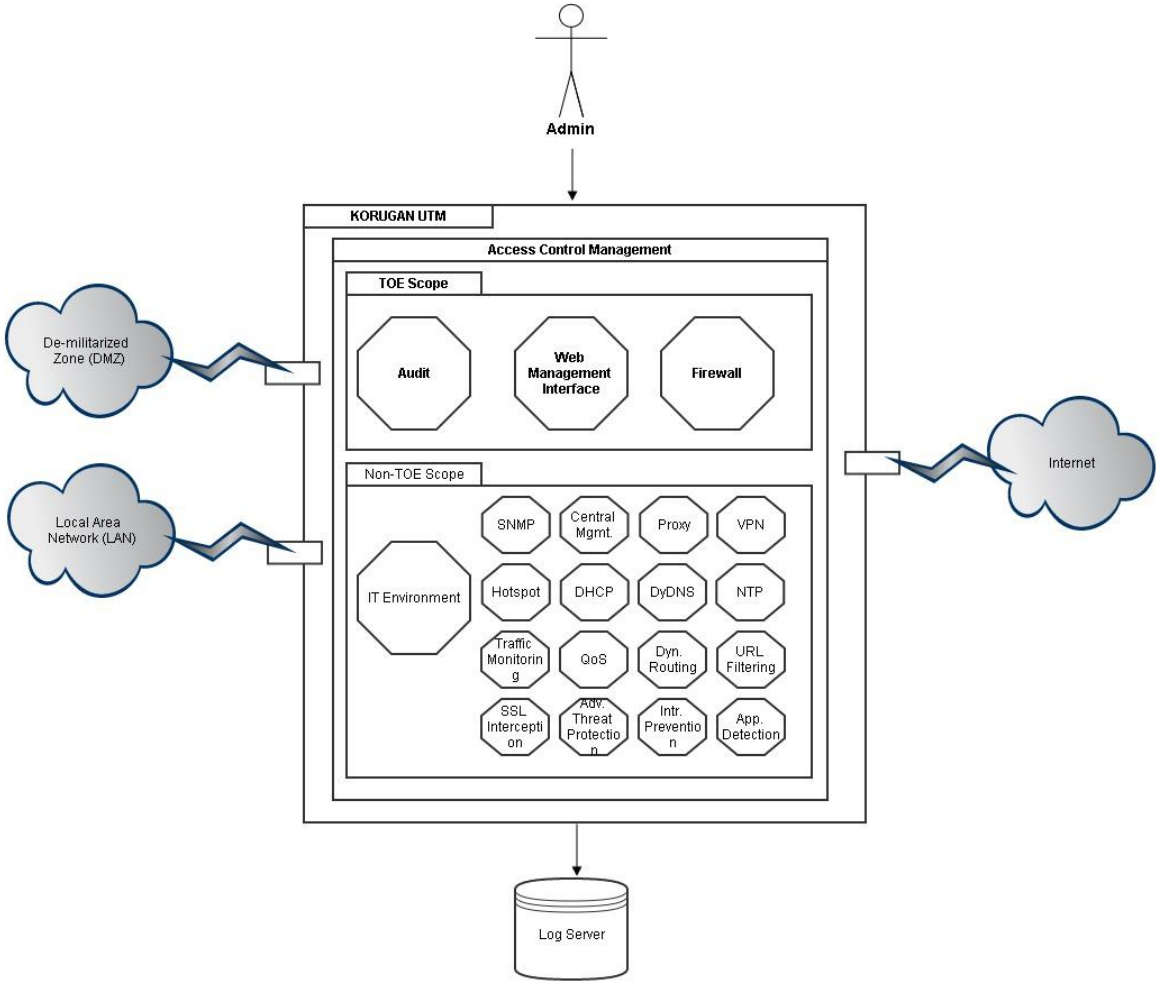


**Figure 1: Physical and Logical scope of the TOE**

SECURE ENVIRONMENT: Environment which is probably the server room of the company or institution. Authorized company personnel may access this room but they may be unauthorized to use TOE, which means that they may not be authorized administrators of the TOE. System administrator use administrator workstation in secure environment to use TOE. TOE may be accessed from web browsers over secured channel.
Demilitarized Zone is a special intra network, which has server systems on it and it must be protected from other networks. These servers are servicing both the internet and the intranet for different purposes.

### 1.3.5.2 Logical Scope

TOE includes following features:

#### 1.3.5.2.1 Information Flow Management

All policies, which control the information flow between internal network and external network, are managed by TOE components. These policies are related with IP packet filtering, IP routing, network address translation and port address translation.
Nodes in the external and internal network may be subject to firewall rules that are specific to their IP addresses. TOE administrator specifies these rules.

1.3.5.2.2 Access Control Management

Access control feature enables authorized administrators to manage firewall rules applied to information flow and control traffic between different network domains that are configured by TOE.

1.3.5.2.3 Audit Logging Management

System logs are generated by TOE and non-TOE components and TOE collects audit data to forward external logging service consumers such as log management and correlation tools.
Generated log types are:

- System management logs.
- System Activity Logs
- Information flow logs
- Operational logs
- Policy Violation Logs

1.3.5.2.4 Management Interface

Korugan UTM Management Interface is able to configure management functions:

- Modification of network traffic filter rules
- Modification of configuration data

TOE is used by TOE administrators to first authenticate them to TOE and then administer it in same secure environment. They can change access rules, manage packet filtering and packet-filtering policies.

### 1.3.5.3 Components Out of TOE Scope:

Listed components below are out of TOE scope:

- SNMP
- Central Management
- Proxy
- VPN
- Hotspot
- DHCP Server
- Dynamic DNS
- Time Server
- Traffic Monitoring
- Quality of Service
- Dynamic Routing

- URL Filtering
- SSL Interception
- Advanced Threat Protection
- Intrusion Prevention
- Application Detection
- SSH Console

# 2. CONFORMANCE CLAIM

## 2.1 CC Conformance Claim

This Security Target claims conformance to:

- 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,

As follows;

- Part 2 conformant,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
- CCMC, ST sanitizing for publication, CCDB-2006-04-004, Version 1.0, April 2006

has to be taken into account.

## 2.2 PP and Package Claim

### 2.2.1 Protection Profile (PP) Claim

This Security Target does neither claim conformance to a Protection Profile.

### 2.2.2 Package Claim

This Security Target is conformant to the following security requirements package:

- Assurance package EAL4 augmented by ALC_FLR.2 to CC, part 3.

ALC_FLR.2 adds flaw reporting procedures to the assurance package EAL4.

## 2.3 Conformance Claim Rationale

As this Security Target does neither claim conformance to a Protection Profile nor to a security requirement package, a conformance claim rationale is not necessary.

# 3. SECURITY PROBLEM DEFINITION

This chapter introduces the security problem definition of the TOE. This comprises:

- The **assets** which have to be protected by the TOE.
- The **external entities** which are interacting with the TOE.
- The **assumptions** which have to be made about the environment of the TOE.
- The **threats** which exist against the assets of the TOE
- The **organizational security policies** (OSP) the TOE has to comply to.

