Profiler Blade System Version 5.0 Security Target

Version 1.0

August 16, 2005

Prepared for:
Mazu Networks, Inc.
125 Cambridge Park Drive, 4th Floor
Cambridge, MA 02140-2314

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 Security Target, TOE and CC Identification

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level (EAL) 2. Products evaluated at EAL2 are intended provide defence against attackers who possess a low attack potential.

ST Title:	Profiler Blade System Version 5.0 Security Target
ST Version:	1.0
ST Publication Date:	August 16, 2005
ST Author:	Booz Allen Hamilton
TOE Identification:	Profiler Blade System Version 5.0
CC Identification:	Common Criteria (CC) for Information Technology Security Evaluation, Version 2.2, January 2004 incorporated with Common Criteria Interpretations Management Board (CCIMB) final interpretations at evaluation commencement
ST Evaluator:	Booz Allen Hamilton Common Criteria Testing Laboratory
Keywords:	Network integrity system, anomaly detection system, real-time traffic analysis, real-time traffic modelling, network behavioural modelling, and behavioural security

1.2 TOE Overview

The Profiler Blade System is a distributed “behavioural” network security solution that is designed to protect the critical, core applications and services inside the enterprise network. The Profiler Blade System does not use the signature-based method of detection, whereby systems compare the electronic characteristics of network traffic against a database of known, malicious packet types. Rather, it uses real-time analysis to focus on deviations or anomalies from how the network is typically used.

The Profiler Blade System itself is an appliance that is deployed in the enterprise network operations or security operations centre. The Profiler Blade System takes in network traffic data from Mazu Sensors, NETScout probes and NetFlow-enabled routers. The Profiler Blade System uses this data to create and maintain a dynamic model of behaviour in a network showing how assets and services in the network are typically used and by whom.

The Profiler Blade System's network traffic profiling engine transforms this data into a single, network-wide, baseline of "host-to-host connections" in the network: who is talking to whom, using which ports, and which protocols. It also maintains this baseline automatically over time, evolving the model as the network grows and changes. It analyses this data in real time at both a host level and a host-group level. Hosts can be grouped automatically based on how they use the network, or grouped using data from an enterprise asset management system.

The Profiler Blade System's event detection heuristics analyse new traffic data in real-time in order to uncover threats, attacks and other operationally relevant events. The ability to perform this analysis on all network activity from a single model enables the highest degree of accuracy. This accuracy, in turn, enables the Profiler Blade System to help enterprises quickly and efficiently contain, thwart, and then recover from a range of malicious activities, including known, unknown, internal and external attacks.

1.3 Conformance Claims

This ST is CC Part 2 conformant and is CC Part 3 conformant for EAL2 incorporated with CCIMB final interpretations at evaluation commencement.

This ST does not claim Protection Profile conformance.

1.4 Conventions, Terminology and Acronyms

This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.4.1 Conventions

This section describes the conventions used to denote CC operations on Security Functional Requirement (SFR) and Security Assurance Requirement (SAR) components to distinguish text with special meaning. The operations performed on the SFR and SAR components contained in this ST adhere to the following conventions:

- Iteration: Allows a component to be used more than once with varying operations. In this ST, a number in parenthesis appended to a component indicates iteration. For example, FMT_MOF.1 Management of security functions behaviour (1) and FMT_MOF.1 Management of security functions behaviour (2) indicate that the ST includes two iterations of the FMT_MOF.1 component.

- Assignment: Allows the specification of an identified parameter. Assignments are indicated using italicised text and are surrounded by brackets (e.g., [*assignment*]).

- Selection: Allows the specification of one or more elements from a list. Selections are indicated using bold italicised text and are surrounded by brackets (e.g., [***selection***]).

- Refinement: Allows the addition of details. Refinements are indicated using bold text for additions to the requirements (e.g., **refinement**). In addition, refinements based upon CCIMB interpretations are indicated in red italicised text for additions, and strikethrough red italicised text for deletions (e.g., *text added* ~~*text removed*~~).

1.4.2 Terminology

The following is a listing of CC terms along with their definitions based on their use in this ST:

- Evaluation Assurance Level (EAL): A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

- Protection Profile (PP): An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

- Security Function (SF): A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

- Security Target (ST): A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

- Strength of Function (SOF): A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

- SOF-basic: A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

- Target of Evaluation (TOE): An IT product or system and its associated guidance documentation that is the subject of an evaluation.

- TOE Security Functions (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

- TOE Security Policy (TSP): A set of rules that regulate how assets are managed, protected and distributed within a TOE.

- TSF Scope of Control (TSC): The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

The following additional terms are specific to this ST:

- Operator: A role recognized by the TOE that can change settings but not manage user accounts.

- Event Viewer: A role recognized by the TOE that can only view event reports.

- Monitor: A role recognized by the TOE that can view all pages, but can change only the display settings.

- Administrator: A role recognized by the TOE that can change settings and manage user accounts.

1.4.3 Acronyms

The following acronyms are used in this ST:

CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAL	Evaluation Assurance Level
HTTPS	HyperText Transfer Protocol Secure
IT	Information Technology
MPCP	Mazu Profiler Communication Protocol
NTP	Network Time Protocol

PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol

2 TOE Description

2.1 Overview of the Profiler Blade System

The TOE is the Profiler Blade System Version 5.0. The TOE is an appliance-based anomaly detection system that builds profiles of hosts and services as a baseline for normal network activity. Data is fed to the TOE from Mazu Sensors, NETScout probes and NetFlow-enabled routers, thus enabling the TOE to build models for the connection behaviours of each machine, rather than profiling the entire network. Upon receipt of data, the TOE compares the captured traffic to mathematically derived profiles of typical traffic patterns for the current time and day of the week. When deviations are detected, the TOE reports and alerts to anomalous behaviours occurring on the network.

The TOE identifies security and operational events by changes in connection behaviour rather than by comparison to stored signatures commonly used by an intrusion detection system. The TOE determines the operational relevance of connection anomalies by applying a set of sophisticated heuristics to connection data contained in a profile. These heuristics continually compare current network activity to a profile of typical network activity for the time of day, week, month, and year to detect connection behaviours that indicate suspicious activities. Such heuristics are designed to identify and characterise the following types of events:

- Denial of Service/Bandwidth Surge: significant increase of traffic that conforms to the characteristics of a Denial of Service attack.

- Worm: increase in connections that typically result from the spread of a worm. The TOE traces these connections over time through the network to identify how the worm spreads from infected hosts to new hosts.

- Host Scan: monitored hosts are being pinged.

- Port Scan: ports of a host are being tested for running services or being in a “listening” or “accepting” state.

- Anomalous Connection: communication between two hosts that have been on the monitored network for some period of time, but which do not normally communicate with one another (ex., an Engineering department host connecting to a Finance department host).

- New Host: a host that has not been seen before has joined the network.

- Silent host: a host that normally generates some amount of traffic has stopped entirely.

- New Service: the TOE has discovered that a host or group of hosts is providing or using a service that is new to that host or group of hosts.

