Marconi SA-400 Firewall Version 1.3 Security Target

May 27, 2004
Document No. F2-0504-007

Prepared for:

Marconi Communications Federal, Inc.
5457 Twin Knolls Road, Suite 101
Columbia, Maryland 21045
Phone: 410-884-5648
Fax: 410-884-5600

Prepared By:

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587
Phone: 301-498-0150
Fax: 301-498-0855

Marconi and COACT, Inc. assume no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Marconi SA-400 Firewall Version 1.3. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives and security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	May 27, 2004, initial release.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS LIST

AAL ..... ATM Adaptation Layer
ATM..... Asynchronous Transfer Mode
CC ..... Common Criteria
CCTL ..... Common Criteria Testing Lab
EAL..... Evaluation Assurance Level
FCP ..... Firewall Control Processor
FIP..... Firewall Inline Processor
GUI .....Graphical User Interface
ICMP..... Internet Control Message Protocol
IDE..... Integrated Drive Electronics
IGMP..... Internet Group Multicast Protocol
ILMI..... Interim Local Management Interface
IP ..... Internet Protocol
IT..... Information Technology
LANE.....Local Area Network Emulation
MPOA.....Multi-Protocol Over ATM
NNI ..... Network-to-Network Interface
NSAP .....Network Service Access Point
PCI ..... Peripheral Component Interconnect
PNNI ..... Private Network-to-Network Interface
PP .....Protection Profile
PVC..... Permanent Virtual Connection
SAP ..... SPANS Service Access Point
SHTTP ..... Secure Hypertext Transfer Protocol
SPANS ..... Simple Protocol for ATM Network Signaling
ST..... Security Target
SVC.....Switched Virtual Connection
TCP .....Transmission Control Protocol
TOE..... Target of Evaluation
TSF.....TOE Security Function
TSP.....TOE Security Policy
UDP..... User Datagram Protocol
UNI .....User-to-Network Interface
URL..... Uniform Resource Locator
VCI.....Virtual Channel Identifier
VPI .....Virtual Path Identifier

CHAPTER 1

1. Security Target Introduction

1.1 Security Target Identification

This section provides identifying information for the Marconi SA-400 Firewall, Version 1.3 Security Target (ST), by identifying information regarding the Target of Evaluation (TOE).

1.1.1 Security Target Name

Marconi SA-400 Firewall Version 1.3 Security Target, dated May 27, 2004.

1.1.2 TOE Identification

Marconi SA-400 Firewall Version 1.3.

1.1.3 Evaluation Status

This ST has been evaluated against the *Common Methodology for Information Technology Security Evaluation Part 2 Version 1.0*.

1.1.4 Evaluation Assurance Level

Functional claims conform to Part 2 of the Common Criteria Version 2.1. Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from Part 3 of the Common Criteria Version 2.1. Both the functional and assurance claims contained in this ST have been updated to incorporate all applicable national and international interpretations through 16 April 2002.

1.1.5 Keywords

Firewall, Security, Asynchronous Transfer Mode (ATM), Internet Protocol (IP), Marconi, packet filter, SA-400 and traffic filter.

1.2 Security Target Overview

This ST describes the objectives, requirements and rationale for the SA-400 Firewall. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1* and the *ISO/IEC JTC 1/SC27, Guide for the Production of PPs and STs, Version 0.9*. As such, the spelling of terms is presented using the internationally accepted English.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the SA-400 TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the SA-400 to satisfy the security functional and assurance requirements.

Chapter 7 provides a rationale for claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides rationale statements to justify the TOE meeting its claimed security objectives.

1.3 Common Criteria Conformance

The SA-400 Firewall is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) conformant and assurance requirements (Part 3) conformant for EAL2.

1.4 Protection Profile Conformance

The SA-400 Firewall does not claim conformance to any Protection Profile.

CHAPTER 2

2. TOE Description

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

2.1 TOE Description

The Target of Evaluation is the Marconi SA-400 Firewall, Version 1.3. The SA-400 provides Enterprise Networks with reliable IP/ATM Firewall capabilities at OC-12 line rate. The appliance is managed by a web interface accessible by a 10/100 Ethernet port. This allows the administrator to configure, save and load filtering tables via a simplified Graphical User Interface (GUI). The interface also allows the administrator to start, stop, and reset the Firewall. A log is available to review administrator and system interactions.

The SA-400 Firewall is comprised of a number of sub-systems including hardware, software and firmware. At the highest level, the SA-400 appears as an industrial PC chassis in a standard 19" rack-mount configuration. At this level, externally visible interfaces are evident. These interfaces are: the A.C. Power Entry Module, a 9 pin Serial Port, a standard 10/100 Ethernet port and OC-12 Multi-mode fiber optic Inside and Outside network ports. Moving in or down a level reveals redundant power supplies, a PC Motherboard, an IDE Hard Drive and Firewall PCI card that occupies slot 1.

The Firewall PCI card communicates to the Software sub-system via the 32-bit 33 MHz PCI Bus. PCI slot 1 is set up as the bus master. A dedicated software driver is used by the Software sub-system to communicate to the card. Flows from the Inside or Outside port that are registered in the FPGA on the PCI card are processed at line rates. Flows that are not registered in hardware on the PCI card must be sent to the software via the PCI interface.

The two major systems that enforce the security policy on the unit are the Firewall Inline Processor (FIP) which resides in the FPGA on the PCI line card and the Firewall Control Processor (FCP) which is part of the SA-400 software application which resides on the local hard drive. The figures below identify the TOE architecture.

