ISS PROVENTIA™ A Version 7.0-2003.167, PROVENTIA™ G Version 8.0-2004.219, Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4

Security Target

Version 2.25

11 April 2006

Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, GA 30328

Table of Contents

List of Tables

1 SECURITY TARGET INTRODUCTION

This Chapter presents 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 that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL2.

ST Title:	ISS Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, Network Sensor 7.0, and SiteProtector 2.0 Service Pack 4 Security Target
ST Version:	Version 2.25
Publication Date:	11 April 2006
Authors:	Internet Security Systems, Inc.
TOE Identification:	ISS Proventia A Version 7.0-2003.167 with patch RSNetSnsr70_MU_24_2, Proventia G Version 8.0-2004.219 with patches RSNetSnsr70_Linux_XXX_ST_4_3 and RSNetSnsr70_MU_24_2, Network Sensor Version 7.0-2003.24 (for Linux) with patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19, Network Sensor Version 7.0-2002.155 (for Windows) with patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19 and SiteProtector 2.0 Service Pack 4 with patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11
	Target of Evaluation (TOE)

CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
Keywords:	Intrusion Detection System

1.2 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, version 2.2, CCIMB-2004-01-001.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, version 2.2, CCIMB-2004-01-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, version 2.2, CCIMB-2004-01-003.
[CEM]	Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, dated January 2004, version 2.2.

1.3 Acronyms, Abbreviations, and Definitions

The following acronyms and abbreviations are used in this Security Target:

Acronyms/ Abbreviations	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CPU	Central Processing Unit
DBMS	Database Management System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High Level Design
Inc.	Incorporated
IDS	Intrusion Detection System
ISS	Internet Security Systems
IT	Information Technology
Mbps	Megabits per second
NIC	Network Interface Card

Acronyms/ Abbreviations	Definition
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

The following definition is used in this Security Target:

Word/Phrase	Definition
DBMS Data	Data stored and process by a DBMS.

1.4 Security Target Overview

This Security Target addresses the ISS Proventia A Version 7.0-2003.167 with patch RSNetSnsr70_MU_24_2, Proventia G Version 8.0-2004.219 with patches RSNetSnsr70_Linux_XXX_ST_4_3 and RSNetSnsr70_MU_24_2, Network Sensor Version 7.0 with patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19 and SiteProtector 2.0 Service Pack 4 with the patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11 applied Target of Evaluation (TOE). Note that this document uses “Network Sensor Version 7.0” to describe both Network Sensor Version 7.0-2003.24 (for Linux) and Network Sensor Version 7.0-2002.155 (for Windows) since the only difference is the operating system on which they execute.

The TOE is an automated real-time intrusion detection system designed to protect 10/100/1000 Mbps and 1000 Mbps SX network segments.

The TOE is a manager/agent distributed product that monitors and responds to threats based upon configurable security levels spanning an entire enterprise or a single logical segment within a distributed network.

Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219 and Network Sensor Version 7.0 detect and report potential security violations to a software managed central console, SiteProtector 2.0 Service Pack 4. Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219 and Network Sensor Version 7.0 are deployed to interactively and automatically provide network-wide IDS functionality.

A summary of the TOE security functions can be found in Section 2, TOE Description. A detailed description of the security functions can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance Claim

This ST conforms to Part 2 extended and Part 3 conformant EAL2 of the CC, Version 2.2.

2 TOE DESCRIPTION

This section provides an overview of the ISS Proventia A Version 7.0-2003.167 with patch RSNetSnsr70_MU_24_2, Proventia G Version 8.0-2004.219 with patches RSNetSnsr70_Linux_XXX_ST_4_3 and RSNetSnsr70_MU_24_2, Network Sensor Version 7.0 with patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19 and SiteProtector 2.0 Service Pack 4 with the patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11 applied Target of Evaluation (TOE). This section also defines the physical and logical boundaries of the TOE and describes the evaluated configuration of the TOE.

2.1 Overview

The ISS Proventia A Version 7.0-2003.167 with patch RSNetSnsr70_MU_24_2, Proventia G Version 8.0-2004.219 witch patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_Linux_XXX_ST_4_3, Network Sensor Version 7.0 with patches, RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19 and SiteProtector 2.0 Service Pack 4 with the patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11 applied TOE is an automated real-time intrusion detection system (IDS) designed to protect 10/100/1000 Mbps copper and 1000 Mbps SX network segments. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE is comprised of four components:

A) Proventia A Version 7.0-2003.167;

B) Proventia G Version 8.0-2004.219;

C) Network Sensor Version 7.0 and

D) SiteProtector 2.0 Service Pack 4.

Three of the TOE components, Proventia A Version 7.0-2003.167 (hereafter referred to as Proventia A Version 7.0-2003.167 or Proventia A), Proventia G Version 8.0-2004.219 (hereafter referred to as Proventia G Version 8.0-2004.219 or Proventia G) and Network Sensor Version 7.0 (hereafter referred to as Network Sensor Version 7.0 or Network Sensor), provide the IDS functionality. Proventia A, Proventia G and Network Sensor monitor a network or networks and compare incoming packet or packets against known packet patterns that indicate a potential security violation. If a match occurs, Proventia A, Proventia G and/or Network Sensor will create an audit record. Proventia A, Proventia G and Network Sensor each provide the same security functionality claimed by this ST and are collectively referred to as Sensor or Sensors in the remaining of this document. The fourth component of the TOE, SiteProtector 2.0 Service Pack 4 (hereafter referred to as SiteProtector 2.0 Service Pack 4 or SiteProtector), provides management, monitoring and configuration functions to users.

The Sensors monitor one or more 10/100/1000 Mbps copper or 1000 Mbps SX fiber network segments (the sensed, monitored network). Additionally, each Sensor deployed is also connected to a secure network, the secure management network, for dedicated communication to a SiteProtector.

Several patches are applied to the TOE and to the IT Environment of the TOE. The patches applied to the TOE have been done to help in the mitigation of vulnerabilities discovered in the TOE. Patches have been applied to the IT Environment of the TOE to help in configuring the TOE's IT Environment to support the functioning of the TOE and to help put the IT Environment in a state that can help in the protection of the TOE. The patches for the TOE are RSNetSnsr70_Linux_XXX_ST_4_3, RSNetSnsr70_MU_20_19, RSNetSnsr70_MU_24_2, RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11.

The patches for the IT Environment are RSNetSnsr70_Linux_2.4.18-10smp_ST_4_1, RSNetSnsr70_Linux_2.4.18-10smp_ST_4_2, SPIA_POLICY_20050208, SPNS_POLICY_20050208, DB_SR_1_1_20040915, DB_SR_1_2_20041020, DB_SR_1_3_20041022, DB_XPU_1_44_20040628, DB_XPU_1_45_20040719, DB_XPU_1_46_20040812, DB_XPU_1_47_20040915, DB_XPU_1_48_20041014, DB_XPU_1_49_20041111 DB_XPU_1_50_20041221, and DB_XPU_1_51_20050119. These are also identified in the sections below.

The patches applied to the TOE do not affect the version number of the TOE. The patches are listed in the TOE after installation of the TOE has occurred so that an end user knows that they have the evaluated configuration with the patches applied.

2.2 TOE Components

The four components of the TOE: Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219, Network Sensor Version 7.0 and SiteProtector 2.0 Service Pack 4 are described in the following sections.

