ATES 1.0 Intelligent Intrusion Detection System

Security Target

Document Version 2.9

18.8.2017

ICterra Bilgi ve İletişim Teknolojileri San. ve Tic.A.Ş
Galyum Blok Kat:2, No:3 ODTÜ-Teknokent
06531 Ankara, TÜRKİYE

Document History

Version	Date	Description
1.0	8.6.2016	Initial revision
1.1	15.7.2016	Some additions
1.2	1.8.2016	Some additions
1.3	8.8.2016	Some additions
1.4	12.8.2016	Some additions
1.5	22.8.2016	Some additions
1.6	1.9.2016	Some additions
1.7	9.9.2016	Some additions
1.8	14.10.2016	Some additions
1.9	11.11.2016	Some additions
2.0	25.1.2017	Some additions
2.1	26.1.2017	Some additions
2.2	27.1.2017	Some additions
2.3	1.2.2017	Some additions
2.4	17.2.2017	Some additions
2.5	17.3.2017	Some additions
2.6	24.3.2017	Some additions
2.7	11.4.2017	Some additions
2.8	14.8.2017	Some additions
2.9	18.8.2017	Graphic improvements

Table of Contents

List of Tables

List of Figures

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), ATES 1.0 Intelligent IDS, which is a new generation intrusion detection system. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

1. Introduction

This section identifies the Security Target (ST) of ATES 1.0 Intelligent IDS which contains Target of Evaluation (TOE), conformance claims, Security Target organization, document conventions, and terms and definitions besides an overview of the evaluated product.

1.1 ST Reference

ST Title	ATES 1.0 Intelligent Intrusion Detection System Security Target
ST Revision	2.9
ST Publication Date	18.8.2017
Author	ICterra Cyber Security Group

1.2 TOE Reference

TOE Identification:	ATES 1.0 Intelligent Intrusion Detection System
TOE Version:	ATES Control Center 1.0
	ATES IDS Agent 1.0
TOE Platform:	Runs on multiple platforms. Detailed below.
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 as of September 2012 for parts 1, 2 and 3.
Evaluation Assurance Level:	EAL 4 augmented by ALC_FLR.1
PP Conformance:	None

1.3 Document Organization

Sec.	Title	Description
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claim	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Security Requirements	Contains the functional and assurance requirements for this TOE
6	TOE Summary Specification	Identifies the IT security functions provided by the TOE as well as the assurance measures targeted to meet the assurance requirements.

Table 1 – ST organization and section descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 4 of the Common Criteria.

Although Common Critera allows four operations on functional requirements, only three of these operations are used in this Security Target: The assignment operation, the selection operation and the iteration operation. Presentation method for these operations are briefly defined below to assist the Security Target reader:

- **Assignment**: The assignment operation provides the ability to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, such as [assigned value].

- **Selection**: The selection operation allows the specification of one or more items from a list. Selections are depicted using *italics text* and are surrounded by square brackets such as *[selection]*.

- **Iteration**: The iteration operation allows the specification of multiple requirements based on the same component. Iterations are indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, such as, “FAU_SAR.1(1) Audit Review by Administrator”, “FAU_SAR.1(2) Audit Review by Auditor” and so on.

1.5 Document Terminology

The table below consists of a list of terms and acronyms used within this document:

Term	Definition
ATES	Akıllı TEhdit izleme Sistemi
CC	Common Criteria version 3.1 (ISO/IEC 15408)
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
SFR	Security Functional Requirement
SMF	Security Management Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms used in Security Target

1.6 TOE Overview

1.6.1 TOE Type

TOE is application layer software of an Intrusion Detection System, called ATES.

ATES belongs to the “Boundary Protection Devices and Systems” product category in the CC Portal.

ATES is a next generation network security system which helps secure institutions’ networks from external threats. ATES consists of two major components: ATES agent and ATES Control Center, which is a web based application.

1.6.2 Non-TOE Hardware/Software/Firmware required by TOE

TOE requires, as non-TOE hardware,

- A computer to be configured as ATES Agent,
- A computer to be configured as ATES Control Center and
- A computer to be configured as Terminal.

TOE requires, as non-TOE software in ATES Agent,

- CentOS operating system,
- Suricata intrusion detection system.

TOE requires, as non-TOE software in ATES Control Center,

- CentOS operating system,
- Play web application framework,
- Google AngularJS web application framework.

TOE requires, as non-TOE software in both ATES Control Center and ATES Agent,

- Apache ActiveMQ message broker,
- MySQL relational database management system.

Information about the minimum requirements for hardware and specific versions of software is available under “1.7.2 TOE Platform” title of this document.

1.6.3 Usage of the TOE

ATES agents are Intrusion Detection Systems. Agents listen to traffic flowing in the corporate network. Neither the ATES Control Center nor the ATES agents make or execute any decision to pass/drop network datagrams. ATES components do not generate any traffic to intervene user sessions either. Their sole transmission on network is for communicaton among TOE components.

ATES components are intelligent network monitoring and intrusion detection tools. ATES uses both signature and anomaly based IDS signature databases to detect cyber attacks. ATES also uses well-known IP reputation algorithms as well as its own IP reputation algorithm to further detect IP domains generating abnormal traffic.

ATES agents can sniff all user traffic received by their network interface cards. ATES agents analyze this traffic by comparing IP addresses, port numbers or other parts of datagrams to predefined patterns, called attack signatures. ATES can also investigate some time dependent patterns, called “anomalies” in the monitored network traffic. Attack patterns are both defined locally by TOE and obtained from several external sources. Anomaly detection algorithms are developed by TOE designers. ATES Agents can create customizable reports indicating the findings and statistics generated according to the patterns that are being sought within the monitored traffic.

