Version Date October 28, 2004
Version 2.7p
Ref. AKV3-CRT-EAL2-ST

ARKOON FAST Firewall v3.0
SECURITY TARGET

Prepared for

ARKOON Network Security
13A avenue Victor HUGO
F-69160 Tassin La Demi-Lune

By

netXper / ARKOON

TABLE OF CONTENTS

LIST OF TABLES

140 LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This introductory section presents security target (ST) identification information and an overview of the ST structure.

1.1 ST Overview

This document is the security target which provides the basis for the evaluation of the ARKOON FAST Firewall v3.0.

The ARKOON FAST Firewall v3.0 Target of Evaluation (TOE) enforces information flow policies between internal and external networks. The TOE implements a software traffic and application-filter firewall which performs stateful inspection of every packet forwarded from one network to another. In particular, the ARKOON FAST firewall performs advanced applicative controls with regard to the state of a packet's connection while maintaining performance and scalability. Typically, the FAST software is embedded into an ARKOON appliance equipped with an Intel-based hardware architecture. The FAST Administration Consoles provide the FAST firewall administrator with management and monitoring tools to administrate the security policy enforcement and review relevant audit information.

An ST document provides the basis for the evaluation of an information technology (IT) product or system (e.g., target of evaluation (TOE)). In addition to this Security Target introductory section, an ST features:

- A TOE description describing the scope and the boundary, physical as well as logical, of the TOE (in Section 2, TOE Description).

- The security aspects of the environment in which the TOE will be used. It includes a set of assumptions about the security aspects of the environment, a description of threats which the product is intended to counter, and any known organizational security policy with which the product must comply (in Section 3, TOE Security Environment).

- A set of security objectives for the TOE and its environment and a set of functional and assurance security requirements to meet these objectives for the TOE (in Sections 4 and 5, Security Objectives and TOE Security Requirements, respectively).

- The TOE summary specification defining the instantiation of the security requirement for the TOE (in Section 6, TOE Summary Specification).

- PP claims and Rationale demonstrating the completeness, coherency and effectiveness of the requirements and the TOE summary specification with regard to the security environment and PP claims (in Sections 7 and 8, PP Claims and Rationale, respectively).

The ST for a TOE is a basis for agreement between the developers, evaluators, and consumers on the security properties of the TOE and the scope of the evaluation. The audience for the ST is not confined to those responsible for the production of the TOE and its evaluation. This ST is also directed towards readers responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE.

The structure and contents of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.2 ST, TOE and CC Identification

This section provides ST and TOE control and identification information.

ST Title:	ARKOON FAST v3.0 Security Target
ST Version:	2.7p
ST Date:	October 28, 2004
ST Authors:	Frédéric ROBERT, Benoit BRODARD
TOE Identification:	**ARKOON FAST Firewall v3.0/11 + certification-eal2-qualification package**
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 ISO 15408
Assurance Level:	Evaluation Assurance Level 2 (EAL2), augmented by AVA_VLA.2, ADV_HLD.2, AVA_MSU.1, ALC_DVS.1 and ALC_FLR.3.
ST Evaluation:	realized by Oppida

1.3 Conformance Claim

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 2.1, August 1999, ISO/IEC 15408-1 [CCIMB-99-031].
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.1, August 1999, ISO/IEC 15408-2 [CCIMB-99-032].
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.1, August 1999, ISO/IEC 15408-3, augmented [CCIMB-99-033].
- Evaluation Assurance Level 2 (EAL2), augmented by AVA_VLA.2, ADV_HLD.2, AVA_MSU.1, ALC_DVS.1, ALC_FLR.3.
- Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology, Version 1.0, August 1999, [CEM-99/045].
- Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology, Supplement ALC_FLR – Flaw Remediation, Version 1.1, February 2002, [CEM-2001/0015R].

1.4 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information and acronyms used throughout the remainder of the document.

1.4.1 Conventions

This section describes the conventions used to denote CC operations on security requirements and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allow several operations to be performed on functional requirements; *assignment, iteration, refinemen*t, and *selection* are defined in paragraph 2.1.4 of Part 2 of the CC v2.1.

a) The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
b) **Iteration** of a component is used when a component is repeated more than once with varying operations. Iterated components are given unique identifiers by an iteration number or name in parenthesis appended to the component and element identifiers.
c) The **refinement** operation is used to add detail to a requirement, and thus further restrict a requirement. Refinement of security requirements is denoted by **bold text** for additions and ~~strike-through~~ for deletions.
d) The **selection** operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized text.*

Plain *italicized text* is used for both official document titles and text meant to be emphasized over plain text.

1.4.2 Terminology

Section 2.3 of Part 1 of the Common Criteria v2.1 defines several terms which are used in a specialized way throughout the CC. A subset of these definitions is produced below to aid the Security Target reader.

Authentication data - Information used to verify the claimed identity of a user.
External IT entity - Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Human user - Any person who interacts with the TOE.
Identity - A representation (e.g., a string) uniquely identifying an authorized user, which can be either the full or abbreviated name of that user or a pseudonym.
Role - A predefined set of rules establishing the allowed interactions between a user and the TOE.
User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

In addition to the above general definitions, this Security Target provides the following specialized definitions:

Authorized external IT entity - Any IT product or system, outside the scope of the TOE that may administrate the security parameters of the TOE. Such entities are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.
Authorized Administrator - A role which human users may be associated with to administrate the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

1.4.3 Acronyms

The following abbreviations from the Common Criteria are used in this Security Target:

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FIPS	PUB Federal Information Processing Standard Publication
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

The following non CC-specific abbreviations are used in this Security Target:

DNS	Domain Name Service
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
NAT	Network Address Translation
NIC	Network Interface Card
OS	Operating System
PAT	Port Address Translation
SME	Small to Medium Enterprise
SMTP	Simple Mail Transfer Protocol

2 TOE DESCRIPTION

This Chapter provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 General overview

The ARKOON FAST Firewall implements a traffic-filter and application-level firewall. For this latter purpose, it utilizes an exclusive technology of data streams filtering embedded into the product kernel, called FAST. The FAST Applicative Shield Technology permits finer-grain applicative level analysis and control with minimal degradation of network performance.

ARKOON markets a whole range of network security appliances allowing companies to efficiently protect their information systems with easy-to-administrate solutions. ARKOON products are based on hardware architectures whose technical features guarantee performance, quality and availability specific to critical systems.

The software product line can run on the whole range of ARKOON hardware appliances. These appliances share a very similar architecture (Via C3 or Intel Pentium processor based) and core system features based on the AKS OS, a Linux-based system distribution tuned to ARKOON's security requirements. ARKOON appliances also export the same type of interfaces although each model has been engineered to operate at a specific performance level in terms of number of concurrent connections, throughput and overall performance.

The source code base for all platforms described within this ST document is identical; however, the code must be compiled and built into a different system image for each processor architecture. Table 1 identifies the specificities of ARKOON appliance models to emphasize that the differences between any two of them have no impact on the security functions claimed in this Security Target.

Table 1: Technical summary datasheet of TOE Appliance models

	A200	**A500**	**A2000**	**A5000**
CPU	Via C3 667MHz	Intel P3 1GHz	Intel P3 2GHz	Intel P3 Bipro 1,2GHz
Memory	128Mo	256Mo	512Mo	512Mo/1Go
Hard Drive	20Go	40Go	40Go	36,7Go SCSI
PCMCIA slots	1	2	2	2

Flash	32Mo (System)	16Mo(Config)
		32Mo(System)
			16Mo(Config)
			32Mo(System)
				16Mo(Config)
				32Mo(System)

Ethernet Ports	4	4	4	4
OS	AKS	AKS	AKS	AKS
Throughput(Mb/s)	190	300	425	1700
Connections/s	5700	14400	23000	25000
Max. Conn. #	190000	450000	980000	2000000
Max. VPN #	50	500	10000	25000
AES Thrpt (Mb/s)	32	130	200	250

2.2 Architecture

The TOE comprises two major components:

The FAST Firewall runs on rack mounted ARKOON FAST Appliances and relies on the AKS OS, a Linux-based system distribution tuned to ARKOON's security requirements. All appliances are manufactured to ARKOON's specifications by sub-contracted manufacturers. The ARKOON appliances that meet the definition of the TOE include models A200, A500, A2000 and A5000.

The FAST Administration Consoles consist of the FAST Monitoring Console and the FAST Management Console and run on the FAST Administration Station. This station runs an up-to-date version of Windows 2000 OS.

Figure 1 shows an overview of the TOE architecture.

2.2.1 FAST Firewall

The FAST Firewall is architectured around the components described below.

The FAST Engine enforces the rules that allow or deny a new connection to get established and enforces the respect of network and transport level protocols (IP, TCP, UDP and ICMP). It provides session tracking mechanisms, limitation of the number of established and pending connections, Network Address Translation mechanisms and authentication mechanisms. It includes the **FAST Analyzer:** a module that enforces the respect of the Applicative_SFP with rules toward application protocols (HTTP, FTP, SMTP, and DNS).