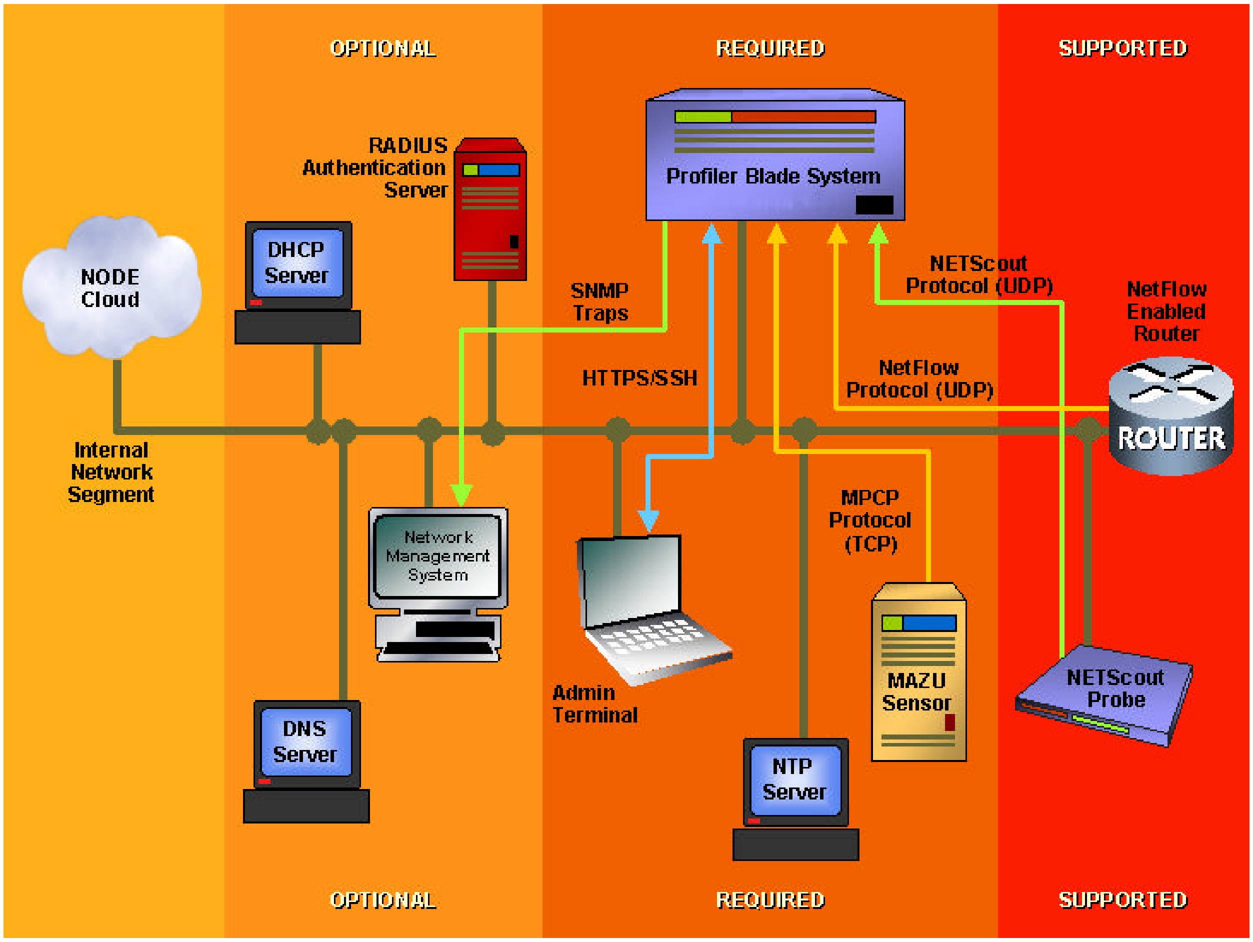
- Rule-based Event: an event that can be defined by specifying a series of conditions and assigning a severity level.

- Sensor Down: a sensor that has been communicating with the TOE is no longer reachable.

- Sensor Invalid: The TOE is attempting to communicate with a sensor but is not receiving data in the expected format. This could be the result of a problem on the sensor, such as time not being set up correctly or a software error.

The following figure identifies the resources utilized when deploying the TOE.

Figure 1 - Profiler Blade System Deployment



As depicted in the above figure, the TOE utilizes the following IT environment resources:

- Required Resources:
  - Mazu Sensor: monitors traffic through the use of network taps or span/mirror ports. The collected statistics are then forwarded to the TOE via the Mazu Profiler Communication Protocol (MPCP) for aggregation and analysis.
  - NTP Server: provides for time synchronization between nodes on the network.

    - Admin Terminal: a node on the network that uses its local web browser to interact with the TOE via HTTPS.

- Supported Resources:

    - NetFlow-enabled Routers: provides data to the TOE (via the NetFlow protocol) for additional aggregation and analysis of activities occurring on the network.

    - NETScout Probes: provides data to the TOE (via the NETScout protocol) for additional aggregation and analysis of activities occurring on the network.

- Optional Resources:

    - RADIUS Authentication Server: the TOE uses its local database as a primary means of authenticating users. If it does not find the authentication information locally, it can be configured to check a RADIUS Server. If this method of authentication is utilized, the TOE will only grant the user with access at the lowest permission level once the user has successfully authenticated.

    - Network Management System: the TOE can be configured to send SNMP traps to a Network Management System when an alert message has been generated on the TOE.

    - DNS Server: allows the TOE to lookup the hostname associated with an IP address.

    - DHCP Server: allows the TOE to use lease information from a DHCP Server as the basis for tracking the connection behaviour of a host when its IP address lease expires and the DHCP Server assigns the host a new IP address.

2.2 Scope and Boundaries of the Evaluated Configuration

This section provides information for the purpose of evaluating the TOE. This includes descriptions of the TOE physical and logical boundaries for the purpose of evaluation.

2.2.1 Physical Boundary

The physical boundary of the TOE includes the Profiler Blade System Version 5.0 appliance that is comprised of the following:

- Hardware:

    - One IBM eServer BladeCenter Type 8677 7U chassis hardware platform

    - One or more Analyser mBlades (IBM eServer BladeCenter HS 20, Type 8832 blade server plug-in module): each Analyzer mBlade provides support to monitor between 20,000-40,000 hosts on the network.

    - One Database mBlade (IBM eServer BladeCenter HS20, Type 8832 blade server plug-in module)
    - One Manager mBlade (IBM eServer BladeCenter HS 20, Type 8832 blade server plug-in module)
    - One IBM eServer BladeCenter HS20, SCSI Storage Expansion Unit
    - One IBM eServer BladeCenter 4-Port Gb Ethernet Switch Module
    - Two IBM Distributed Power Interconnect Front-end Power Distribution Units

- Software:
    - Mazu Profiler Version 5.0 that includes:
        - Linux kernel version 2.4.25 – with Mazu patches
        - openssh-3.7.1p2 – Secure Shell
        - openssl-0.9.7d – Secure Socket Layer
        - ntp-4.1.2 – Network Time
        - Mazu snmp 5.0 – SNMP
        - Mazu Apache 5.0 – Web Server
        - php-4.3.9 – Scripting Language
        - postgreSQL-7.4.5 - SQL

2.2.2 Logical Boundary

This section describes the logical boundary of the TOE.

2.2.2.1 Security Audit

The TOE receives audit data that has been collected and generated by a Mazu Sensor via the MPCP. In addition, the communications link between the Mazu Sensor and the TOE is established through the use of a shared secret. Once the TOE has received audit data, it stores the information in a profile. Complex heuristics are then applied to the profile to identify anomalous behaviour on the network that deviates from normal activity. The TOE then generates alerts based upon triggered events that have surpassed a configured threshold rating.