Figure 1 - SA-400 Physical Boundary

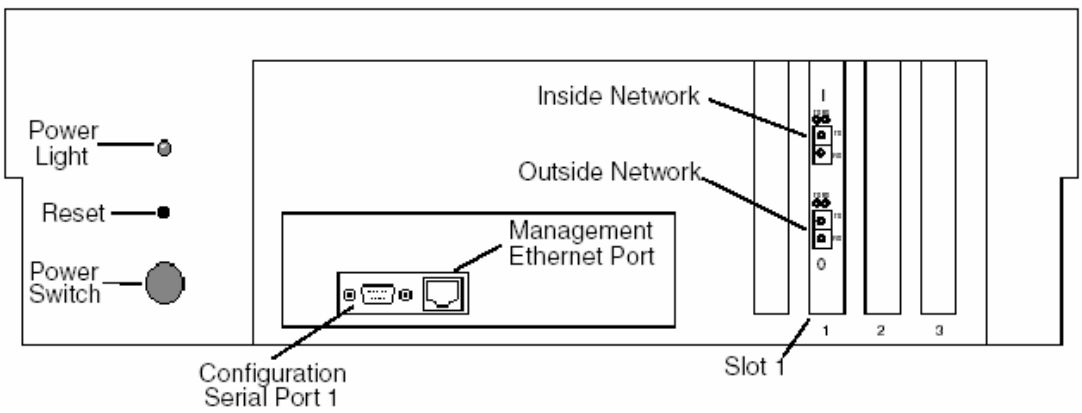
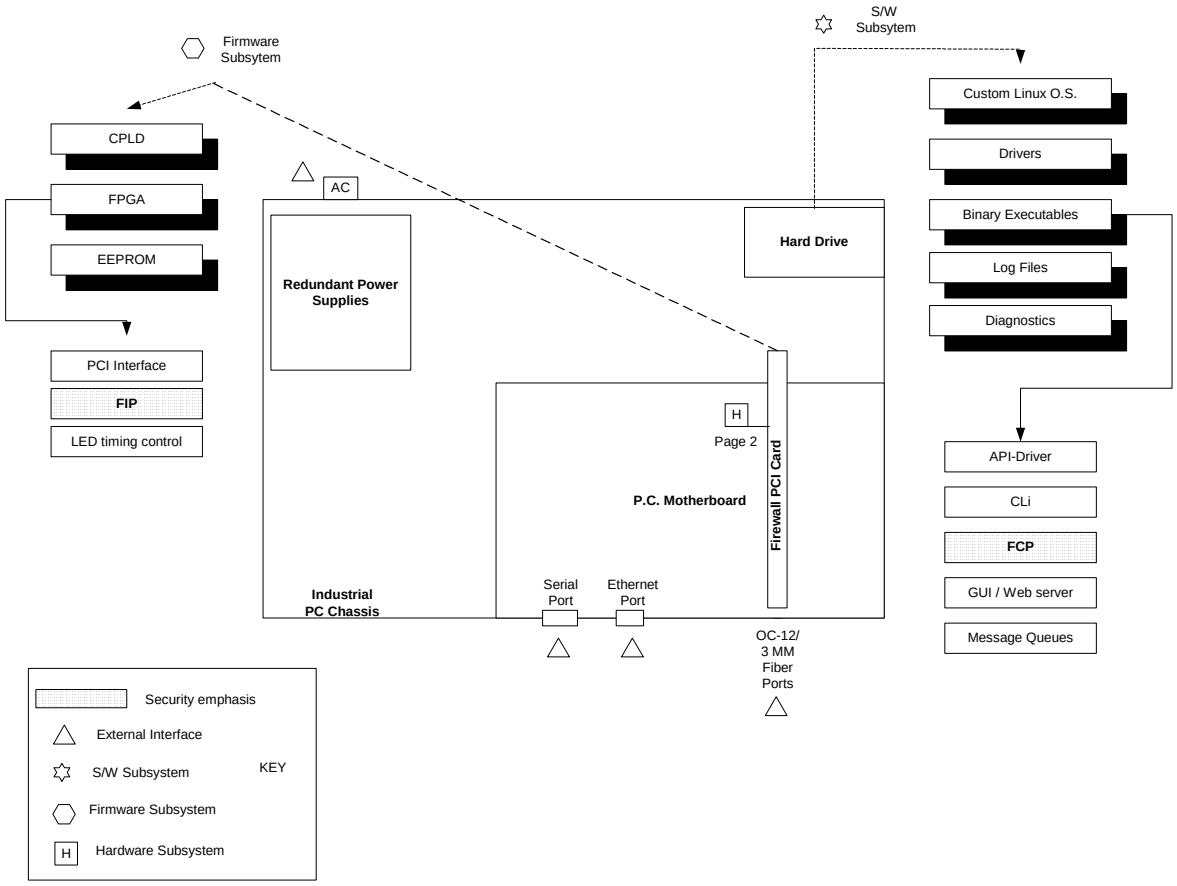


Figure 2 - SA-400 Logical Boundary



2.2 TOE Features

The SA-400 implements the following firewall features:

A) IP Filtering Support based on:

1) IP Source and Destination Address
2) IP Protocol
3) TCP
4) UDP
5) ICMP
6) IGMP

B) ATM NSAP Filtering Support

C) VPI/VCI Filtering

D) Statistics and Counters

E) Flexible Web Interface

F) Command Line Interface - Administrator Configuration

2.3 Evaluated Configuration

The evaluated configuration requires:

A) Local logging and storage of audit records

B) Local timestamp generator for use in audit records

C) Serial and Ethernet ports used to manage the TOE are connected to a LAN that contains only trusted administration systems (e.g. only the management workstation)

2.4 TOE Features Outside the Scope of the Evaluated Configuration

The following features are outside the scope of the evaluated configuration of the TOE:

A) Remote Logging and Storage of Records

B) Network Time Protocol Server – Used to generate time stamps for audit records

C) Software Upgrades

D) SSL Encryption

E) Dual Redundant, Hot Swappable AC Power Supply

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies threats (T), organisational security policies (P) and assumptions (A). For assumptions, threats or policies that apply to the environment, the initial character is followed by a period and then an 'E'. For example, T.E.USE is a threat to be countered by the security environment to ensure proper configuration and administration of the TOE.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Personnel Assumptions

A.USERS Users of the TOE shall be trained and are trusted to enforce the security aspects of the TOE relevant to them.

3.2.2 Physical Assumptions

A.LOCATE The TOE shall be located in a secure facility that mitigates unauthorised physical access.

3.3 Threats

3.3.1 Threats Addressed by the TOE

T.DIRECT An unauthorised user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions of the TOE.

T.REPLAY An unauthorised user may use valid identification and authentication data obtained to access functions provided by the TOE.

T.BYPASS An unauthorised user may attempt to bypass the information flow control policy.

T.DATA An unauthorised user may read, modify or destroy security critical TOE configuration data.

3.3.2 Threats Addressed by the TOE Environment

T.E.USE The TOE may be inadvertently configured, used and administered in an insecure manner by either authorised or unauthorised users.

3.4 Organisational Security Policies

There are no organisational security policies required for the TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

All of the objectives listed in this section ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives (O) for the SA-400 Firewall are:

O.FILTER The TSF will enforce defined filtering rules to allow or deny network traffic to pass through the TOE.

O.ADMIN The TOE will allow the administrator the capability to securely manage the TOE / TSF data.

4.2 Security Objectives for the IT Environment

O.E.CONNECT Users shall ensure that the TOE is located in a physically controlled environment that mitigates unauthorised tampering.

O.E.USERS Users of the TOE shall be trained and are trusted to enforce the security aspects of the TOE relevant to them.

4.3 Security Objectives Rationale

Table 1 demonstrates the correspondence between the security objectives listed in Sections 4.1 and 4.2 to the assumptions identified in Section 3.2.