The Management Services interact with the **FAST Engine** to load the configuration defined by authorized administrators. **The Management Services** are accessed by authorized administrators, once they have been authenticated, through two **Management Interfaces**:

- A **minimal configuration interface**: a configuration tool on the FAST firewall that allows an Authorized Administrator to initialize the FAST firewall. The initialization procedure includes the hard drive initialization, the creation of a system administrator account (root), the initialization of a Certificate Authority and the creation of the FAST firewall certificate, the definition of the allowed network administration interface and the IPs of the FAST Management and Monitoring consoles, the creation and installation of a primary configuration allowing network communication with the FAST Management and Monitoring consoles.
- An **advanced graphical configuration interface**: a configuration tool on the FAST Management Console that allows an authorized administrator to configure the FAST firewall on a day-to-day basis.

The Audit Services comprise a set of services used for monitoring purpose which interact with the FAST Engine for logging data to the embedded database and with the Monitoring Console for audit review. They notify the authorized administrators when a triggering event is detected. They are also responsible for the communication between the Monitoring Console and the FAST firewall: they will receive requests sent by the Monitoring Console and will have them processed by the embedded database.

The Authentication Services comprise two services:

- One, based on the FAST Appliance Console login shell, used to authenticate an authorized administrator before granting her access to the FAST Appliance Console.
- A second one, based on certificates, used to authenticate an authorized administrator before granting her access to the FAST Management and Audit services through the FAST Management and Monitoring Consoles.

The FAST Appliance Console provides local access to the FAST Firewall through a character display and a keyboard to which a command line shell is connected.

The FAST Appliance is an ARKOON appliance equipped with at least 3 NICs and executing the FAST Firewall.

Some Additional modules are implemented by the FAST Firewall: User Authentication, Virtual Private Networking, Content Filtering, Virus Detection, Quality of Service Management, High Availability Services, Multi ARKOON centralized Management, Applicative relaying (SMTP, POP, HTTP, FTP).

Note: The additional modules are not part of the evaluated TOE configuration.

2.2.2 FAST Administration Consoles

The FAST Management Console is an application which runs on the administration workstation, interacts with the Management Services and provides a graphical user interface to define the TSP, transmit it the FAST firewall and request its installation.

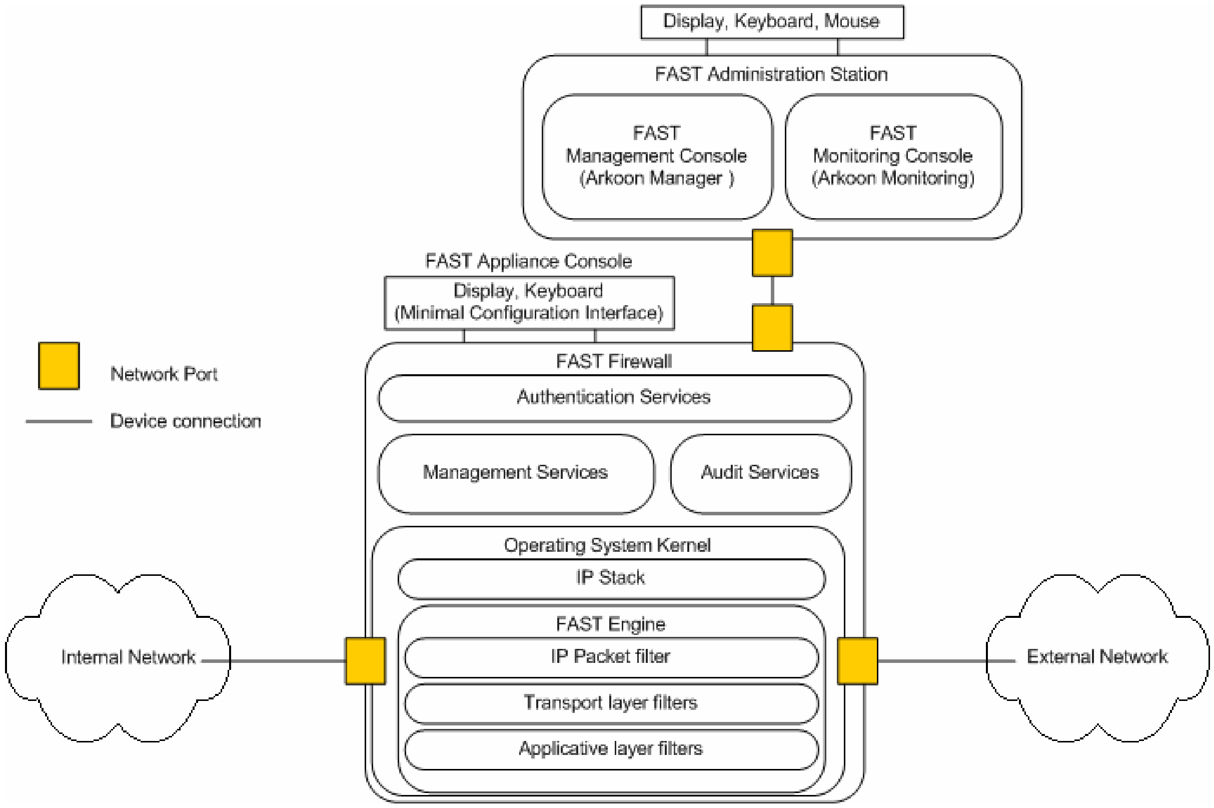
420

The FAST Monitoring Console is an application which runs on the administration workstation, interacts with the Audit Services and provides a graphical user interface to monitor dynamic information related to the FAST firewall and query the log database on the FAST Firewall.

Note: The FAST Administration Consoles run on the FAST Administration Station.

The FAST Administration Station: a machine installed with an up-to-date version of Windows 2000 OS which runs the FAST Administration Consoles and has no extra software package installed other than those provided by ARKOON Network Security.

Figure 1 - TOE Architecture Overview



2.3 Scope and Boundaries of the TOE

This section describes both physical and logical boundaries of the TOE

2.3.1 Physical Boundaries

The physical boundary of the ARKOON appliances is the physical appliance itself. The character display and the keyboard which provide access to the minimal configuration interface are part of the TOE environment.

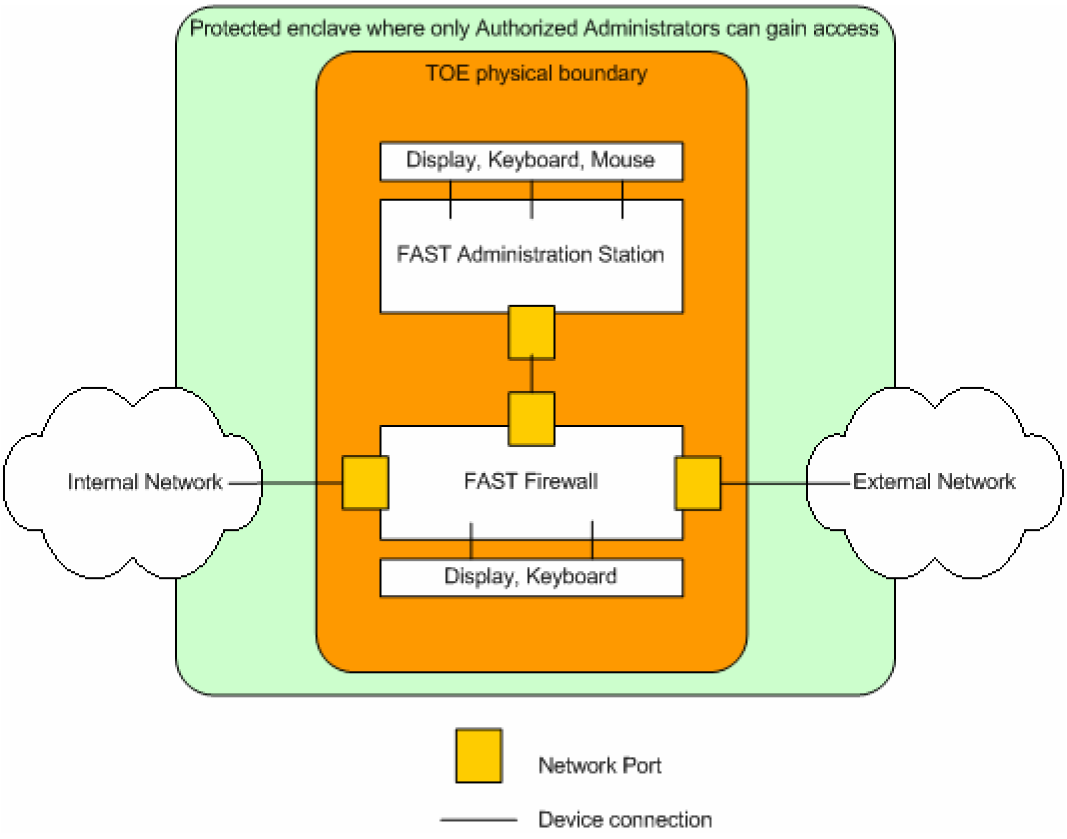
The ARKOON appliance attaches to a physical network separated into three logical networks (administrative, internal, external networks) through three port interfaces.

On A2000 and A5000 models, a floppy disk drive is provided to facilitate license and certificate installation.

The TOE shall remain in a protected area where only Authorized Administrators can gain physical access. The FAST Administration Station on which runs the FAST Administration Consoles shall remain in the same protected area.

The communication between the FAST Administration Station and the FAST Appliance will be established on a dedicated interface on the FAST Appliance, and via a dedicated cable. The Authorized Administrator must restrict the authorized administration services and port interface through the minimum configuration interface.