2.2.2.2 Identification and Authentication

The TOE provides an HTTPS interface that is utilized in order to access its security functions. During initial configuration, a user establishes a connection to the TOE using their local web browser running on the Admin Terminal as depicted in Figure 1. Next, the user is prompted to provide the identification and authentication credentials required to log onto the TOE under the Administrator role. Once the user has successfully assumed the Administrator role, they can then create additional roles that the TOE will recognize when other users attempt to identify and authenticate themselves over the HTTPS interface from the Admin Terminal.

2.2.2.3 Security Management

The TOE provides for the management of its security functions via the HTTPS interface from the Admin Terminal. Once a user has been successfully identified and authenticated, they will then be granted access to the TOE that is limited based upon the role that the user has been assigned. The roles supported by the TOE each have varying levels of access rights with respect to viewing or modifying the way in which the security functions of the TOE behave. These roles include the Administrator, Operator, Monitor, and Event Viewer that are defined in Section 1.4.2.

2.2.2.4 Protection

Since the TOE is an appliance-based system, most of the protection features are implemented in its hardware and software structures. These structures provide for process execution as well as process separation. In addition, management of the TOE is enforced by limiting user access by requiring each to identify and authenticate prior to being granted access over the HTTPS interface. Additional aspects related to protection of the TOE are addressed via assumption statements identified in Section 3.1.

2.2.3 TOE Exclusions

The following TOE functionality is beyond the scope of this evaluation:

- Import of audit data collected and generated by NetFlow-enabled Routers and NETScout Probes

- Authenticating users by utilizing a RADIUS Server

- Receiving lease information from a DHCP Server to track the behaviour of hosts when they have been assigned a new IP address

- SSH interface providing the capability to:

    - Import specifications for rule-based events

    - Importing DHCP data

    - Backup and restoring the Profiler software and data

3 Security Environment

This chapter provides a statement of the TOE security environment to identify:

- Significant assumptions about the operational environment of the TOE
- IT related threats addressed by the TOE
- Environmental threats that must be addressed by the IT environment
- Organizational security policies that must be enforced to operate the TOE in a secure manner

3.1 Secure Usage Assumptions

The specific conditions listed in this section are assumed to exist in the TOE environment. These assumptions are necessary as a result of practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.1.1 Personnel Assumptions

A.CONFIG The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation.

A.NOEVIL The authorized users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

A.PASSWD The authorized users of the TOE will use best commercial practices when establishing passwords.

3.1.2 Physical Assumptions

A.LOCATE The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unauthorised physical access.

3.1.3 Logical Assumptions

A.PEER IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

3.2 Threats to Security

This section defines the threats to security. They have been categorized based on those addressed by the TOE verses those addressed by the environment.

3.2.1 Threats addressed by the TOE

T.ACCESS A user could attempt to establish an unauthorised session with the TOE.

T.COLLECT An unauthorised user could remove or modify statistical data collected by the TOE that is used for analysing the behaviour of normal network activity.

T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

3.2.2 Threats addressed by the Environment

T.E.SENSOR A user on an internal or external network could perform hostile actions on the internal network without having such actions captured for analysis and review.

T.E.TIME A user may attempt to spoof timestamp values provided by an NTP server thereby causing the TOE and/or IT components with which the TOE communicates to maintain deferring time values.

3.3 Organisational Security Policies

There are no organisational security policies required.

4 Security Objectives

This chapter provides a listing of security objectives to ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives are divided into Security Objectives for the TOE (Section 4.1) and Security Objectives for the Environment (Section 4.2).

4.1 Security Objectives for the TOE

The following security objectives are to be satisfied by the TOE.

O.IDACTS The TOE must accept data from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers and then apply analytical processes and information to derive conclusions about anomalies (past, present, or future).

O.INTEGR The TOE must ensure the integrity of all audit data.

O.MANAGE The TOE will provide authorised users with the capability to perform analysis of activities occurring on the local network and modify its configuration settings.

O.REPORT The TOE will provide authorised users with alerts to network behavioural anomalies and the capability to generate statistical reports based on collected heuristics.

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.RESTRICT The TOE will restrict access to its security features to authorised users.

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order for the TOE to fulfil its security objectives.

O.E.CONFIG The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation.

O.E.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

O.E.PASSWD The authorized users of the TOE will use best commercial practices when establishing passwords.

O.E.LOCATE The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unauthorised physical access.

O.E.PEER IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

O.E.SENSOR At least one Mazu Sensor will be deployed in the IT environment and configured to route collected events to the TOE for processing and analysis.

O.E.TIME The TOE and all IT components with which the TOE communicates will be configured to receive reliable timestamps from a protected NTP server.

5 IT Security Requirements

This chapter identifies the security requirements for the TOE and its environment. The operations performed on Security Functional Requirement and Security Assurance Requirement components contained in this section adhere to the conventions as prescribed in Section 1.4.1 of this ST.

5.1 TOE Security Functional Requirements

The following table provides a summary of the Security Functional Requirement components implemented by the TOE.

Table 1 - TOE Security Functional Requirement Components

Security Functional Class	Security Functional Requirement Component
Security audit (FAU)	FAU_ARP.1 Security alarms
	FAU_SAA.2 Profile based anomaly detection
	FAU_SAR.1 Audit review (1)
	FAU_SAR.1 Audit review (2)
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.2 Guarantees of audit data availability
	FAU_STG.4 Prevention of audit data loss
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security management (FMT)	FMT_MOF.1 Management of security functions behaviour (1)
	FMT_MOF.1 Management of security functions behaviour (2)
	FMT_MTD.1 Management of TSF data (1)
	FMT_MTD.1 Management of TSF data (2)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation

The following subsections present the details for each of the TOE Security Functional Requirement components.

5.1.1 Security audit (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [*inform the authorized user*] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

5.1.1.2 FAU_SAA.2 Profile based anomaly detection

Hierarchical to: FAU_SAA.1

FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [*hosts, host groups, and service groups*].

FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each **event** whose **host** activity is recorded in a profile, where the suspicion rating represents the degree to which the **host's** current activity is found inconsistent with the established patterns of usage represented in the profile.

FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a **host's** suspicion rating exceeds the following threshold conditions [*event severity and event alerting thresholds reaching a certain pre-configured or user assigned value*].

Dependencies: FIA_UID.1 Timing of identification

Application Note: *The FAU_SAA.2 security functional requirement component uses heuristics to detect anomalous patterns of usage. Heuristics in this case are mathematical formulas applied to collected events that are then compared to a baseline in order to report deviations from normal activity.*

5.1.1.3 FAU_SAR.1 Audit review (1)

Hierarchical to: No other components.

FAU_SAR.1.1(1) The TSF shall provide [*the Administrator, Operator and Monitor roles*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2(1) 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

5.1.1.4 FAU_SAR.1 Audit review (2)

Hierarchical to: No other components.

FAU_SAR.1.1(2) The TSF shall provide [*the Event Viewer role*] with the capability to read [*event reports*] from the audit records.

FAU_SAR.1.2(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

5.1.1.5 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

5.1.1.6 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting, ordering***] of audit data based on [*specific attributes contained in individual traffic reports and historical logs, saved reports, and event data logs*].

Dependencies: FAU_SAR.1 Audit review

5.1.1.7 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [***prevent***] unauthorised modifications to the audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [*35GB of*] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.8 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall [***'overwrite the oldest stored audit records'***] and [*perform no other actions*] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2 Identification and authentication (FIA)

5.1.2.1 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 **Profiler** users: [*user identification, password, role*].