## 3.1 Assets

| Asset | Description and Examples |
|---|---|
| **TSF Data (on TOE)** | TSF data stored on the TOE which are necessary for its own operation.<br>• User Credentials<br>• Access Rights of Users and Role Definitions<br>• Configuration Data of provided services stored<br>• Packet filter rules |
| **Resources** | The resources in the connected networks that the TOE components are supposed to protect. The resources are outside the TOE components |
| **Generated Logs** | Generated logs of user activity regarding TOE.<br>• Logs involving configuration data<br>• Logs involving data passing over TOE. |

**Table 4 Assets using TOE resources**

## 3.2 External Entities

- **User:** Users are clients of TOE, having their traffic passed over and managed by TOE with active configuration.
- **Administrator:** Administrators are the people who are authorized to perform different configuration actions on TOE. Administrators can either be regular or super (root) administrators.
- **Attacker:** Attackers, either insider or outsider, performs malicious actions on either TOE or legitimate users served by TOE to gain unauthorized access and execute arbitrary actions.

## 3.3 Threats

Threats averted by TOE and its environment are described in this section. Threats described below results from assets which are protected or stored by TOE or from usage of TOE with its environment.

Either the TOE or the IT environment addresses the following threats.

### 3.3.1 Threats addressed by the TOE

Possible threat agents considered for TOE are unauthorized persons or external IT entities, which are not authorized to use TOE. Threat agents are considered independent entities with a low level of attack sophistication, which are not able to perform organized attacks on TOE.

| | |
|---|---|
| **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. |

**Table 5 Threats addressed by TOE only**

### 3.3.2 Threats met by the TOE and TOE Security Environment

The following threats are met by TOE and TOE Security Environment together.

| | |
|---|---|
| **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. |

**Table 6 Threats met by TOE and TOE Security Environment**

### 3.3.3 Threat to be addressed by TOE Security Environment

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

**Table 7 Threats Addressed by TOE Security Environment**

## 3.4 Organizational Security Policies (OSP)

The following security policies shall be applied by the organization hosting the TOE.

| | |
|---|---|
| **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 |

**Table 8 Organizational Security Policies for TOE Environment**

## 3.5 Assumptions

The following conditions are assumed to exist in the operational environment.

| | |
|---|---|
| **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.<br>The administrator is responsible for the secure operation of the TOE |
| **A.PHYSEC** | TOE is physically secure and controlled environment.<br>It is assumed that:<br>• There are no physical attacks on platforms<br>• Physical access right is granted only to authorized administrators.<br>• TOE shall only be accessed and managed from a Secure Environment using a computer system without known malware infection.<br>• 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 |

**Table 9 Operational Environment Assumptions for TOE**

# 4. SECURITY OBJECTIVES

This chapter describes security objectives for the TOE and its environment.

## 4.1 Security Objectives for the TOE

Following objectives shall be met by TOE. These are objectives, which shall be satisfied without imposing technical requirements on the TOE. The following conditions are assumed to exist in the operational environment.
The following are the environmental security objectives for the TOE:

| | |
|---|---|
| **O.IDAUTH** | The TOE must uniquely identify and authenticate the claimed identity all users, before granting a user access to TOE functions. |
| **O.SECFUN** | The TOE must provide functionality that enables an authorized administrator and authorized super administrator to use the TOE security functions which he is authorized to use, and must ensure that only authorized administrators and authorized super administrators are able to access that authorized functionality. |
| **O.LIMEXT** | The TOE must provide the means for an authorized administrator and authorized super administrator to control and limit access to TOE security functions by an authorized external IT entity |
| **O.SELPRO** | The TOE must protect itself by configuring the IT environment, against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. |
| **O.AUDREC** | The TOE must provide a means to access the record of readable audit trail of security related events stored either in an external system or in operating environment, with accurate dates and times, and TOE must provide means to search the audit trail based on relevant attributes using operating environment capabilities. |
| **O.ACCOUN** | The TOE must provide a means to establish user accountability for information flow through the operating environment. The TOE must generate user accountability information for authorized administrator and authorized super administrator, for their use of security functions related to audit. |
| **O.MANAGEMENT** | The TOE verifies the identification information of an administrator provided by the environment (application) before any management function can be performed. The TOE must provide the necessary management functions in order to modify the configuration data or the traffic filter rules. |
| **O.FILTER** | The TOE must filter the incoming and the outgoing data traffic of all data between all connected networks according to the rule sets. |

**Table 10 Environmental Security Objectives for TOE**

## 4.2 Security Objectives for the Operational Environment

Following objectives shall be met by TOE environment. These are objectives, which shall be satisfied without imposing technical requirements on the TOE.
The following conditions are assumed to exist in the operational environment.

| | |
|---|---|
| **OE.SELPRO** | The operating environment must protect itself and TOE, against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions or security functions provided by operating environment itself. |
| **OE.AUDREC** | The operating environment must provide an interface to TOE to record a readable audit trail of security related events, with accurate dates and times, and an interface to search the audit trail based on relevant attributes. |
| **OE.ACCOUN** | The operating environment must provide user accountability for information flows through the operating environment and for authorized administrator and authorized super administrator use of security functions related to audit. |
| **OE.ENV** | The TOE is used in a controlled environment. Specifically it is assumed:<br>• That only the administrator gains physical access to the TOE,<br>• That the administrator handles the authentication secrets (see O.IDAUTH) with care, specifically that he will keep them secret and can use it in a way that nobody else can read it. |
| **OE.NOEVIL** | The administrators and authorized super administrator of the TOE shall be non-hostile, well trained and has to know the existing documentation of the TOE.<br>The administrators are responsible for the secure operation of the TOE.<br>They shall behave in a correct manner and they shall not aim to attack TOE by any means. |
| **OE.SECINIT** | The TOE is securely initialized, i.e. that the initialization is done according the procedure described in the documentation |
| **OE.INFLOW** | The administrator must assure that the packet filter components provide the only connection for the different networks. |
| **OE.CONFW** | The network components (TOE and application) must be configured to accept only protected data (e. g. SSL) from the management machine. |
| **OE.TSP** | The IT environment provides reliable timestamps (NTP server) |
| **OE.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 |
| **OE.AUDIT** | The IT environment provides a Syslog server and a means to present a readable view of the audit data. |
| **OE.CORRECT** | The server, where management server runs, shall correctly transmit the information to the server over secured channel privacy and integrity and receive the information correctly, which is sent to it by the server from the same secure channel. If there is a physical malfunction or a problem in establishing a secure channel, software would not behave as correctly. |
| **OE.PHYSEC** | TOE, administrative and non-administrative environmental units (except monitor, keyboard and mouse) where server application is running shall be kept in a physically secure environment. Web client connection should be established over secure channel assuring privacy and integrity of transmission. TOE shall be protected from physical attacks by authorized administrator and authorized super administrator. |
| **OE.GENPUR** | TOE Environment shall not have general-purpose computing capabilities, which allow installation of non-TOE related software, which may endanger the |

| | |
|---|---|
| | operation of TOE by preventing trusted execution of the TSF"s. |
| **OE.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 due to threats that can be introduced by access of remote users or applications to TOE hosting platforms. |
| **OE.SINGEN** | TOE shall be installed according to the following defined firewall architectures.<br>These are bastion host, screened host, multi-homed and screened subnet with n-tier architectures. These architectures ensure that the configured gateway by the TOE is the single point that data must flow through. There must not be covert channels that data can flow from external to internal network or in the opposite direction. |
| **OE.GUIDAN** | The TOE must be delivered, installed, administered, and operated in a manner that maintains security. TOE delivery, installation and administration process shall not be compromised or masqueraded by adversaries. Only authorized entities shall deliver, install and operate TOE. |
| **OE.ADMTRA** | Authorized administrators are trained about the establishment and maintenance of security policies and practices. TOE administrators shall be trained before TOE installation and operation. They shall be informed of all possible configurations and made aware of the network security concepts before operating the TOE. Trainings shall be long enough to cover all topics of the administrative guidance documents. |