Figure 2 - TOE Physical Boundary and Environment



2.3.2 Logical scope

2.3.2.1 Audit

The FAST Firewall Management Services provide the Authorized Administrator with the ability to specify which traffic-filter and application-filter events to log. Logs are time stamped, recorded and stored locally on the FAST Appliance. The logs can be viewed by the Authorized Administrator using the FAST Monitoring Console.

2.3.2.2 User Data Protection – Information Flow Policy

The FAST Engine enforces the information flow Security Policy based on network and application layer rules for all flows passing through the TOE. The FAST Firewall will first enforce the Unauthenticated_SFP, and then may enforce the Applicative_SFP.

- The Unauthenticated_SFP will enforce the security policy based on network layer information.
- The Applicative_SFP will enforce the security based on application protocols. The FAST Protocol Analyzer provides SMTP, HTTP, FTP and DNS application level protection.

2.3.2.3 Identification and Authentication

The TOE supports two authentication mechanisms for Administrators, depending upon which administrative interface is accessed.

- Password authentication through a local authentication database is used to allow administrative access through the FAST Appliance Console.
- Certificate authentication through a local, self-trusted Certification Authority is used to allow administrative access through the FAST Administration Consoles.

There are three administrative roles supported by the FAST Firewall, though for the purposes of this Security Target the three of them are treated as a single “Authorized Administrator” role:

- “root” administrator (administrative access through the FAST Appliance Console)
- Read/write administrator (administrative access through the FAST Administration Consoles)
- Read-only administrator (administrative access through the FAST Administration Consoles)

2.3.2.4 Security Management

A FAST Appliance provides three administrative interfaces to define and manage the information flow security policy enforced by the FAST Firewall: the Minimal Configuration Interface on the FAST Appliance Console, the FAST Management Console and the FAST Monitoring Console on the FAST Administration Station. Before gaining access to any of these interfaces, the Authorized Administrators are required to identify and authenticate themselves. Per configuration of the TOE, only Administrators accounts are supported on the TOE.
By default, the FAST Firewall rejects any communication through its network interfaces until it has been configured by the Authorized Administrator.

2.3.2.5 Protection of the TOE

The protection of the TOE is partly ensured by its environment which must prevent physical tampering with the TOE and logical tampering with administrative accesses to the TOE. The interface between the external and internal networks is provided by, and only by, the FAST Firewall Appliance so that it cannot be bypassed. The TOE configuration protects its management functions by isolating them in a physically secure environment, on a dedicated network interface and by restricting access to these functions through mandatory identification and authentication.

2.3.2.6 Privacy

The TOE provides Network and Port Address Translation (NAT and PAT) mechanisms that hide the internal network architecture from the external network.

2.3.3 Assets requiring protection

Assets requiring protection are security relevant elements of the TOE that include TSF data and user data:

- User data are external IT data flows through the TOE.
- TSF data comprise
    - All configuration-related information installed by an Authorized Administrator through the administrative interfaces to the Management Services, including user credentials, the firewall Certificate Authority, the firewall security policy.
    - The TOE connection table managed by the FAST Engine.

External Assets requiring protection are described by the global security policy defined by IT Administrators. Examples of such assets are application servers and the data they host, the network architecture … However, an exhaustive list of such assets is out of the scope of this Security Target.

3 TOE SECURITY ENVIRONMENT

This statement of TOE security environment provides a description of the environment in which the TOE is intended to be used and of the manner in which it is expected to be used. It includes a presentation of the *assumptions* made about the security environment for a secure usage of the TOE, the *threats* addressed by the TOE and the *threats* addressed by the security environment.

The TOE mediates information flows between two networks such as an internal and an external network. The implementation of the TOE must ensure that all information flows from one network to the other cannot bypass the TOE and hence are processed by the TOE. The TOE's purpose is to enforce the security policy defined by an Authorized Administrator regarding the access to services and/or information provided on the internal network from the external network and to protect applications on the internal network against typical attacks attempted from the external network.

3.1 Assumptions

The assumptions presented in Table 2 are assumed to exist in the operational environment.

Table 2 : Assumptions

Name	Description
A.PHYSEC	The processing resources of the TOE that depend on hardware security features are located within controlled access facilities that mitigate unauthorized, physical access.
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.PUBLIC	The TOE does not host public data.
A.NOEVIL	Authorized Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
A.DIRECT	Human users within the physically secure boundary protecting the TOE may only attempt to access the TOE from some direct connection through the FAST Administration Consoles or through the FAST Appliance Console.
A.NOREMO	Human users cannot access the TOE remotely from the internal or external networks for administrative purpose.
A.LOCATE	The physical access to the FAST Administration Station and to the FAST Appliance is restricted to the Authorized Administrators.
A.OSVER	The Operating System installed on the Administration Station is an up-to-date version of Windows 2000 OS.
A.SINUSE	The environment prevents an unauthorized person from trying to replay a former authentication process in order to launch attacks on the TOE.

Note: The A.GENPUR assumption is concerned with the Firewall Appliance and the Administration Station with the exception of the operating system and the associated system tools.

3.2 Threats

540 ### 3.2.1 Threats Addressed by the TOE

The threats against which specific protection within the TOE is required are described in Table 3.

Table 3 : Threats addressed by the TOE

Name	Description
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security 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.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.PROT_MIS	A person or an external IT may attempt to take control of an application (i.e. HTTP FTP, SMTP or DNS) server or client by using debug or badly formatted commands with regard to the associated applicative protocol.
T.PRIVACY	With knowledge of the real IP addresses of external IT entities on the internal network, an attacker may have enough information about the internal network to affect the internal network in an undesirable manner.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because security-relevant events are not logged or audit records are lost or not reviewed by the Authorized Administrator, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.NODETECT	An unauthorized person may continuously attempt to bypass the TSP without detection in order to successfully send information through the TOE.
T.SYNFLOOD	A person or an external IT may try to syn-flood an internal resource in order to deny access to normal users and/or to crash the resource.

3.2.2 Threats to be addressed by Operating Environment

The threats against which specific protection within the TOE's environment is required are described in Table 4. They must be countered by procedural measures and/or administrative methods.

Table 4 : Threats addressed by the operating environment

Name	Description
TE.USAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by an Authorized Administrator.

3.3 Organizational Security Policies

No organizational security policy is specified.

4 SECURITY OBJECTIVES

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives: Security objectives for the TOE, and Security objectives for the Operating Environment.

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives countering security threats that are directly addressed by the TOE are described in Table 5, together with a mapping to countered threats. For a detailed mapping between threats and the IT security objectives listed below see Section 8.1 Rationale for IT Security Objectives.

Table 5 : Security objectives for the TOE

Name	Description	Countered threats
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.	T.NOAUTH T.REPEAT
O.MEDIAT	The TOE must mediate (i.e. accept, block, reject) the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information is not transmitted in any way.	T.ASPOOF T.MEDIAT T.OLDINF T_SYNFLOOD
O.MEDIATAPP	The TOE must screen the flow of all HTTP, SMTP, DNS, and FTP information from users on a connected network to users on another connected network to mediate the flow according to protocol conformance and mediation rules defined by an authorized administrator.	T.MEDIAT T.PROT_MIS
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.	T.NOAUTH T.MEDIAT T.PROT_MIS T.SELFPRO
O.SELFPRO	The TOE must protect itself against attempts by unauthorized user to bypass, deactivate, or tamper with TOE security functions.	T.SELFPRO T.AUDFUL
O.AUDREC	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 based on relevant attributes.	T.AUDACC T.NODETECT
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to initial setup, definition of the TSP and audit.	T.AUDACC T.NODETECT
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	T.NOAUTH T.AUDFUL
O.PRIVACY	The TOE must ensure that users on the external network can not determine the addresses of the IT external entities on the internal network.	T.PRIVACY

560

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The security objectives countering security threats that are directly addressed by the TOE environment are described in Table 5, together with a mapping to countered threats or addressed assumptions.

Table 6 : Security objectives for the environment

Name	Description	Addressed Assumptions / Countered Threats
OE.PHYSEC	The processing resources of the TOE that depend on hardware security features are located within controlled access facilities that mitigate unauthorized, physical access.	A.PHYSEC
OE.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	A.GENPUR
OE.PUBLIC	The TOE does not host public data.	A.PUBLIC
OE.NOEVIL	Authorized Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	A.NOEVIL
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	A.SINGEN
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may only attempt to access the TOE from some direct connection through the FAST Administration Consoles or through the FAST Appliance Console.	A.DIRECT
OE.NOREMO	Human users cannot access the TOE remotely from the internal or external networks for administrative purpose.	A.NOREMO
OE.LOCATE	The access to the FAST Administration Station and to the FAST Appliance shall be restricted to the authorized administrators.	A.LOCATE
OE.OSVER	The Operating system installed on the Administration Station shall be an up-to-date version of Windows 2000 OS.	A.OSVER
OE.SINUSE	The environment shall prevent an unauthorized person from trying to replay a former authentication process in order to launch attacks on the TOE.	A.SINUSE
OE.GUIDAN	Those responsible for the TOE must ensure that the TOE is delivered, installed, administrated, and operated in a manner that maintains security according to the security recommendations provided by Arkoon FAST Administration Guides.	TE.USAGE
OE.ADMTRA	Authorized Administrators are trained as to establishment and maintenance of sound security policies and practices.	TE.USAGE

5 TOE SECURITY REQUIREMENTS

IT security requirements include: TOE security requirements, and (optionally) security requirements for the TOE's IT environment that is, for hardware, software, or firmware external to the TOE and upon which satisfaction of the TOE's security objectives depends.