Dependencies: No dependencies

5.1.2.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: *The FIA_UAU.2 security functional requirement component includes a Strength of Function claim that is provided in Section 8.6.*

5.1.2.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

5.1.3 Security management (FMT)

5.1.3.1 FMT_MOF.1 Management of security functions behaviour (1)

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to [***disable, enable, modify the behaviour of***] the functions [*all settings and management of user accounts*] to [*the Administrator role*].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.1.3.2 FMT_MOF.1 Management of security functions behaviour (2)

Hierarchical to: No other components.

FMT_MOF.1.1(2) The TSF shall restrict the ability to [***disable, enable, modify the behaviour of***] the functions [*all settings with the exception of management of user accounts*] to [*the Administrator role*].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.1.3.3 FMT_MTD.1 Management of TSF data (1)

Hierarchical to: No other components.

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***change_default, query, modify, clear***] the [*all settings and recorded events*] to [*the Administrator role*].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.1.3.4 FMT_MTD.1 Management of TSF data (2)

Hierarchical to: No other components.

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***change_default, query, modify, clear***] the [*recorded events and all settings with the exception of management of user accounts*] to [*the Administrator role*].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

5.1.3.5 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [*Security Audit, Identification and Authentication, Security Management, and Protection*].

Dependencies: No dependencies

5.1.3.6 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator, Operator, Monitor and Event Viewer*].

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

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Protection of the TSF (FPT)

5.1.4.1 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

5.1.4.2 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

5.2 IT Environment Security Functional Requirements

The following table provides a summary of the Security Functional Requirement components that are to be enforced by the IT environment.

Table 2 - IT Environment Security Functional Requirement Components

Security Functional Class	Security Functional Requirement Component
Security audit (FAU)	FAU_GEN.1 Audit data generation
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamps

The following subsections present the details for each of the IT environment Security Functional Requirement components.

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The **IT Environment** 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) [*none*].

FAU_GEN.1.2 The **IT Environment** 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

5.2.2 Protection of the TSF (FPT)

5.2.2.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The **IT Environment** shall be able to provide reliable time-stamps for its own use **and for use by the TOE**.

Dependencies: No dependencies

5.3 TOE Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2. Justification for this assurance level is provided in Section 8.3.

5.3.1 Configuration management (ACM)

5.3.1.1 ACM_CAP.2 Configuration items

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.

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 labelled with its reference.

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

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

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

Dependencies: None

5.3.2 Delivery and operation (ADO)

5.3.2.1 ADO_DEL.1 Delivery procedures

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.

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.

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

Dependencies: None

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

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

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

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.

Dependencies: AGD_ADM.1 Administrator Guidance

5.3.3 Development (ADV)

5.3.3.1 ADV_FSP.1 Informal functional specification

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

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.

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.

Dependencies: ADV_RCR.1 Informal correspondence demonstration

5.3.3.2 ADV_HLD.1 Descriptive high-level design

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

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 subsystem of the TSF are externally visible.

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.

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

5.3.3.3 ADV_RCR.1 Informal correspondence demonstration

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

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.

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

Dependencies: None

5.3.4 Guidance documents (AGD)

5.3.4.1 AGD_ADM.1 Administrator guidance

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

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 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.1.7C 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.

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

Dependencies: ADV_FSP.1 Informal correspondence demonstration

5.3.4.2 AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

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 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.

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

Dependencies: ADV_FSP.1 Informal correspondence demonstration

5.3.5 Tests (ATE)

5.3.5.1 ATE_COV.1 Evidence of coverage

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

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.

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

Dependencies: ADV_FSP.1 Informal correspondence demonstration

ATE_FUN.1 Functional testing

5.3.5.2 ATE_FUN.1 Functional testing

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

ATE_FUN.1.2D The developer shall provide test documentation.

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.

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

Dependencies: None

5.3.5.3 ATE_IND.2 Independent testing - sample

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

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.

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.

Dependencies: ADV_FSP.1 Informal functional specification

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

ATE_FUN.1 Functional testing

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 AVA_SOF.1 Strength of TOE security function evaluation

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.

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 of SOF-basic.

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 of SOF-basic.

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.

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

5.3.6.2 AVA_VLA.1 Developer vulnerability analysis

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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.

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive-high-level design

AGD_ADM.1 Administrator guidance

AGD_USR.1 User guidance

6 TOE Summary Specification

This chapter describes each Security Function (SF) enforced by the TOE and details the assurance measures provided for evaluation.

6.1 Security Functions

This section describes the Security Functions provided by the TSF mapped to their corresponding Security Functional Requirement components. The following table identifies this mapping.

Table 3 - Security Function to Security Functional Requirement Component Mapping

Security Function	Security Functional Requirement Component
Security Audit Function	FAU_ARP.1 Security alarms
	FAU_SAA.2 Profile based anomaly detection
	FAU_SAR.1 Audit review (1)
	FAU_SAR.1 Audit review (2)
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.2 Guarantees of audit data availability
	FAU_STG.4 Prevention of audit data loss
Identification and Authentication Function	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management Function	FMT_MOF.1 Management of security functions behaviour (1)
	FMT_MOF.1 Management of security functions behaviour (2)
	FMT_MTD.1 Management of TSF data (1)
	FMT_MTD.1 Management of TSF data (2)
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Protection Function	FPT_RVM.1 Non-bypassability of the TSP
	FPT_SEP.1 TSF domain separation

The following sections identify each Security Function and describe them in terms of how they implement each of the TOE Security Functional Requirement components appearing in Section 5.1. By using this method of presentation, each Security Function is described and supporting rationale is provided as to how each Security Functional Requirement component has been satisfied.

6.1.1 Security Audit Function

In describing the security audit function, this section makes reference to auditable events. The Profiler Blade System has the following categories of auditable events:

- Traffic profiles and historical logs: Traffic profiles are dynamic, mathematically derived, representations of traffic. Historical logs are records of actual, individual traffic flows between hosts.

- Saved reports: These are specific to the time spans and other parameters of the queries used to generate them. They can report traffic volumes based on profiles or based on historical logs.

- Event data: This is detailed data about particular network events that caused alerts. The Profiler Blade System uses this data to generate Event Reports and Event Detail Reports.

It is necessary to describe the storage and availability of these types of audit records individually in some cases, as they are not handled identically.

6.1.1.1 FAU_ARP.1 Security alarms

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF triggers security alarms (alerts) based upon thresholds configured for each type of network event. In addition, the thresholds can be configured to indicate the severity of the event being that of high, medium, and low. When an event exceeds the specified threshold, an alert is displayed on the top of the user's screen (alerts can also be sent to a Network Management System via SNMP traps however this functionality has been excluded from the evaluated configuration). Links are also provided to the user to access the event details that triggered the alert. Individual thresholds can be set for each type of event and each host group on the monitored network with the exception of the New Host, Silent Host, Sensor Down, and Sensor Invalid event types. Access to this function is denied to users assigned to the Event Viewer role.

6.1.1.2 FAU_SAA.2 Profile based anomaly detection

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF builds profiles of hosts and services operating on the network and establishes a baseline to identify normal network activity. Once this baseline has been established, the TSF utilizes complex heuristics to model the connection behaviours of each host. This is performed through the use of profiles that identify typical traffic patterns for the current time and day of the week. Anomalies are then grouped based on the following event types: Denial of Service/Bandwidth Surge, Worm, Host Scan, Port Scan, Anomalous Connection, New Host, Silent Host, Sensor Down, Sensor Invalid, New Service, and Rule-based Event. In addition, the TSF allows for the specification of host groups and service groups. Host groups are used to assign hosts to a particular group if they share similar connection behaviours.