**Table 11 Operational Environment Security Objectives**

## 4.3 Security Objective Rationale

Table provides security problem definition covered by security objectives. Threats and OSPs are addressed by security objectives of the TOE and TOE's environment.

| | OE.SELPRO | OE.AUDREC | OE.ACCOUN | OE.ENV | OE.NOEVIL | OE.SECINIT | OE.INFLOW | OE.CONFW | OE.TSP | OE.PROT | OE.AUDIT | OE.CORRECT | OE.PHYSEC | OE.GENPUR | OE.PUBLIC | OE.SINGEN | OE.GUIDAN | OE.ADMTRA | O.IDAUTH | O.SECFUN | O.LIMEXT | O.SELPRO | O.AUDREC | O.ACCOUN | O.MANAGEMENT | O.FILTER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A.CORRECT** | | | | | | | | | | | | X | | | | | | | | | | | | | | |
| **A.NOEVIL** | | | | | X | | | | | | | | | | | | | | | | | | | | | |
| **A.PHYSEC** | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| **A.SECINIT** | | | | | | X | | | | | | | | | | | | | | | | | | | | |
| **A.INFLOW** | | | | | | | X | | | | | | | | | | | | | | | | | | | |
| **A.CONFW** | | | | | | | | X | | | | | | | | | | | | | | | | | | |
| **A.TSP** | | | | | | | | | X | | | | | | | | | | | | | | | | | |
| **A.PROT** | | | | | | | | | | X | | | | | | | | | | | | | | | | |
| **A.AUDIT** | | | | | | | | | | | X | | | | | | | | | | | | | | | |
| **T.REPLAY** | | | | | | | | | | | | | | | | | | | | **X** | | | | | | |
| **T.REPEAT** | | | | | | | | | | | | | | | | | | | **X** | | | | | | | |
| **T.BYPASS** | | | | **X** | | | **X** | | | **X** | | | | | | | | | | | | | | | | **X** |
| **T.WEAKNESS** | | | | | | | | **X** | | | **X** | | | | | | | | | | | | **X** | | **X** | |
| **T.AUDACC** | | **X** | **X** | | | | | | | | | | | | | | | | | | | | **X** | **X** | | |
| **T.NOAUTH** | **X** | | | | | | | | | | | | | | | | | | **X** | **X** | **X** | | | | | |
| **T.SELPRO** | **X** | | | | | | | | | | | | | | | | | | | **X** | **X** | **X** | | | | |
| **T.USAGE** | | | | | | | | | | | | | | | | | **X** | **X** | | | | | | | | |
| **P.GENPUR** | | | | | | | | | | | | | | **X** | | | | | | | | | | | | |
| **P.PUBLIC** | | | | | | | | | | | | | | | **X** | | | | | | | | | | | |
| **P.SINGEN** | | | | | | | | | | | | | | | | **X** | | | | | | | | | | |

**Table 12 Security Objectives – Assumptions – Threats – Policies Matrix for TOE**

**OE.SELPRO** This environmental security objective is necessary to counter the threats: **T.SELPRO** and **T.NOAUTH**. Operating environment shall protect itself and TOE from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions, in addition to modify configuration in any way by using proper configuration provided by TOE.

**OE.AUDREC** This environmental security objective is necessary to counter the threats: **T.AUDACC**. Operating environment shall provide an interface for TOE to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes to provide accountability and disallow untraceable actions.

**OE.ACCOUN** This environmental security objective is necessary to counter the threat: **T.AUDACC**. Operating environment shall provide user accountability for information flowing through it and for authorized administrator and authorized super administrator use of security functions related to audit. All actions should be accountable and traceable.

**OE.ENV** is necessary to counter the threat **T.BYPASS.** TOE is used in a controlled environment that only the administrator gains physical access to the TOE, administrators handles the authentication secrets and authentication secrets are kept as secret using methods to prevent being revealed.

**OE.NOEVIL** is necessary to cover **A.NOEVIL.** Authorized super administrator and authorized administrators are non-hostile. They shall behave in a correct manner in general, follow guidance and they shall not aim to attack TOE by any means.

**OE.SECINIT** is necessary to cover **A.SECINIT**. The TOE should be securely initialized, the initialization effort is performed according the procedure described in the documentation.

**OE.INFLOW** is necessary to cover **A.INFLOW**. No information flows between the internal and external networks unless it passes through the packet filtering components of TOE

**OE.CONFLOW** is necessary to counter threat **T.WEAKNESS** and necessary to cover **A.CONFLOW**. The network components (TOE and application) are configured to accept only protected data (e. g. SSL) from the management machine and should not be exploited by a protocol weakness.

**OE.TSP** is necessary to cover **A.TSP**. The environment provides reliable timestamps (using services such as NTP server)

**OE.PROT** is necessary to counter the threats **T.BYPASS** and to cover **A.PROT**. The data flow between the management machine and the network components (TOE and service

application) is protected by cryptographic transforms (e. g. SSL authorization and SSL transport protection.

**OE.AUDIT** is necessary to counter the threat **T.WEAKNESS** and to cover **A.AUDIT**. The operational environment provides a Syslog server and a means to present a readable view of the audit data.

**OE.CORRECT** is necessary to cover **A.CORRECT**. The platform, which management interface runs, shall correctly transmit the information to the server by secured link, and transmit all information correctly, which is sent to it by the server from the same secured connection.

**OE.PHYSEC** is necessary to cover **A.PHYSEC.** TOE, administrative and non-administrative environmental units (except monitor, keyboard and mouse) where Korugan UTM Appliance runs should be kept in a physically secure container.

**OE.GENPUR** is necessary to cover **P.GENPUR**. TOE Environment shall not have general-purpose computing capabilities, which allow installation of non-TOE related software, which may endanger the operation of TOE by preventing trusted execution of the TSF' s.

**OE.PUBLIC** This objective is necessary to cover **P.PUBLIC**. The platforms where TOE runs shall not host public data.

**OE.SINGEN** is necessary to cover **P.SINGEN**. Environment of TOE shall be the single point that data must flow through. There must not be covert channels that data can flow from external to internal network or opposite direction.

**OE.GUIDAN** is necessary to counter the threat **T.USAGE**. The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

**OE.ADMTRA** is necessary to counter the threat: **T.USAGE** .Authorized administrators shall be trained as to establishment and maintenance of security policies and practices. TOE administrators shall be trained before TOE installation and operation. They shall be informed of all possible configurations and made aware of the network security concepts before operating the TOE. Trainings shall be long enough to cover all topics of the administrative guidance documents.