These requirements are discussed separately below.

5.1 TOE Security Functional Requirements

The SFRs for the TOE are listed in Table 7. These requirements were derived from the CC Part 2 Security Functional Requirements.

The overall minimum Strength of Function claim for the TOE SFRs is SOF-HIGH. The FIA_UAU.1 SFR requires that the TOE have an authentication mechanism that has a probability of authentication data being guessed which is less than one in 10^{15}.

580 Since the TOE will not be remotely accessed for administrative purpose, and since only the authorized administrator can access the TOE, some SFR requirements shall have their scope reduced to user consideration by exception to the authorized administrator consideration: FIA_UAU.1.

Table 7 : TOE Security Functional Requirements

Security Functional Class	Security Functional Components
Security Audit FAU	FAU_GEN.1 Audit Data Generation.
	FAU_SAR.1 Audit review
	FAU_SAR.3 (1) Selectable audit review
	FAU_SAR.3 (2) Selectable audit review
	FAU_STG.1 Protected audit trail storage
	FAU_STG.4 Prevention of audit data loss
User Data Protection FDP	FDP_IFC.2 Subset information flow control
	FDP_IFF.1 (1) Simple security attributes
	FDP_IFC.1 Subset information flow control
	FDP_IFF.1 (2) Simple security attributes
	FDP_IFF.2 Complete Information Flow Control
	FDP_RIP.1 Subset residual information protection
Identification and Authentication FIA	FIA_UAU.1 Timing of authentication
	FIA_UID.2 User identification before any action
	FIA_ATD.1 User attribute definition
Security Management FMT	FMT_MOF.1 Management of security function behavior
	FMT_MSA.1 (1) Management of security attributes
	FMT_MSA.1 (2) Management of security attributes
	FMT_MSA.1 (3) Management of security attributes
	FMT_MSA.1 (4) Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 (1) Management of TSF data
	FMT_MTD.1 (2) Management of TSF data
	FMT_SMR.1 Security roles
Protection of the TSF FPT	FPT.STM.1 Reliable Time Stamps
	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation
Privacy FPR	FPR_PSE.1 (1) Pseudonimity
	FPR_PSE.1 (2) Pseudonimity

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Security 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 **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 8**; and
c) [The event in Table 8 listed at the “extended” level].

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 column four of Table 8].

Table 8 : Auditable events with specified level

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of **the authorized administrator** role.	The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role
FIA_UID.2	basic	All use of the user identification mechanism.	The user identities provided to the TOE
FIA_UAU.1	basic	Any use of the authentication mechanism.	The user identities provided to the TOE
FDP_IFF.1 (1)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FPT_STM.1	minimal	Changes to the time.	The identity of the authorized administrator performing the operation
FMT_MOF.1	extended	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation

FAU_SAR.1 Security audit review

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all 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.

FAU_SAR.3 (1) Selectable audit review (1)

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches* of audit data based on [
a) presumed subject address;
b) date and time;
c) ranges of addresses;
d) network service;
e) the TOE action (accept, deny, reject)]

FAU_SAR.3 (2) Selectable audit review (2)

FAU_SAR.3.1 The TSF shall provide the ability to perform *sorting* of audit data based on [

a) the chronological order of audit event occurrence.]

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* and [shall limit the number of audit records lost] if the audit trail is full.

5.1.2 Class FDP: User Data Protection

FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [Unauthenticated_SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.

b) information: all traffic sent through the TOE from one subject to another]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

FDP_IFF.1 (1) Simple security attributes (1)

FDP_IFF.1.1 (1) The TSF shall enforce the [Unauthenticated_SFP] based on the following types of subject and information security attributes: [

a) subject security attributes:
   - presumed address;
   - {no other subject attributes}.

b) information security attributes:
   - presumed address of source subject;
   - presumed address of destination subject;
   - transport layer protocol;
   - service;
   - range of dates and/or times;
   - {no other information security attributes}].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
   - the presumed address of the source subject, in the information translates to an internal network address;
   - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all

possible combinations of the values of the information flow security attributes, created by the authorized administrator;

- the presumed address of the source subject, in the information translates to an external network address;
- and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 - The TSF shall enforce the [none].
Note: There is no additional information flow control SFP rule.

FDP_IFF.1.4 - The TSF shall provide the [none].
Note: There is no additional SFP capability.

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].
Note: There is no rule, based on security attributes, that explicitly authorizes information flows.

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules: [

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external it entity on the external network;
c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;
e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject;
f) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is the same as the destination subject;
g) For network protocols supported by the TOE (IP, TCP, UDP and ICMP), the TOE shall reject malformed network service requests.
h) The TOE shall reject requests for access or services where the information arrives in a TCP packet with a sequence number that is not an expected connection sequence number.
i) The TOE shall reject requests for access or services when the counter of concurrent active connection concerned with this rule reaches the ‘number of permitted concurrent connections’ attributes].

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [Applicative_SFP] on [

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another.
b) information: HTTP, FTP, DNS and SMTP traffic sent through the TOE from one subject to another;
c) operation: pass information].

FDP_IFF.1 (2) Simple security attributes (2)

FDP_IFF.1.1 (2) - The TSF shall enforce the [Applicative_SFP] based on the following types of subject and information security attributes: [

a) subject security attributes:
   - presumed address;
   - {no other subject attributes}.

b) information security attributes:
   - presumed address of source subject;

- presumed address of destination subject;
- source and destination services;
- applicative command and parameters of the following services: HTTP, FTP, DNS or SMTP;
- {no other information security attributes}].

FDP_IFF.1.2 (2) - The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold: [

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator].

FDP_IFF.1.3 - The TSF shall enforce the [none].
Note: There is no additional information flow control SFP rule.

FDP_IFF.1.4 (2) - The TSF shall provide the following [

a) masquerading of the FTP and SMTP service banner].

FDP_IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].
Note: There is no rule, based on security attributes, that explicitly authorizes information flows.

FDP_IFF.1.6 (2) - The TSF shall explicitly deny an information flow based on the following rules:

a) For application protocols supported by the TOE (DNS, HTTP, SMTP and FTP), the TOE shall reject applicative commands not identified in Table 9 and not authorized by the authorized administrator.

Table 9 : Authorized applicative commands

HTTP							
OPTIONS	GET	HEAD	POST	PUT	DELETE	TRACE	CONNECT
SMTP							
HELO	MAIL	RCPT	DATA	RSET	SEND	SOML	SAML
VRFY	EXPN	NOOP	HELP	QUIT	AUTH	EHLO	ETRN
STARTTLS							
FTP							
USER	PASS	ACCT	CWD	CDUP	SMNT	QUIT	REIN
PORT	PASV	TYPE	STRU	MODE	RETR	STOR	STOU
APPE	ALLO	REST	RNFR	RNTO	ABOR	DELE	RMD
MKD	PWD	LIST	NLST	SITE	SYST	STAT	HELP
NOOP	MKD	XRMD	XPWD		XCUP	MDTM	SIZE
FEAT	MLST	MLSD	OPTS				
DNS							
NS	CNAME	SOA	WKS	PTR	HINFO	MINFO	MX
TXT	AAAA	AXFR	IN				

b) For the HTTP, FTP, SMTP and DNS application protocols, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC).

c) For the HTTP, FTP, SMTP and DNS application protocols, the TOE shall reject applicative commands that are not allowed by the authorized administrator.

d) For the HTTP application protocol, the TOE shall deny access or service requests that violate applicative options configured by the authorized administrator:
   - Maximum URL size
   - Forbidden words in URL
   - Forbidden HTTP client headers
   - Maximum client header line size
   - Forbidden HTTP server headers
   - Maximum server header line size

e) For the FTP application protocol, the TOE shall deny access or service requests that violate applicative options configured by the authorized administrator:
   - Authorized users
   - Maximum command line size

f) For the SMTP application protocol, the TOE shall deny access or service requests that violate applicative options configured by the authorized administrator:
   - Maximum command line size

g) For the DNS application protocol, the TOE shall deny access or service requests that violate applicative options configured by the authorized administrator:
   - DNS Types authorized by the authorized administrator
   - DNS Classes authorized by the authorized administrator

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [resources that are used by the subjects of the TOE to communicate through the TOE to other subjects].

5.1.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attributes definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to **~~individual users~~ an authorized administrator**: [

a) Identity;
b) association of a human user with the authorized administrator role;
c) password or certificate].

Note: The certificates are provided by the Certificate Authority created on the FAST Firewall during the Initialization Procedure.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 - The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the ~~user~~ **authorized administrator** accessing the TOE, to be performed before the ~~user~~ **authorized administrator** is authenticated.

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

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each ~~user~~ **authorized administrator** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Class FMT: Security Management

FMT_MOF.1 – Management of security functions behavior

FMT_MOF.1.1 - The TSF shall restrict the ability to ***perform*** the functions: [

a) start-up and shutdown;
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;

c) archive, delete, empty, and review the audit trail;
d) enable and disable remote administration from internal and external networks;
e) restrict addresses from which remote administration can be performed;]

to [an authorized administrator].