2.2.1 Proventia A Version 7.0-2003.167 TOE Component

The Proventia A Version 7.0-2003.167 component of the TOE is one of three components of the TOE that provide IDS security functionality. The Proventia A Version 7.0-2003.167 is offered by one of the following appliances: Proventia A201, Proventia A604, Proventia A604-200, Proventia A1204, Proventia A1204F, Proventia A1204F-400.

2.2.2 Proventia G Version 8.0-2004.219 TOE Component

The Proventia G Version 8.0-2004.219 component of the TOE is one of three components of the TOE that provide IDS security functionality. The Proventia G Version 8.0-2004.219 is offered by one of the following appliances: Proventia G100, Proventia G200, Proventia G1000, Proventia G1000F, Proventia G1200, Proventia G1200CF, or the Proventia G1200F

2.2.3 Network Sensor Version 7.0 TOE Component

The Network Sensor component of the TOE is one of three components of the TOE that provide IDS security functionality. The Network Sensor Version 7.0 is offered by one of the following products:

a) RealSecure Gigabit Network Sensor 7.0 for Windows
b) RealSecure Gigabit Network Sensor 7.0 for Red Hat Linux
c) RealSecure Network Sensor 7.0 for Windows
d) RealSecure Network Sensor 7.0 for Red Had Linux

Each of the above software products offers Network Sensor 7.0. Although the products vary by offering different network interfaces and operate on different operating systems, the operating system and network drivers are not included in the security functionality claimed by the TOE. Therefore, all of the above appliances offer the same Network Sensor 7.0 TOE component.

2.2.4 SiteProtector 2.0 Service Pack 4 TOE Component

The SiteProtector 2.0 Service Pack 4 component of the TOE is a software product that enables users to monitor and manage the Sensor components of the TOE.

2.3 TOE Functionality Overview

2.3.1 Sensors

Sensors monitor packets on a sensed, monitored network or networks and compare the incoming packet or packets against signatures. Signatures are known packet or packet patterns that indicate a possible attack or intrusion against hosts or network segments. If a match occurs, the Sensors create an event (audit record). This audit data is sent to the TOE's SiteProtector which enables a user to view and analyze the audit information.

Signatures are configured on the Sensors by Policy Files. Policy Files identify a sub-set of signatures based on attack type. At TOE installation time, the SiteProtector is installed with a set of Policy Files and the Sensors are configured with one default Policy File and the signature files that apply to all Policy Files. SiteProtector enables a user to disable/enable signatures in a Sensor's current Policy File or select and apply a new Policy File selected from the set of Policy Files.

2.3.2 SiteProtector

The SiteProtector is used as the central controlling point for Sensors deployed on the network. The SiteProtector performs the following functionality:

A) Manages and monitors Sensors and SiteProtector sub-components,
B) enables an administrator to view TOE component configuration data,

C) displays audit records,

D) initiates and maintains the network connection between SiteProtector and the Sensors it is configured to monitor.

SiteProtector relies on its host OS in performing identification and authentication (I&A) of users. For a user of the TOE to properly gain access to SiteProtector the user roles on the host OS and the roles maintained by SiteProtector need to be insync with each other. SiteProtector User Groups (User Roles) are automatically created during the installation of SiteProtector. The installation procedures create the three roles supported by SiteProtector: Operator, Analyst and Administrator. The IT Environment Administrator is responsible for defining user names, passwords and associating the User Groups to the user name/password pairs to enable successful SiteProtector login.

SiteProtector relies on the host OS to verify the user name and password entered into the SiteProtector GUI login screen. The login screen is invoked by users and requires users to identify and authenticate themselves. If the user name/password pair is not successfully verified by the host OS, the SiteProtector login screen refreshes by clearing the entered user name and password and not allowing any further actions. If the user name and password are successfully verified, SiteProtector obtains from the host OS the User Group associated with the user name/password pair. If the User Group (User Role) is a non-supported SiteProtector User Role, SiteProtector will not allow any further actions. If the User Role is a supported SiteProtector role, SiteProtector uses this User Role to determine the privilege level of the user. Users assigned the User Role of Analyst or Administrator are considered privileged users and have access to all GUIs. Users assigned the User Role of Operator have limited privileges. Operators can view TSF Data but cannot modify TSF Data or invoke any functions that affect the TSF.

2.3.2.1 SiteProtector Components

The SiteProtector is divided into the following components and depicted in Figure 2 below.

a) SiteProtector Console – The SiteProtector Console is a graphical user interface (GUI) that provides a user interface that enables a user to configure and monitor the Sensors.

b) SiteProtector Event Collector – The SiteProtector Event Collector is a software process that is responsible for receiving data from the Sensors and storing the data in the IT Environment supplied DBMS.

c) SiteProtector Application Server – The SiteProtector Application Server is a software process that is responsible for providing communication between the IT Environment supplied DBMS and the SiteProtector Console.

d) SiteProtector Sensor Controller – The SiteProtector Sensor Controller is a software process that is responsible for processing command and control information from the SiteProtector Console and the IT Environment supplied DBMS and sending the command and control information to the Sensors or the SiteProtector Event Collector.

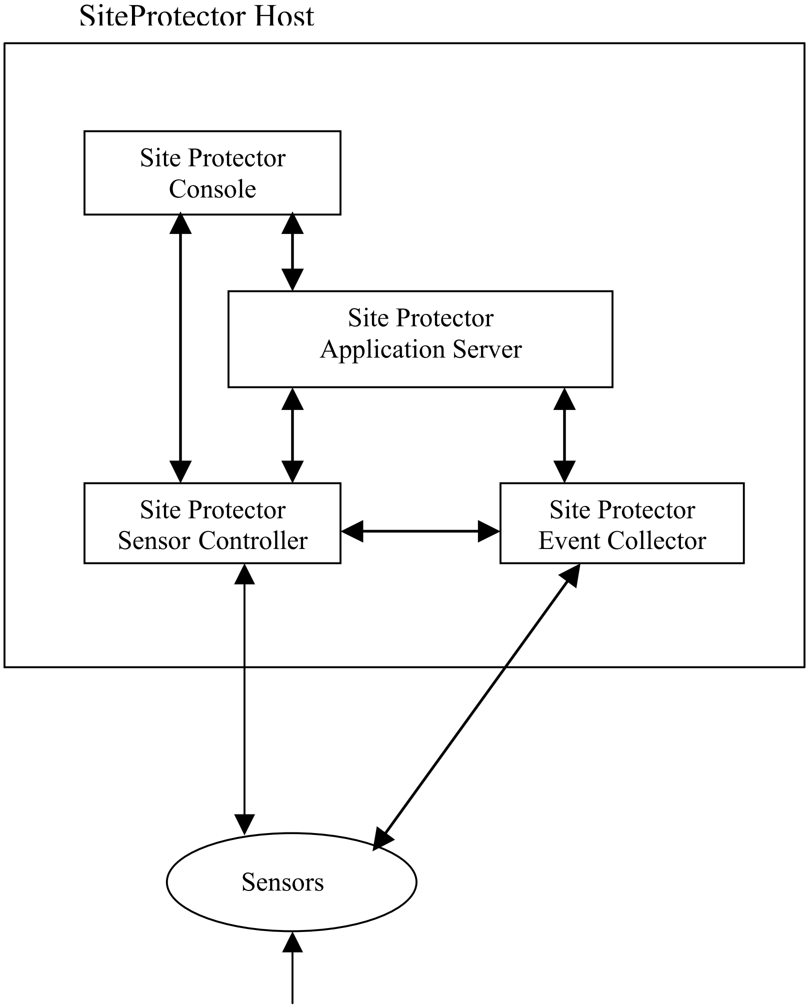
SiteProtector Host
Site Protector Console
Site Protector Application Server
Site Protector Sensor Controller
Site Protector Event Collector
Sensors

Figure 1 SiteProtector Components

2.4 TOE Physical Boundary

The physical boundary for the Proventia A TOE component is the Proventia A Version 7.0-2003.167 software application with the patch RSNetSnsr70_MU_24_2 applied. The physical boundary for the Proventia G TOE component is the Proventia G Version 8.0-2004.219 software application with the patches RSNetSnsr70_Linux_XXX_ST_4_3 and

RSNetSnsr70_MU_24_2 applied. The physical boundary for the Network Sensor TOE component is the Network Sensor Version 7.0 software application with the patches RSNetSnsr70_MU_24_2 and RSNetSnsr70_MU_20_19 applied.