**O.IDAUTH** is necessary to counter the threat **T.NOAUTH** and **T.REPEAT** because it requires that users should be uniquely identified and authenticated by TOE before accessing to management functions.

**O.SELPRO** is necessary to counter the threats: **T.SELPRO**. TOE shall protect itself from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

**O.AUDREC** is necessary to counter the threats: **T.AUDACC and T.WEAKNESS**. TOE shall provide a means to record a readable audit trail of security related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. TOE should have audit recording capability to ensure detection of attempts to compromise the fenced network including the network component that includes the TOE

**O.ACCOUN** is necessary to counter the threat: **T.AUDACC**. TOE shall provide user accountability for information flowing through the TOE and for authorized administrator and authorized super administrator use of security functions related to audit.

**O.SECFUN** is necessary to counter the threats: **T.NOAUTH**, **T.REPLAY**, and **T.SELPRO**. TOE shall provide functionality that enables an authorized administrator and authorized super administrator to use the TOE security functions, and must ensure that only authorized administrators and authorized administrator are able to access such functionality.

**O.LIMEXT** is necessary to counter the threats **T.NOAUTH** and **T.SELPRO** because the TOE must provide the means for an authorized administrator and authorized super administrator to control and limit access to TOE security functions by an authorized external IT entity.

**O.MANAGEMENT** is necessary to counter the threat **T.WEAKNESS**. Identification and authorization for an administrator is performed by the environment using given credentials before any management function can be accessed and managed. The TOE must provide sufficient privileges to administrator for necessary management functions in order to modify the configuration data or the traffic filter rules

**O.FILTER** is necessary to counter the threat **T.BYPASS**. TOE checks and filters the incoming and the outgoing data traffic of all data between all connected networks according to the rule sets (policies).

# 5 EXTENDED COMPONENT DEFINITION

This Security Target does not use any components defined as extensions to CC part 2.

# 6 SECURITY REQUIREMENTS

## 6.1 Security Functional Requirements for the TOE

This chapter defines the security functional requirements for the TOE according to the functional requirements components drawn from the CC part 2 version 3.1 revision 4.

### 6.1.1 Overview

The security functional requirements (SFR) for this ST consist of the following components from Part 2 of the CC, summarized in the following table:

| # | Identifier | Name |
|---|---|---|
| 1 | FAU_GEN.1 | Audit data generation |
| 2 | FAU_SAR.1 | Audit review |
| 3 | FAU_SAR.2 | Restricted audit review |
| 4 | FAU_SAR.3 | Selectable audit review |
| 5 | FDP_ACC.1 | Subset access control |
| 6 | FDP_ACF.1 | Security attribute based access control |
| 7 | FDP_IFC.1 | Subset information flow control |
| 8 | FDP_IFF.1 | Simple security attributes |
| 9 | FIA_ATD.1 | User attribute definition |
| 10 | FIA_UAU.2 | User authentication before any action |
| 11 | FIA_UID.2 | User identification before any action |
| 12 | FMT_MOF.1 /SUPERADMINISTRATOR | Management of security functions behavior |
| 13 | FMT_MOF.1 /ADMINISTRATOR | Management of security functions behavior |
| 14 | FMT_MSA.1/ACCESSCONTROL | Management of security attributes |
| 15 | FMT_MSA.1 /PACKETFILTER | Management of security attributes |
| 16 | FMT_MSA.3/ACCESSCONTROL | Static attribute initialization |
| 17 | FMT_MSA.3/PACKETFILTER | Static attribute initialization |
| 18 | FMT_SMF.1 | Specification of Management Functions |
| 19 | FMT_SMR.1 | Security roles |

**Table 13 TOE Security Functional Requirements**

### 6.1.2. Security Function Requirements

#### 6.1.2.1 FAU_GEN.1 Audit data generation

In audit generation, following case is considered:

**Hierarchical to:** No other components.

**Dependencies:** FPT_STM.1 Reliable time stamps

**FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[not specified]*** level of audit; and

c) [Events specified in Table 14 ].

**FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in second column of Table 14].

| Auditable Event | Other Audit Relevant Information |
|---|---|
| **All authentication attempts** | – Submitted user id by the user if authentication is successful,<br>– IP address of the user's host used for connection,<br>– IP address, userid and attempt date-time if authentication is not successful (access control policy violation). |
| **Modifications to the group of users that are part of a role** | User access level change for an authorized administrator, new access level, profile, affected sub-menu name |
| **Firewall policy write** | Policy name, operation type write |
| **Firewall policy removal** | Policy name, operation type remove |
| **Firewall policy installation** | Policy name, operation type install |
| **starting of network components** | Component Name |
| **IP datagrams matching log filters in packet filter rules (network policy violation)** | Description of the packet violating the rules and violated/matched rule id |
| **Enable/Disable actions performed on remote syslog server connection** | Operation type:enable/disable, component name |

**Table 14 Auditable Events by TOE**

### 6.1.2.2 FAU_SAR.1 Audit review

**Hierarchical to:** No other components.
**Dependencies:** FAU_GEN.1 Audit data generation
**FAU_SAR.1.1** The TSF shall provide [authorized administrators and authorized super administrators] with the capability to read [instantly created audit trail data] from the audit records.

**FAU_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### 6.1.2.3 FAU_SAR.2 Restricted audit review

**Hierarchical:** No other components.
**Dependencies:** FAU_SAR.1 Audit review
**FAU_SAR.2.1** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

### 6.1.2.4 FAU_SAR.3 Selectable audit review

**Hierarchical to:** No other components.
**Dependencies:** FAU_SAR.1 Audit review
**FAU_SAR.3.1** The TSF shall provide the ability to apply [filters] of audit data based on:[
a) basic text based filter;]

### 6.1.2.5 FDP_ACC.1 Subset access control

**Hierarchical to:** No other components.
**Dependencies:** FDP_ACF.1 Security attribute based access control
**FDP_ACC.1.1** The TSF shall enforce the [ACCESS CONTROL SFP] on [entities defined inTable 15].