FMT_MSA.1 (1) Management of security attributes (1)

FMT_MSA.1.1 (1) - The TSF shall enforce the [Unauthenticated_SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule,] the security attributes [listed in section FDP_IFF1.1 (1)] to [the authorized administrator].

FMT_MSA.1 (2) Management of security attributes (2)

FMT_MSA.1.1 (2) - The TSF shall enforce the [Applicative_SFP] to restrict the ability to [add attributes to a rule, delete attributes from a rule, modify attributes in a rule,] the security attributes [listed in section FDP_IFF1.1 (2)] to [the authorized administrator].

FMT_MSA.1 (3) Management of security attributes (3)

FMT_MSA.1.1 (3) - The TSF shall enforce the [Unauthenticated_SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in FDP_IFF.1 (1)] to [the authorized administrator].

FMT_MSA.1 (4) Management of security attributes (4)

FMT_MSA.1.1 (4) - The TSF shall enforce the [Applicative_SFP] to restrict the ability to [create and delete] the security attributes [information flow rules described in FDP_IFF.1 (2)] to [the authorized administrator].

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [Unauthenticated_SFP and potentially the Applicative_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 [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 (1) Management of TSF data (1)

FMT_MTD.1.1 (1) - The TSF shall restrict the ability to *query, modify, delete, [assign]* the [user attributes defined in FIA_ATD.1.1] to [the authorized administrator].

FMT_MTD.1 (2) Management of TSF data (2)

FMT_MTD.1.1 (2) - The TSF shall restrict the ability to *[set]* the [time and date used to form the timestamps in FPT_STM.1.1] to [the authorized administrator].

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the role [authorized administrator].

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

5.1.5 Class FPR: Privacy

Note: In the security function requirements FPR_PSE.1 (Dynamic) and FPR_PSE.1 (Static), users are external IT entities on the internal network and are identified by an IP address which stands for their real name.

FPR_PSE.1 Pseudonymity (Dynamic)

FPR_PSE.1.1 (Dynamic) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real user name bound to [external IT entities on the internal network that generate connections to external IT entities on the external network].

FPR_PSE.1.2 (Dynamic) The TSF shall be able to provide [10000] aliases of the real user name to [external IT entities on the internal network].

FPR_PSE.1.3 (Dynamic) The TSF shall *determine an alias for a user* and verify that it conforms to the [none].

FPR_PSE.1 Pseudonymity (Static)

FPR_PSE.1.1 (Static) The TSF shall ensure that [external IT entities on the external network] are unable to determine the real user name bound to [external IT entities on the internal network].

FPR_PSE.1.2 (Static) The TSF shall be able to provide [255] aliases of the real user name to [external IT entities on the internal network].

FPR_PSE.1.3 (Static) The TSF shall *determine an alias for a user* and verify that it conforms to the [static NAT rules as specified by the authorized administrator].

5.1.6 Class FPT: Protection of the TOE Security Functions

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2 TOE Security Assurance Requirements

The security assurance components drawn from CC Part 3 Security Assurance Requirements EAL 2 are identified in Table 10. Augmented security assurance components with regards to EAL2 are followed by (*).

Table 10 : TOE Security Assurance Requirements: EAL2 augmented

Assurance Class	**Assurance Component**		**Dependencies**
Configuration Management	ACM_CAP.2	Configuration items	None
Delivery and Operation	ADO_DEL.1	Delivery procedures	None
	ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
Development	ADV_FSP.1	Informal functional specification	ADV_RCR.1
	ADV_HLD.2(*)	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
	ADV_RCR.1	Informal correspondence demonstration	None
Guidance Documents	AGD_ADM.1	Administrator guidance	ADV_FSP.1
	AGD_USR.1	User guidance	ADV_FSP.1
Tests	ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
	ATE_FUN.1	Functional testing	None
	ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1 AGD_USR.1, ATE_FUN.1
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
	AVA_VLA.2(*)	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.2 AGD_ADM.1, AGD_USR.1 ADV_IMP.1 and ADV_LLD.1 are not applicable.
	AVA_MSU.1(*)	Examination of guidance	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
Life Cycle	ALC_DVS.1(*)	Identification of security measures	None
	ALC_FLR.3(*)	Systematic Flaw Remediation	None

5.2.1 Configuration Management ACM

5.2.1.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

960 ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery Procedure ADO

5.2.2.1 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development ADV

5.2.3.1 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance Documents AGD

5.2.4.1 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Security Testing ATE & AVA

5.2.5.1 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 ATE_IND.2 Independent testing – sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.5.4 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.2.5.5 AVA_VLA.2 Independent vulnerability analysis

Developer action elements:

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

Evaluator action elements:

AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

5.2.5.5 AVA_MSU.1 Examination of guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.2.6 Life cycle support ALC

5.2.6.1 ALC_DVS.1

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.6.2 ALC_FLR.3

Developer action elements:

ALC_FLR.3.1D The developer shall document the flaw remediation procedures.

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D The developer shall designate one or more specific points of contact for user reports and inquiries about security issues involving the TOE.

Content and presentation of evidence elements:

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.7C The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

1380 Evaluator action elements:

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3 Security Requirements for the IT Environment

The TOE has no security requirement allocated to its IT environment.

6 TOE SUMMARY SPECIFICATION

This Chapter presents a functional overview of the TOE; the security functions implemented by the TOE; and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

This Section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1. The overall minimum Strength of Function claim for the TOE SFRs is SOF-HIGH.

6.1.1 Security Audit

FAU_GEN.1 Audit Data Generation

Auditing involves identification, recording, storage and review of information related to security relevant events. The TOE generates log messages that provide a rich information basis to detect tampering with the TOE security mechanisms or the TSP. These messages can be of two types: Alerts and IP logs. IP logs are generated when a connection is mediated by the TOE or when a data packet is blocked or rejected because of the TSP. Alert messages are generated for all other security relevant events.

The TOE is able to generate audit records for auditable events defined below:

a) Start-up and shutdown of the FAST Firewall;
b) Start-up and shutdown of the audit services
c) All auditable events for the level of audit as specified in table listed in FAU_GEN.1.1;
d) The decision whether a packet is to be dropped, blocked or accepted according to the TSP;

The security audit function addresses this requirement.

FAU_SAR.1 Audit Review

The TOE provides a graphical Monitoring Console installed on the FAST Administration Station for authorized administrators to review all the log entries of audited events and detect tampering with the TOE security mechanisms or the TSP. Alert messages are reported by type and severity with the time of occurrence and a description of the event. IP log messages are reported with extensive details related to the packet or the connection causing the event. Alert and IP logs messages are documented, as well as the meaning of the messages, and the appropriate action that an authorized administrator needs to take.

The security audit function addresses this requirement.

FAU_SAR.3 (1) Selectable Audit Review

Graphical interface windows of the Monitoring Console provide the authorized administrator with the mean to review the logs and search by specific attributes of each audited event.

The security audit function addresses this requirement.

FAU_SAR.3 (2) Selectable Audit Review

Graphical interface windows of the Monitoring Console provide the authorized administrator with the mean to sort the logs by chronological order.

The security audit function addresses this requirement.

FAU_STG.1 Protected Audit Trail Storage

The log database can be accessed either through the FAST Monitoring Console or through the FAST Appliance Console. Since both are in the protected enclave, they can only be accessed by the authorized administrator. The means to access the audit logs is therefore limited to authorized administrators to prevent unauthorized deletion.

The security audit function addresses this requirement.

FAU_STG.4 Prevention of Audit Data Loss

ARKOON appliances presented in this Security Target provide a hard disk storage that is used to store millions of log entries. The log database allows an authorized administrator to export the data for storage outside of the TOE. In the case where a table of the log database or a log queue reaches a size close to its maximum size, the TOE prevents further auditable events, except those taken by the authorized administrator to prevent audit data loss.

The security audit function addresses this requirement.

6.1.2 User Data Protection

FDP_IFC.2: Complete information flow control (Unauthenticated_SFP)

The TSF enforces the Unauthenticated_SFP on all IT entities that send and receive information through the TOE to one another to mediate the flow of all information at the network and transport levels. This TSF includes network information sent and received over the following protocols: ICMP, TCP, IP, and UDP.

ARKOON appliances act as stateful inspection firewalls that examine each packet and track network and transport-layer information for each connection. The state of connections considered *active* is stored in a state table. The FAST engine uses this table and the information flow security policy rules to determine whether a data packet is legitimate as part of an existing or a new connection. The data packet can then be dropped, rejected or passed to the next analysis step according to the TSP. By default, an ARKOON FAST firewall denies all network traffic.

The user data protection function addresses this requirement.

FDP_IFC.1 (2): Information Flow Control (Applicative_SFP)

For the HTTP, FTP, SMTP and DNS protocols, ARKOON appliances can be configured to act as stateful inspection firewalls that examine each packet and track information *up to the application layer* to mediate the flow of all information at the application level. When the packet has successfully passed the Unauthenticated_SFP analysis and conforms to the associated rules, it may pass through the Applicative_SFP if this SFP is invoked by an authorized administrator.