The physical boundary for the SiteProtector is the SiterProtector 2.0 Service Pack 4 application software with the patches RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11 applied. The SiteProtector runs on a SiteProtector host. The SiteProtector host requires Windows 2000 Server OS; Microsoft SQL Server 2000 that supplies the (DBMS); and Microsoft Internet Explorer and Java RTE that supply the web browser and Java interpreter that support the SiteProtector Console GUI interface. The TOE component of the SiteProtector host is SiteProtector 2.0 Service Pack 4.

Included in the physical boundary is TSF Data. The TSF data includes Policy Files that define signature events and audit records generated by the Sensors. The transfer of TSF Data between the SiteProtector and the Sensors is protected by the IT Environment supplied secure, management network and the DBMS protects TSF data that is being stored on the SiteProtector host. SiteProtector Host resident TSF Data is collectively referred to as the SiteProtector database. The SiteProtector database is managed by an IT Environment supplied third-party database management system (DBMS). The DBMS provides a SiteProtector Host resident human user interface and a programmatic SQL interface. Both interfaces support user initiated storage commands, modification commands, and enable users to extract information to/from the database.

ISS offers two types of patches that are updates that are necessary to put the TOE into the evaluated configuration. The two types of patches are service packs (SPs) and express updates (XPUs). Some of the patches update items in the IT environment while other patches update TOE components. The lists below indicate which patches are updating items in the IT environment and which patches are updating TOE components.

The demarcation of the TOE components and the IT Environment are listed below and depicted in Figure 3.

TOE Components:

A) Proventia A Version 7.0-2003.167 application software

B) Proventia G Version 8.0-2004.219 application software

C) Network Sensor Version 7.0

D) SiteProtector 2.0 Service Pack 4

E) Sensor resident signature files, current active Policy File, commands, and audit records (before transfer to the SiteProtector)

F) SiteProtector resident default Policy Files and audit data

G) Patches RSNetSnsr70_Linux_XXX_ST_4_3, RSNetSnsr70_MU_20_19, RSNetSnsr70_MU_24_2, RSEvntCol69_WINNT_XXX_ST_1_9, RSEvntCol69_WINNT_XXX_ST_1_10, and RSEvntCol69_WINNT_XXX_ST_1_11.

IT Environment:

A) Appliance hardware the Proventia A Version 7.0-2003.167 or Proventia G Version 8.0-2004.219 resides on.

B) Workstation hardware each Network Sensor Version 7.0 or SiteProtector subcomponents resides on.

C) Proventia A Version 7.0-2003.167 and Proventia G Version 8.0-2004.219 appliance operating system, Red Hat 8.0.

D) Network Sensor Version 7.0 operating system (Microsoft Windows 2000 or Red Hat Linux 7.3).

E) SiteProtector 2.0 Service Pack 4 workstation operating system (Microsoft Windows 2000 Server).

F) Database Management System implementation (Microsoft SQL Server 2000).

G) SiteProtector Console workstation's Web browser (Microsoft Internet Explorer 5.0 or higher) and Java RTE.

H) Network software and hardware on each TOE component that provides a connection to the secure management network that provides communication between the Sensors and the SiteProtector. The security being provided by the network software and hardware is confidentiality and integrity of the data being transported by the secure management network.

I) Network software and hardware that provides a connection to the sensed, monitored network for Proventia A appliance(s), Proventia G appliance(s) and/or Network Sensor host(s).

J) An IT Environment supplied timer that is used by the components of SiteProtector.

K) The IT environment provides the appliance hardware, the OS, the network software and hardware that provides a connection to the secure management network and the network software and hardware that provides a connection to the sensed, monitored network.

L) The Network Sensor host operates on either Windows or a standard non-hardened Red Hat Linux OS.

M) RSNetSnsr70_Linux_2.4.18-10smp_ST_4_1, RSNetSnsr70_Linux_2.4.18-10smp_ST_4_2, SPIA_POLICY_20050208, SPNS_POLICY_20050208, DB_SR_1_1_20040915, DB_SR_1_2_20041020, DB_SR_1_3_20041022, DB_XPU_1_44_20040628, DB_XPU_1_45_20040719, DB_XPU_1_46_20040812, DB_XPU_1_47_20040915,

DB_XPU_1_48_20041014, DB_XPU_1_49_20041111
DB_XPU_1_50_20041221, and DB_XPU_1_51_20050119

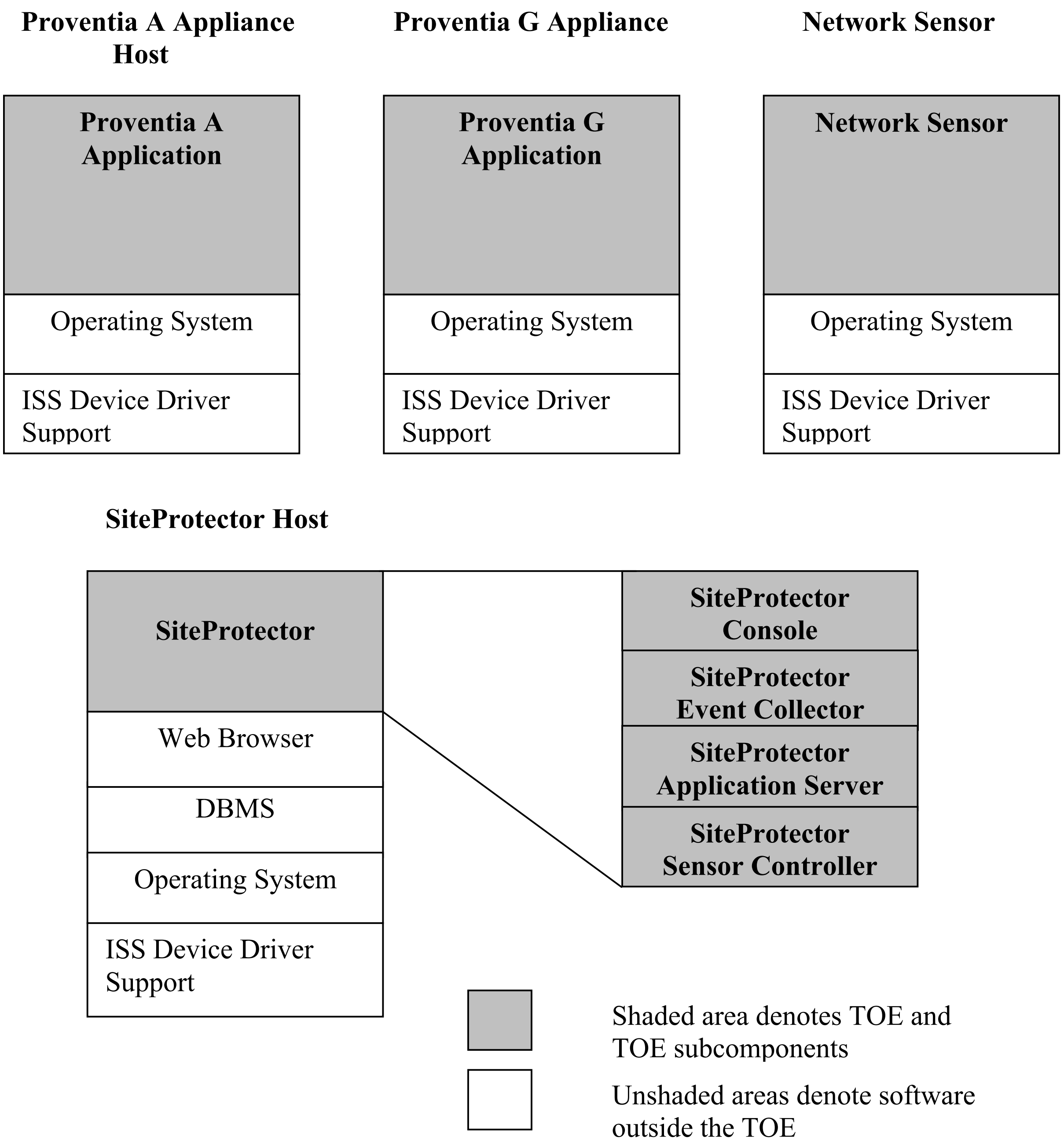
Proventia A Appliance Host
Proventia G Appliance
Network Sensor
Proventia A Application
Operating System
ISS Device Driver Support
Proventia G Application
Operating System
ISS Device Driver Support
Network Sensor
Operating System
ISS Device Driver Support
SiteProtector Host
SiteProtector
Web Browser
DBMS
Operating System
ISS Device Driver Support
SiteProtector Console
SiteProtector Event Collector
SiteProtector Application Server
SiteProtector Sensor Controller
Shaded area denotes TOE and TOE subcomponents
Unshaded areas denote software outside the TOE