ATES has a control center where all agents of the TOE can be monitored and controlled remotely. TOE security function interfaces are on the ATES Control Center as well.

ATES agents do not have an IP address connected to the network interface card that is used to sniff network traffic. Agents have an IP address connected to a second network interface card, which is used to communicate with the Control Center.

1.6.4 Major Security Features of the TOE

TOE controls access to security management functions through user roles called Product_Admin, Administrator, Auditor and Operator. Product_Admin role is held by the TOE developer to create the initial Administrator and Auditor accounts. Then, the management of TOE is passed on to the customer.

All authorized users are forced to verify their user identities and passwords through session initiation.

Execution of security management functions such as user creation or deletion are subject to audit logging.

“Segregation of duties” principle is implemented through separation of Administrator and Auditor roles. Administrators are not allowed to delete the audit logs generated through their actions and Auditors are not allowed to execute the tasks subject to audit logging.

Operating systems of platforms running TOE components and Administrators of these operating systems (which will be called “Operating System Administrator” in the rest of that document) are outside the scope of TOE.

1.7 TOE Description

1.7.1 Physical Boundaries

The TOE is a software and consists of the following components:

- ATES Control Center Application
- ATES IDS Agents Application

Applications execute on (at least) two separate computers: The Control Center computer and (at least) one Agent computer(s).

ATES Control Center Application is a web application. Hence, a third computer, a “terminal computer” is required to access the services provided by the Control Center. Terminal Computer is outside the scope of TOE.

Control Center Application deals with management and monitoring of agents. Security features are initiated through the Control Center application as well.

Agent Application listens to network traffic, conducts the analysis requested by the Control Center and returns the results to the Control Center.

Like most application software, TOE components depend on the services provided by the operating system as well as other software to execute their functions. Figure 1 given below briefly summarizes the software organization of the platforms hosting TOE components: The Control Center computer and the Agent computer. TOE components, operating systems and the other third party software the TOE components depend on are observable on Figure 1. Hence Figure 1 presents both the TOE components and their operational environment.

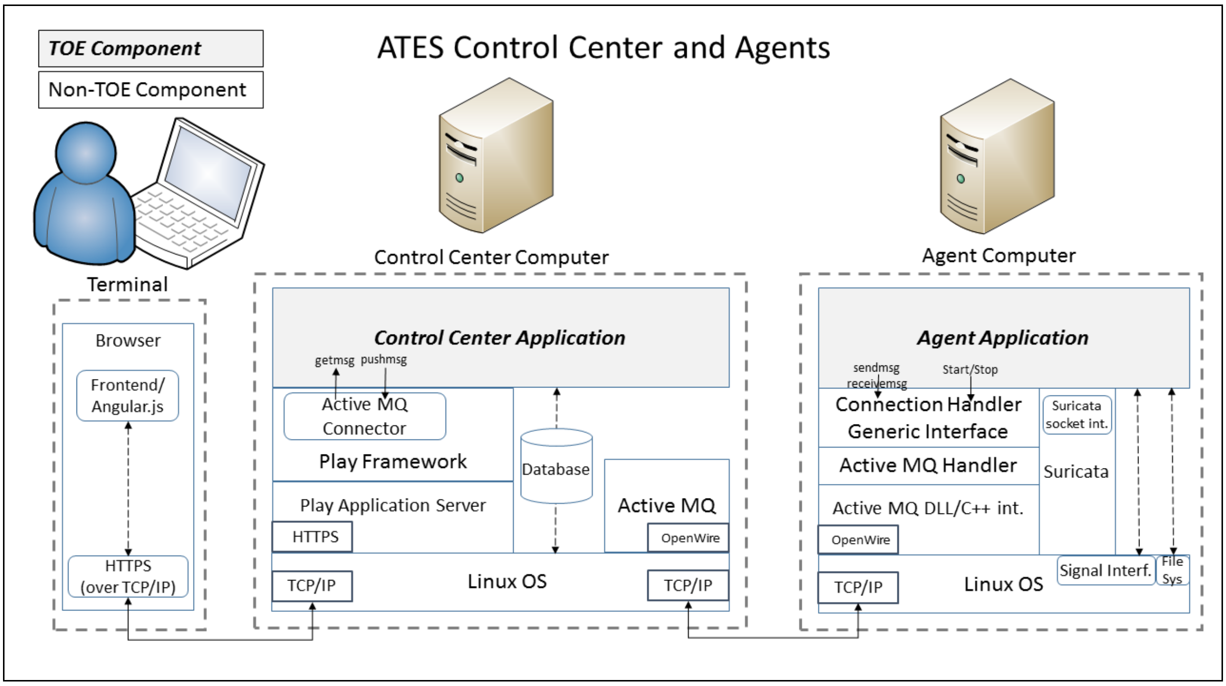

Figure 1 – TOE Boundary

1.7.2 TOE Platform

1.7.2.1 Software Requirements of the TOE

The TOE components run with the following software:

Software	Version / Model number
Operating System	CentOS 7 64-bit
Other Software	Apache ActiveMQ 5.14.0 Play Framework 2.4.3 MySQL 5.7.x Google AngularJS 1.4
WEB browser (running on terminal)	Google Chrome 49.0.x (min.)