The TSF enforces the Applicative_SFP on all IT entities that send and receive information through the TOE to one another when the SFP is invoked.

The application information is processed through the Protocol Analyzer which will verify it conforms to the well known application protocol standards and the FAST options configured by the authorized administrator.

The user data protection function addresses this requirement.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1 (1): Simple Security Attributes (Unauthenticated_SFP)

The Unauthenticated_SFP enforces the use of an information flow rule established by an authorized administrator to filter on certain external IT entities and to take an appropriate action depending on the content of a packet or the default policy. An information flow rule contains at least the following elements:

- addresses of source and destination subjects;
- transport layer protocol;

- service;
- range of dates and/or times;

The information flow rules can be configured to build a security policy based on all combinations of these elements.

The FAST appliance physically separates connected networks and by default denies all network traffic. The FAST Engine will enforce the security policy based on network information attributes to prevent impermissible information to flow from one network to another, being the only way to pass through the appliance.

FDP_IFF.1 (2): Simple Security Attributes (Applicative_SFP)

The Applicative_SFP enforces the use of an information flow rule established by an authorized administrator to filter on certain external IT entities and to take an appropriate action depending on the content of a packet or the default policy. An information flow rule contains at least the following elements:

- addresses of source and destination subjects;
- transport layer protocol;
- service + associated FAST module;
- range of dates and/or times;

The information flow rules can be configured to build a security policy based on all combinations of these elements. The FAST module element is used to perform in-depth stateful analysis of the application-layer data and verify that each packet conforms to the application protocol standards and to the options configured by the authorized administrator.

The FAST appliance physically separates connected networks and by default denies all network traffic. The FAST Engine will enforce the security policy based on network and application information attributes to prevent impermissible information to flow from one network to another, being the only way to pass through the appliance.

FDP_RIP.1 Subset Residual Information Flow

Full residual information protection is implemented in the FAST Firewall and the processing of packets through the FAST Firewall ensures that this requirement is met. Hence, residual information from a previous information flow is not transmitted in any way.

The User Data Protection function addresses this requirement.

6.1.3 Identification and Authentication

FIA_ATD.1 (1) User attribute Definition

To uniquely identify and authenticate all users before they are granted access to the TOE functions, the TSF maintains an identity and credentials for each authorized administrator authorized to manage the security configuration of the TOE. Each authorized administrator is defined by a username, credentials, and a role: Read or Read-Write authorized administrator.

The security identification and authentication function addresses this requirement.

FIA_UAU.1 Timing of Authentication

To prevent unauthorized access to the TOE functions as well as reliable accountability for authorized administrator use of security functions, the ARKOON FAST Administration and Appliance Consoles require authorized administrators to perform authentication before they may access any of the TOE functions or data.

The authentication policy required to meet the assurance requirements of AVA_SOF.1 is described below. Passwords for authentication through the appliance console or the administration consoles must conform to the rules:

1) Minimum of 8 characters
2) The possible characters belong to the character sets :
   a. a-z,
   b. A-Z,
   c. 0-9,
   d. &”~#’{([-|`_\@)]+=}<>$*%!/:.;?,
3) Characters must be chosen among at least three of the above character sets.

This policy ensures a very low probability of guessing the password while eliminating the possibility to choose trivial passwords that could be guessed using a dictionary attack.

If these rules are followed, the probability of guessing the password is less than one in 10^{15}. The strength of function claim for this SFR is SOF-HIGH.

The security identification and authentication function addresses this requirement.

FIA_UID.2 User Identification before any Action

To prevent unauthorized access to the TOE functions as well as reliable accountability for authorized administrator use of security functions, an authorized administrator has to identify and authenticate through a login interface before any action on the FAST Firewall. When accessing the FAST Firewall through the Appliance Console, the authorized administrator will be prompted for her login and password before any other action on the console. When accessing the FAST firewall through the Administration Consoles, the authorized administrator will be prompted for her PKCS#12 personal information file and passphrase before any other action on the console that may impact the TOE.

The security identification and authentication function addresses this requirement.

6.1.4 Security Management

FMT_MOF.1 (1) Management of security functions behavior

Only authorized administrators can enter the protected area and access the Administration Consoles or the FAST Appliance Console, using their login/password or PKCS#12 personal information file /passphrase respectively. These consoles are the only interfaces to:

- start up, shutdown the FAST Firewall;
- create, delete, modify, and view information flow security policy rules that permit or deny information flows;
- archive, delete, empty, and review the audit trail;
- enable and disable remote administration from internal and external networks;
- restrict addresses from which remote administration can be performed.

The Security Management Function addresses this requirement.

FMT_MSA.1 (1) and FMT_MSA.1 (3)

Only authorized administrators can enter the protected area and access the Administration Consoles or the FAST Appliance Console, using their login/password or PKCS#12 personal information file /passphrase respectively. These consoles are the only interfaces to set up the Unauthenticated_SFP on the FAST Firewall.

The Security Management Function addresses these requirements.

FMT_MSA.1 (2) and FMT_MSA.1 (4)

Only authorized administrators can enter the protected area and access the Administration Consoles or the FAST Appliance Console, using their login/password or PKCS#12 personal information file /passphrase respectively. These consoles are the only interfaces to set up the Applicative_SFP on the FAST Firewall.

The Security Management Function addresses this requirement.

FMT_MSA.3 Static Attribute Initialization

By default, the FAST Firewall will deny any information flow to pass through the FAST Appliance. Hence, by default the TOE cannot compromise its resources or those of any connected network. The authorized administrator is instructed in the administrative guidance how to set up a security policy.

The Security Management function addresses this requirement.

FMT_SMR.1 Security Roles

To ensure that only authorized administrators can access the TOE security functions, the FAST Firewall provides three security roles: an appliance console, a read-only and a read-write administrative role. Read-only authorized administrators will be able to view network and applicative information flow security policy, while read-write authorized administrators will be able to create, delete, modify and view it. Appliance console authorized administrators will be able to initialize the firewall.

Concerning the audit review, the two roles have the same rights.

The Security Management function addresses this requirement

FMT_MTD.1 (1) Management of TSF Data

Only authorized administrators can enter the protected area and access the Administration Station or the FAST Appliance which are the two only ways to query, modify, delete and assign the identity of a human user and its association with the authorized administrator role.

The Security Management Function addresses this requirement.

FMT_MTD.1 (2) Management of TSF Data

Only authorized administrators can enter the protected area and access the Administration Station or the FAST Appliance which are the two only ways to set up or modify the time and date on the FAST Firewall.

The Security Management Function addresses this requirement.

6.1.5 Privacy

FPR_PSE.1 Pseudonymity (Dynamic)

Dynamic NAT hides the protected network addresses from External IT on the external network. Hosts elsewhere on the external network only see the external IP address of the FAST Firewall. Dynamic NAT translates addresses of TCP, UDP and ICMP-based transmissions.
The packets are mapped to an available port on the FAST Firewall, their source addresses are re-written with the IP address of the FAST Firewall, and the selected port number.
When a packet comes to the FAST Firewall, it is checked against the connection table and if translation is needed, it will map the packet IP addresses to those of the masqueraded host.

This address translation is called dynamic because a new port for masquerading is used for each connection.

FPR_PSE.1 Pseudonymity (Static)

Static NAT provides mapping of External IT on the Internal Network toward the External Network. Upon definition of the mapping of an IP address and port number of an External IT on the Internal Network with an IP Address and port number on the FAST Firewall, any connection to the combination IP address and port number will be re-written by the FAST Firewall with the IP address and port number of the destination External IT.

Static NAT is generally used for public services like Web Servers.

6.1.6 Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

By default the TOE will not allow any flow in any direction, and after the setting up of a policy, the FAST engine will process the information to meet the TSPs, being the only way to pass through the FAST appliance from one interface to the other.

The Protection of the TOE security function addresses this requirement.

FPT_SEP.1 TSF Domain Separation

The TOE remains in an area protected from interference and tampering by untrusted subjects.

The connectivity between the security domains is enclosed in the security area; the TOE will always be separating the different domains and can not be bypassed.

The Management Console running on the Administration Station, providing identification and authentication, and giving access to the TSF’s management is protected through a certificate mechanism, physically protected, and can only be accessed by authorized administrators.

For security application embedded on the FAST Appliance but not part of the TOE, by default they are not activated.

The Protection of the TOE security function addresses this requirement.

FPT_STM.1 Reliable time stamps

FAST appliance provides a reliable clock, and the FAST Engine uses this clock to provide reliable time stamps. Moreover, the database keeps the track of the record number which is unique and incremental.

The Protection of the TOE security function addresses this requirement.

6.2 Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements as defined in Common Criteria part 3:

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Life Cycle Support
- Tests
- Vulnerability Assessment

Some assurance measures satisfy augmented requirements as detailed in Section 8.4 Assurance Requirements Rationale.

Configuration Management

The configuration management measures applied by ARKOON Network Security ensure that configuration items are uniquely identified and their content is controlled. The related procedures and activities are documented in

- Firewall ARKOON: Gestion de Configuration.

The configuration management assurance measures satisfy the ACM_CAP.2 assurance requirements.

