Antikor Next Generation Firewall and

Security Management v2

Security Target Lite Version 1.1

Contents

List of Tables

1 Introduction

This ST describes the objectives, requirements and rationale for the Antikor Next Generation Firewall and Security Management v2.

ST Title	Antikor Next Generation Firewall and Security Management v2 Security Target
ST Version	1.1
TOE Title	Antikor Next Generation Firewall and Security Management v2
TOE Version	2.0
Assurance Level	EAL4+
CC Identification	• Common Criteria Part 1 Version 3.1 Revision 5 • Common Criteria Part 2 Version 3.1 Revision 5 • Common Criteria Part 3 Version 3.1 Revision 5 • Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 5

Table 1.1: Toe and ST references

2 Overview

TOE is a next generation firewall and security management software. The software builds a security suite on top of the operating system facilities and networking applications by providing a streamlined interface and work flow to the security functions of its environment. TOE provides

- components that allow management of the firewall of the operating system and the other security services
- extensive logging and auditing capabilities of the facilities it manages and internal configuration data
- an access control facility to secure configuration data and audit logs

3 Assumptions

Assumptions regarding the environment in which the TOE will reside are listed in table 2.1.

Assumption	**Description**
A.ADMIN	It is assumed that authorized administrator who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experienced, trained and meet the security conditions.
A.PROTECT	It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secure data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.
A.CONFW	The configuration interface refuses all connections. It can be only controlled physically using management console.
A.TSP	The IT environment provides reliable time stamps.
A.PROT	The connection between the management machine and the network components is protected by cryptographic transforms.
A.AUDIT	The IT environment provides a logging server and a means to present a readable view of the audit data.

Table 2.1: Assumptions

4 Threats

The threat agents are described below.

- Attackers who have knowledge of how the TOE operates and are assumed to possess a basic skill level, and intend to alter TOE configuration settings and operation while having no physical access to the TOE.
- TOE users who have extensive knowledge about the TOE operations and are assumed to have a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE.

Applicable threats for the TOE are listed in table 3.1

Threat	Description
T.UNAUTH	Attacker could gain unauthorized access to the TOE data by bypassing the authentication requirements.
T.DOS	In this threat the service provided by the TOE or the TOE system itself is made unusable or inaccessible by an attacker for a period of time to a specific user or all users.
T.CHANNEL	Users could gain the valuable information (passwords and enterprise data) of authorized administrator by sniffing the traffic.
T.BRUTE	Attacker may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.WEAKNESS	Attacker may 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.

Table 3.1: Threats

5 Organizational Security Policies

Organisational security policies are listed in table 4.1.

Threat	Description
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.

Table 4.1: Organisational policies

6 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment.

6.1 Security Objectives for the TOE

Security objectives for the TOE are listed in table 5.1.

Security objective	Description
O.MANAGEMENT	The TOE must provide management functions in order to modify its configuration. User identification is provided by the environment.
O.AUDIT	The TOE must provide an audittrail of security-related events.
O.PASSWORD	Passwords used in the TOE will be strong enough to resist most brute force attacks.

Table 5.1: Security objectives for the TOE

6.2 Security Objectives for the Operational Environment

Security objectives for the TOE are listed in table 5.2.

Security objective	Description
OE.SECENV	Operational environment of the TOE shall ensure physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components.
OE.CREDENTIALS	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.
OE.TSP	The IT environment provides reliable time stamps.
OE.PROT	The connection between the management machine and the network components is secured cryptographically.

OE.AUDIT	The IT environment provides a logging server and a means to present a readable view of the audit data.

Table 5.2: Operational security objectives

6.3 Security Objectives Rationale

Table 5.3 demonstrates that all security objectives trace back to threats, OSPs and assumptions in the security problem definition.