6.1.1.3 FAU_SAR.1 Audit review (1)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF allows the Administrator, Operator and Monitor roles with the capability to read all of the information recorded in the audit trail. Events that have been recorded can be sorted based on Event ID, Severity of the Threat, Source, Destination, and Start Time. The TSF also supports the generation of Event Reports and Traffic Reports. An Event Report displays a list of events that have triggered an alert. These reports can be generated to identify an individual type of event or for all types of events. A Traffic Report can be generated to identify results that relate to top usage, basic queries, and advanced queries as received from the user.

6.1.1.4 FAU_SAR.1 Audit review (2)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF allows the Event Viewer role the capability to read only the contents of Event Reports. All other audit review functionality is limited to the Administrator, Operator and Monitor roles.

6.1.1.5 FAU_SAR.2 Restricted audit review

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. Each user is required to identify and authenticate themselves to the TOE before the TSF grants the user access based upon their assigned role. In addition, the TSF restricts access to the audit records based upon the specific role that the user has been assigned.

6.1.1.6 FAU_SAR.3 Selectable audit review

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF provides the capability to perform selectable audit review on audited events and this functionality is limited to the Administrator, Operator and Monitor roles. The Event Viewer role does not have the permissions to perform any actions with respect to this function. Selectable audit review can be performed on traffic profiles and historical logs, saved reports, and event data. These are discussed individually in the following subsections.

6.1.1.6.1 Traffic Profiles and Historical Logs

The advanced query page on the Profiler Blade System provides the ability to perform searches, sorting, and ordering of audit data based on:

- Hosts by IP address: Inside a specified range, outside a specified range, or all.
- Hosts by host Group membership: Inside a selected host group, outside a selected group, or all.
- Services provided or consumed: By service name, port number (individually or in ranges), port/protocol combination, or service groups. Each can be specified either individually or in Boolean combinations.
- Peer hosts by address: Inside a specified range, outside a specified range, or all.
- Peer hosts by host group membership: Inside a selected host group, outside a selected host group, or all.

Searches can be based upon:

- A specified time span for the historical logs.

- A traffic profile in the current profile scheme.

The results of a search can be sorted and displayed by:

- Services
- Service Groups
- Protocols
- Hosts
- Hosts excluding peers
- Host-pairs
- Groups
- Groups excluding peers
- Group-pairs

Lists on reports resulting from a search can be ordered by:

- Bits per second, minute, hour, week, month, or year
- Packets per second, minute, hour, week, month, or year
- Connections per second, minute, hour, week, month, or year

6.1.1.6.2 Saved Reports

The reports + saved queries page of the Profiler Blade System provides the ability to perform ordering of the list of saved reports by:

- Report owner
- Report name
- Run date and time
- Size

It also provides for listing all saved reports or limiting the list to the reports owned by the user. Each list can be further limited to time periods of one or more days, weeks, or months.

6.1.1.6.3 Event Data

The overview page of the Profiler Blade System provides the ability to perform sorting of the list of event details reports based on:

- Event ID
- Severity
- Event Type
- Source
- Destination
- Start time

The event reports page of the Profiler Blade System provides the ability to perform searching of event details report database by event type and a user-specified time span.

6.1.1.7 FAU_STG.2 Guarantees of audit data availability

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. Role-based access control measures are utilised to prevent unauthorised access to the audit events. The HTTPS does not provide for deleting any data other than saved reports, which can be regenerated. Also, backup and restore functions are provided.

6.1.1.8 FAU_STG.4 Prevention of audit data loss

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TOE provides 20GB database storage for reports (Event Reports and Traffic Reports). In the event of audit storage exhaustion, the oldest report will be overwritten (this does not apply to saved reports marked to be retained indefinitely). The size of the traffic profiles is a function of the traffic volume during the profile period and does not accumulate over time. The storage capacity for traffic profiles and historical logs is 35GB.

6.1.2 Identification and Authentication Function

6.1.2.1 FIA_ATD.1 User attribute definition

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The Administrator is the only role that can define new Profiler Blade System user accounts authorised to access the TOE. The Administrator can create multiple user accounts of each type: Administrator, Operator, Monitor and Event Viewer. All user credentials are stored in the local database.

6.1.2.2 FIA_UAU.2 User authentication before any action

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TOE must perform successful identification and authentication of Profiler Blade System users before the TSF grants the user access other Security Functions provided. User authentication is enforced through the use of a password mechanism described in Section 8.6.

6.1.2.3 FIA_UID.2 User identification before any action

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TOE must perform successful identification and authentication of Profiler Blade System users before the TSF grants the user access other Security Functions provided.

6.1.3 Security Management Function

6.1.3.1 FMT_MOF.1 Management of security functions behaviour (1)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The Administrator role is also referred to as root in the user and administrator guidance documentation. This role has the capability to manage the behaviour of all of the Security Functions provided by the TOE (Security Audit, Identification and Authentication, Security Management, and Protection) to include the configuration of Profiler Blade System user roles.

6.1.3.2 FMT_MOF.1 Management of security functions behaviour (2)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The Administrator role can manage the behaviour of all Security Functions provided by the TOE (Security Audit, Identification and Authentication, Security Management, and Protection) with the exception of configuring Profiler Blade System user roles.

6.1.3.3 FMT_MTD.1 Management of TSF data (1)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The Administrator can change all configuration settings.

6.1.3.4 FMT_MTD.1 Management of TSF data (2)

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The Administrator can change all configuration settings with the exception of creating or modifying user accounts.

6.1.3.5 FMT_SMF.1 Specification of management functions

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF provides restricted access to its Security Functions (Security

Audit, Identification and Authentication, Security Management, and Protection) based on roles that have been configured by the Administrator.

6.1.3.6 FMT_SMR.1 Security roles

The HTTPS interface on the TOE is utilized in accessing this function from the Admin Terminal as depicted in Figure 1. The TSF provides restricted access to its security features based upon the role assigned to each user. These roles include the Administrator, Operator, Monitor and Event Viewer. The Administrator manages the user assignment to each of these roles over the HTTPS interface on the TOE from the Admin Terminal.

6.1.4 Protection Function

6.1.4.1 FPT_RVM.1 Non-bypassability of the TSP

The TOE is an appliance-based system and as such it manages all processes within its local domain. The TSF ensures that all processes are executed and succeed before allowing the TOE to assume an operational state.

6.1.4.2 FPT_SEP.1 TSF domain separation

The TOE is an appliance-based system and as such it manages all processes within its local domain. The data analysis, event detection, alerting, user authentication, and data storage processes running on the TOE execute in an environment that is not accessible to users.

6.2 TOE Security Assurance Measures

This section identifies the assurance measures provided by the developer in order to meet the Security Assurance Requirement components for EAL2. These measures are identified in the following table.

Table 4 - TOE Security Assurance Measures

Component	Document(s)	Rationale
ACM_CAP.2 Configuration items	*Configuration Guide, Profiler 5.0, January 27, 2005* *Profiler Blade System Version 5.0.1.0.P8200.4.20050201 Configuration List, August 15, 2005* *Configuration Management Process Description, Version 1.1* *Mazu Profiler Blade System Version 5 Hardware Platforms, February 2005* *5.0-profiler.info.txt* *5.0-profiler.packages.txt*	The listed documentation evidence provides for the unique identification of the TOE as well as a reference to its components in the form of a configuration management list and process description.