| Entity | Type | Explanation |
|---|---|---|
| **Authorized Super Administrator** | Subject | He/she is the super user entity who has the all of the available rights defined ACCESS CONTROL SFP and |

| | | |
|---|---|---|
| | | can carry out all administrative operations. There is only one predefined authorized super administrator, no more authorized super administrator can be added to system and his/her rights cannot be lessened. This administrator type is also referred to as authorized root administrator interchangeably. |
| **Authorized administrator** | Subject | He/she is the user entity who has restricted rights defined in User Attributes Database. He/she can be configured to have the right to carry out all administrative operations the same as super administrator, however his/her rights are manageable. |
| **TOE Modules** | Object | A TOE module is a group of functions, which is used for a specific task. Each TOE module has a name and this name is used to determine if authorized administrator has access to a TOE module function that manipulates ACCESS CONTROL SFP objects. |
| **User Attribute Database** | Object | User Attribute Database, which stores user id, TOE module name, operation triplet, for each authorized administrator |
| **Firewall Policies** | Object | Firewall Policies are information flow policies saved in the internal format of TOE. Firewall policies are part of Packet Filter SFP. |
| **Firewall Script** | Object | This script is the compiled information flow policies |
| **Interface Script** | Object | Interface script is used to manipulate the TOE's physical and virtual network interface card configuration(s). |
| **Log Agent** | Object | Log agent includes a shell and web based interface used to access audit trail |
| **Power** | Object | Power interface used to shut down or reboot the operating system |
| **Backup Storage** | Object | Backup storage is used to access or restore backups and factory settings. |
| **Date** | Object | Date is used to change system time of operating system, can be interpreted to include not only date but also time and time zone settings in addition to NTP services. |
| **None** | Operation | If a TOE module function can be used by an authorized administrator, who has "none" value, defined in User Attribute Database for that TOE module, using this function is a "none" operation. |
| **Read-Only** | Operation | If a TOE module function can be used by an authorized administrator, who has "read-only" value, defined in User Attribute Database for that TOE module, using this function is a "read-only" operation. |

| | | |
|---|---|---|
| **Read-Write** | Operation | If a TOE module function can be used by an authorized administrator, who has "read-write" value, defined in User Attribute Database for that TOE module, using this function is a "read-write" operation. |

**Table 15 Entities covered by ACCESS CONTROL SFP**

### 6.1.2.6 FDP_ACF.1 Subset Access Control

**Hierarchical to:** No other components
**Dependencies:** FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization
**FDP_ACF.1.1** TSF shall enforce the [ACCESS CONTROL SFP] to objects based on the following :
[Subjects and objects controlled and relevant security attributes defined in Table 16].

| Entity | Relevant Security Attributes |
|---|---|
| Authorized Administrator | One of none, read-write accesses for each TOE module are granted. |
| TOE Modules | Each TOE module requires varying operation accesses to allow use of its various functions depending on the functions nature. |
| User Attribute Database | Reading User Attributes Database requires read-write access for System Users Management Interface module.<br>Adding, removing authorized administrators or changing an authorized administrator's attributes other than passwords requires read-write access for System Users Management Interface module.<br>Changing user password of an authorized administrator other than own password requires read-write access for System Users Management Interface module.<br>Changing own user password of an authorized super administrator requires read-write access for System Users Management Interface module.<br>Changing any password requires current password. |
| Firewall Policies | Accessing and managing firewall policies |

| | |
|---|---|
| | requires read-write access level for Firewall Management Interface Module. |
| FW Script | Executing the FW Script to change information flow control policy on TOE, particularly effecting Firewall subsystem (i.e. Packet Filter, Iptables, NAT, Connection Tracking, Ulogd modules) requires read-write access for Firewall Management Interface Module. Script is implemented to run automatically in policy management page. |
| Interface Script | Executing the Interface Script to change information flow control policy of the gateway, which TOE runs, requires read-write access for Network Interfaces Management Interface module. |
| Log Agent | Reading audit trail via Log Agent requires read-write access for Log Report and Management Interface module. |
| Power | Shutdown and rebooting operating system via power interface requires read-write access for Shutdown Interface module. |
| Backup Storage | Taking backup or restoring backup including restoration of factory settings require read-write access to Backup Interface module. |
| Date | Reading system date requires read-write access for Time Server Interface Module. Changing system date, time zone and NTP settings require read-write access for Time Server Interface module. |

**Table 16 Subjects and objects controlled and relevant security attributes**

**FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) Accessible operation level on an object for subject is determined using the User Attributes Database object. User id of the subject and name of the TOE module, which encapsulates the function that accessing the object, used to find the corresponding operation type.

b) An operation on an object is allowable only if the accessing subject has read-write access for operation on the object.

c) Operation access level order from greater to lesser is read-

write and none.]

**FDP_ACF.1.3** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [
a) Authorized super administrator has access to all objects for all operations ]

**FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[
a) For all objects, operations that require read-write access right are not accessible by the authorized administrators.]

### 6.1.2.7 FDP_IFC.1 Subset Information Flow Control

**Hierarchical to:** No other components.
**Dependencies:** FDP_IFF.1 Simple security attributes
**FDP_IFC.1.1** The TSF shall enforce the [Packet Filter SFP] on [
*Subjects:* users (external entities) that send and/or receive information through the TOE to one another;
*Information:* data sent from one subject through the TOE to one another;
*Operation:* allow/deny/reject the data].

**Application Note:**
The Packet Filter SFP is given in FDP_IFF. The subject definitions are identical to the users defined in the external entities definition in Ch. 3.2

### 6.1.2.8 FDP_IFF.1 Simple Security Attributes

**Hierarchical to:** No other components
**Dependencies:** FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization
**FDP_IFF.1.1** The TSF shall enforce the [Packet Filter SFP] based on the following types of subject and information security attributes: [
*Subjects:* users (external entities) that send and/or receive information through the TOE to one another;
*Subject security attributes:* none;
*Information:* data sent from one subject through the TOE to one another;
*Information security attributes:*

- source address of subject,
- destination address of subject,
- transport layer protocol,
- interface on which the traffic arrives and departs,
- port,
- time

]

**FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [
Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information policy rules].

**FDP_IFF.1.3** The TSF shall enforce the [reassembly of fragmented IP datagrams before inspection].

**FDP_IFF.1.4** The TSF shall explicitly authorize an information flow based on the following rules: [none].

**FDP_IFF.1.5** The TSF shall explicitly deny an information flow based on the following rules: [

a) The TOE shall reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject does not belong to the network associated with the interface (spoofed packets);
b) The TSF shall drop IP datagrams with the source routing option;
c) The TOE shall reject fragmented IP datagrams which cannot be reassembled completely within a bounded interval].

### 6.1.2.9 FIA_ATD.1 User Attribute Definition

**Hierarchical to:** No other components.
**Dependencies:** No dependencies.
**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [

a) username;

b) association of a human user with the authorized administrator role or authorized super administrator role;
c) and an access profile, which identifies the group of access privileges accorded to the user.]

### 6.1.2.10 FIA_UAU.2 User Authentication Before Any Action

**Hierarchical to:** FIA_UAU.1 Timing of authentication
**Dependencies:** FIA_UID.1 Timing of identification
**FIA_UAU.2.1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

### 6.1.2.11 FIA_UID.2 User Identification Before Any Action

**Hierarchical to:** FIA_UID.1 Timing of identification
**Dependencies:** No dependencies.
**FIA_UID.2.1** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### 6.1.2.12 FMT_MOF.1/SUPERADMINISTRATOR Management of Security Functions Behavior

**Hierarchical to:** No other components
**Dependencies:** FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions
**FMT_MOF.1.1** The TSF shall restrict the ability to ***[disable]*** the functions:[
a) Permission to reboot and shutdown;
b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) Create, read, modify, delete user attribute values defined in FIA_ATD.1;
d) Modify and set the time, date, time zone and NTP server settings ;
e) Permission to review the instant audit records;
f) Backup of user attribute values, information flow security policy rules,
g) Recover to the state following the selected backup or factory defaults
h) Modification of modules' configuration data;] *to* [an authorized super administrator].