Figure 2 TOE Physical Boundary

2.5 Logical Scope and Boundary

The TOE’s logical boundary is described below:

Audit Security Function

The TOE's Audit Security Function provides audit data generation, selective auditing, audit data viewing and selective audit data viewing.

Detection Security Function

The TOE provides Detection Security Functionality by continuously monitoring network traffic and monitoring the TOE components to report network outages.

Protect Security Function

The TOE Protect Security Functionality provides functionality that protects its TSF Data and TOE functions from unauthorized access.

Management Security Function

The TOE's Management Security Function provides an interface that enables a user to manage and monitor the TOE.

The TOE's logical scope does not include Sensors' network device drivers or the intrusion prevention functionality provided by Proventia G. The Proventia G system is configured as an IDS system at system installation.

2.5.1 Exclusions from TOE Security Functions

This section presents a delineation of components that are in the TOE, but do not contribute to meeting any of the Security Functional Requirements (SFRs) and hence are excluded from the TOE Security Functions (TSF).

- The Intrusion Prevention System (IPS) Component
- The Incident and Exception Component

2.6 TSF Data

Policy files and audit records are TSF data. The Policy files affect how the TSF enforces the TSP defined in this ST. A policy file defines signature events. Signature events are patterns that a Sensor searches for in network traffic captured from the IT environment. The audit records are generated by the TOE based on events the TOE recognizes based on the Policy file signatures.

2.7 Security Attributes

The security attributes of the TOE are roles. The role of a user defines the privileges that the user has and the privileges a user has defines the operations that the user may carry out while having an active user session with the TOE.

2.8 User Data

There is no user data for this TOE.

2.9 Rationale for Non-Bypassability and Separation

The TOE is composed of multiple software components. The different software components execute in an IT environment that provides the underlying system that includes hardware and software required for operation of the TOE. Therefore, responsibility for non-bypassability and domain separation is split between the TOE and IT Environment.

2.9.1 Rationale for Non-Bypassability and Separation for the TOE

The rationales for non-bypassability and separation for the TOE are broken into two rationales in the following sections. There is a rationale for the Proventia A, Proventia G, and Network Sensor TOE components and a rationale for the SiteProtector component of the TOE.

2.9.1.1 Rationale for the Proventia A, Proventia G and Network Sensor 7.0 Components of the TOE

The following two sub-sections describe the rationales for non-bypassability and domain separation for the Proventia A, Proventia G, and Network Sensor TOE components.

2.9.1.1.1 Rationale for Non-Bypassability

The Proventia A, Proventia G, and Network Sensor TOE components have monitoring interfaces to their host IT environment which are used to collect network packets received by the host IT environment interfaces that are connected to the monitored network. The monitoring interfaces of the Proventia A, Proventia G, and Network Sensor TOE components only carry out one function and that is to read packets from the host IT Environment and immediately apply the TSP enforcement functions that deal with processing and analyzing network packets for security violations (intrusions) as specified in the policy file for the Proventia A, Proventia G, or Network Sensor TOE components. No other function is able to be carried out through the Proventia A, Proventia G, or Network Sensor TOE components monitoring interfaces. Further, the monitoring interfaces of the Proventia A, Proventia G, and Network Sensor TOE components do not provide any programmatic interfaces or functions that may be invoked by users and do not accept commands from users on the monitored network.

The other interface to the Proventia A, Proventia G, and Network Sensor TOE components is the management interfaces that communicate with SiteProtector. The management security enforcing interfaces ensure that all enforcement functions successfully succeed before allowing any other actions dealing with the management of the Proventia A, Proventia G, or Network Sensor TOE components to proceed.

2.9.1.1.2 Rationale for Domain Separation

The Proventia A, Proventia G, and Network Sensor TOE components maintain a security domain by having well defined monitoring and management interfaces and only allowing a strictly controlled set of functionality to be carried out through these interfaces that deal with enforcing the TSP. Only authorized subjects are allowed to connect and communicate with the management interface of the Proventia A, Proventia G, and Network Sensor TOE components. The monitoring interfaces of the Proventia A, Proventia G, and Network Sensor TOE components only allows for the collection of network packets so no functionality is provided to un-authorized or authorized subjects through the monitoring interfaces. The strictly controlled functionality provided by the interfaces allows for the Proventia A, Proventia G, and Network Sensor TOE components to have a security domain that protects it from interference and tampering.

2.9.1.2 Rationale for the SiteProtector Component of the TOE

The following two sub-sections describe the rationale for non-bypassability and domain separation for the SiteProtector TOE component.

2.9.1.2.1 Rationale for Non-bypassability

SiteProtector provides graphical user interfaces (GUIs) used by users to manage and monitor the Sensors. Further, SiteProtector has several network and application interfaces that interact with the host IT Environment communicating with the Sensors and to communicate with the host IT Environment of SiteProtector.

The GUIs provide strictly controlled functionality to the users within the TSC. By limiting the functionality, the TSF is protected from corruption or compromise from users within the TSC. SiteProtector interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). Human users must identify and authenticate themselves through the host IT environment before being allowed to use the features of SiteProtector. Identification and authentication (I&A) of the user with the IT Environment establishes the user as an authorized user of SiteProtector and is necessary before they may carry out any other action within the TSC.

The network and application interfaces of SiteProtector are interfaces that are used to collect data from the Sensors and IT Environment and to communicate commands to the Sensors and IT environment. The network and application interfaces are established to communicate only with Sensors and the host IT Environment. Whenever the network and application communication interfaces of SitProtector are used they invoke the TSP enforcement functions before any other action that is to be carried out by the SiteProtector is allowed to proceed.