		Threats					OSPs	Assumptions					
		T.UNAUTH	T.DOS	T.CHANNEL	T.BRUTE	T.WEAKNESS	P.ACCOUNTABILITY	A.ADMIN	A.PROTECT	A.CONFW	A.TSP	A.PROT	A.AUDIT
Security objectives for TOE	O.MANAGEMENT			X									
	O.AUDIT	X					X						
	O.PASSWORD	X			X								
Security objectives for operational environment	OE.SECENV		X	X	X	X			X	X		X	
	OE.CREDENTIALS	X		X				X					
	OE.TSP										X		
	OE.PROT	X		X								X	
	OE.AUDIT	X					X						X

Table 5.3: Security objectives rationale

- **T.UNAUTH:** O.AUDIT security objective is responsible for The TOE that generate audit reports to trace user and administrator access events and OE.AUDIT ensures that the audit reports are kept externally and easily analyzable. O.PASSWORD enables the TOE provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources. OE.CREDENTIALS is an operational environment objective which provides that all user credentials are protected appropriately by users and they are not negligent. Finally, OE.PROT aims to protect sensitive authentication data.
- **T.DOS:** OE.SECENV enables necessary measures to facilitate access barriers for arbitrary access to management components.
- **T.CHANNEL:** O.MANAGEMENT and OE.PROT are responsible for securing communications during operation. OE.SECENV complements O.MANAGEMENT externally. OE.CREDENTIALS provides protection from user negligence.

- **T.BRUTE:** O.PASSWORD requires the TOE to detect repeating authentication attempts. OE.SECENV is required for additional assurance to address attacks from the operational environment.
- **T.WEAKNESS:** This threat is countered by configuration of the TOE accordingly and making sure that operational environment is sufficiently secure to block most attacks, provided by OE.SECENV.
- **P.ACCOUNTABILITY:** This policy is ensured by operational and environmental auditing provided by O.AUDIT and OE.AUDIT.
- **A.ADMIN:** OE.CREDENTIALS ensures proper authentication protection for administrators.
- **A.PROTECT:** Environmental security assumption is backed by OE.SECENV, making sure the physical system is secure.
- **A.CONFW:** This assumption asserts that precautions for the environment has been taken by OE.SECENV.
- **A.TSP:** Requirement for a consistent timestamping of audit logs are provided by OE.TSP.
- **A.PROT:** Secure connection between the TOE and network components are provided by OE.SECENV and OE.PROT.
- A.AUDIT: Making sure the logs are processed and kept secure is provided by OE.AUDIT.

7 Security Requirements

In this section, functional and assurance requirements specific to the TOE and the trace between SFR and the security objectives for the TOE will be provided.

7.1 SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application.

- **Assignment**: The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows **[assignment]**.
- **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 as follows *[selection]*.
- **Refinement**: The refinement operation allows the addition of extra detail to arequirement. Refinements are indicated using **bolded text** for additions, and ~~strike-through~~ for deletions.
- **Iteration**: The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by an identifier at the end of the component identifier as follows FDP_ACC.1/IDENTIFIER

7.2 Security Functional Requirements

The TOE uses two subjects: Input and Output. These represent the input and output of the TOE. The TOE satisfies the SFRs listed in the table 6.1

SFR class	**Requirement**	**Description**
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
User data protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
User identification (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UID.1	Timing of identification
	FIA_UAU.1	Timing of authentication
Security management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination

Table 6.1: Operational security objectives

7.2.1 Audit Data Generation – FAU_GEN.1

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 *[detailed]* level of audit; and

(c) **[start-up and shut-down of the underlying system]**.

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 PP/ST, **[Logging events related to FIA_UID.1 is not applicable.]**.

7.2.2 User Identity Association – FAU_GEN.2

Hierarchical to No other components

Dependencies FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event

7.2.3 Subset Access Control – FDP_ACC.1

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 policy]** on **[subject: administrator; objects: TOE modules, secrets; operations: read, delete, modify and create]**.

7.2.4 Security Attribute Based Access Control - FDP_ACF.1

Hierarchical to	No other components
Dependencies	FDP_ACC.1 Subset access control FMT_MSA.3/SEC Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the **[access control policy]** to objects based on the following: **[** • **Administrators can** **– Modify secrets of users** **– Create or delete users** **– Modify users' status** **– Modify configuration data** **]**.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[administrators are granted access to all functions or resources]**.
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.