Table 1 - Correspondence Between Assumptions, Threats and Policies to Objectives

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = TOE		
Assumption, Threat or Policy	**Security Objectives**	**Rationale**
A.USERS	O.E.USERS	Users of the TOE must be trained and trusted to operate the TOE in a manner that maintains security.
A.LOCATE	O.E.CONNECT	Enforcement of physical access control reduces risk and protects the TOE and its assets from unauthorised modification.
T.DIRECT	O.ADMIN	Only the administrator can manipulate TOE / TSF data through the management path.
T.REPLAY	O.ADMIN	During authentication through the management path, the IP address must match an allowed IP listing

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment, .T = TOE		
Assumption, Threat or Policy	**Security Objectives**	**Rationale**
		stored in the TOE before access is granted to other parts of the TOE.
T.BYPASS	O.FILTER	All traffic passing through the firewall is subject to filtering rules applied on a channel separate from the management path. This prevents circumventing information flow filters enforced by the TOE.
T.DATA	O.ADMIN	The administrator is the only authorised user of the TOE and performs configuration of the TOE through a separate management path. Traffic passing through the firewall is processed on a separate channel to prevent unauthorised modification to the TOE.
T.E.USE	O.E.CONNECT O.E.USERS	It is the responsibility of the administrator to ensure that the TOE is securely configured, used and managed in their environment.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC).

The strength of function required for all applicable Security Functional Requirements in this TOE is basic. The requirements realised by probabilistic or permutational mechanisms include FIA_UAU.2 and FIA_UID.2.

5.1 Security Functional Requirements

Table 2 lists the functional requirements and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 2 have been satisfied.

Table 2 - Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Component Helps Address
FAU_GEN.1	Audit Data Generation	No Other Components	FPT_STM.1	O.FILTER
FAU_SAR.1	Audit Review	No Other Components	FAU_GEN.1	O.ADMIN
FAU_SAR.2	Restricted Audit Review	No Other Components	FAU_SAR.1	O.ADMIN
FAU_STG.1	Protected Audit Trail Storage	No Other Components	FAU_GEN.1	O.ADMIN
FAU_STG.3	Action in Case of Possible Audit Data Loss	No Other Components	FAU_STG.1	O.ADMIN
FDP_IFC.1	Subset Information Flow Control	No Other Components	FDP_IFF.1	O.FILTER
FDP_IFF.1	Simple Security Attributes	No Other Components	FDP_IFC.1, FMT_MSA.3	O.ADMIN
FIA_ATD.1	User Attribute Definition	No Other Components	None	O.ADMIN
FIA_UAU.2	User Authentication Before any Action	FIA_UAU.1	FIA_UID.1	O.ADMIN

CC Component	Name	Hierarchical To	Dependency	Objectives Component Helps Address
FIA_UAU.6	Re-Authenticating	No Other Components	None	O.ADMIN
FIA_UAU.7	Protected Authentication Feedback	No Other Components	FIA_UAU.1	O.ADMIN
FIA_UID.2	User Identification Before any Action	FIA_UID.1	None	O.ADMIN
FIA_USB.1	User-Subject Binding	No Other Components	FIA_ATD.1	O.ADMIN
FMT_MOF.1	Management of Security Functions Behaviour	No Other Components	FMT_SMR.1 FMT_SMF.1	O.ADMIN O.FILTER
FMT_MSA.1	Management of Security Attributes	No Other Components	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	O.ADMIN O.FILTER
FMT_MSA.3	Static Attribute Initialisation	No Other Components	FMT_MSA.1, FMT_SMR.1	O.ADMIN O.FILTER
FMT_MTD.1	Management of TSF Data	No Other Components	FMT_SMR.1, FMT_SMF.1	O.ADMIN O.FILTER
FMT_MTD.2	Management of Limits on TSF Data	No Other Components	FMT_MTD.1, FMT_SMR.1	O.ADMIN O.FILTER
FMT_SMF.1	Specification of Management Functions	No Other Components	None	O.ADMIN O.FILTER
FMT_SMR.1	Security Roles	No Other Components	FIA_UID.1	O.ADMIN
FPT_RVM.1	Non-Bypassability of the TSP	No Other Components	None	O.ADMIN

CC Component	Name	Hierarchical To	Dependency	Objectives Component Helps Address
FPT_SEP.1	TSF Domain Separation	No Other Components	None	O.ADMIN
FPT_STM.1	Reliable Time Stamps	No Other Components	None	O.ADMIN O.FILTER
FTA_SSL.1	TSF-Initiated Session Locking	No Other Components	FIA_UAU.1	O.ADMIN
FTA_TSE.1	TOE Session Establishment	No Other Components	None	O.ADMIN

The functional requirements that appear in Table 2 are described in more detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.1* with the exception of italicised items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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

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

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

C) [*events as defined for the following:*

1) *System Log: system initialisation, hardware PCI card detection, status of firewall control processor (active/idle), results of diagnostic tests, hardware specification of PCI card, link-up/link-down status, transmit and receive cell counters, login for serial and Ethernet interfaces, and management of TSF data;*

2) *Web Interface Log: User login identification and method of access, source IP, management of TSF data, recording of rule modifications and maintenance;*

3) *Monitor Log: protocol (including number), source IP, destination IP, source port and destination port;*

4) *Disallowed Packets Log: for all packets that are not allowed source IP address, destination IP address, protocol (including number), source port and destination port; and*

5) *Open Connections Log (dynamic): VPI, VCI, source NSAP address and destination NSAP address]*.

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, [*none*].

Dependencies: FPT_STM.1 Reliable Time Stamps.

Rationale: Auditing on the SA-400 is performed using a System Log, Web Interface Log, Monitor Log, Disallowed Packets Log and an Open Connections Log (dynamic). These logs are stored in a protected partition on the local hard drive and are used to audit events both locally and remotely.

5.1.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [*the administrator*] with the capability to read [*all audit information*] 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.

Dependencies: FAU_GEN.1 Audit Data Generation.

Rationale: The TOE provides the facility to review the audit records using the standard SA-400 Web Graphical User Interface on the local machine. These records are individual logs stored as flat files. Note that the flat files use spaces to delineate separate fields.

5.1.1.3 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit Review.

Rationale: Only the administrator has the capability to read the audit records.

5.1.1.4 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

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

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

Dependencies: FAU_GEN.1 Audit Data Generation.

Rationale: The TOE does not permit the deletion of events from the audit logs. Once the logs have reached their storage capacity, the oldest records are overwritten with the most recent events.

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

Hierarchical to: No other components.

FAU_STG.3.1 The TSF shall take [*overwrite the oldest audit records*] if the audit trail exceeds [*the defined limits as follows:*

A) *System Log: 100 files (1/2MB limit per file)*

B) *Web Interface Log: 100 files (1/2MB limit per file)*

C) *Monitor Log: 100 files (2MB limit per file)*

D) *Disallowed Packets Log: 100 files (2MB limit per file)*

E) *Open Connections Log (dynamic): 2MB total*].