### 6.1.2.13 FMT_MOF.1/ADMINISTRATOR Management of Security Functions Behavior

**Hierarchical to:** No other components
**Dependencies:** FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions
**FMT_MOF.1.1** The TSF shall restrict the ability to ***[disable, enable]*** the functions:[
a) Permission to reboot and shutdown;
b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) Create, read, modify, delete user attribute values defined in FIA_ATD.1;
d) Modify and set the time, date, time zone and NTP server settings ;
e) Permission to review the instant audit records;
f) Backup of user attribute values, information flow security policy rules,
g) Recover to the state following the selected backup or factory defaults,
h) Modification of modules' configuration data;] *to* [an authorized administrator].

**Application Note:** Difference with previous section: SUPERADMINISTRATOR has naturally have listed all rights described and keep them as inalienable rights, whereas authorized administrators can have a subset of all rights available or not at all.

### 6.1.2.14 FMT_MSA.1/ACCESSCONTROL Management of Security Attributes

| | |
|---|---|
| **Hierarchical to:** | No other components |
| **Dependencies:** | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| **FMT_MSA.1.1** | The TSF shall enforce the [ACCESS CONTROL SFP] to restrict the ability to ***[create, modify, delete, view, backup, recover]*** the security attributes [defined in FIA_ATD.1.1] to the [authorized administrator and authorized super administrator]. |

### 6.1.2.15 FMT_MSA.1/PACKETFILTER Management of Security Attributes

| | |
|---|---|
| **Hierarchical to:** | No other components |
| **Dependencies:** | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| **FMT_MSA.1.1** | The TSF shall enforce the [Packet Filter SFP] to restrict the ability to ***[modify, [no other operations]]*** the security attributes [network traffic filter rules and configuration data] to [authorized administrator and authorized super administrator]. |

### 6.1.2.16 FMT_MSA.3/ACCESSCONTROL Static Attribute Initialization

| | |
|---|---|
| **Hierarchical to:** | No other components |
| **Dependencies:** | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |
| **FMT_MSA.3.1** | The TSF shall enforce the [ACCESS CONTROL SFP] to provide ***[restrictive]*** default values for security attributes (access policy attributes defined in FDP_ACC.1) that are used to enforce the SFP. |
| **FMT_MSA.3.2** | The TSF shall allow the [nobody] to specify alternative initial values to |

override the default values when an object or information is created.

**Application Note:** The default values for the attributes appearing in FDP_ACC.1 are intended to be restrictive in the sense that access denied by the TOE until the default values are modified by an authorized administrator and authorized super administrator. For example, default operation level for created authorized administrator entities is lowest available operation level for all modules, which prevents authorized administrator to do any actions until authorized super administrator grants higher access.

### 6.1.2.17 FMT_MSA.3/PACKETFILTER Static Attribute Initialization

**Hierarchical to:** No other components
**Dependencies:** FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles
**FMT_MSA.3.1** The TSF shall enforce the [Packet Filter SFP] to provide ***[restrictive]*** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2** The TSF shall allow the [no roles] to specify alternative initial values to override the default values when an object or information is created.

### 6.1.2.18 FMT_SMF.1 Specification of Management Functions

**Hierarchical to:** No other components
**Dependencies:** No dependencies.
**FMT_SMF.1.1** The TSF shall be capable of performing the following security management functions: [

a) Reboot and shutdown
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows
c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;
d) modify and set the time, date, time zone and NTP service parameters;
e) review instant audit records;
f) backup of user attribute values, information flow security policy rules and

g) recover to the state either selected backup or factory settings
h) Modification of modules' configuration data ]

#### 6.1.2.19 FMT_SMR.1 Security Roles

**Hierarchical to:** No other components
**Dependencies:** FIA_UID.1 Timing of identification
**FMT_SMR.1.1** The TSF shall maintain the roles [authorized administrator(s) and authorized super administrator].

**FMT_SMR.1.2** The TSF shall be able to associate users with roles.

**Application Note:** authorized administrator role is a generic role for multiple sub-roles, which are managed using group structures named profiles, each of which can have a subset of all available rights on TOE. All rights given to authorized administrators are revocable.. Authorized super administrator is a special user type and sole member of his/her role, which provides full and inalienable rights on actions. Each user is assigned to a profile in user creation.

### 6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are chosen as the predefined assurance package EAL4.

| Assurance Class | Assurance Components | |
|---|---|---|
| ADV: 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 |
| AGD: Guidance documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| ALC 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_FLR.2* | *Flaw Reporting Procedures (not in EAL4, for +)* |
| | ALC_LCD.1 | Developer defined life-cycle model |

| | | |
|---|---|---|
| | ALC_TAT.1 | Well-defined development tools |
| ASE 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 |
| ATE Tests | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.1 | Testing: basic design |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing – sample |
| AVA: Vulnerability assessment | AVA_VAN.3 | Focused vulnerability analysis |

**Table 17 TOE Security Assurance Levels**

## 6.3 Security Requirements Rationale

### 6.3.1 Security Functional Requirements Rationale

Rationale for security TOE functional requirements are shown in Table 18. In this table, security objectives and security functional requirements are cross-linked and their dependency is shown.

| | O.IDAUTH | O.SELPRO | O.AUDREC | O.ACCOUN | O.SECFUN | O.LIMEXT | O.MANAGEMENT | O.FILTER |
|---|---|---|---|---|---|---|---|---|
| **FAU_GEN.1** | | | X | X | | | | |
| **FAU_SAR.1** | | | X | | | | | |
| **FAU_SAR.2** | | | X | | | | | |
| **FAU_SAR.3** | | | X | | | | | |
| **FDP_ACC.1** | | X | | | X | | | |
| **FDP_ACF.1** | | X | | | X | | | |
| **FDP_IFC.1** | | | | | | | | X |
| **FDP_IFF.1** | | | | | | | | X |
| **FIA_ATD.1** | X | | | X | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **FIA_UID.2** | X | X | | | | | X | |
| **FIA_UAU.2** | X | X | | | | | | |
| **FMT_MSA.1 /ACCESSCONTROL** | X | | | | X | | X | |
| **FMT_MSA.1 /PACKETFILTER** | X | | | | | | X | X |
| **FMT_MSA.3 /ACCESSCONTROL** | X | | | | X | | | |
| **FMT_MSA.3 /PACKETFILTER** | X | | | | X | | | X |
| **FMT_MOF.1 /SUPERADMINISTRATOR** | | | | | X | X | | |
| **FMT_MOF.1 /ADMINISTRATOR** | | | | | X | X | | |
| **FMT_SMF.1** | | | | | X | X | X | |
| **FMT_SMR.1** | | | | | X | | X | |

**Table 18 Rationale for TOE Security Functional Requirements**

**FAU_GEN.1 Audit data generation**
This component defines requirements to identify the auditable events for which audit records shall be generated, and the information to be provided in the audit records. O.AUDREC and O.ACCOUN objectives are in the scope of this component.

**FAU_SAR.1 Audit Review**
This component ensures that the audit records are understandable. This component traces back to and helps meeting the objective O.AUDREC.