Component	Document(s)	Rationale
ADO_DEL.1 Delivery procedures	*Profiler Blade System Version 5.0 Delivery Process Description, Version 2.0* *IBM BladeCenter 4-Port GB Ethernet Switch Module Installation Guide* *Chassis Blade Packing Slip* *Tracking Slip from Falcon Air Freight* *FW UPS Ship notification Tracking Number 1ZYF97240196682626*	The listed documentation evidence provides a description of the procedures used by the developer to securely deliver the TOE to the client.
ADO_IGS.1 Installation, generation, and start-up procedures	*Installation Process Description, Version 1.0* *Software installation procedures.html, February 22, 2005*	The TOE is delivered in a configured state. The listed documentation evidence provides specific details to allow the user to modify the default security parameters to meet the requirements for the environment that the TOE is deployed.
ADV_FSP.1 Informal functional specification	*Mazu Profiler Data Requirements, May 2003* *Profiler 5.0 Blade System Functional Specification, Version 5.0*	The listed documentation evidence provides for the definition of all external interfaces to the TOE and describes them in terms of their purpose, method and use.
ADV_HLD.1 Descriptive high-level design	*Profiler Blade System High Level Design Specification, Version 6.0, August 15, 2005*	The listed documentation evidence separates the TOE into logical enforcement structures used to enforce the Security Functions provided by the TOE.
ADV_RCR.1 Informal correspondence demonstration	*Profiler Blade System Representation Correspondence, Version 1.2, August 16, 2005*	To be completed after receipt of evidence.

Component	Document(s)	Rationale
AGD_ADM.1 Administrator guidance	*Mazu Profiler Version 5.0-5 User's Manual* *Mazu Profiler 5.0 Release Notes* *IBM eServer BladeCenter HS20, Type 8832 Installation and User's Guide* *IBM eServer HS20, SCSI Storage Expansion Unit* *IBM eServer BladeCenter, Type 8677 Installation and User's Guide* *IBM BladeCenter 4-Port Gb Ethernet Switch Module Installation Guide* *IBM Distributed Power Interconnect Front-end Power Distribution Unit Installation & Maintenance Guide* *Mazu Networks Support Services Handbook*	The TOE is delivered in a configured state. The listed documentation evidence provides specific details to allow the user to modify the default security parameters to meet the requirements for the environment that the TOE is deployed.

Component	**Document(s)**	**Rationale**
AGD_USR.1 User guidance	*Mazu Profiler Version 5.0-5 User's Manual* *Mazu Profiler 5.0 Release Notes* *IBM eServer BladeCenter HS20, Type 8832 Installation and User's Guide* *IBM eServer HS20, SCSI Storage Expansion Unit* *IBM eServer BladeCenter, Type 8677 Installation and User's Guide* *IBM BladeCenter 4-Port Gb Ethernet Switch Module Installation Guide* *IBM Distributed Power Interconnect Front-end Power Distribution Unit Installation & Maintenance Guide* *Mazu Networks Support Services Handbook*	The TOE is delivered in a configured state. The listed documentation evidence provides specific details to allow the user to modify the default security parameters to meet the requirements for the environment that the TOE is deployed.
ATE_COV.1 Evidence of coverage	*Profiler 5.0 Blade System Security Function Test Plan, Version 6, July 29, 2005*	The listed documentation evidence describes the scope of the Security Functional Requirements included in this ST that have been tested by the developer..
ATE_FUN.1 Functional testing	*Profiler 5.0 Blade System Security Function Test Plan, Version 6, July 29, 2005*	The listed documentation evidence describes the scope of testing, the test cases, test procedures and test evidence produced by the developer.
ATE_IND.2 Independent testing	No developer documentation evidence required	No rationale is required for this component.
AVA_SOF.1 Strength of TOE security function evaluation	*Mazu Networks, Inc. Profiler Password Strength of Function Analysis, July 13, 2004*	The *Mazu Networks, Inc. Profiler Password Strength of Function Analysis* provides the metrics and justification to support the strength of function claim for the password mechanism implemented by the TOE.
AVA_VLA.1 Developer vulnerability analysis	*Profiler 5.0 Blade System Developer Vulnerability Analysis, July 13, 2005*	The listed documentation evidence describes the vulnerability assessment and penetration analysis performed by the developer to demonstrate that the TOE provides adequate protection of its Security Functions when deployed in the evaluated configuration.

7 Protection Profile Claims

This ST does not claim Protection Profile conformance.

8 Rationale

This chapter provides the rationale for completeness and consistency of the Security Target. This rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependency
- TOE Summary Specification
- Strength of Function
- PP Claims

8.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated assumptions, threats and organizational security policies.

Table 5 - Security Environment to Security Objectives Mapping

Assumption, Threat, Organisational Security Policy	Security Objective	Rationale
A.CONFIG: The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation.	O.E.CONFIG: The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation.	During installation and operation of the TOE, it is important that all users follow the procedures and instructions provided by the TOE guidance documentation.
A.NOEVIL: The authorized users are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	O.E.CONFIG: The TOE will be installed, configured, and managed in accordance with its evaluated configuration as defined by its guidance documentation. O.E.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	Authorized users must protect their authentication credentials and abide by the guidance documentation when interacting with the security features provided by the TOE.

Assumption, Threat, Organisational Security Policy	Security Objecti ve	Rationale
A.NOTRST: The TOE can only be accessed by authorized users.	O.E.CREDEN: Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security. O.E.LOCATE: The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unauthorised physical access.	Since the TOE is to be installed in a protected environment, it is imperative that authorized users protect their identification and authentication credentials.
A.PASSWD: The authorized users of the TOE will use best commercial practices when establishing passwords.	O.E.PASSWD: The authorized users of the TOE will use best commercial practices when establishing passwords.	Authorized users must establish strong password credentials used for authentication to the TOE.
A.LOCATE: The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unauthorised physical access.	O.E.LOCATE: The TOE will be installed on an internal network segment and will be located within controlled access facilities that will prevent unau thorised physical access.	The TOE must be installed in a protected environment in order to mitigate the probability of attacks from malicious users.
A.PEER: IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.	O.E.PEER: IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.	IT components that communicate with the TOE must be deployed and administered in a manner to ensure security and accuracy of information transmissions.
T.ACCESS: A user could attempt to establish an unauthorised session with the TOE.	O.RESTRICT: The TOE will restrict access to its security features to authorised users.	The TOE will only establish a connection with a user once they have been successfully identified and authenticated.
T.COLLECT: An unauthorised user could remove or modify statistical data collected by the TOE that is used for analysing the behaviour of normal network activity.	O.MANAGE: The TOE will provide authorised users with the capability to perform analysis of activities occurring on the local network and modify its configuration settings. O.REPORT: The TOE will provide authorised users with alerts to network behavioural anomalies and the capability to generate statistical reports based on collected heuristics. O.RESTRICT: The TOE will restrict access to its security features to authorised users.	The TOE collects events from Mazu Sensors and allows for authorised users to perform analysis on the data collected. In addition, access to the reporting and heuristic mechanisms of the TOE requires that the user be authorised with respect to their assigned role.