Delivery and Operation

ARKOON Network Security follows documented production and delivery procedures to identify the TOE, package the TOE, allow detection of unauthorized modifications of the TOE. ARKOON’s Getting Started Guidance describes ARKOON’s appliances and the procedures to be used for secure installation, generation and start-up of the TOE. The related procedures and activities are documented in

- Firewall ARKOON: Procédures d’intégration et de livraison ;
- Firewall ARKOON: Guide de prise en main.

The delivery and operation assurance measures satisfy the ADO_DEL.1 and ADO_IGS.1 assurance requirements.

Development

ARKOON Network Security provides functional specifications for the TOE. These specifications include the identification and description of the TOE external interfaces. The high-level design documentation describes the main sub components of the TOE, how they participate to the implementation of the TOE security functions and how they operate together through internal interfaces. Correspondence documentation shows that the TOE functions, the functional specifications and the high-level design are consistent. The development documentation consists of the following documents:

- Firewall ARKOON : Description des Fonctions de Sécurité ;
- Firewall ARKOON: Architecture et Conception de Haut Niveau ;
- Firewall ARKOON: Analyse de correspondance.

The development assurance measures satisfy the ADV_FSP.1, ADV_HLD.2 and ADV_RCR.1 assurance requirements.

Guidance Documents

ARKOON Network Security provides administrator guidance on how to administer the TOE in a secure manner and how to make effective use of the TSF. The administrator guidance also describes the TOE administration interfaces, the outputs and the associated steps to take to maintain the desired TOE security level. The administrator guidance consists of the following documents:

- Firewall ARKOON: Guide de l’Administrateur ;
- AkMon Aide en ligne ;
- AkMan Aide en ligne ;
- Firewall ARKOON: Guide de prise en main.

As the administrator of an ARKOON FAST firewall is also its main user, the guidance documents assurance measures satisfy the AGD_ADM.1 and AGD_USR.1 assurance requirements.

Life Cycle Support

ARKOON Network Security follows documented policies and procedures to ensure the security of the TOE development environment and remediate to flaws discovered in the TOE while it is supported. A whole department of ARKOON Network Security is dedicated to customer service and ensures that detected flaws are identified, repaired and distributed together with information and guidance to the consumers. The related procedures and activities are documented in

- Firewall ARKOON : Description de l’environnement de développement ;
- Firewall ARKOON : Support Utilisateur ;
- Firewall ARKOON: Veille technologique.

The life cycle support assurance measures satisfy the ALC_DVS.1 and ALC_FLR.3 assurance requirements.

Tests

ARKOON Network Security provides functional coverage evidence of its testing of the TOE security requirements stated in this ST. A set of test cases corresponding to the TSF describes for each test which interfaces and functions are tested, how they are tested, the expected outcome of the test and the actual outcome. The TOE and the test documentation are also submitted to functional independent testing. Testing of the TOE is documented in

- Firewall ARKOON: Dossier de tests de la cible d’évaluation.

The tests assurance measures satisfy the ATE_COV.1, ATE_FUN.1 and ATE_IND.2 assurance requirements.

Vulnerability Assessment

ARKOON Network Security performs systematic vulnerability analyses of the TOE to search for potential weaknesses that could be exploited in the TOE. Vulnerability analyses are documented in

- Firewall AKOON: Etude de vulnérabilité.

ARKOON Networks Security provides administrator guidance which enables an administrator to determine if the TOE is configured and operating in a manner that is insecure. The administrator guidance consists of the following documents:

- Firewall ARKOON: Guide de l’Administrateur ;
- AkMon Aide en ligne ;
- AkMan Aide en ligne ;
- Firewall ARKOON: Guide de prise en main.

All of the SOF claims are based on password space calculations documented in

- ARKOON Firewall: Strength of function analysis.

The vulnerability assessment assurance measures satisfy the AVA_VLA.2, AVA_SOF.1 and AVA_MSU.1 assurance requirements.

1820 Table 11 shows which assurance measures are traced to the assurance requirements identified in Section 5.2 TOE Security Assurance Requirements.

Table 11 : Summary of Mapping between Assurance Measures, Assurance Requirements and Documentation

Assurance Measure	Assurance Requirements	Documentation
Configuration Management	ACM_CAP.2 Configuration items	Gestion de Configuration
Delivery and Operation	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation, and start-up procedures	Procédures d'intégration et de Livraison Guide de prise en main
Development	ADV_FSP.1 Informal functional specification ADV_HLD.2 Descriptive high-level design ADV_RCR.1Informal correspondence demonstration	Description des Fonctions de Sécurité Architecture et Conception de Haut Niveau Analyse de correspondance
Guidance Documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance	Guide de l'Administrateur AkMon Aide en ligne AkMan Aide en ligne Guide de prise en main
Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing-sample	Dossier de tests de la cible d'évaluation
Vulnerability Assessment	AVA_SOF.1 Strength of TOE security function evaluation AVA_VLA.2 Developer vulnerability analysis AVA_MSU.1 Examination of guidance	Etude de vulnérabilité Guide de l'Administrateur AkMon Aide en ligne AkMan Aide en ligne Guide de prise en main
Life Cycle Support	ALC_DVS.1 Identification of security measures ALC_FLR.3 Systematic Flow Remediation	Description de l'environnement de développement Support Utilisateur Veille technologique

7 PP CLAIMS

This Security Target does not claim to comply with any PP.

8 RATIONALE

This section provides the rationale for:

- Security Objectives;
- Security Requirements;
- TOE Summary Specification;
- Security Functional Requirement Dependencies; and
- Internal Consistency.

8.1 Rationale for IT Security Objectives

O.IDAUTH This security objective is necessary to counter the threats T.NOAUTH and T.REPEAT because it requires that users be uniquely identified before accessing the TOE.

O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT, T.OLDINF and T.SYNFLOOD which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

O.MEDIATAPP This security objective is necessary to counter threats: T.MEDIAT and T.PROT_MIS because it requires that the TOE screens applicative (HTTP, SMTP, DNS and FTP) information flow and deny illegitimate information flows.

O.SECSTA This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH, T.MEDIAT, T.PROT_MIS and T.SELPRO.

O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC This security objective is necessary to counter the threats: T.AUDACC and T.NODETECT by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

O.ACCOUN This security objective is necessary to counter the threats: T.AUDACC and T.NODETECT because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.

O.PRIVACY This security objective is necessary to counter the threat: T.PRIVACY because it requires that the TOE hide addresses of the IT external entities on the internal network from the external network.

Table 12 maps Threats to TOE Security Objectives. A straightforward reverse analysis of both the summary of mappings between threats and IT security objectives and the rationale for each IT security objective shows that each and every threat is countered by a set of one or more objectives and how it is countered.

Table 12: Summary of Mappings Between Threats and IT Security Objectives

THREATS **OBJECTIVES**	T.NOAUTH	T.REPEAT	T.ASPOOF	T.MEDIAT	T.PROT_MIS	T.OLDINF	T.AUDACC	T.SELFPRO	T.AUDFUL	T.PRIVACY	T.NODETECT	T.SYNFLOOD
O.IDAUTH	**X**	**X**										
O.MEDIAT			**X**	**X**		**X**						**X**
O.MEDIATAPP				**X**	**X**							
O.SECSTA	**X**			**X**	**X**			**X**				
O.SELFPRO								**X**	**X**			
O.AUDREC							**X**				**X**	
O.ACCOUN							**X**				**X**	
O.SECFUN	**X**								**X**			
O.PRIVACY										**X**		

8.2 Rationale for Security Objectives for the Environment

OE.PHYSEC The processing resources of the TOE that depend on hardware security features are located within controlled access facilities that mitigate unauthorized, physical access.

OE.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.

OE.PUBLIC The TOE does not host public data.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

OE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.

OE.DIRECT Human users within the physically secure boundary protecting the TOE may only attempt to access the TOE from some direct connection through the FAST Administration Consoles or through the FAST Appliance Console.

OE.NOREMO Human users cannot access the TOE remotely from the internal or external networks for administrative purpose.

OE.LOCATE The access to the FAST Administration Station and to the FAST Appliance shall be restricted to the authorized administrators.

OE.OSVER The Operating System installed on the Administration Station shall be an up-to-date version of Windows 2000 OS.

OE.SINUSE The environment shall prevent an unauthorized person from trying to replay a former authentication process in order to launch attacks on the TOE.

OE.GUIDAN This non-IT security objective is necessary to counter the threat: TE.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

OE.ADMTRA This non-IT security objective is necessary to counter the threat: TE.TUSAGE because it ensures that authorized administrators receive the proper training.

Since the rest of the security objectives for the environment are, in part, a re-statement of the security assumptions, those security objectives trace to all aspects of the assumptions.

Table 13 maps Threats and Assumptions to the Objectives for the environment. A straightforward reverse analysis of both the summary of mappings between threats and security objectives for the environment and the rationale for each security objective for the environment shows that each and every threat and assumption is countered by a set of one or more objectives for the environment and how it is countered.

Table 13 : Summary of Mapping between Threats and Security Objectives for the Environment

	TE.USAGE	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.PHYSEC	A.NOREMO	A.LOCATE	A.OSVER	A.SINUSE
OE.GUIDAN	X										
OE.ADMTRA	X										
OE.GENPUR		X									
OE.PUBLIC			X								
OE.NOEVIL				X							
OE.SINGEN					X						
OE.DIRECT						X					
OE.PHYSEC							X				
OE.NOREMO								X			
OE.LOCATE									X		
OE.OSVER										X	
OE.SINUSE											X

8.3 Rationale for Security Requirements

The rationale for the chosen level of SOF-high is based on the medium attack potential of the threat agents identified in this Security Target. Those security objectives imply probabilistic or permutational security mechanism and that the metrics defined should be good enough for SOF-high.