7.2.5 Authentication Failure Handling - FIA_AFL.1

Hierarchical to	No other components
Dependencies	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when **[configurable amount (default 5) of]** unsuccessful authentication attempts occur related to **[login attempts by an administrator]**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *[met]*, the TSF shall **[deny access to the originating IP address for a configurable amount of time]**.

7.2.6 Verification of Secrets - FIA_SOS.1

Hierarchical to No other components

Dependencies No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[the following metrics:**

1. **at least configurable amount (default 1) uppercase character (A-Z)**
2. **at least configurable amount (default 1) lowercase character (a-z)**
3. **at least configurable amount (default 1) digit (0-9)**
4. **at least configurable amount (default 1) special character (punctuation)**
5. **at least configurable amount (default 6) characters**

].

7.2.7 Timing of Identification - FIA_UID.1

Hierarchical to No other components

Dependencies No dependencies

FIA_UID.1.1 The TSF shall allow **[only access of data designated as public]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.8 Timing of Authentication - FIA_UAU.1

Hierarchical to No other components

Dependencies FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[only access of content designated as public]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.9 Management of Security Attributes - FMT_MSA.1

Hierarchical to No other components

Dependencies [FDP_ACC.1 Subset access control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **[access control SFP]** to restrict the ability to *[change, query, modify and delete]* the security attributes **[subject identity, metrics for verification of secrets and maximum number of failed login attempts]** to **[all users]**.

7.2.10 Static Attribute Initialization - FMT_MSA.3

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 **[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 **[administrators]** to specify alternative initial values to override the default values when an object or information is created.

7.2.11 Specification of Management Functions - FMT_SMF.1

Hierarchical to No other components

Dependencies No dependencies

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[create, query, modify and delete the security attributes and audit configuration]**.

7.2.12 Security Roles - FMT_SMR.1

Hierarchical to	No other components
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles **[administrator]**.
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

7.2.13 TSF Initiated Termination - FTA_SSL.3

Hierarchical to	No other components
Dependencies	No dependencies
FTA_SSL.3.1	The TSF shall terminate an interactive session after a **[a configurable amount of time, with a default value of 10 minutes and minimum value of 1 minute]**.

7.2.14 User Initiated Termination - FTA_SSL.4

Hierarchical to	No other components
Dependencies	No dependencies
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.

8 TOE Summary Specifications

This section provides the TOE summary specifications, a definition of the security functions claimed to meet the functional requirements.

8.1 Security Audit

The TOE generates audit logs that consist of auditable events and actions taken by the users. These logs are produced with a reliable time stamp provided by operational environment.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2,

8.2 Identification and Authentication

The Identification and Authentication security function provides the TOE with the ability to restrict access for users. The TOE ensures that an administrator identity is established and verified before access to the TOE is allowed. Prior to allowing access, the TOE requires administrator to be identified using a user name and password. Passwords are enforced to meet a sufficient amount of complexity. Before successful completion of the security function, an administrator is unable to perform any of the relevant functions. Once identified and authenticated, the users are able to access the functions or resources available to their roles. Information flow on input and output is mediated by the TOE, making sure that accessing the configuration and secrets require administrative authentication. When a configurable amount of unsuccessful authentication attempt has been met, login functionality is disabled for a configurable amount of time.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FIA_AFL.1, FIA_SOS.1, FIA_UID.1 and FIA_UAU.1

8.3 Security Management

The TOE provides mechanisms to govern which users can access with resources or functions. The Security Management function allows the administrator to properly configure this functionality. Authorized administrator can assign additional administrative users.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1

8.4 TOE Access

The TSF provides a method for controlling the establishment of an administrator’s session based on a termination of session after a specified period of inactivity. Inactive sessions are automatically logged out and returned to the login page. The TOE also allows user-initiated termination of the user’s own interactive session.

TOE Security Functional Requirements Satisfied: FTA_SSL.3 and FTA_SSL.4.

9 PP Conformance Claims

This Security Target does not claim conformance to a Protection Profile.

9.1 PP Package Claims

This Security Target claims augmented conformance to the assurance package EAL4+, by adding the Security Assurance Requirement of ALC_FLR.1.