Assumption, Threat, Organisational Security Policy	Security Objecti ve	Rationale
T.COMINT: An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.	O.INTEGR: The TOE must ensure the integrity of all audit data. O.MANAGE: The TOE will provide authorised users with the capability to perform analysis of activities occurring on the local network and modify its configuration settings. O.REPORT: The TOE will provide authorised users with alerts to network behavioural anomalies and the capability to generate statistical reports based on collected heuristics. O.RESTRICT: The TOE will restrict access to its security features to authorised users.	The TOE requires user identification and authentication prior to providing access to its security features. Only authorized users have the ability to access the data collected by the TOE from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers. In addition, the TOE enforces authentication upon the sensors, probes and routers that exist in the environment in order to validate their inputs.
T.FALACT: The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.	O.IDACTS: The TOE must accept data from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers and then apply analytical processes and information to derive conclusions about anomalies (past, present, or future). O.RESPON: The TOE must respond appropriately to analytical conclusions.	The TOE will respond to anomalous activity that deviates from normal network usage patterns.
T.NOHALT: An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.	O.IDACTS: The TOE must accept data from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers and then apply analytical processes and information to derive conclusions about anomalies (past, present, or future). O.RESTRICT: The TOE will restrict access to its security features to authorised users.	The TOE requires user identification and authentication prior to providing access to its security features. In addition, the TOE will collect all attempts to halt its execution by analyzing the data collected on the network from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers. As a result, this provides the TOE with resistance against direct attacks.
T.E.SENSOR: A user on an internal or external network could perform hostile actions on the internal network without having such actions captured for analysis and review.	O.E.SENSOR: At least one Mazu Sensor will be deployed in the IT environment and configured to route collected events to the TOE for processing and analysis.	It is important that the TOE receive audit data that has been collected by Mazu Sensors in order for the TOE to provide analysis and detection of network anomalies. The TOE will provide defence against attackers who possess a low attack potential.
T.E.TIME: A user may attempt to spoof timestamp values provided by an NTP server thereby causing the TOE and/or IT components with which the TOE communicates to maintain deferring time values.	O.E.TIME: The TOE and all IT components with which the TOE communicates will be configured to receive reliable timestamps from a protected NTP server.	It is important that the TOE and all IT components with which it communicates receive time from a reliable source. This is to ensure that all components are synchronized and report events for analysis consistently.

8.2 Security Functional Requirements Rationale

This Security Target does not contain explicitly stated Security Functional Requirement components. The following table provides a mapping to identify the Security Functional Requirement components that address the stated objectives.

Table 6 - Security Objective to Security Functional Requirement Component Mapping

Security Objective	Security Functional Requirement Component	Rationale
O.IDACTS: The TOE must accept data from Mazu Sensors, NETScout Probes, and NetFlow Enabled Routers and then apply analytical processes and information to derive conclusions about anomalies (past, present, or future).	FMT_MOF.1 Management of security functions behaviour (1)	The security functional requirement component FMT_MOF.1 supports O.IDACTS by limiting access to functions that control the operation of the TOE to an authorised user.
	FMT_MOF.1 Management of security functions behaviour (2)	The security functional requirement component FMT_MOF.1 supports O.IDACTS by limiting access to functions that control the operation of the TOE to an authorised user.
	FMT_MTD.1 Management of TSF data (1)	The security functional requirement component FMT_MTD.1 supports O.IDACTS by limiting access to analysis and operational functions that control the TOE to an authorised user.
	FMT_MTD.1 Management of TSF data (2)	The security functional requirement component FMT_MTD.1 supports O.IDACTS by limiting access to analysis and operational functions that control the TOE to an authorised user.
	FAU_SAA.2 Profile based anomaly detection	The security functional requirement component FAU_SAA.1 supports O.IDACTS by providing the capability to monitor the behaviour of hosts compared to a historical baseline. Heuristics are used and alerts are generated when alerting thresholds have reached a certain value.
O.INTEGR: The TOE must ensure the integrity of all audit data.	FAU_STG.2 Guarantees of audit data availability	The security functional requirement component FAU_STG.2 supports O.INTEGR by providing storage capabilities for collected audit data to prevent unauthorized deletion.
	FPT_RVM.1 Non-bypassability of the TSP	The security functional requirement component FPT_RVM.1 supports O.INTEGR by restricting the possibility of users or application processes subverting the security policy enforced by the TOE.

Security Objective	**Security Functional Requirement Component**	**Rationale**
	FPT_SEP.1 TSF domain separation	The security functional requirement component FPT_SEP.1 supports O.INTEGR by providing a protected environment used while managing the TOE.
O.MANAGE: The TOE will provide authorised users with the capability to perform analysis of activities occurring on the local network and modify its configuration settings.	FMT_MOF.1 Management of security functions behaviour (1)	The security functional requirement component FMT_MOF.1 supports O.MANAGE by limiting access to functions that control the operation of the TOE to an authorised user.
	FMT_MOF.1 Management of security functions behaviour (2)	The security functional requirement component FMT_MOF.1 supports O.MANAGE by limiting access to functions that control the operation of the TOE to an authorised user.
	FMT_MTD.1 Management of TSF data (1)	The security functional requirement component FMT_MTD.1 supports O.MANAGE by limiting access to analysis and operational functions that control the TOE to an authorised user.
	FMT_MTD.1 Management of TSF data (2)	The security functional requirement component FMT_MTD.1 supports O.MANAGE by limiting access to analysis and operational functions that control the TOE to an authorised user.
	FMT_SMF.1 Specification of management functions	The security functional requirement component FMT_SMF.1 supports O.MANAGE by providing the capability manipulate the security features provided by the TOE to authorised users.
	FMT_SMR.1 Security roles	The security functional requirement component FMT_SMR.1 supports O.MANAGE by providing the Administrator with the capability to assign users to specific roles maintained by the TOE.
	FPT_RVM.1 Non-bypassability of the TSP	The security functional requirement component FPT_RVM.1 supports O.MANAGE by restricting the possibility of users or application processes subverting the security policy enforced by the TOE.
	FPT_SEP.1 TSF domain separation	The security functional requirement component FPT_SEP.1 supports O.MANAGE by providing a protected environment used while managing the TOE.

Security Objective	**Security Functional Requirement Component**	**Rationale**
O.REPORT: The TOE will provide authorised users with alerts to network behavioural anomalies and the capability to generate statistical reports based on collected heuristics.	FAU_ARP.1 Security alarms	The security functional requirement component FAU_ARP.1 supports O.REPORT by generating alarms to authorised users as a result of detection of a security violation.
	FAU_SAA.2 Profile based anomaly detection	The security functional requirement component FAU_SAA.1 supports O.REPORT by providing the capability to monitor the behaviour of hosts compared to a historical baseline. Heuristics are used and alerts are generated when alerting thresholds have reached a certain value.
	FAU_SAR.1 Audit review (1)	The security functional requirement component FAU_SAR.1 supports O.REPORT by providing audit data to specific roles.
	FAU_SAR.1 Audit review (2)	The security functional requirement component FAU_SAR.1 supports O.REPORT by providing audit data to specific roles.
	FAU_SAR.2 Restricted audit review	The security functional requirement component FAU_SAR.2 supports O.REPORT by limiting access to audit data to specific roles.
	FAU_SAR.3 Selectable audit review	The security functional requirement component FAU_SAR.3 supports O.REPORT by limiting access to selection criteria on audit data to specific roles.
	FAU_STG.2 Guarantees of audit data availability	The security functional requirement component FAU_STG.2 supports O.REPORT by providing storage capabilities for collected audit data.
	FAU_STG.4 Prevention of audit data loss	The security functional requirement component FAU_STG.4 supports O.REPORT by preventing the loss of recent activities catalogued by the audit records.
O.RESTRICT: The TOE will restrict access to its security features to authorised users.	FIA_ATD.1 User attribute definition	The security functional requirement component FIA_ATD.1 supports O.RESTRICT by providing the Administrator with the capability to specify credentials for authorised users that are allowed to access the TOE security functions.