Table 3 – ATES Control Center software requirements

Software	Version / Model number
Operating System	CentOS 7 64-bit
Other Software	Apache ActiveMQ 5.12.0 Suricata 3.1.2 MySQL 5.7.x

Table 4 – ATES IDS Agent software requirements

1.7.2.2 Hardware requirements of the TOE

Minimum hardware requirements of ATES components are listed below:

Aspect	Minimum requirements
CPU	64-bit
RAM	8 Giga Byte
Hard Disk	20 Tera Bytes of free space
Network Interface Card	CentOS 7 64-bit compatible

Table 5 – Hardware requirements of ATES Control Center

Aspect	Minimum requirements
CPU	64-bit, dual core
RAM	8 Giga Byte
Hard Disk	20 Tera Bytes of free space
Network Interface Card	CentOS 7 64-bit compatible

Table 6 – Hardware requirements of ATES IDS agents

1.7.3 Logical Boundaries

TSF	Description
Security Management	Administrators can configure the TOE, accessing the Control Center interface via a web browser.
Security Audit	The TOE generates audit logs of management functions as well as several system events. Audit logs may be reviewed on the ATES Control Center interface.
User Data Protection	The TOE enforces discretionary access rules using an access control list with user attributes. Some user attributes may be refined during initialization or modified later at the ATES Control Center interface by authorized administrators.
Identification and Authentication	Legitimate users defined by Administrators are forced to authentication at the Control Center interface via declaration of user attributes (user name and password).

Table 7 – Logical boundary descriptions

1.7.4 TOE Security Functional Policies

The TOE supports the following roles, which are the subjects of the “User Access Control Policy”:

a. Product_Admin

b. Administrator
c. Auditor
d. Operator

User Access Control Policy is enforced through user authentication and audit generation policies. The TOE implements an access control SFP named User Access Control SFP. This SFP determines the privileges associated with the roles briefly described below:

1.7.4.1 "Product_Admin" Role

The sole responsibility of the Product_Admin, who is an employee of the deveoloper, is defining a user with Administrator privilege and another user with Auditor privilege before the product is activated by the customer.

1.7.4.2 "Administrator" Role

An authorized administrator can create administrators, operators and modify the privileges of administrators via the ATES Control Center. Administrators can execute specific management functions via the ATES Control Center interface as well.

1.7.4.3 "Auditor" Role

Auditor role's access to TOE is limited to audit logs. Auditor is entitled to requesting and deleting audit logs, which are the role's only privileges. The Auditors are not entitled to execute any other management functions.

1.7.4.4 "Operator" Role

Operator role has limited access to TOE. An operator can read attack alarms via the ATES Control Center, which is the role's only privilege.

1.7.5 TOE Product Documentation

The TOE includes the following product documentation:

- ATES IDS User Guide

2. Conformance Claims

This chapter contains the following sections:

- CC conformance claims
- Package claim

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria 3.1 Revision 4 (September 2012):

> In order to provide a complete description of the functional requirements addressed by the TOE, functional components of part 2 of the Common Criteria framework were used.
>
> For the description of the requirements due to the trustworthiness of the TOE, only security assurance requirements of CC part 3 were used.
>
> Evaluation Assurance Level: EAL4 augmented by ALC_FLR.1

2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE claims conformance to the EAL4 assurance requirements package augmented by ALC_FLR.1.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- This chapter identifies assumptions as A.assumption, threats as T.threat and policies as P.policy.

3.1 Threats

The following threats are to be countered by the TOE or a combination of TOE and the operational environment.

Threat	Description
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.
T.DELETE_LOG	An authorised administrator, using his/her privileges, may purposefully delete the audit logs to cover his/her malicious activities.

Table 8 – Threats addressed by the TOE

The IT Environment does not explicitly address any threats.

3.2 Organizational Security Policies

The following organizational security policies are to be enforced by the enviroment in which the TOE is intended to be used, or a combination of TOE and the operational environment:

Policy	Description
P.ACCESS	None of the authorized users (users associated to Product_Admin, Administrator, Auditor and Operator roles) shall have access to TOE through Internet. Authorized users shall not have direct access to the agents either. Authorized users shall access the agents only through the Control Center. Figure 2 gives a general overview of TOE and the corporate network.
P.AUDIT	Personnel and procedures shall be in place to monitor and manage the audit logs generated by ATES components.

Policy	Description
P.SEGREGATION	Personnel and procedures shall be in place to segregate the "Auditor" and "Administrator" roles.