2.9.1.2.2 Rationale for Domain Separation

The SiteProtector maintains a security domain by having a well defined GUI and network and application communication interfaces, only allowing a strictly controlled set of functionality to be carried out through these interfaces, and not offering any general purpose computing or programming capabilities. The strictly controlled functionality provided by the interfaces allows for SiteProtector to have a security domain that protects it from interference and tampering..

2.9.2 Rationale for Non-Bypassability and Domain Separation for the IT Environment

The following subsections describe the rationales for non-bypassability and domain separation offered by the IT Environment that the TOE components execute on. Further, each subsection is broken out into the different IT Environment that exists for the Proventia A and Proventia G TOE components, the Network Sensor TOE component, and the SiteProtector TOE component.

2.9.2.1 Rationale for Non-Bypassability

The rationale for non-bypassability supplied by the IT Environment is broken into three different descriptions. The three different descriptions are non-bypassability supplied by the IT Environment for the Proventia A and Proventia G TOE components, non-bypassability supplied by the IT Environment for the Network Sensor TOE component, and non-bypassability supplied by the IT Environment for the SiteProtector TOE component. This rationale section was decomposed in this manner because there are different IT Environments that the Proventia A and Proventia G TOE components operate in, that the Network Sensor TOE components operate in, and that the SiteProtector TOE component operates in.

2.9.2.1.1 Proventia A and Proventia G TOE Components IT Environment

The host IT Environment for the Proventia A and Proventia G TOE components is composed of the Red Hat 8.0 operating system (OS), ISS device drivers, and the hardware appliances which provide the CPU, memory, hard disk, and network resources which the Proventia A and Proventia G TOE components execute on. Red Hat 8.0 provides an architecture which supports non-bypassability. Red Hat 8.0 provides identification and authentication functionality along with mediating all interfaces to include the networking interfaces that connect the hardware appliances to the monitored networks and the management network. By Red Hat 8.0 mediating access to the system and mediating the interfaces it provides the capability to help in making sure that the TSP enforcing interfaces of the Proventia A and Proventia G TOE components are used and are not bypassed.

Red Hat 8.0 ensures that the management interfaces and the monitoring interfaces of the TOE are used. Red Hat 8.0 ensures that the management interfaces of the Proventia A and Proventia G TOE components are used by providing for administratively configured encrypted links between the Proventia A and Proventia G management interfaces and the SiteProtector management interface.

Red Hat 8.0 further provides a network driver interface using the ISS device drivers supplied by the IT Environment which supports collection of packets from the monitored network. The network driver only provides for the capability to collect data from the monitored network. Further, the Red Hat 8.0 driver architecture allows for the Proventia A and Proventia G TOE components to interface with the network driver to read the network packets collected by the hardware appliance and Red Hat 8.0 which is the mechanism that ensures that the Proventia A and Proventia G monitoring interfaces read the network packets and is therefore not bypassed.

2.9.2.1.2 Network Sensor TOE Component IT Environment

The host IT Environment for the Network Sensor TOE component is either Red Hat 7.3 OS or Windows 2000 OS, ISS device driver support, and the hardware workstation which provides the CPU, memory, hard disk, and network resources which the Network Sensor TOE component executes on.

Red Hat 7.3 and Windows 2000 provide an architecture which supports non-bypassability. Red Hat 7.3 and Windows 2000 provide identification and authentication functionality along with mediating all interfaces to include the networking interfaces that connect the hardware appliances to the monitored networks and the management network. By Red Hat 7.3 and Windows 2000 mediating access to the system and mediating the interfaces it provides the capability to help in making sure that the TSP enforcing interfaces of the Network Sensor TOE component are used and are not bypassed.

Red Hat 7.3 and Windows 2000 ensure that the management interfaces and the monitoring interfaces of the Network Sensor are used. Red Hat 7.3 and Windows 2000 ensures that the management interfaces of the Network Sensor are used by providing for administratively configured encrypted links between the Network Sensor TOE component management interfaces and the SiteProtector management interface.

Red Hat 7.3 and Windows 2000 further provide an ISS network driver supplied by the IT Environment interface that supports the network driver to collect packets from the monitored network. The network driver only provides for the capability to collect data from the monitored network. Further, Red Hat 7.3 and Windows 2000 driver architecture allows for the Network Sensor TOE components to interface with the network driver to read the network packets collected by the hardware appliance and either Red Hat 7.3 or Windows 2000 which is the mechanism that ensures that the Network Sensor monitoring interfaces read the network packets and is therefore not bypassed.

2.9.2.1.3 SiteProtector TOE Component IT Environment

The host IT Environment for the SiteProtector TOE component is composed of the Windows 2000 Server OS, ISS device driver support, Microsoft SQL Server, and the hardware which provides the CPU, memory, hard disk, and network resources which SiteProtector executes on.

Windows 2000 Server provides an architecture which supports non-bypassability. Windows 2000 Server provides identification and authentication functionality along with mediating all interfaces to include the networking interfaces that connect the hardware platform to the management network. By Windows 2000 Server mediating access to the system and mediating the interfaces it provides the capability to help in making sure that the TSP enforcing interfaces of SiteProtector are used and are not bypassed.

Windows 2000 Server ensures that the management interface of SiteProtector is used. Windows 2000 Server ensures that the management interfaces of SiteProtector are used by providing for administratively configured encrypted links between the Proventia A, Proventia G, and Network Sensor TOE component management interfaces and the SiteProtector management interface. Further, Windows 2000 Server supports the non-bypassability of SiteProtector management interfaces by controlling access to the SiteProtector GUI interface and supporting the identification and authentication of users trying to access the management capabilities of SiteProtector and making sure that they are accesses only after success identification and authentication and that it is only done through the TSP enforcing GUI interface supplied to human users of SiteProtector.

The IT Environment supplies a database management system (DBMS) implementation which in this case is Microsoft SQL Server. The DBMS provides protected storage of TSF data and requires identification and authentication of users which helps in providing and supporting non-bypassability of SiteProtector.

2.9.2.2 Rationale for Domain Separation

The rationale for domain separation supplied by the IT Environment is broken into three different descriptions. The three different descriptions are domain separation supplied by the IT Environment for the Proventia A and Proventia G TOE components, domain separation supplied by the IT Environment for the Network Sensor TOE component, and domain separation supplied by the IT Environment for the SiteProtector TOE component. This rationale section was decomposed in this manner because there are different IT Environments that the Proventia A and Proventia G TOE components operate in, that the Network Sensor TOE component operates in, and that the SiteProtector TOE component operates in.

2.9.2.2.1 Proventia A and Proventia G TOE Components IT Environment

The host IT Environment for the Proventia A and Proventia G TOE components is composed of the Red Hat 8.0 OS, ISS device driver support, and the hardware appliances which provide the CPU, memory, hard disk, and network resources which the Proventia A and Proventia G TOE components execute on.

The Red Hat 8.0 OS provides for process isolation. This process isolation provided by Red Hat 8.0 provides for isolation of the Proventia A and Proventia G application while these applications are executing on the Red Hat 8.0 OS. The process isolation provided by Red Hat 8.0 to the Proventia A and Proventia G applications help in providing a separate execution domain for these TOE components. Red Hat 8.0 along with the memory provided by the hardware appliances provide the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for the Proventia A and Proventia G applications running on their respective hardware appliances. With the Red Hat 8.0 OS and the hardware appliances working together the IT Environment is supplying an execution domain for the Proventia A and Proventia G TOE components that helps protect these TOE components from interference and tampering.