Dependencies: FAU_STG.1 Protected Audit Trail Storage.

Rationale: If the System Log, Web Interface Log, Monitor Log and Disallowed Packets Log grow beyond their defined limits, the oldest logs will be over-written with the most recent. The Open Connections Log is dynamic and is limited to 2MB.

5.1.2 User Data Protection

5.1.2.1 FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [*Firewall Filtering Flow Control Policy*] on [*source subject: TOE interface on which information is received, destination subject: TOE interface on which information is destined, information: data types (UNI, SPANS, PVC, IP) to explicitly allow or deny access based upon data type attributes (VPI, VCI, source port and address, destination port and destination address, protocol)*].

Application Note: In a firewall, the central issue is that there are two "subjects" (the sender of the packet (information) and the receiver of the packet) neither of which are under the control of the TOE. In order to use the FDP_IF requirements, the potential set of subjects is associated with a firewall interface.*

Dependencies: FDP_IFF.1 Simple Security Attributes.

Rationale: The SA-400 implements a structured flow of control of information between a subject and the Access Control List (ACL) on the H/W PCI Firewall card. The security policy processing is accomplished with interaction between the FCP, Driver and FIP.

5.1.2.2 FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [*Firewall Filtering Flow Control Policy*] based on the following types of subject and information security attributes: [*subjects information and attributes as defined in Table 3*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*subject rules on operations as defined in Table 3*].

Table 3 - Information, Attributes and Operations

Information	Attributes	Operations
UNI Filtering	Src NSAP Address	Allow, Deny, Forward for IP Filtering
	Dest NSAPAddress	Allow, Deny, Forward for IP Filtering
	Direction	Incoming, Outgoing, Both
SPANS Filtering	Src Address	Allow, Deny, Forward for IP Filtering
	Src SAP	Allow, Deny, Forward for IP Filtering
	Dest Address	Allow, Deny, Forward for IP Filtering
	Dest SAP	Allow, Deny, Forward for IP Filtering
	Direction	Incoming, Outgoing, Both
PVC Filtering	VPI	Allow, Deny, Forward for IP Filtering
	VCI	Allow, Deny, Forward for IP Filtering
	Direction	Incoming, Outgoing, Both
IP Filtering	Src Address	Allow, Deny, Monitor
	Src Port	Allow, Deny, Monitor
	Dest Port	Allow, Deny, Monitor
	Dest Address	Allow, Deny, Monitor
	Protocol	Allow, Deny, Monitor
	Direction	Incoming, Outgoing, Both

FDP_IFF.1.3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4 The TSF shall provide the following [*no additional rules*].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based upon the following rules: [*no additional rules*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based upon the following rules: [*all information flows are denied unless explicitly authorised rules have been defined in accordance with the Firewall Filtering Flow Control Policy*].

Dependencies: FDP_IFC.1 Subset Information Flow Control,

FMT_MSA.3 Static Attribute Initialisation.

Rationale: Authorized users of the SA-400 may configure filtering rules based on the information and attributes shown in the table above to control the Firewall Filtering Flow Control Policy. If there is an omission of an operational parameter associated with any particular subject, then an explicit deny is in place. This explicit deny prohibits all information to flows for the subject.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*login ID, password and IP address*].

Dependencies: No dependencies.

Rationale: The TOE provides a serial connection that allows access to the TSF through a Command Line Interface. This interface is used to configure the security attributes for the administrator role. The IP address of the remote machine that will access the TOE through the web interface must be configured also. The TSF then stores the security attributes in a protected partition on the hard drive. Once this has been configured, the user will be able to access the TOE through the web interface (10/100 Ethernet connection) using their identification and authentication information. Once this action has successfully completed, the user will then be recognised as an administrator of the TOE.

5.1.3.2 FIA_UAU.2 User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication.

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of Identification.

Rationale: The TSF requires all users to be identified and authenticated through the web interface (Ethernet) and serial interface for command line access prior to allowing any other TSF-mediated actions on behalf of that user. The Strength of Function claim for this probabilistic / permutational mechanism is rated as basic.

5.1.3.3 FIA_UAU.6 Re-Authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [*30-3600 seconds of inactivity (180 seconds default) or after logging off of the TOE through the web interface (10/100 Ethernet connection)*].

Dependencies: No dependencies.

Rationale: Once an administrator has been authenticated by the TSF through the web interface (10/100 Ethernet), re-authentication is required after a period of inactivity that is configurable by the administrator. This period of inactivity is set at 180 seconds by default and can be modified by the administrator to a range between 30-3600 seconds. In addition, once the administrator has logged off of the TOE the TSF also requires re-authentication.

5.1.3.4 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only [*the number of characters (marked as asterisks) typed for the 'Password'*] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of Authentication.

Rationale: When a user logs onto the TOE through the serial interface for command line access or the web interface (10/100 Ethernet), the characters entered for the 'Login' are displayed, while characters entered for the password are masked with asterisks to represent keystrokes.

5.1.3.5 FIA_UID.2 User Identification Before any Action

Hierarchical to: FIA_UID.1 Timing of Identification.

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

Dependencies: No dependencies.

Rationale: The TSF requires all users to be identified and authenticated through the web interface (Ethernet) and serial interface for command line access prior to allowing any other TSF-mediated actions on behalf of that user. The Strength of Function claim for this probabilistic / permutational mechanism is rated as basic.

5.1.3.6 FIA_USB.1 User-Subject Binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User Attribute Definition.

Rationale: After a user has been successfully identified and authenticated, the TSF uses the appropriate user security attributes with processes on the TOE that are acting on behalf of the user.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable, enable, modify the behaviour of*] the functions [*all functions covered by the Firewall Filtering Flow Control Policy to allow or deny an information flow*] to [*the administrator*].

Dependencies: FMT_SMR.1 Security Roles and FMT_SMF.1 Management of Security Functions.

Rationale: The administrator is the only role recognised by the TOE. The functions managed through the serial Command Line Interface are limited to configuring the TOE to allow for administrator credential definitions and setting the system clock. The functions managed through the web interface (10/100 Ethernet) include starting/stopping the firewall, viewing/modifying rules, viewing log files and control of the firewall functions available on the navigation page and sub-menus.

5.1.4.2 FMT_MSA.1 Management of Security Attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [*Firewall Filtering Flow Control Policy*] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [*all attributes covered by the Firewall Filtering Flow Control Policy to allow or deny an information flow*] to [*the administrator*].