**FAU_SAR.2 Restricted Audit Review**
This component ensures that audit records are selectable and searchable for only a limited set among all possible users, which are already authorized. This component traces back to and helps meeting the objective O.AUDREC.

**FAU_SAR.3 Selectable Audit Review**
This component ensures that a variety of searches can be performed on the audit records. This component traces back to and aids in meeting the objective O.AUDREC.

**FDP_ACC.1 Subset Access Control**
This exists to define subjects, objects and operations of ACCESS CONTROL SFP. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

**FDP_ACF.1 Security Attribute Based Access Control**

This exists to describe the rules of ACCESS CONTROL SFP. This component traces back to and aids in meeting the objectives O.SELPRO and O.SECFUN.

**FDP_IFC.1 (Subset information flow control) and FDP_IFF.1 (Simple Security Attributes)**

The security objective O.FILTER is met by a combination of FDP_IFC.1, FDP_IFF.1, and FMT_MSA.3/PACKETFILTER. FDP_IFC.1 and FDP_IFF.1 describe the information flow controls and information flow control policy. Together, the SFRs describe how the packet filter information flow policies apply. FMT_MSA.3/PACKETFILTER enforces restrictive attribute initialization.

**FIA_ATD.1 User Attribute Definition**

This component exists to set user attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the objectives O.IDAUTH and O.ACCOUN.

**FIA_UAU.2 User authentication before any action**

This component ensures that users are authenticated before performing any action on behalf of a user; user's identity is authenticated to the TOE. This component traces back to and aids in meeting the objective O.IDAUTH and O.SELPRO.

**FIA_UID.2 User identification before any action**

This component ensures that before anything occurs on behalf of a user, user's identity is identified to the TOE. This component traces back to and aids in meeting the objective O.IDAUTH, O.SELPRO and O.MANAGEMENT

**FMT_MSA.1 Management of Security Attributes (FMT_MSA.1/ACCESSCONTROL)**

This component requires TSF to allow authorized administrators and authorized super administrator to manage the specified security attributes and aided in meeting the objectives O.IDAUTH, O.SECFUN and O.MANAGEMENT.

**FMT_MSA.1 Management of Security Attributes (FMT_MSA.1/PACKETFILTER)**

This component requires TSF to allow authorized administrators and authorized super administrator to manage the specified information flow rules and policies and aided in meeting the objectives O.IDAUTH, O.MANAGEMENT and O.FILTER.

**FMT_MSA.3 Static attribute initialization (FMT_MSA.3/ACCESSCONTROL)**

This component ensures that there is default "none" access level for authorized administrators. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.

**FMT_MSA.3 Static attribute initialization (FMT_MSA.3/PACKETFILTER)**
This component ensures that there is restrictive default deny policy for definition of information flow control policies (Packet Filter SFP). This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SECFUN.
The SFR is therefore sufficient to satisfy the objective O.FILTER and mutually supportive.

**FMT_MOF.1 Management of security functions behavior (FMT_MOF.1/SUPERADMINISTRATOR)**
This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate authorized super administrator related TOE management/administration/security functions. This component traces back to and aids in meeting the objectives O.SECFUN, O.LIMEXT.

**FMT_MOF.1 Management of security functions behavior (FMT_MOF.1/ADMINISTRATOR)**
This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate authorized administrator related TOE management/administration/security functions. This component traces back to and aids in meeting the objectives O.SECFUN, O.LIMEXT

**FMT_SMF.1 Specification of Management Functions**
This component ensures presence of specific management functions provided by TSF and aided in meeting the objectives O.SECFUN and O.LIMEXT and O.MANAGEMENT.

**FMT_SMR.1 Security roles**
Each of the CC class FMT components in this ST is dependent to this component. This component aids in meeting the objectives: O.SECFUN and O.MANAGEMENT.
FMT_SMR.1 requires that the TOE will at least maintain the role authorized administrator(s) grouped under profiles identified by names and authorized super administrator.

### 6.3.2 Rationale for Security Functional Requirements Dependencies

Table 19 shows the TOE Security Functional Requirements and associated dependencies. It also indicates whether the ST explicitly addresses each dependency. Notes are provided for those cases where the dependencies are satisfied by components, which are hierarchical to the specified dependency.

| SFR | Dependencies | Dep. Satisfied? | Notes |
|---|---|---|---|
| **FAU_GEN.1** | FPT_STM.1 | Yes | FPT_STM.1 dependency is satisfied by TOE Security Environment |

| | | | |
|---|---|---|---|
| **FAU_SAR.1** | FAU_GEN.1 | Yes | - |
| **FAU_SAR.2** | FAU_SAR.1 | Yes | - |
| **FAU_SAR.3** | FAU_SAR.1 | Yes | - |
| **FDP_ACC.1** | FDP_ACF.1 | Yes | - |
| **FDP_ACF.1** | FDP_ACC.1<br>FMT_MSA.3 | Yes<br>Yes | - |
| **FDP_IFC.1** | FDP_IFF.1 | Yes | - |
| **FDP_IFF.1** | FDP_IFC.1<br>FMT_MSA.3 | Yes | - |
| **FIA_ATD.1** | None | N/A | - |
| **FIA_UID.2** | None | N/A | - |
| **FIA_UAU.2** | FIA_UID.1 | Yes | FIA_UID.2 is hierarchical to FIA_UID.1 |
| **FMT_MSA.1 /ACCESSCONTROL** | [ FDP_ACC.1 or FDP_IFC.1 ]<br>FMT_SMF.1<br>FMT_SMR.1 | Yes<br>Yes<br>Yes | FDP_ACC.1 due to use of Access Control SFP in ACCESSCONTROL iteration |
| **FMT_MSA.1 /PACKETFILTER** | [ FDP_ACC.1 or FDP_IFC.1 ]<br>FMT_SMF.1<br>FMT_SMR.1 | Yes<br>Yes<br>Yes | FDP_IFC.1 due to use of Packet Filter SFP in PACKETFILTER iteration |
| **FMT_MSA.3 /ACCESSCONTROL** | FMT_MSA.1<br>FMT_SMR.1 | Yes<br>Yes | - |
| **FMT_MSA.3 /PACKETFILTER** | FMT_MSA.1<br>FMT_SMR.1 | Yes<br>Yes | - |
| **FMT_MOF.1 /SUPERADMINISTRATOR** | FMT_SMF.1<br>FMT_SMR.1 | Yes<br>Yes | - |
| **FMT_MOF.1 /ADMINISTRATOR** | FMT_SMF.1<br>FMT_SMR.1 | Yes<br>Yes | - |
| **FMT_SMF.1** | None | N/A | - |
| **FMT_SMR.1** | FIA_UID.1 | Yes | FIA_UID.2 is hierarchical to FIA_UID.1 |

**Table 19 Security Functional Requirements Dependencies**

### 6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance packet EAL4 augmented with ALC_FLR.2. EAL4 is chosen because the threats that were chosen are consistent with an attacker of medium attack potential.