2.9.2.2.2 Network Sensor TOE Component IT Environment

The host IT Environment for the Network Sensor TOE components is composed of either the Red Hat 7.3 OS or the Windows 2000 OS, network drivers, and the hardware which provides the CPU, memory, hard disk, and network resources which the Network Sensor TOE component executes on.

The Red Hat 7.3 OS or the Windows 2000 OS provides for process isolation. This process isolation provided by either Red Hat 7.3 OS or the Windows 2000 OS provides for isolation of the Network Sensor TOE component while it is executing on the host OS. The process isolation provided by either Red Hat 7.3 OS or the Windows 2000 OS to the Network Sensor TOE component helps in providing a separate execution domain for this TOE component. Red Hat 7.3 OS or the Windows 2000 OS along with the memory provided by the hardware the OS is loaded on provides the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for the Network Sensor TOE component. With the Red Hat 7.3 OS, Windows 2000 OS, and the hardware supplied by the workstation working together the IT Environment is supplying an execution domain for the Network Sensor TOE component that helps protect it from interference and tampering.

2.9.2.2.3 SiteProtector TOE Component IT Environment

The host IT Environment for the SiteProtector TOE component is composed of the Windows 2000 Server OS, network drivers, and the hardware which provides the CPU, memory, hard disk, and network resources which SiteProtector executes on.

Windows 2000 Server provides for process isolation. This process isolation provided by Windows 2000 Server provides for isolation of the SiteProtector TOE component while it is executing on the host OS. The process isolation provided by Windows 2000 Server to the SiteProtector TOE component helps in providing a separate execution domain for this TOE component. Windows 2000 Server along with the memory provided by the hardware the OS is loaded on provides the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for SiteProtector.

2.10 TOE Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia A Version 7.0-2003.167, Proventia G Version 8.0-2004.219 or Network Sensor Version 7.0 TOE component) and one instance of SiteProtector 2.0 Service Pack 4.

The following list itemizes configuration options for the TOE for the evaluated configuration along with TOE IT Environment resources and configuration used by the TOE when the TOE is in the evaluated configuration:

1. All Sensors are configured (by default) with the Response Field in Policy Files set to LOGDB and Display. All Sensors are configured (by default) with the options RSKill, Log Evidence, and View session disabled in the Response Field in the Policy Files.

2. Telnet server support in the Sensors is disabled by default. Incidents and Exceptions is disabled by selection of 'Show Uncategorized' in the Incidents/Exception pane because the evaluated configuration of the TOE does not support Incidents and Exceptions.

3. The evaluated configuration of SiteProtector does not have Internet access to the ISS website. An automatic retrieve is disabled. Therefore, SiteProtector will not periodically check the ISS website for new software updates and automatic retrieve and store the updates on the SiteProtector system.

4. Intrusion Prevention functionality provided by Proventia G Version 8.0-2004.219 is not included in the evaluated configuration.

5. SiteProtector components are resident on one workstation (a remote SiteProtector Console is not supported in the evaluated configuration).

6. SiteProtector components and the IT Environment supplied DBMS are resident on one workstation.

7. The IT Environment supplied Secure Sockets Layer (SSL) is used for the communication between Sensors and SiteProtector.

8. SSL or encrypted SQL is used for the communication between SiteProtector and the DBMS.

3 SECURITY ENVIRONMENT

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.

This document identifies assumptions as A.*assumption* with *assumption* specifying a unique name. Threats are identified as T.*threat* with *threat* specifying a unique name. Threats that apply to the IT environment are identified as T.E.*threat* with *threat* specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT 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.

3.1.1 IT Environment Assumptions

A.DBASE The IT environment's DBMS implementation will be properly configured, reliable, protected, and securely administered.

A.DEDICATE The TOE components will be installed on dedicated systems. A dedicated system is a computer system that contains no other software other than the TOE component(s), the ISS network driver support software and the required supporting third party software, as defined by the evaluated configuration.

A.I&A The operating systems of the computers the TOE is installed on require identification and authentication of users.

A.NETWORK The IT environment will provide a secure network dedicated to communication between SiteProtector and the Sensors.

3.1.2 Personnel Assumptions

A.INSTALL The authorised administrator will install the hardware, operating systems and software required for the TOE in a manner that maintains IT security with the proper network and configured according to ISS installation guides.

A.NOEVIL The authorised administrators of the TOE will not be careless, wilfully negligent, or hostile.

3.1.3 Physical Assumptions

A ENVIRON

The hardware running the TOE is located in an environment that provides controlled physical access. Only authorized personnel have physical access to the hardware running the TOE. Additionally, the environment provides reliable power and air conditioning controls to insure reliable operation of the hardware.

3.2 Threats

The following are threats addressed by the TOE and the IT Environment.

T.DELIVFAIL

An unauthorized user may attempt to access the TOE via any means (sensed, monitor network, secure management network or user, management user interface) and compromise the communication between components of the TOE (the secure management network) with the intent of causing an interruption to the operation of the TOE resulting in delivery failure of events or the loss of stored event data.

T.MALICE

A malicious agent may undertake activity on the system or network that the TOE is monitoring (the sensed, monitored network) attempting exploitation of information and/or unauthorized access to those systems or networks resulting in exploitation of information and/or unauthorized access.

T.UNAUTH

An unauthorized user may gain access to the TOE via any means (sensed, monitor network, secure management network or user, management user interface) with the intent of disclosing, removing or modifying TSF data or acquiring unauthorized access to TSF management functions resulting in disclosing, deleting, modifying TSF data or acquiring unauthorized access to TSF management functions.

T.TSF_COMPROMISE

A user or process may cause, through an unsophisticated attack, TSF data or executable code to be modified.

3.3 Organizational Security Policies

There are no security policies applicable to the TOE.

4 SECURITY OBJECTIVES

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.*objective* with *objective* specifying a unique name. Objectives that apply to the IT environment are designated as O.E.*objective* with *objective* specifying a unique name. Objectives that apply to the Non-IT environment are designated as O.N.*objective* with *objective* specifying a unique name.

4.1 Security Objectives for the TOE

O.ACCESS — The TOE only allows authorised users who have the appropriate user role assignment access to TOE functions and TSF data.

O.AUDIT — The TOE will generate an audit record upon detection of a potential security violation or detection of a malfunction in communication between the TOE components.

O.NETMON — The TOE will monitor network connectivity to the secure network and report any apparent network outages between TOE components.

O.MONITOR — The TOE Sensors will unobtrusively monitor all data that is sent across the sensed, monitored network segments and compare this data to optionally enabled signatures that indicated known attack patterns.

O.PSELF_PROTECT — The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

O.E.AUDIT — The IT Environment will generate audit records when the SiteProtector Sensor Controller, SiteProtector Event Collector, or SiteProtector Application Server components of the TOE are stopped or started.

O.E.DBASE The IT Environment will provide a properly configured, reliable, protected, and securely administered implementation of a Database Management System (DBMS).

O.E.DEDICATE The TOE components will be installed on dedicated systems. A dedicated system is a computer system that contains no other software other than the TOE component(s), the ISS network driver support software and the required supporting third party software, as defined by the evaluated configuration. General purpose computing is excluded.

O.E.ENFORCE The IT Environment ensures that all functions are invoked and succeed before the next function may proceed.

O.E.ENVIRON The TOE is located in an environment providing controlled physical access facilities and power and air conditioning controls for reliable operation of the hardware.