Dependencies: [FDP_ACC.1 Subset Access Control

or

FDP_IFC.1 Subset Information Flow Control],

FMT_SMR.1 Security Roles and

FMT_SMF.1 Management of Security Functions.

Rationale: The administrator is the only role recognised by the TOE. Attributes managed through the serial Command Line Interface include the Login ID, Password and IP address for administrator and clock settings acquired by the real-time clock. Attributes managed through the web interface (10/100 Ethernet) include applying filtering rules to allow or deny network traffic, session idle time before re-identification and re-authentication is required.

5.1.4.3 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [*Firewall Filtering Flow Control Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*the administrator*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of Security Attributes,

FMT_SMR.1 Security Roles.

Rationale: Default values are set to explicitly deny all information flows without administrator modification of the filtering rules. The default value for session idle time before re-authentication is required is set at 180 seconds. The administrator can specify an alternative value between 30-3600 seconds of inactivity.

5.1.4.4 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [*change_default, query, modify, delete, clear*] the [*functions and attributes covered by the Firewall Filtering Flow Control Policy*] to [*the administrator*].

Dependencies: FMT_SMR.1 Security Roles and FMT_SMF.1 Management of Security Functions.

Rationale: The administrator manages all TSF data identified in the Firewall Filtering Flow Control Policy.

5.1.4.5 FMT_MTD.2 Management of Limits on TSF Data

Hierarchical to: No other components.

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [*IP active rules (500 maximum), ATM active rules (500 maximum) and audit data*] to [*the administrator*].

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [*IP rules (save additional rules in an inactive state), ATM rules (save additional rules in an inactive state) and audit data (overwrite the oldest audit records)*].

Dependencies: FMT_MTD.1 Management of TSF Data,

FMT_SMR.1 Security Roles.

Rationale: The administrator can create a maximum of 64,000 IP rules and 128,000 ATM rules however; only 500 rules for each can be active at any given time.

5.1.4.6 FMT_SMF.1 Specification of Management Function

Hierarchical to: No other components.

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions **through the CLI interface**[Refinement]: [*configure IP, SSL, user account, FCP, GUI, web server, and log parameters; perform diagnostics; update software; manage the system clock; and shutdown or reboot the system.*]

FMT_SMF.1.1(2) The TSF shall be capable of performing the following security management functions **through the GUI interface**[Refinement]: [*configure filtering rules, upload rules, view open connections, display statistics, start and stop the FCP, and viewing logs.*]

Dependencies: No dependencies.

Rationale: There are two distinct interfaces used to access the security management functions provided by the TOE. Together they provide the entirety of the security management functions.

5.1.4.7 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [*the administrator*].

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

Dependencies: FIA_UID.1 Timing of Identification.

Rationale: The administrator is the only role recognised by the TOE.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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.

Dependencies: No dependencies.

Rationale: The TSF is enforced under its own domain. All functions are loaded prior to processing operations as defined in the Firewall Filtering Flow Control Policy.

5.1.5.2 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

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.

Dependencies: No dependencies.

Rationale: TSF data is stored within the TOE on a hard drive and Firewall Inline Processor (FIP) chip located on the firewall PCI card. TSF data is protected during transmission between these two parts of the TOE through a management channel. User data is filtered on a separate channel. During filtering, if user data traffic violates the TSP rules, then the event is copied to the audit logs and the traffic flow is denied.

5.1.5.3 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies.

Rationale: The Real-Time Clock on the motherboard is used for the generation of time stamps.

5.1.6 TOE Access (FTA)

5.1.6.1 FTA_SSL.1 TSF-Initiated Session Locking

Hierarchical to: No other components.

FTA_SSL.1.1 The TSF shall lock an interactive session after [*30-3600 seconds (default is 180 seconds) if inactivity on the serial interface*] by:

A) clearing or overwriting display devices, making the current contents unreadable;

B) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*re-authentication*].

Dependencies: FIA_UAU.1 Timing of Authentication.

Rationale: After the administrator has been locked out after a period of inactivity, re-authentication is required.

5.1.6.2 FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*invalid username, password or IP address*].

Dependencies: No dependencies.

Rationale: For a user to initiate a session with the TOE, they must first have a record in the TSF that defines their username, password and IP permissions. If any of these items do not match what is stored in the TSF, then TOE session establishment will not be allowed.

5.2 TOE Security Assurance Requirements

The assurance components for the TOE are summarised in Table 4.

Table 4 - Assurance Components

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.1	Descriptive High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_COV.1	Evidence of Coverage
Tests	ATE_FUN.1	Functional Testing

Assurance Class	Component ID	Component Title
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

The following subsections provide more detail for the assurance components listed in Table 4.

5.2.1 Configuration Management (ACM)

5.2.1.1 ACM_CAP.2 Configuration Items

Dependencies: No dependencies.

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.

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 and Operation (ADO)

5.2.2.1 ADO_DEL.1 Delivery Procedures

Dependencies: No dependencies.

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

Dependencies: AGD_ADM.1 Administrator Guidance.

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

Dependencies: ADV_RCR.1 Informal Correspondence Demonstration.

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.1 Descriptive High-Level Design

Dependencies: ADV_FSP.1 Informal Functional Specification,

ADV_RCR.1 Informal Correspondence Demonstration.

Developer Action Elements:

ADV_HLD.1.1D The developer shall provide a high-level design of the TSF.

Content and Presentation of Evidence Elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C 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.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator Action Elements:

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

ADV_HLD.1.2E 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

Dependencies: No dependencies.

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

Dependencies: ADV_FSP.1 Informal Functional Specification.

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 administrative 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 behaviour 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 relative 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

Dependencies: ADV_FSP.1 Informal Functional Specification.

Developer Action Elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and Presentation of Action 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 behaviour found in the statement of TOE security environment.

AGD_USR.1.5C 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 Tests (ATE)

5.2.5.1 ATE_COV.1 Evidence of Coverage

Dependencies: ADV_FSP.1 Informal Functional Specification,

ATE_FUN.1 Functional Testing.

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

Dependencies: No dependencies.

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 tests 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 tests 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

Dependencies: ADV_FSP.1 Informal Functional Specification,

AGD_ADM.1 Administrator Guidance,

AGD_USR.1 User Guidance,

ATE_FUN.1 Functional Testing.

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 resourced 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.

5.2.6 Vulnerability Assessment (AVA)

5.2.6.1 AVA_SOF.1 Strength of TOE Security Function Evaluation

Dependencies: ADV_FSP.1 Informal Functional Specification,

ADV_HLD.1 Descriptive High-Level Design.

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.

5.2.6.2 AVA_VLA.1 Developer Vulnerability Analysis

Dependencies: ADV_FSP.1 Informal Functional Specification,

ADV_HLD.1 Descriptive High-Level Design,

AGD_ADM.1 Administrator Guidance,

AGD_USR.1 User Guidance.