FAU_GEN.1 Audit data generation

This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU_SAR.1 Audit review

This component ensures that the audit trail is usable and understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_SAR.3 (1-2) Selectable audit review

This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU_STG.1 Protected audit trail storage

This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FAU_STG.4 Prevention of audit data loss

This component ensures that audit data for new auditable events as defined in FAU_GEN.1 will be correctly generated and stored even if the audit trail should come close to its maximum size. A limited set of the oldest entries of the audit trail is expunged and an alert is logged for this event. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

FDP_IFC.2 Complete information flow control

This component identifies the entities involved in the Unauthenticated information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFF.1 (1) Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the Unauthenticated SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP_IFC.1 Subset information flow control

This component identifies the entities involved in the Applicative information flow control SFP (i.e., users sending HTTP, FTP, SMTP or DNS information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIATAPP.

FDP_IFF.1 (1) Simple security attributes

This component identifies the attributes of the users sending and receiving the information in the Applicative SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIATAPP.

FDP_RIP.1 Subset residual information protection

This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

FIA_ATD.1 User attributes definition

This component exists to provide authorized administrators with attributes to distinguish one authorized administrators 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 following objective: O.IDAUTH.

FIA_UAU.1 Timing of authentication

This component ensures that authorized administrators are authenticated at the TOE. Identification is the only action allowed before authentication. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. An additional SOF metric for this requirement is defined in Section 5.1.3 Class FIA: Identification and Authentication to ensure that the authentication mechanism chosen cannot be easily bypassed. This component traces back to and aids in meeting the following objective: O.IDAUTH.

FIA_UID.2 User identification before any action

This component ensures that before anything occurs on behalf of an authorized administrator, the authorized administrator identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FMT_MOF.1 Management of security functions behavior

This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.

FMT_MSA.1 (1-4) Management of security attributes

These components ensure that only an authorized administrator can administrate the rules and their related attributes that implement the Unauthenticated and Applicative SFPs. These components trace back to and aid in meeting the following objectives: O.SECFUN and O.SECSTA.

FMT_MSA.3 Static attribute initialization

This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

FMT_MTD.1 (1-2)

These components ensure that only an authorized administrator can administrate the user attributes defined in FIA_ATD.1.1 and time and date used to form the timestamps in FPT_STM.1.1. They aid in meeting the objectives O.SELPRO and O.SECFUN.

FMT_SMR.1 Security roles

Each of the CC class FMT components in this Security Target depend on this component which defines the authorized administrator role. This component traces back to and aids in meeting the following objective: O.SECFUN.

FPR_PSE.1 Pseudonimity (Dynamic)

This component ensures that the internal network pseudonimity can be achieved by dynamically masquerading connections from external IT entities on the internal network to external IT entities on the external network behind a single source address and dynamically allocated ports. This component traces back to and aids in meeting the following objective: O.PRIVACY.

FPR_PSE.1 Pseudonimity (Static)

This component ensures that the internal network pseudonimity can be achieved by statically masquerading connections from external IT entities on the internal network to external IT entities on the external network behind a static source address associated to an IT entity on the internal network. This component traces back to and aids in meeting the following objective: O.PRIVACY.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_SEP.1 TSF domain separation

This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT_STM.1 Reliable time stamps

FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

Table 14 maps SFRs to the TOE Security Objectives. A straightforward reverse analysis of both the summary of mappings between SFRs and the TOE Security Objectives and the rationale for each SFR shows that each and every TOE Security Objective is countered by a set of one or more SFRs and how it is countered.
Besides, the ST satisfies the functional requirement dependencies of the Common Criteria as shown in Table 15.

Table 14 : Mapping SFRs to the TOE Security Objectives

CLASS	OBJECTIVES SFR	O.IDAUTH	O.MEDIAT	O.MEDIATAPP	O.SECSTA	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.PRIVACY
SECURITY AUDIT	FAU_GEN.1						X	X		
	FAU_SAR.1						X			
	FAU_SAR.3 (1-2)						X			
	FAU_STG.1					X			X	
	FAU_STG.4					X			X	
USER DATA PROTECTION	FDP_IFC.2		X							
	FDP_IFF.1 (1)		X							
	FDP_IFC.1			X						
	FDP_IFF.1 (2)			X						
	FDP_RIP.1		X							
IDENTIFICATION AND AUTHENTICATION	FIA_UAU.1	X								
	FIA_UID.2	X						X		
	FIA_ATD.1	X								
SECURITY MANAGEMENT	FMT_MOF.1				X				X	
	FMT_MSA.1 (1-4)				X				X	
	FMT_MSA.3		X		X				X	
	FMT_MTD.1 (1-2)				X				X	
	FMT_SMR.1								X	
PROTECTION OF THE TSF	FPT_STM.1						X			
	FPT_RVM.1					X				
	FPT_SEP.1					X				
PRIVACY	FPR_PSE.1 (1)									X
	FPR_PSE.1 (2)									X

8.4 Assurance Requirements Rationale

EAL2 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the postulates that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

2120 AVA_VLA.1, ADV_HLD.1 were augmented to AVA_VLA.2, ADV_HLD.2 to rise the resistance level of the security target as specified in the Memento v1.0 on the Standard Level - Security Product Qualification Process by the DCSSI.

AVA_MSU.1 was added to the EAL2 regular components to ensure that guidance to install, initialize and administrate the ARKOON FAST Firewall enables an administrator to understand if the firewall is configured and operated in an insecure manner.

ALC_DVS.1 and ALC_FLR.3 were added to the EAL2 regular components to ensure that Security Target development and maintenance are conducted according to good security practices.

Section 6.2 shows which assurance measures are traced to the assurance requirements identified in Section 5.2 TOE Security Assurance Requirements and how assurance requirements are fulfilled.

Rationale for not satisfying all dependencies

Although assurance component AVA_VLA.2 depends on assurance components ADV_IMP.1 and ADV_LLD.1, these components are not requested by in the Memento v1.0 on the Standard Level - Security Product Qualification Process by the DCSSI which this Security Target complies with.

8.5 Requirement Dependency Rationale

2140 The ST satisfies the functional requirement dependencies of the Common Criteria as shown in Table 15.

Table 15 : Security Functional Requirements Dependencies

Class	SFR	Dependencies	Satisfied
SECURITY AUDIT	FAU_GEN.1	FPT_STM.1	YES
	FAU_SAR.1	FAU_GEN.1	YES
	FAU_SAR.3 (1-2)	FAU_SAR.1	YES
	FAU_STG.1	FAU_GEN.1	YES
	FAU_STG.4	FAU_STG.1	YES
USER DATA PROTECTION	FDP_IFC.2	FDP_IFF.1	YES
	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	YES YES
	FDP_IFC.1	FDP_IFF.1	YES
	FDP_IFF.1 (1)	FDP_IFC.1 FMT_MSA.3	YES YES
	FDP_RIP.1	None	NA
IDENTIFICATION AND AUTHENTICATION	FIA_UAU.1	FIA_UID.1	YES
	FIA_UID.2	None	N/A
	FIA_ATD.1	None	N/A
SECURITY MANAGEMENT	FMT_MOF.1 (1-2)	FMT_SMR.1	YES
	FMT_MSA.1 (1-4)	FDP_IFC.1 FMT_SMR.1	YES YES
	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES YES
	FMT_MTD.1 (1-2)	FDP_IFC.1 FMT_SMR.1	YES YES
	FMT_SMR.1	FIA_UID.1	YES
PROTECTION OF THE TSF	FPT_STM.1	None	N/A
	FPT_RVM.1	None	N/A
	FPT_SEP.1	None	N/A
PRIVACY	FPR_PSE.1 (1)	None	N/A
	FPR_PSE.1 (2)	None	N/A

Note: N/A means Not Applicable

8.6 Summary Specification Rationale

The TOE Summary Specification chapter describes every Security Function of the TOE, meeting the requirements of every SFR. Within the description of the SF, a rationale is provided. All the SFs are presented in Table 16; this table maps SFRs to SFs. This demonstrates that the Security Functions fulfill every SFR.

Table 16 : Mapping Security Functional Requirements to Security Functions

SECURITY FUNCTIONS SFR	SECURITY AUDIT	USER DATA PROTECTION	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF THE TSF	PRIVACY
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.3 (1-2)	X					
FAU_STG.1	X					
FAU_STG.4	X					
FDP_IFC.2		X				
FDP_IFF.1		X				
FDP_IFC.1 (1)		X				
FDP_IFF.1 (2)		X				
FDP_RIP.1		X				
FIA_UAU.1			X			
FIA_UID.2			X			
FIA_ATD.1			X			
FMT_MOF.1 (1-2)				X		
FMT_MSA.1 (1-4)				X		
FMT_MSA.3				X		
FMT_MTD.1 (1-2)				X		
FMT_SMR.1				X		
FPT_STM.1					X	
FPT_RVM.1					X	
FPT_SEP.1					X	
FPR_PSE.1 (1-2)						X