Security Objective	Security Functional Requirement Component	Rationale
	FIA_UAU.2 User authentication before any action	The security functional requirement component FIA_UAU.2 supports O.RESTRICT by allowing users and the Administrator with the capability to specify a unique password used for authentication to the TOE.
	FIA_UID.2 User identification before any action	The security functional requirement component FIA_UID.2 supports O.RESTRICT by limiting the capability to create user accounts on the TOE to the Administrator.
O.E.SENSOR: At least one Mazu Sensor will be deployed in the IT environment and configured to route collected events to the TOE for processing and analysis.	FAU_GEN.1 Audit data generation	The security functional requirement component FAU_GEN.1 supports O.E.SENSOR by functioning as a collection engine for network events to be sent to the TOE for statistical analysis.
O.E.TIME: The TOE and all IT components with which the TOE communicates will be configured to receive reliable timestamps from a protected NTP server.	FPT_STM.1 Reliable time stamps	The security functional requirement component FPT_STM.1 supports O.E.TIME to ensure that the TOE and IT components with which the TOE communicates maintain consistent time values used during the reporting of events.

8.3 Security Assurance Requirements Rationale

This Security Target does not contain explicitly stated Security Assurance Requirement components. Section 6.2 identifies the assurance measures provided for evaluation as well as rationale to describe how the assurance measures meet each Security Assurance Requirement component for EAL2. EAL2 was selected as the target assurance level in order to demonstrate that defence is provided against attackers who possess a low attack potential.

8.4 Requirement Dependency Rationale

8.4.1 Security Functional Requirements Dependency Rationale

The following table identifies the Security Functional Requirement components of the TOE mapped to their respective dependencies. All component dependencies have been satisfied except where noted.

Table 7 - TOE SFR Dependency Mapping

	Component Dependency						
SFR Component	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_SMF.1	FMT_SMR.1
FAU_ARP.1		X[2]					
FAU_SAA.2					X[4]		
FAU_SAR.1(1)	X[1]						
FAU_SAR.1(2)	X[1]						
FAU_SAR.2			X				
FAU_SAR.3			X				
FAU_STG.2	X[1]						
FAU_STG.4				X[3]			
FIA_ATD.1							
FIA_UAU.2					X[4]		
FIA_UID.2							
FMT_MOF.1(1)						X	X
FMT_MOF.1(2)						X	X
FMT_MTD.1(1)						X	X
FMT_MTD.1(2)						X	X
FMT_SMF.1							
FMT_SMR.1					X[4]		
FPT_RVM.1							
FPT_SEP.1							

[1] The TOE has not met this dependency. The component addressing the audit data generation function has been levied to the IT environment.
[2] FAU_SAA.2 is hierarchical to FAU_SAA.1 and thus this dependency has been met.
[3] FAU_STG.2 is hierarchical to FAU_STG.1 and thus this dependency has been met.
[4] FIA_UID.2 is hierarchical to FIA_UID.1 and thus this dependency has been met.

The following table identifies the Security Functional Requirement components of the IT environment mapped to their respective Security Functional Requirement component dependencies.

Table 8 - IT Environment SFR Dependency Mapping

	Component Dependency
SFR Component	FPT_STM.1
FAU_GEN.1	X
FPT_STM.1	

8.4.2 Security Assurance Requirements Dependency Rationale

The following table identifies the Security Assurance Requirement components for the TOE mapped to their respective dependencies. All component dependencies have been satisfied for EAL2.

Table 9 - TOE SAR Dependency Mapping

	Component Dependency					
SAR Component	AGD_ADM.1	AGD_USR.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	ATE_FUN.1
ACM_CAP.2						
ADO_DEL.1						
ADO_IGS.1	X					
ADV_FSP.1					X	
ADV_HLD.1			X		X	
ADV_RCR.1						
AGD_ADM.1			X			
AGD_USR.1			X			
ATE_COV.1			X			X
ATE_FUN.1						
ATE_IND.1	X	X	X			X
AVA_SOF.1			X	X		
AVA_VLA.1	X	X	X	X		

8.5 TOE Summary Specification Rationale

Rationale for the TOE Summary Specification is provided in Chapter 6. Section 6.1 describes each Security Function provided by the TOE as well adding rationale to elaborate on how the TOE implements each Security Functional Requirement component. Section 6.2 identifies the assurance measures provided for evaluation as well as rationale to describe how the assurance measures meet each Security Assurance Requirement component for EAL2.

8.6 Strength of Function Rationale

This Security Target includes one probabilistic or permutational function that is implemented by the TOE via the FIA_UAU.2 Security Functional Requirement component. This component utilizes a password function that requires a minimum of six characters be used when authenticating users through the HTTPS interface on the TOE. The implementation of this password function meets the level requirements for Strength of Function-basic (SOF-basic) in that the mechanism provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. The metric used to support this claim is as follows:

Minimum password space: 6 characters

Password values: Acceptable values for each space in the password include:

- 52 alphabetic characters (upper and lower case)
- 10 numeric characters
- 19 special characters (!, @, #, $, %, ^, &, *, (,), _, -, +, =, |, <, >, :, ;)
- Total of 81 possible values

Password combinations:

81^6 = (81*81*81*81*81*81) = 282,429,536,481 total password combinations

The Profiler requires manual entry for each password used during the authentication process. In addition, after three unsuccessful authentication attempts, the Profiler will lock out the user's account for 30 minutes before additional authentication attempts can be made on that user's account. The following calculation defines the maximum number of authentication attempts that can occur in a one hour period.

(60 / 30) * 3 = 6 password guesses per hour (based on account lockout)

Assuming that, on average, an attacker would have to cycle through half the non-valid inputs before choosing the valid input, an attacker would have to enter 141,214,768,240.5 (282,429,536,481 / 2) password attempts over a period of 23,535,794,706.75 (141,214,768,240.5 / 6) hours before guessing the correct password. This equates to approximately 2,684,895.58 (23,535,794,706.75 / 24 / 365.25) years to complete.

A scenario exists in which a user does not adhere to accepted practices for constructing strong passwords and might use a more easily guessed password consisting of a common word, name, or place. In this scenario, the user's account could be subjected to a "dictionary attack" wherein all such likely passwords may be attempted.

According to Dr. John Mitchell, Professor of Computer Science at Stanford University, a "typical password dictionary" used for such attacks would contain 1,000,000 entries of common passwords – including people's names, common pet names, etc. in addition to ordinary words. Using such a dictionary, the average number of passwords that an attacker would have to enter before guessing the correct password would be calculated as:

1,000,000 / 2 = 500,000 password combinations

The number of days required to conduct a successful attack would thus be calculated as follows:

500,000 / 6 / 24 = 3,472.22 days to successfully determine the password

An additional *worst case* scenario exists in which a user does not adhere to accepted practices for constructing strong passwords. In this scenario, the user could establish a password utilizing the same value in each space (ex. aaaaaa, 111111, etc.). This would equate to a *worst case* scenario of 81 possible password combinations. Assuming that, on average, an attacker would have to cycle through half the non-valid inputs before choosing the valid input, an attacker would have to enter 40.5 (81 / 2) guesses over a period of 6.75 (81 / 6 attempts per hour) hours before guessing the correct password.

It is important to note that the above two scenarios are not expected to occur, as the Security Target assumes that users will follow best commercial practices and establish more complex passwords for authentication.

In summary, the above calculations would indicate that the implementation of the password enforcement mechanism is at least resistant to an attacker with low attack potential in order to meet or exceed the SOF-basic claim.

8.7 PP Claims Rationale

This ST does not claim Protection Profile conformance.