O.E.I&A The operating system of the computers on which the TOE components are installed will require identification and authentication of users to ensure only authorised users have access to the TOE and only allows authorised users who have the appropriate user role assignment access to TOE functions and TSF data.

O.E.ITACCESS The IT Environment only allows authorised users who have the appropriate user role assignment to assign new users roles, access the DBMS and to delete DBMS data.[1]

O.E.NETWORK The IT environment will provide a secure, trusted network for communication between the SiteProtector and the Sensors.

4.2.2 Security Objectives for the Non-IT Environment

O.N.INSTALL An authorised user will install and configure the hardware, operating systems and software required for the TOE and IT Environment in accordance with ISS installation guides.

O.N.NOEVIL The authorised users of the TOE will not be careless, wilfully negligent, or hostile.

[1] This covers modification also because having access to and ability to delete DBMS data allows for the modification of data.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2* and all National Information Assurance Partnership (NIAP) and international interpretations with the exception of the items listed below.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC.

Assignments: *indicated in italics*.

Selections: indicated in underlined text.

Assignments within selections*: indicated in italics and underlined text*.

Refinements: indicated in **bold text** with the addition of details and **~~bold text~~** when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g. FAU_SAR.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FAU_SAR.1.1(1)). This document continues the iteration numbering for Security Functional Requirements that apply to both the TOE and the IT Environment.

Explicitly stated SFRs are identified by having the explicitly stated requirements listed in the last section of the TOE and IT Environment security functional requirements sections in a section that are labelled as ‘Explicit Stated SFRs for the TOE’ or ‘Explicit Stated SFRs for the IT Environment’.

5.1 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 1 are described in more detail in the following subsections.

Table 1: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
Class FAU: Security Audit	

Functional Component ID	Functional Component Name
FAU_SAA.3	Simple Attack Heuristics
FAU_SAR.1	Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
Class FDP: User Data Protection	
FDP_ACC.1(1)	Subset Access Control
FDP_ACF.1(1)	Security Attributes Based Access Control
Class FMT: Security Management	
FMT_MOF.1	Management of Security Functions Behavior
FMT_MTD.1	Management of TSF Data
FMT_SMF.1(1)	Specification of Management Functions
FMT_SMR.1(1)	Security Roles
Explicitly Stated SFRs for the TOE	
FAU_GEN_EXP.1	Audit Data Generation - Explicit
FPT_RVM_SFT_EXP.1	Non-Bypassability of the TSP for Software TOEs - Explicit
FPT_SEP_SFT_EXP.1	TSF Domain Separation for Software TOEs - Explicit

5.1.1 Class FAU: Security Audit

5.1.1.1 Security audit analysis (FAU_SAA)

5.1.1.1.1 FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events *denial of service, unauthorized access attempts, pre-attack probes* that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of *incoming network packets*.

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies

5.1.1.2 Security audit review (FAU_SAR)

5.1.1.2.1 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide *an authorized user* with the capability to read *event type, date, time, source and destination IP address, sensor host IP address* 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

5.1.1.2.2 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on *attacker, time and date, Event name, Sensor that generated the event, Target Object and Target*.

Dependencies: FAU_SAR.1 Audit review

5.1.1.3 Security audit event selection (FAU_SEL)

5.1.1.3.1 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type

b) no additional attributes.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

5.1.2 Class FDP: User Data Protection

5.1.2.1 Access control policy (FDP_ACC)

5.1.2.1.1 FDP_ACC.1(1) Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1(1) The TSF shall enforce the *Access Control SFP* on *the subjects, objects and operations among subjects and objects listed below*.

Table 2: FDP_ACC.1(1) Detail

Subject	*Object*	*Operation among Subject and Object covered by the SFP*
User	*Policy Files*	*Apply, view, modify*
	Audit Data	*View, sort, search*

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.2.2 Access control functions (FDP_ACF)

5.1.2.2.1 FDP_ACF.1(1) Security Attribute Based Access Control

Hierarchical to: No other components.

FDP_ACF.1.1(1) The TSF shall enforce the *Access Control SFP* to objects based on the following: *objects, subject, subject security attributes identified below*.

Table 3: FDP_ACF.1.1(1) Detail

Subject	*Subject Security Attribute*	*Object*	*Access Control SFP Rules*
User	*User Role*	*Policy Files*	*1. Any User with a User Role of Operator, Analyst or Administrator may view Policy Files.* *2. Any User with a User Role of Analyst or Administrator may modify and apply a Policy Files to a Sensor.*
		Audit Data	*3. Any User with a User Role of Operator, Analyst or Administrator may view, search and sort Audit Data.*

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules identified in Rule column in above table.*

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the *no additional rules*.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

5.1.3 Class FMT: Security Management

5.1.3.1 Management of functions in TSF (FMT_MOF)

5.1.3.1.1 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 the functions *sensing and collecting audit records* to *Users who have been assigned an Analyst or Administrative User Role*.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.2 Management of TSF data (FMT_MTD)

5.1.3.2.1 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to modify the *Sensor Policy Files which define the enabled or disabled signatures* to *users with assigned Administrator or Analyst User Role.*

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.3.3 Specification of management functions (FMT_SMF)

5.1.3.3.1 FMT_SMF.1(1) Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions:

1. *Start Sensors,*
2. *Stop Sensors,*
3. *Start SiteProtector Event Collector,*
4. *Stop SiteProtector Event Collector,*
5. *apply Policy Files, and*
6. *modification of TSF Data.*

Dependencies: No Dependencies

5.1.3.4 Security management roles (FMT_SMR)

5.1.3.4.1 FMT_SMR.1(1) Security roles

Hierarchical to: No other components.

FMT_SMR.1.1(1) The TSF shall maintain the roles *Operator, Analyst, Administrator.*

.

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.4 Explicitly Stated SFRs for the TOE

5.1.4.1 FAU_GEN_EXP.1 Audit data generation - Explicit

Hierarchical to: No other components.

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

a) imminent security violation

b) enabling (starting) or disabling (stopping) of a Sensor (sensing functionality) and SiteProtector Event Collector (audit record collection functionality) for FMT_MOF.1 and FMT_SMF.1

c) applying a Policy File for FDP_ACC.1(1) and FDP_ACF.1(1)

d) network outages.

FAU_GEN_EXP.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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no other information*.

Dependencies: FPT_STM.1 Reliable time stamps

5.1.4.2 FPT_RVM_SFT_EXP.1 Non-Bypassability of the TSP for Software TOEs - Explicit

Hierarchical to: No other components.

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

Dependencies: None

5.1.4.3 FPT_SEP_SFT_EXP.1 TSF Domain Separation for Software TOEs - Explicit

Hierarchical to: No other components.

FPT_SEP_SFT_EXP.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by un-trusted subjects in the TSC.

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

Dependencies: None

5.2 Security Functional Requirements for the IT Environment

This section describes the security functional requirements for the IT environment. The security functional requirements are identified in Table 4 and are described in more detail in the following subsections.

Table 4: IT Environment Security Functional Requirements

Security Functional Requirement Component	IT Environment Security Functional Requirement Component Name
Class FAU: Security Audit	
FAU_STG.1	Protected Audit Trail Storage
Class FDP: User Data Protection	
FDP_ACC.1(2)	Subset Access Control
FDP_ACF.1(2)	Security Attributes Based Access Control
Class FIA: Identification and authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_SMF.1(2)	Specification of Management Functions
FMT_SMR.1(2)	Security Roles
Class FPT: Protection of the TSF	
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable Time Stamps
Explicitly Stated SFRs for the IT Environment	
FAU_GEN.1-NIAP-0347	Audit data generation
FPT_RVM_OS_DBMS_EXP.1	Non-Bypassability of the TSP of the TSP for the OSs and DBMS - Explicit
FPT_SEP_OS_EXP.1	TSF Domain Separation for the OSs - Explicit

5.2.1 Class FAU: Security Audit

5.2.1.1 Security audit event storage (FAU_STG)

5.2.1.1.1 FAU_STG.1

Hierarchical to: No other components.