Table 9 – Organizational Security Policies

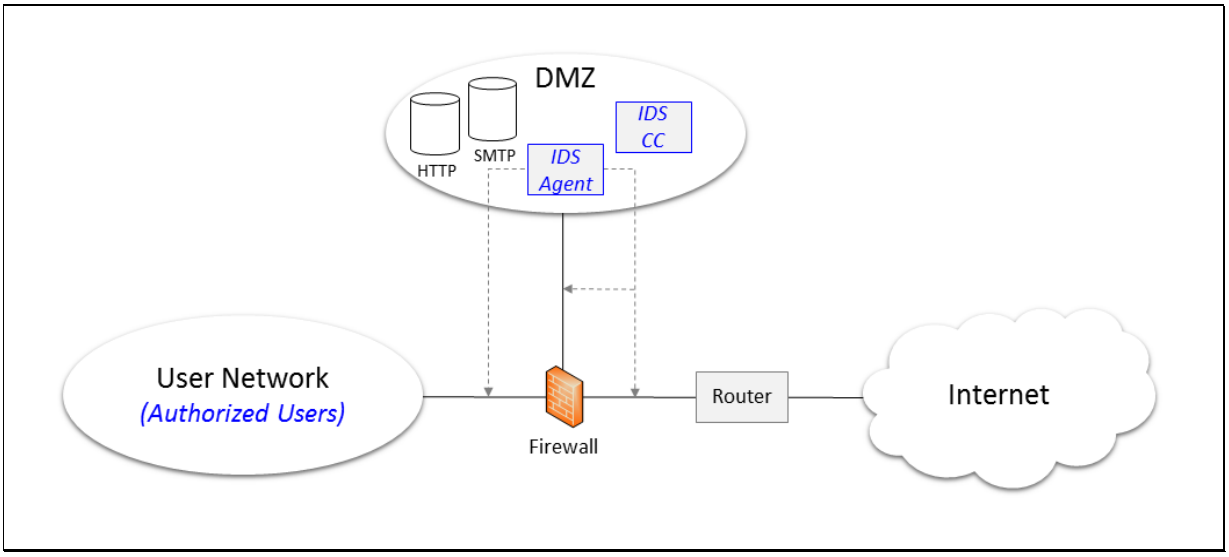

Figure 2 – Locations of TOE components and authorized users in corporate network

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The following specific conditions are assumed to exist in an environment where the TOE is employed.

Assumption	Description
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Operating system administrators of platforms where TOE components are running and users accessing the local area network are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.HARDENING	Operating system and virtualization software executing on platforms where TOE components are running are hardened according to industry standards.
A.LOCATE	The platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.TIMESOURCE	The system where TOE is located has, or allows access to, an NTP

Assumption	Description
	server.
A.PHYSEC	The TOE is physically secure. Only authorized personnel has physical access to the system which hosts the TOE.

Table 10 – Assumptions

4. Security Objectives

This chapter contains the following sections:

- Security objectives for the TOE
- Security objectives for the operational environment
- Security objectives rationale

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are listed below:

Objective	Description
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.
O.AUDIT_REC	The TOE must 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. The TOE will also generate notification messages regarding the state of log storage memory in order to minimize the possibility of overwriting previous log messages.
O.LOG_SECURITY	The TOE shall support an “Auditor” role as well as an “Administrator” role. Through consistent execution of access control policies, Administrator will be authorised to execute management functions except managing the audit logs, whereas “The Auditor” will be authorized to manage audit logs but will not be able to execute any other management functions.

Table 11 – TOE security objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

Objective	Description
OE.TIME	The TOE operating environment shall provide, or allow access to a source providing an accurate timestamp (via a reliable NTP server).
OE.ACCESS_CONTROL	Flow of management traffic between the Control Center and the authorized users must be assured by a network access control device such as a stateful firewall. The firewall will be configured to allow access to TOE CC management IP/Port by authorized users only from the corporate network. No other connections will be allowed to TOE Control Center or TOE Agents.

Objective	Description
OE.PERSONNEL	Authorized users of TOE follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE. Operating system administrators of platforms where TOE components run are non-hostile.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.
OE.AUDIT	Users of TOE must be sufficienty trained and working due to formal procedures to manage the logs and log memory notification messages being generated by TOE, assuring the TOE components are running with suficient log memory and logs generated by TOE are processed properly and in timely manner.
OE.SEGREGATION	The instituiton using the TOE should assign separate staff fulfilling the “Administrator” and “Auditor” roles provided by TOE, which would help reduce the risk of accidental or deliberate misuse of Administrator privileges. The institution should consider further measures to minimize the possibility of collusion between the administrators and auditors.
OE.SW_SECURITY	Operating system administrators of platforms where TOE components are running should have sufficient expertise and institutional support to harden, according to industry-standard practices, the operating system and virtualization software of these platforms, in order to assure secure and continuous operation of TOE.

Table 12 – Operational Environment security objectives

4.3 Security Objectives Rationale

This section provides the summary of how all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

	O.AUDIT_REC	O.SEC_ACCESS	O.LOG_SECURITY	OE.TIME	OE.ACCESS_CONTROL	OE.PERSONNEL	OE.AUDIT	OE.SEGREGATION	OE.PHYSEC	OE.SW_SECURITY
A.MANAGE						X				
A.NOEVIL						X				
A.HARDENING										X
A.LOCATE									X	
A.TIMESOURCE				X						
A.PHYSEC									X	
T.NO_AUTH		X			X	X			X	
T.NO_PRIV	X	X								
T.DELETE_LOG		X	X							
P.ACCESS					X					
P.AUDIT							X			
P.SEGREGATION			X					X		

Table 13 – Mapping of assumptions, threats and OSPs to security objectives

4.3.1 Rationale for Security Objectives

Assumption/ Threat/Policy	Rationale
A.MANAGE	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered by a competent, security aware and appropriately trained personnel. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that operating system administrators of TOE platforms and users on the local area network are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.HARDENING	This assumption is addressed by OE.SW_SECURITY, which ensures that operating system administrators of TOE platforms have