EAL 4+ (ALC_FLR.2) was chosen to provide a methodically designed tested and reviewed frame for TOE evaluation. On EAL 4 level assurance, developers or users gain moderate level assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is considered as the highest level of assurance for an existing product line and outcomes are economically feasible commodity products.
EAL 5 and other higher levels require semiformal or formal design, test and verification. Applications used for managing network perimeter security are sophisticated, have multiple interfaces and integration products. Development activity for formal design these multiple interfaced applications are resource consuming when considered in terms of cost. TOE assurance level EAL 4+ (ALC_FLR.2) is sufficient for identified objectives, threats and proposed TOE usage when compared with other products to be competed in boundary network device section.
Comodo Yazılım claims that the TOE complies to EAL 4 augmented with ALC_FLR.2 and is resistant to threats that may be originated from subjects that are sending or receiving information through TOE even in case of independent vulnerability assessment analysis.

# 7. TOE SUMMARY SPECIFICATIONS

The following security functions are implemented in order to satisfy the Security Functional Requirements in 6.1.2 of this Security Target. TOE Security Functions is demonstrated in Table 20.

| Security Function | Description |
|---|---|
| **F.MHI** | Authorized super administrator can manage security with Machine Human Interface functions explained below, which can be accessed from management interfaces:<br>a) Permission to reboot and shutdown;<br>b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;<br>c) Create, read, modify, delete user attribute values defined in FIA_ATD.1;<br>d) Modify and set the time, date, time zone and NTP server settings ;<br>e) Permission to review the instant audit records;<br>f) Backup of user attribute values, information flow security policy rules,<br>g) Recover to the state following the selected backup or factory defaults;<br>Authorized administrator can manage security with Machine Human Interface functions explained below of which can be accessed from management interface:<br>a) Permission to reboot and shutdown;<br>b) Permission to create, delete, modify, and view information flow security policy rules that permit or deny information flows;<br>c) Create, read, modify, delete user attribute values defined in FIA_ATD.1;<br>d) Modify and set the time, date, time zone and NTP server settings ;<br>e) Permission to review the instant audit records;<br>f) Backup of user attribute values, information flow security policy rules,<br>g) Recover to the state following the selected backup or factory defaults.<br>Authorized administrator can have either none, a limited subset or |

| | |
|---|---|
| | even all of defined management functions according to defined profile.<br>This function meet FIA_ATD.1, FMT_MOF.1/SUPERADMINISTRATOR, FMT_MOF.1/ADMINISTRATOR, FMT_SMF.1, FMT_SMR.1 |
| **F.AUDLOG** | TOE is capable of generating logs for events explained below in addition to collecting logs generated by non-TOE components.<br>a) Start-up and shutdown of the audit functions; and<br>b) All auditable events specified in Table 14.<br>This function meet FAU_GEN.1 |
| **F.AUDDET** | TOE has minimal audit log detail. Entries explained below exist in TOE for each audit log event.<br>a) Date and time of the event;<br>b) type of event;<br>c) subjects' identities;<br>d) outcome [success or failure] of the event; and<br>e) for each audit event type, based on the auditable event definitions of the functional components included in the ST, the information specified in second column of Table 14<br>This function meet FAU_GEN.1 |
| **F.AUDLST** | Authorized administrator and authorized super administrator can access instantly created TOE audit trails and TOE Security Environment audit trails. He can perform search among logged entries according to text based filters.<br>This function meet FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 |
| **F.ADMIN** | Only authorized administrators and authorized super administrators, who use the management interface, which operates in secure environment, can access TOE.<br>This function meet FDP_ACC.1, FDP_ACF.1 and FIA_ATD.1 |
| **F.IDAUTH** | Authorized administrators and authorized super administrators shall first identify and authenticate themselves to TOE before doing any operation – which all needs authorization - on TOE. Probability that authentication data can be guessed is smaller than $\mathbf{10^{-11}}$**.**<br>This function meet FDP_ACC.1, FDP_ACF.1, FIA_UAU.2, FIA_UID.2 |
| **F.DEFVAL** | Security attributes and information flow control policies that are used to enforce TOE SFP's have restrictive initial values (none, default deny). Authorized administrators with appropriate profiles can override these default values by editing object properties after new information flow policy object or authorized administrator entity is created.<br>This function meet FMT_MSA.1/ACCESSCONTROL, FMT_MSA.1/PACKETFILTER, FMT_MSA.3/ACCESSCONTROL and |

| | |
|---|---|
| | FMT_MSA.3/PACKETFILTER |
| **F.IFP** | **SF1.1:** The TSF implements the information flow control (as routers) on the network layer (IP) and transport layer (TCP/UDP). In order to define packet filter rules the TSF provides packet filter criteria and packet filter actions. The packet filter criteria are:<br>• source address<br>• destination address<br>• transport layer protocol<br>• interface on which traffic arrives and departs<br>• port<br>• time<br>The packet filter actions are:<br>• accept/permit<br>• reject/ deny<br>• drop<br>In order to apply the packet filter rules the network components take the information from the IP and TCP/UDP-Header (where applicable).<br>**SF1.2:** The TSF reassembles IP datagrams before further processing is performed. IP datagrams which cannot be reassembled in a predefined span of time are dropped.<br>**SF1.3:** The TSF drops packets with spoofed source- or destination-IP addresses. Packets with source routing options are also dropped.<br>*SF1.1 meets FDP_IFC.1. SF1.1,*<br>*SF1.2 and SF1.3 meet FDP_IFF.1* |
| **F.SECAUD** | **SF2.1:** The TSF generates audit records for<br>• start-up and shutdown of the audit functions. It must be noted that the shutdown of the audit functions mentioned in FAU_GEN.1.1 is not directly visible as a separate audit record. However, a shutdown of the audit functions of the TOE always correlates with a shutdown of the underlying system supporting the TOE. Furthermore, the shutdown of the underlying system always generates an audit record. For that reason, whenever an audit record of the shutdown of the system is generated, one can be assured that the audit functions of the TOE are shut down as well.<br>• datagrams received or sent through a network components network interfaces if they match configured patterns<br>**SF2.2:** Each record includes:<br>• Time and Date<br>• Affected network component<br>• Subject identity (source IP)<br>• Type of event<br>• Affected Interface |

| | |
|---|---|
| | • Direction<br>• Action (accept, drop or reject)<br>• Optional depending on the protocol: IP addresses and ports<br>*SF2.1 and SF2.2 meet FAU_GEN.1* |
| **F.MANAGEMENT** | **SF3.1:** The TSF is capable of performing the following management functions:<br>• Modification of network traffic filter rules,<br>• Modification of configuration data,<br>**SF3.2:** In order to modify the security attributes network traffic filter rules and configuration data<br>The TOE maintains the role administrator. The TOE verifies the identification information of an administrator provided by the environment (see O.IDAUTH) before any management function can be performed. Therefore the TOE verifies if the user id is equal to zero.<br>**SF3.3:** The TOE is initialized with a strict packet filter rule set, i.e. everything is dropped.<br>*SF3.1 meets FMT_SMF.1.*<br>*SF3.2 meets FIA_UID.2, FMT_MSA.1/PACKETFILTER and FMT_SMR.1*<br>*SF3.3 meets FMT_MSA.3/PACKETFILTER.* |

**Table 20 TOE Security Functions**