Developer Action Requirements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and Presentation of Evidence Elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator Action Elements:

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

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.3 Security Requirements for the IT Environment

There are no security requirements on the IT environment.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The major functions implemented by the TOE are:

A) Main Extraction Process (FIP)

The Main extraction process buffers incoming cells that are entering the firewall Inside or Outside port. It buffers the data until a complete packet is assembled. While buffering, it extracts the header information revealing ATM VP, VC and PTI fields. It sends cells to the Call Set-up process, the PVC process or the SVC process.

B) Call Set-up Process (FIP, FCP)

The Call Set-up process sends ATM signaling message cells to the firewall output port (either Inside or Outside) and to the FCP call set-up process. The process consists of the FIP (firmware- PCI card) and the FCP (S/W). The FIP portion sends the cells to the output port while the FCP simultaneously processes the Connect, Ack, Release messages within the data. This is done to prevent a noticeable delay in the call set-up procedure between the switches. The signaling protocol and this process set up a SVC between two endpoints and create a table of VC, VP pairs with an associated SVC flag.

C) PVC Filtering Process (FIP, FCP)

PVCs allows a direct connection between ATM endpoints. They guarantee availability of a connection and do not require a call set-up procedure between ATM switches. They must be configured manually and are static in nature. The SA-400 is shipped with default PVC settings (VP, VC) that are used to allow dedicated signaling messages to flow freely between ATM switches.

When the firewall is in the static state, the PVC function communicates with the GUI during rule configuration (described in Management). When the firewall is in the active state, the PVC function receives cells from the Extraction Process and makes a decision to: Allow (send to output port), Deny (discard) or forward those cells to the IP module for further processing.

D) SVC ATM Filtering Process (FIP, FCP)

SVCs are created and released dynamically by the ATM network and remain in use as long as data is being transferred between network elements. SVCs require a signaling protocol to execute between ATM endpoints and an ATM switch to decide upon a usable VP/VC combination. The VP/VC values have only local significance. As the connection spans multiple switches, these VP/VC values may change. The two signaling protocols interpreted by the SA-400 are UNI and SPANS.

When the firewall is in the static state, the SVC function communicates with the GUI during rule configuration (described in Management). When the firewall is in the dynamic or active state, the SVC function receives cells from the Extraction Process and makes a decision based on configuration bits and rules to Allow, Deny or forwards those cells to the IP module for further processing. It also interacts with the Call Set-up Process and Management Process to log connection information about the particular SVC that is set-up or torn down.

UNI Signaling

The SA-400 must pass through UNI 3.1 and be able to be connected between two NNI nodes. The UNI filtering attributes shall include Source NSAP Address, Destination NSAP Address and an Action (Allow, Deny or Forward for IP Filtering).

SPANS Signaling

The SA-400 must recognise FORE IP SVC call setup information. The filtering attributes shall include Source Address, Source Access Point, Destination Address and Destination Access Point and an Action (Allow, Deny or Forward for IP Filtering)

E) IP Filtering Process (FIP, FCP)

The IP Process is a second level filtering function that is called by either the PVC or SVC function when the attribute of IP is selected in the rules. In the firewall's dynamic state, once a flow has passed the ATM filtering of PVC, SVC and has its configuration bits set to IP, it gets subjected to the filtering attributes of the IP module which are Source address, Destination address, Source port, Destination port, Protocol and Action. The IP settings are common to all PVC and SVC flows that have IP selected as an Action. For example, it isn't possible to subject PVC 0,100 and PVC 0,200 with separate IP rules. If any of the PVCs or SVCs has their "Action" set to IP, the same IP rules apply to all PVCs or SVCs.

When the firewall is in the static state, the IP function communicates with the GUI during rule configuration (described in Management). Changes to rules do not take affect until the firewall is Stopped/ Started or Restarted.

F) Monitor Process

When the attribute of "Monitor" is selected in the IP rules, the Monitor Process is executed. The purpose of the monitor function is to force designated ATM flows to create an entry into a Monitor Log for surveillance purposes. Since each flow is being processed and monitored in S/W, this causes noticeable delays to the monitored flows.

G) GUI Rule Management Process

All of the processes listed above (PVC, SVC, IP and Monitor) have interfaces with the GUI process. The administrator is able to select a

function such as PVC and obtain a visual display (HTML format) of the PVC rule data that is stored on the system hard drive. For a complete description of the entire GUI's interaction with the previous processes including configurable attributes, reference the SA-400 User's Manual and/or other sections of this document.

H) Auditing Process

The SA-400 provides auditing/logging functions to record TSF security relevant events on its local hard drive. The logs shall be separated into System Logs, Web Interface Logs, Connections Logs, Monitor Log and Disallowed Connections Log. An authorised user shall have the ability to review these files from the GUI on the local machine. Each authorised user shall have equal access to the security functions. The Log files shall be saved on a protected portion of the local hard drive and have a means to control the size and number of log files. For security purposes, a user cannot purge the log files. The "SYSLOG" function along with the "logrotate" facility manages the log files.

I) Identification/Authorisation/Access Process

The identification process is a sub-set of the Administrator Management Process. It is used to verify that the administrator has proper identification by means of "login name" and "password" before allowing interaction with the SA-400. Proper identification will allow the administrator to have access to the CLI and Web interface.

J) Administrator Management

The SA-400 shall be managed by a serial interface for configuration (setting IP address, allowable GUI users, SSL configuration, selecting speed of the OC-12 card, Inactivity timeout period, diagnostics, system shutdown, SYSLOG) and an Ethernet interface for configuring the security functions and associated attributes. Before being able to manage the Firewall, the user must be authorised through the identification/authorisation process. Ultimately, the administrator must verify that the rules they assign/establish are correct for their network security policy. For detailed information on managing specific policies, configurations, etc., refer to the SA-400 User's Manual.

Table 5 - Security Functional Requirements to Functions Mapping

Functional Requirement	Functions	Rationale
FAU_GEN.1	Auditing Process	The Auditing Process function implements the FAU_GEN.1 Functional Requirement by collecting and generating records for auditable events.