Assumption/ Threat/Policy	Rationale
	awareness, training and other means to harden the operating systems and virtualization software of platforms where TOE components are running.
A.LOCATE	This assumption is addressed by OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the availability of an accurate time source.
A.PHYSEC	This assumption is addressed by OE.PHYSEC which ensures that TOE is physically secure and that only authorized personnel has physical access to the system which hosts the TOE.
T.NO_AUTH	This threat is countered by the following: • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications, • OE.ACCESS_CONTROL, which limits the attack surface of Control Center, that may be subject to brute-force and similar attacks, to corporate network. • OE.PERSONNEL, which ensures that the TOE is managed and administered by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that the administrators are responsible for installing, managing and operating TOE in a secure manner, • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.
T.NO_PRIV	This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration and associated data only by authorized users and applications and O.AUDIT_REC, which ensures the reliable generation of an audit trail of security related events.
T.DELETE_LOG	This threat is countered by O.SEC_ACCESS, which ensures access to TOE by authorized users, and O.LOG_SECURITY, which ensures the segregation of Administrator and Auditor roles, separating the privileges of executing the security management functions and managing the audit logs genereted by the execution of these security management functions.
P.ACCESS	This policy is addressed by OE.ACCESS_CONTROL, which ensures that the traffic from and to TOE shall be controlled by a network access control device.

Assumption/ Threat/Policy	Rationale
P.AUDIT	This policy is addressed by OE.AUDIT which ensures 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
P.SEGREGATION	This policy is addressed by OE.SEGREGATION which ensures assignment of separate personnel to Administrator and Auditor roles, and O.LOG_SECURITY, which restricts deletion of the audit logs of Administrator actions (as well as the actions of other authorized users) to Auditors.

Table 14 – Rationale for assumptions, threats and policies

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.

5.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components:

Class Heading	Class Family	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Audit Protection
	FAU_STG.3	Audit Data Loss
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UID.2	User Identification Before Any Action
	FIA_UAU.2	User Authentication Before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 15 – TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

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) [the events specified in Table 16 - Table of Auditable Events]

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 (if applicable), 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 ST, [the additional information specified in the Details column of Table 16].

Functional Component	Level	Auditable Event	Details
FAU_SAR.1	Basic	Reading information from the audit records.	
FDP_ACF.1	Minimal	Successful requests to perform an operation on an object covered by the SFP.	
FIA_SOS.1	Basic	Rejection or acceptance by the TSF of any tested secret.	
FIA_UAU.2	Basic	All use of the authentication mechanism.	IP address of the terminal involved in unsuccessful user authentication.
FIA_UID.2	Basic	All use of the user identification mechanism, including the user identity provided.	
FMT_MSA.1	Basic	All modifications of the values of security attributes.	
FMT_MSA.3	Basic	Modifications of the default setting of permissive or restrictive rules.	
FMT_MTD.1	Basic	All modifications to the values of TSF data.	
FMT_SMF.1	Minimal	Use of the management functions.	
FMT_SMR.1	Minimal	Modifications to the group of users that are part of a role	

Table 16 – Table of auditable events

5.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1

The TSF shall provide [the Administrator and the Auditor] with the capability to read [audit logs generated within the TOE] 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.

5.1.1.3 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [filtering, searches, sorting] of audit data based on: [

a) user identity;
b) type of event;
c) date;
d) time].

5.1.1.4 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to *[prevent]* unauthorized modifications to the stored audit records in the audit trail.

5.1.1.5 FAU_STG.3 Action In Case of Possible Audit Data Loss

FAU_STG.3.1

The TSF shall [alert users with Administrator role and Auditor role] if the audit trail exceeds [the default capacity limit of 75% of audit log storage area size, whereas that limit can be set to (50-90%) by Auditor].

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 Subset Access Control

The TSF shall enforce the [User Access Control SFP] on [

Subjects: Product_Admin, Administrators, Auditors, Operators

Objects: User Privileges, User Account Attribute, Audit Logs, Attack Alarms, Agent Configurations, Suricata_Service

Operations: Create, Read, Delete, Stop/Start/Restart]

5.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 Security Attribute Based Access Control

The TSF shall enforce the [User Access Control SFP] to objects based on the following: [Combinations defined in Table 17 - Security Attribute Based Access Control Table]

Subject	Subject Attributes	Object	Object Attributes	Operation
Product_Admins	User Identity, Authentication Status, Privileges	User Privileges	None	Create Administratror, Create Auditor
Administrators	User Identity, Authentication Status, Privileges	User Privileges, User Account Attribute, Audit Logs, Agent Configurations	None	All user actions as defined in FMT_SMF.1 ***except*** Create Auditor, Delete Audit Logs
Auditors	User Identity, Authentication Status, Privileges	Audit Logs	None	Read Audit Logs, Delete Audit Logs
Operators	User Identity, Authentication Status, Privileges	Attack Alarms	None	Read Attack Alarms

Table 17 - Security Attribute Based Access Control Table

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [verify the subject’s User Identity, Authentication Status, Privileges].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

1. Authenticated Administrators can Stop, Start and Restart Suricata_Service from Control Center,
2. Authenticated users can change their own passwords].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [invalidation of username/password at session timeout].

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Status, Privileges].

5.1.3.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [the following metrics:

a. User password shall consist of at least six characters,
b. User password shall include at least one character from letters, capital letters and digits,
c. The user shall be forced to change his/her password at the first session initiation after the password is designated or changed by the authorized entity (Product_Admin or Administrator)]

5.1.3.3 FIA_UID.2 User Identification before Any Action

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.

5.1.3.4 FIA_UAU.2 User Authentication Before Any Action

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.

5.1.4 Security management (FMT)

5.1.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the [User Access Control SFP] to restrict the ability to *[change_default, query, modify]* the security attributes [User identity, privileges] to [Administrator].