Functional Requirement	Functions	Rationale
FAU_SAR.1	Auditing Process	The Auditing Process function implements the FAU_SAR.1 Functional Requirement by allowing the administrator the capability to review all audit event records.
FAU_SAR.2	Auditing Process	The Auditing Process function implements the FAU_SAR.2 Functional Requirement by limiting read access to the audit records to the administrator.
FAU_STG.1	Auditing Process	The Auditing Process function implements the FAU_STG.1 Functional Requirement by protecting and preventing modifications to the audit records.
FAU_STG.3	Auditing Process	The Auditing Process function implements the FAU_STG.3 Functional Requirement by overwriting the oldest audit records when the defined log file limits has been exceeded.
FDP_IFC.1	Main Extraction Process (FIP), Call Set-up Process (FIP, FCP), PVC Filtering Process (FIP, FCP), SVC ATM Filtering Process (FIP, FCP), IP Filtering Process (FIP, FCP), Monitor Process	The Main Extraction Process (FIP), Call Set-up Process (FIP, FCP), PVC Filtering Process (FIP, FCP), SVC ATM Filtering Process (FIP, FCP), IP Filtering Process (FIP, FCP) and Monitor Process functions implement the FDP_IFC.1 Functional Requirement by implementing a structured flow of control of information between a user and the Access Control List on the H/W PCI Firewall card.
FDP_IFF.1	Main Extraction Process (FIP), Call Set-up Process (FIP, FCP), PVC Filtering Process (FIP, FCP), SVC ATM Filtering Process (FIP, FCP), IP Filtering Process (FIP, FCP), Monitor Process	The Main Extraction Process (FIP), Call Set-up Process (FIP, FCP), PVC Filtering Process (FIP, FCP), SVC ATM Filtering Process (FIP, FCP), IP Filtering Process (FIP, FCP), Monitor Process functions implement the FDP_IFF.1 Functional Requirement by filtering flows of information passing through the TOE based upon the subject and attributes, and allowed operations.

Functional Requirement	Functions	Rationale
FIA_ATD.1	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FIA_ATD.1 Functional Requirement by providing a serial connection that allows access to the TSF through a Command Line interface. This interface is used to configure and define user security attributes on the TOE.
FIA_UAU.2	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FIA_UAU.2 Functional Requirement by requiring each user to be identified and authenticated prior to allowing any other TSF-mediated action on behalf of the user.
FIA_UAU.6	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FIA_UAU.6 Functional Requirement by requiring each user to be re-authenticated after a defined period of inactivity.
FIA_UAU.7	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FIA_UAU.7 Functional Requirement by displaying the number of characters typed (marked with asterisks) to the user during authentication.
FIA_UID.2	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FIA_UID.2 Functional Requirement by requiring each user to be identified and authenticated prior to allowing any other TSF-mediated action on behalf of the user.
FIA_USB.1	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process implements the FIA_USB.1 Functional Requirement by using the appropriate user security attributes with processes on the TOE that are acting on behalf of the user.

Functional Requirement	Functions	Rationale
FMT_MOF.1	GUI Rule Management Process, Administrator Management	The GUI Rule Management Process and Administrator Management functions implement the FMT_MOF.1 Functional Requirement by restricting the management of functions covered by the Firewall Filtering Flow Control Policy to the administrator.
FMT_MSA.1	GUI Rule Management Process, Administrator Management	The GUI Rule Management Process and Administrator Management functions implement the FMT_MSA.1 Functional Requirement by restricting the management of security attributes covered by the Firewall Filtering Flow Control Policy to the administrator.
FMT_MSA.3	GUI Rule Management Process, Administrator Management	The GUI Rule Management Process and Administrator Management functions implement the FMT_MSA.3 Functional Requirement by providing default values for security attributes and allowing alternative values to be specified by the administrator.
FMT_MTD.1	GUI Rule Management Process, Administrator Management	The GUI Rule Management Process and Administrator Management functions implement the FMT_MTD.1 Functional Requirement by restricting the ability to manage all TSF data to the administrator.
FMT_MTD.2	GUI Rule Management Process, Administrator Management	The GUI Rule Management Process and Administrator Management functions implement the FMT_MTD.2 Functional Requirement by restricting the management of limits on TSF data to the administrator.
FMT_SMF.1 (1)	Administrator Management	Administrator Management function implements the FMT_SMF.1(1) Functional Requirement by providing the administrative functions to configure the GUI management capabilities for the administrator.

Functional Requirement	Functions	Rationale
FMT_SMF.1 (2)	GUI Rule Management Process	GUI Rule Management Process implements the FMT_SMF.1(2) Functional Requirement by providing the administrative functions to configure the firewall filtering rules.
FMT_SMR.1	GUI Rule Management Process, Administrator Management, Identification / Authorisation / Access Process	The GUI Rule Management Process, Administrator Management and Identification / Authorisation / Access Process functions implement the FMT_SMR.1 Functional Requirement by maintaining and associating users to the administrator role.
FPT_RVM.1	GUI Rule Management Process, Administrator Management and Main Extraction Process (FIP)	The GUI Rule Management Process, Administrator Management and Main Extraction Process (FIP) functions implement the FPT_RVM.1 Functional Requirement by ensuring TSP enforcement functions are invoked and succeeded before each function within the TSC is allowed to proceed.
FPT_SEP.1	GUI Rule Management Process, Administrator Management and Main Extraction Process (FIP)	The GUI Rule Management Process, Administrator Management and Main Extraction Process (FIP) functions implement the FPT_SEP.1 Functional Requirement by maintaining a security domain for TSF execution to provide protection from interference from untrusted subjects.
FPT_STM.1	Auditing Process, Administrator Management	The Auditing Process and Administrator Management functions implement the FPT_STM.1 Functional Requirement by providing timestamps for its own use.
FTA_SSL.1	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FTA_SSL.1 Functional Requirement by locking an interactive session after a period of inactivity and then requiring each user to be re-authenticated.

Functional Requirement	Functions	Rationale
FTA_TSE.1	Identification / Authorisation / Access Process	The Identification / Authorisation / Access Process function implements the FTA_TSE.1 Functional Requirement by denying a session establishment with the TOE based on an invalid username, invalid password or invalid IP permissions.

6.2 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in the following table, which provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 6 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Marconi SA-400 Firewall, Version 1.3 Security Target, Revision 8, September 16, 2003 Product Requirements Document (PRD), Rev. 1.7, 02/20/2002 Configuration Management Plan, Rev. A, 05/30/2001 Control of Internal Business Process Documentation Procedure, Rev. A, 09/2000 Control of Unreleased Product (CUP) Checklist, Rev. A, 12/19/2001 Procedure for the Control of Unreleased Product, Rev. C, 08/2000 Engineering Change Notice (ECN) Data Entry Work Instruction, Rev. B, 06/23/2000 Engineering Change Notice Procedure, Rev. H, 06/21/2000 Product Configuration	This documentation describes the configuration management system used for the development of the TOE.