5.1.4.2 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1

The TSF shall enforce the [User Access Control 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 [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1

The TSF shall restrict the ability to *[change_default, query, modify]* the [user privileges] to [Administrator]:

5.1.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

a) Read (Request and view) user account list (of all user roles defined in FMT_SMR.1 except Product_Admin)
b) Create accounts (of all user roles defined in FMT_SMR.1 except Product_Admin)
c) Define User privileges (of Administrator accounts)
d) Modify Privileges (of Administrator accounts)
e) Change Password of accounts
f) Delete accounts (of all user roles defined in FMT_SMR.1 except Product_Admin and Auditor)
g) Read (Request and View) attack alarms
h) Read (Request and View) audit logs
i) Delete audit logs
j) SendAgentConfigurations
k) Stop / Start / Restart Suricata_Service
l) Change Default, Query, Modify the attributes associated with Administrator privileges

5.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1

The TSF shall maintain the roles [Product_Admin, Administrator, Auditor, Operator].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.2 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.1 (printed in bold and italic in the table below). They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in the following Table.

Class Heading	Class Family	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF

Class Heading	Class Family	Description
	ADV_TDS.3	Basic modular design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle 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.1	***Basic flaw remediation***
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
AST: 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: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Analysis	AVA_VAN.3	Focused vulnerability analysis

Table 18 – EAL 4 (augmented) assurance requirements

5.3 Security Requirements Rationale

5.3.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

	O.AUDIT_REC	O.SEC_ACCESS	O.LOG_SECURITY
FAU_GEN.1	X	X	X
FAU_SAR.1	X		
FAU_SAR.3	X		
FAU_STG.1	X	X	
FAU_STG.3	X	X	
FDP_ACC.1		X	X
FDP_ACF.1		X	X
FIA_ATD.1		X	X
FIA_SOS.1		X	X
FIA_UID.2		X	X
FIA_UAU.2		X	X
FMT_MSA.1		X	X
FMT_MSA.3		X	X
FMT_MTD.1		X	
FMT_SMF.1		X	
FMT_SMR.1		X	X

Table 19 – Mapping of TOE security functional requirements and objectives

5.3.2 Dependencies of security functional requirements

The following table presents the dependencies among SFRs and their fulfillment status.

	Requirement (SFR TOE)	Dependencies	Dependency Fulfilled
1	FAU_GEN.1	FPT_STM.1	A.TIMESOURCE
2	FAU_SAR.1	FAU_GEN.1	YES
3	FAU_SAR.3	FAU_SAR.1	YES
4	FAU_STG.1	FAU_GEN.1	YES
5	FAU_STG.3	FAU_STG.1	YES
6	FDP_ACC.1	FDP_ACF.1	YES
7	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES
8	FIA_ATD.1	None	YES
9	FIA_SOS.1	None	YES
10	FIA_UID.2	None	YES
11	FIA_UAU.2	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1) is implemented
12	FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	YES
13	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES
14	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES
15	FMT_SMF.1	None	YES
16	FMT_SMR.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1) is implemented

Table 20 – TOE functional requirements dependencies

The following figure helps visualize the dependencies among SFRs and their fulfillment status.

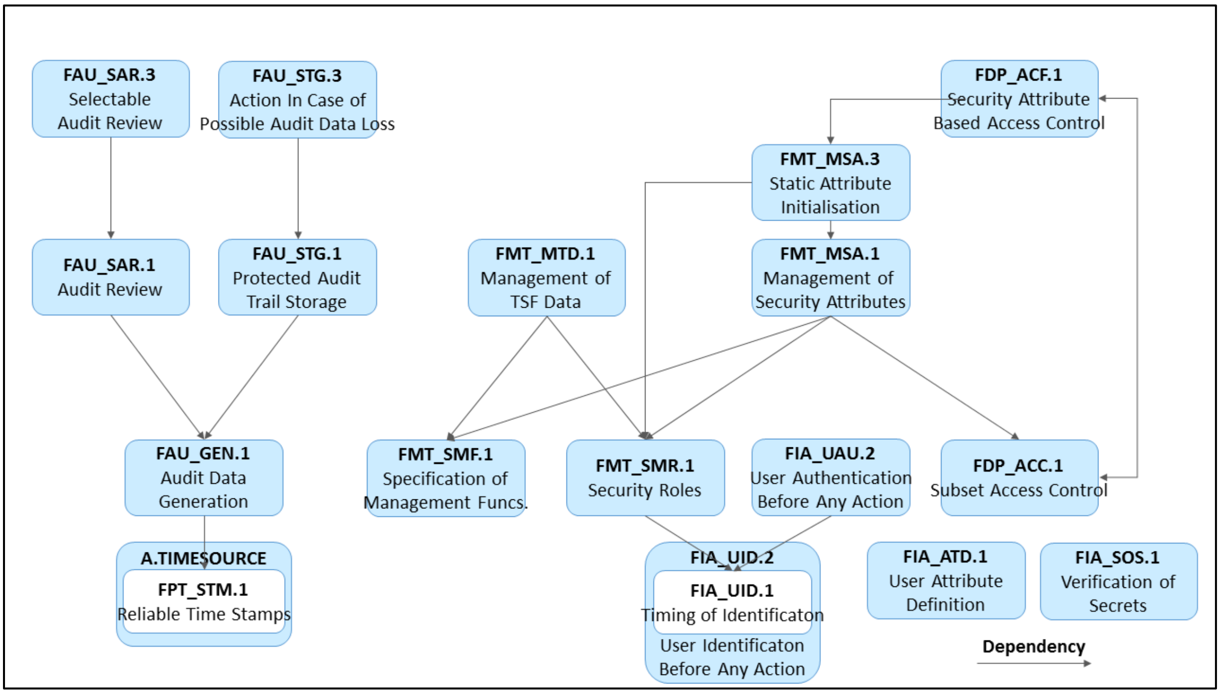

Figure 3 – TOE Functional Requirements Dependencies

5.3.3 Sufficiency of security functional requirements

Table 20 given below explains the mapping of TOE security functional requirements to objectives:

Objective	Rationale
O.SEC_ACCESS	The objective to ensure that only those authorized users and applications are granted access to security functions and associated data, is met by the following security functional requirements: “FMT_SMF.1 Specification of Management Functions” defines the domain access control will be applied, which consists of a number of security management functions. That domain may also be called the “accessed space”. “FMT_SMR.1 Security Management Roles” partitions the user domain, which may also be called the “accessor domain” to several roles, and defines the “accessor space”. “FMT_MSA.1 and FMT_MSA.3 Management of Security Attributes” and “FMT_MTD.1 Management of TSF Data” allows and defines the limits to refinement of user attributes by the administrator. “FDP_ACC.1 Access Control Policy” and “FDP_ACF.1 Access Control Functions” establish the acceptable combinations of user roles and security management functions. Hence the relation between the “accessor space” and the “accessed space” is defined. “FIA_ATD.1 User Attribute Definition”, “FIA_UID.2 User Identification” and “FIA_UAU.2 User Authentication” establishes and validates the identity and security attributes of the users as well as providing the “role” of the user running the current session to TSF. “FIA_SOS.1 Verification of Secrets” enhances the reliability of the user identification process. Hence, TSF have the means to decide, for each security management function, whether the user running the current session is allowed to execute the security management function or not. Finally, “FAU_GEN.1 Audit Data Generation” and “FAU_STG.1 and FAU_STG.3 Audit Data Storage” requirements provide evidence that may be used to validate the reliable execution of access control policies.
O.AUDIT_REC	The objective to ensure that the TOE provides a means to record a readable audit trail of security related events, with accurate dates

Objective	Rationale
	and times, and a means to search and sort the audit trail, is met by the following security functional requirements: FAU_GEN.1 leads to audit data generation, FAU_STG.1 and FAU_STG.3 leads to audit data storage, and FAU_SAR.1 and FAU_SAR.3 leads to audit review capabilities. Hence, the whole cycle of generation, storage and review is covered for audit data.
O.LOG_SECURITY	The objective to ensure that the TOE support an “Auditor” role as well as an “Administrator” role where Administrator is authorised to execute management functions except managing the audit logs, whereas “Auditor” is authorized to manage audit logs but isn’t able to execute any other management functions, is met by the following security functional requirements: “FMT_SMR.1 Security Management Roles” defines Adminstrator and Auditor roles. “FIA_ATD.1 User Attribute Definition” establishes, “FIA_UID.2 User Identification” and “FIA_UAU.2 User Authentication” validate the identity of users claiming Administrator or Auditor roles. “FIA_SOS.1 Verification of Secrets” enhances the reliability of the user identification process. “FDP_ACC.1 Access Control Policy” and “FDP_ACF.1 Access Control Functions” defines the access rights of Administrator and Auditor roles according to the “segregation of duties” principle. That is, Administrator cannot delete and Auditor cannot generate audit logs. “FMT_MSA.1 and FMT_MSA.3 Management of Security Attributes” allows the refinement of user attributes of the Administrator role. FAU_GEN.1 leads to audit data generation. Hence, generation and deletion of audit data is managed according to “segregation of duty” principle and O.LOG_SECUTIY is reached.

Table 21 – Rationale for mapping of TOE SFRs to objectives

6. TOE Summary Specification

This section contains the Security Functions implemented by the TOE.

6.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

6.2 Security Audit

The TOE provides three types of event logs:

1. Audit logs of the following user events:
   a. User creations (in Control Center),
   b. User deletions (in Control Center),
   c. User privilege modifications (in Control Center),
   d. User password change (in Control Center),
   e. Successful user logins (in Control Center),
   f. User login failures (in Control Center),
   g. User logouts (in Control Center),
   h. Audit log read (in Control Center),
   i. Audit log delete (in Control Center),
   j. Attack alarm read (sent from Control Center to agents),
   k. Configuration update (sent from Control Center to agents),
   l. Stop, start and restart commands (sent from Control Center to agents),
2. Audit logs of the following system event:
   a. Audit log storage area exhaustion (in Control Center).
3. Attack alarms generated due to detection of signature/anomaly based attacks (in agents).

Events in 1.a-i are initiated, completed and logged in TOE Control Center.

Events in 1.j-m are initiated in Control Center, processed in agents and completed back in Control Center. These events are logged in ATES Control Center.

Event 2.a occur and is logged in ATES Control Center.

Events in 3 (attacks) occur, they are detected and stored in the agents.

Hence, audit logs are stored in the Control Center and attack alarms are stored in the agents.

Generation, storage and review of attack alarms are outside the scope of TSFs. This preference is due to relatively smaller importance and higher volume of attack alarms with respect to the audit logs.

The following functionalities are within the scope of TSFs and implemented in Control Center component of TOE:

a. Generation, storage, reading and deletion of audit logs,
b. Audit log storage area management,

Functionalities are implemented to secure audit log storage, in order to prevent the depletion of audit log storage area in Control Center component of TOE. That includes,

a. Designation of the threshold level about remaining audit log storage area,
b. Generation of alarm when the threshold level is reached.