Assurance Component	Documentation Satisfying Component	Rationale
	Management System Help, Rev. H, 12/19/2001 New Product Release ECN Requirements Checklist, Rev. A, 12/19/2001 Released Product Change ECN Requirements Checklist, Rev. A, 12/19/2001 Product Deviation Requirements Checklist, Rev. B, 12/19/2001 Bill of Materials Import Management System, 06/24/2002 Bill of Material Structure Report, Rev B, 06/24/2002 Class Code Matrix, 06/26/2002	
ADO_DEL.1	Marconi Document #PRST-4150-001 (Handling, Storage, Preservation, and Delivery of Products), Revision C, 01/23/2002; Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2004; SA-400 Security Firewall Quickstart Guide, Revision C, 07/02/2002; Marconi SA-400 Security Target, Revision 8, 09/16/2003.	This documentation describes the TOE delivery procedures used by the developer.
ADO_IGS.1	Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue	This documentation provides installation, generation and configuration instructions for the

Assurance Component	Documentation Satisfying Component	Rationale
	D, April 16, 2004 SA-400 Security Firewall Quickstart Guide, Revision C, 07/02/2002 Marconi SA-400 Security Target, Revision 8, 09/16/2003	TOE.
ADV_FSP.1	Marconi SA-400 Firewall, Version 1.3 Security Target, Revision 8, September 16, 2003 Marconi SA-400 High Level Design with Security Functional Specifications, Revision 2.3, July 10, 2003 Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2004 Marconi SA-400 Security Firewall Quickstart Guide, Software Version 1.3.0, Revision C, July 02, 2002 SA-400 GUI Error Conditions and Messages, Version 1.1, October 27, 2003 SA-400 CLI Error Conditions and Messages, Version 1.1, October 27, 2003	This document details all of the interfaces and functionality of the TOE.
ADV_HLD.1	Marconi SA-400 High Level Design with Security Functional Specifications, Revision 2.3, July 10, 2003 Marconi SA-400 Firewall, Version 1.3 Security Target, Revision 8, September 16, 2003 Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2003	This document describes the TOE in terms of sub-systems.

Assurance Component	Documentation Satisfying Component	Rationale
ADV_RCR.1	Marconi SA-400 Firewall, Version 1.3 Security Target, Revision 8, September 16, 2003 SA-400 High Level Design Document with Security Functional Specifications, Revision 2.3, July 10, 2003 SA-400 Common Criteria Certification Correspondence Mapping Revision 3.5, November 5, 2003	This document contains the correspondence mapping between the TOE Summary Specification, Functional Specification and High-Level Design documentation.
AGD_ADM.1	Marconi SA-400 Security Firewall User's Manual Software Version 1.3.0, Issue D, April 16, 2004 Marconi SA-400 Security Target, Version 1.3, Revision 8, September 16, 2003 Marconi SA-400 High Level Design Document with Security Functional Specifications, Revision 2.3, July 10, 2003	This documentation describes the responsibilities for the administrator of the TOE.
AGD_USR.1	Marconi SA-400 Security Firewall User's Manual Software Version 1.3.0, Issue D, April 16 2004 Marconi SA-400 Security Target, Version 1.3, Revision 8, September 16, 2003	This documentation provides guidance to non-administrative users of the TOE.
ATE_COV.1	Marconi SA-400 Security Target, Revision 8, September 16, 2003 Marconi SA-400 QA Test Procedures for Release 1.3, Revision 1.7, February 4, 2004 SA-400 High Level Design	This documentation describes the scope of testing performed by the developer against the security features provided by the TOE.

Assurance Component	Documentation Satisfying Component	Rationale
	Document with Security Functional Specifications, Revision 2.3, July 10, 2003 SA-400 Test Coverage, Revision 1.2, 2/11/04	
ATE_FUN.1	Marconi SA-400 Security Target, Revision 8, September 16, 2003 Marconi SA-400 QA Test Procedures for release 1.3, Revision 1.7, 2/4/04 Marconi Test Coverage, Revision 1.2 SA-400 High Level Design Document with Security Functional Specifications, Rev. 2.3, July 10, 2003 Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2004 SA-400 Product Requirements Document (PRD), Rev. 1.7, February 20, 2002 SA-400 Test Results.xls, 6/14/02	This documentation describes the test procedures performed by the developer.
ATE_IND.2	Marconi SA-400 Security Target, Revision 8, September 16, 2003 SA-400 High Level Design Document with Security Functional Specifications, Revision 2.3, July 10, 2003 SA-400 Security Firewall User's Manual Software Version 1.3.0, Issue D, April 16, 2004 SA-400 Installation Guide	This documentation describes the test procedures performed by the developer. The Laboratory will then perform independent testing of the TOE security features.

Assurance Component	Documentation Satisfying Component	Rationale
	"Evaluated Configuration" for Common Criteria Certification (CCC), Revision 1.0, 06-03-2002 Marconi SA-400 QA Test Procedures for Release 1.3, Revision 1.7, Feb 4, 2004 Evaluation Team Test Coverage Analysis of the Marconi Firewall v1.3; March 21, 2003 Marconi SA-400 Firewall (TOE)	
AVA_SOF.1	SA-400 Common Criteria Certification Strength of Function, Revision 1.4, March 17, 2004 Marconi SA-400 Security Target, Revision 8, September 16, 2003 SA-400 High Level Design with Security Functional Specifications, Revision 2.3, July 10, 2003 Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2004	This document describes the strength of function claim for the identification and authentication functions of the TOE.
AVA_VLA.1	Marconi SA-400 Security Target, Version 1.3, Revision 8, September 16, 2003 SA-400 Security Firewall User's Manual, Issue D, April 16, 2004 SA-400 Common Criteria Certification Developer Vulnerability Analysis Revision 1.3, March 1, 2004	This document describes the vulnerability analysis and penetration testing performed by the developer.

6.3 Rationale for TOE Assurance Requirements

The strength of function required for all applicable Security Functional Requirements in this TOE is Basic. The requirements realised by probabilistic or permutational mechanisms include FIA_UAU.2 and FIA_UID.2.

The EAL 2 level of assurance was chosen to provide a moderate level of independently assured security, including confidence that the TOE will not be tampered with during delivery. This level of assurance will provide sufficient security to protect unclassified information such as that found in government organizations. Information with this importance is assumed, by nature, to have a greater threat for disclosure and/or corruption by unauthorized parties.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not include any Protection Profile refinements.

7.3 Protection Profile Additions

This Security Target does not include any Protection Profile additions.

7.4 Protection Profile Rationale

This Security Target does not include any Protection Profile rationale statements.

CHAPTER 8

8. Rationale

8.1 Security Objectives Rationale

The rationale for the security objectives of the TOE is defined in Chapter 4, Section 4.3 Security Objectives Rationale.

8.2 Security Requirements Rationale

The rationale for the security requirements of the TOE is defined in two sections. Rationale for the security functional requirements is given after each functional component description in Chapter 5, Section 5.1 Security Functional Requirements. Rationale for the security assurance requirements is given in Chapter 6, Section 6.3 Rationale for the TOE Assurance Requirements.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.1 TOE Security Functions.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