Audit logs maybe reviewed by authorized users through a graphical user interface provided by ATES Control Center. Interface allowing access to audit logs is enabled only if the active user has sufficient privilege to read the audit logs. Menu, tab etc. user interface components triggering log review functions are disabled and may not be called by the user in case of insufficient user privilege.

Audit log interface provides several functions to ease monitoring the logs, such as sorting with respect to user identity, user name/surname, date/time and event type. Audit logs maybe searched with respect to user identity and filtered with respect to even type and time range as well.

The Security Audit function TSFs are designed and implemented to satisfy the following security functional requirements, which are refined in the previous chapters of this document:

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.3
- FAU_STG.1
- FAU_STG.3

These requirements are about the generation, review and storage of audit logs, respectively.

6.3 User Data Protection

The TOE enforces that only administrators can access system reports, TOE configuration and user account attributes. The TOE also enforces User Access Control SFP by verifying user Identity, authentication status and privileges. TOE sets authentication status based on successful validation of username/password combination.

The TOE enforces that audit logs may be read by Administrators and Auditors whereas the audit logs may only be deleted by Auditors.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1

6.4 Identification and Authentication

The ATES Control Center interface provides a user interface where TOE users can access several TOE functions. The login interface on the ATES Control Center provides web based session initiation to TOE users through supported web browsers. The ATES Control Center maintains authorization information that determines which TOE functions the users can reach.

Users prove their identities to TOE through validation of their passwords at session initiation.

Initial password is designated by the authorized entity (Product_Admin or Administrator) creating the user. The user is then forced to change his/her password with a complex password (consisting of at least six characters, including letters, capital letters and digits) at the first session initiation.

Upon successfull comparison between (User Identity, Password) pairs provided by the user and kept by the Conrol Center, the authentication status related to the user identity of the user who has initiated the session is set to “LOGGED_ON”. Upon termination of the session by the user, authentication status related to the user identity is set to “LOGGED_OFF”. Users who are both “LOGGED_ON” and have sufficient privilege to call a security management function may do so. Privileges of users are constant and depend on their roles; except for Administrators, whose privileges maybe set when they are created, or modified later by another Administrator with sufficient privilege.

Hence ATES Control Center assures due maintenance of (User Identity, Authentication Status, Privilege) information for every single user defined in TOE. This combination is checked to allow/deny access to Security Management Functions when request to call an SMF is received by the ATES Control Center from a user.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_SOS.1
- FIA_UID.2
- FIA_UAU.2

6.5 Security Management

The roles of the users in TOE are described in the following table. There are four possible roles: *Product_Admin*, *Administrator, Auditor* and *Operator*.

The following table presents default privileges for the security roles in TOE and the security management functions each role can access.

ATES Control Center software will be built with a default Product_Admin user. As soon as the TOE is activated, Product_Admin will connect locally to Control Center and create two users: An Administrator and an Auditor.

Initial values of privileges may not be modified when a user is created with Auditor or Operator roles.

Initial values of privileges may not be modified when a user is created with Administrator role (by a Product_Admin) either.

Initial values of privileges may be modified when a user is created with Administrator role (by another Administrator).

All in all, there are three cases of creating a user with Administrator role:

1. An Administrator is created by the Product_Admin and the **default privileges** defined for the Administrator role in Table 22 **are used.**
2. An Administrator is created by another Administrator (who has to have “CretateAdmin” privilege) and the **default privileges** defined for the Administrator role in Table 22 **are used.**
3. An Administrator is created by another Administrator (who has to have “CretateAdmin” privilege) and the **privileges** of the created Administrator **are restricted.** Administrators with restricted privileges are called “Restricted Administrators”.

A Restricted Administrator is an Administrator who does not have “CreateAdmin” privilege. “ModifyAdminPrivileges”, “ChangeAdminPassword” and “DeleteAdmin” privileges are equivalent to “CreateAdmin” privilege and set to “No” automatically for Restricted Administrators. Otherwise, Restricted Administrators would have the chance to

a. Escalate their own privileges,
b. Create another Administrator with unrestricted privileges, or
c. Delete an Administrator.

The following table presents the default privileges to access SMFs for all possible combinations of (User Roles, Security Management Functions).

If the default privilege is written in grey, that means the privilege may not be set to any other value than the default value. If the default privilege is written in black, that means the privilege may be set to the opposite of default value.

	Roles' privileges to call SMFs			
Security Management Functions	**Product_ Admin**	**Administrator**	**Auditor**	**Operator**
ReadUserAccountList	YES	YES	YES	No
CreateAdmin	YES	YES	No	No
ModifyAdminPrivileges	No			
ChangeAdminPassword	No			
DeleteAdmin	No			
CreateAuditor	YES	No	No	No
CreateOperator	No	YES	No	No
ChangeOperatorPassword				
DeleteOperator				
ChangeOwnPassword	YES	YES	YES	YES
ReadAttackAlarms	No	YES	No	YES
ReadAuditLogs	No	YES	YES	No
DeleteAuditLogs	No	No	YES	No
AuditLogStorageDepletion				
Stop / Start / Restart Suricata_Service	No	YES	No	No
SendAgentConfigurations	No	YES	No	No

Table 22 – Roles and their default privileges to access SMFs

The Security management functions are designed to satisfy the following security functional requirements:

- FMT_MSA.1
- FMT_MSA.3
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1