FAU_STG.1.1 The **IT Environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The **IT Environment** shall be able to prevent unauthorised modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation

Rationale for refinement: The refinement of “IT Environment” was done because this is a requirement on the IT Environment of the TOE.

5.2.2 Class FDP: User Data Protection

5.2.2.1 Access control policy (FDP_ACC)

5.2.2.1.1 FDP_ACC.1(2) Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1(2) The **IT Environment** shall enforce the *IT Environment Access Control SFP* on *the subjects, objects and operations among subjects and objects listed below*.

Table 5: FTP_ACC.1(2) Detail

Subject	*Object*	*Operation among Subject and Object covered by the SFP*
User	*User Role*	*Assign*
User	*SiteProtector Database data*	*View, modify and delete*

Dependencies: FDP_ACF.1 Security attribute based access control

Rationale for refinement: The refinement of “IT Environment” was done because this is a requirement on the IT Environment of the TOE.

5.2.2.2 Access control functions (FDP_ACF)

5.2.2.2.1 FDP_ACF.1(2) Security Attribute Based Access Control

Hierarchical to: No other components.

FDP_ACF.1.1(2) The **IT Environment** shall enforce the *IT Environment Access Control SFP* to objects based on the following: *objects, subject, subject security attributes identified below*.

Table 6: FDP_ACF.1.1(2) Detail

Subject	*Subject Security Attribute*	*Object*	*Access Control SFP Rules*
User	*User Role*	*User Role*	*1. Only Users defined by the IT Environment as an Administrator may assign users the SiteProtector supported User Role of Operator, Analyst or Administrator.*
User	*User Role*	*SiteProtector Database data*	*1. Only Users logged into the IT Environment as an Administrator may view, modify, and delete data stored in the SiteProtector Database accessing the data using the SiteProtector Host's external human user interface.*

FDP_ACF.1.2(2) The **IT Environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules identified in Rule column in above table.*

FDP_ACF.1.3(2) The **IT Environment** shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules*.

FDP_ACF.1.4(2) The **IT Environment** shall explicitly deny access of subjects to objects based on the *no additional rules*.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3 Class FIA: Identification and Authentication

5.2.3.1 User authentication (FIA_UAU)

5.2.3.1.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1.

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

Dependencies: FIA_UID.1 Timing of identification

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3.1.2 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1.

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

Dependencies: No dependencies

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3.2 Management of security attributes (FMT_MSA)

5.2.3.2.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The **IT Environment** shall enforce the *IT Environment Access Control SFP* to restrict the ability to *assign* the security attributes *User Role* to *IT Environment users with administrator privileges.*

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3.2.2 FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The **IT Environment** shall enforce the *IT Environment Access Control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The **IT Environment** shall allow the *no users* 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 for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3.3 Specification of management functions (FMT_SMF)

5.2.3.3.1 FMT_SMF.1(2) Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1(2) The **IT Environment** shall be capable of performing the following security management functions:

1. *Assign a user to a role,*
2. *Modify user role.*[2]

Dependencies: No Dependencies

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.3.4 Security management roles (FMT_SMR)

5.2.3.4.1 FMT_SMR.1(2) Security roles

Hierarchical to: No other components.

FMT_SMR.1.1(2) The **IT Environment** shall maintain the roles *Operator, Analyst, Administrator.*

.

FMT_SMR.1.2(2) The **IT Environment** shall be able to associate users with roles.

[2] **Modifying a user role covers deleting a user from a role.**

Dependencies: FIA_UID.1 Timing of identification

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.4 Class FPT: Protection of the TSF

5.2.4.1 Internal TOE TSF Data Transfer (FPT_ITT)

5.2.4.1.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1 The **IT Environment** shall protect TSF data from <u>disclosure</u> **and** <u>modification</u> when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

Rationale for refinement: The word "and" was added to make the requirement read better.

5.2.4.2 Time Stamps (FPT_STM)

5.2.4.2.1 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.

Dependencies: No dependencies

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.5 Explicitly Stated SFRs for the IT Environment

5.2.6 Class FAU: Security Audit

5.2.6.1 FAU_GEN.1-NIAP-0347 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1-NIAP-0347 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 <u>not specified</u> level of audit; and
c) *Those auditable events identified in the Table 5*

FAU_GEN.1.2-NIAP-0347 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 (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no other information*

Dependencies: FPT_STM.1 Reliable time stamps

Table 7 Auditable Events

Audit Event	Description
Start SiteProtector Sensor Controller	The IT Environment will generate an audit record indicating that the SiteProtector Sensor Controller of the TOE has been started.
Stop SiteProtector Sensor Controller	The IT Environment will generate an audit record indicating that the SiteProtector Sensor Controller of the TOE has been stopped.
Start SiteProtector Event Collector	The IT Environment will generate an audit record indicating that the SiteProtector Event Collector component of the TOE has been started.
Stop SiteProtector Event Collector	The IT Environment will generate an audit record indicating that the SiteProtector Event Collector component of the TOE has been stopped.
Start SiteProtector Application Server	The IT Environment will generate an audit record indicating that the SiteProtector Application Server TOE component has been started.
Stop SiteProtector Application Server	The IT Environment will generate an audit record indicating that the SiteProtector Application Server TOE component has been stopped.
Failed logon	The IT Environment will generate an audit record when a user failed to logon.

Successful login to a defined role	The IT Environment will generate an audit record when a user successfully logs into one of the roles of Administrator, Analyst, or Operator.
Assigning a user to a role	The IT Environment will generate an audit record when an Administrator assigns a user to any of the roles of Administrator, Analyst, or Operator.
Modification of a user role	The IT Environment will generate an audit record when an Administrator modifies a user role when the modifications involve the Administrator, Analyst, or Operator roles.

Rationale for refinement: The refinement of "IT Environment" was done because this is a requirement on the IT Environment of the TOE.

5.2.7 Class FPT: Protection of the TSF

5.2.7.1 FPT_RVM_OS_DBMS_EXP.1 Non-Bypassability of the TSP for the OSs and DBMS - Explicit

5.2.7.1.1 FPT_RVM_OS_DBMS_EXP.1 Non-Bypassability of the TSP for the OSs and DBMS

Hierarchical to: No other components.

FPT_RVM_OS_DBMS_EXP.1.1 The security functions of the host OSs and the DBMS shall ensure that the host OS and DBMS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OSs or DBMS is allowed to proceed.

Dependencies: No dependencies

5.2.7.2 FPT_SEP_OS_EXP.1 TSF Domain Separation for the OSs - Explicit

5.2.7.2.1 FPT_SEP_OS_EXP.1 TSF Domain Separation for the OSs

Hierarchical to: No other components.

FPT_SEP_OS_EXP.1.1 The security functions of the host OSs shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OSs .

FPT_SEP_OS_EXP.1.2 The security functions of the host OSs shall enforce separation between the security domains of subjects in the scope of control of the host OSs.

Dependencies: No dependencies

5.3 TOE Security Assurance Requirements

Table 7 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2. The SARs are not iterated or refined from Part 3.

Table 8: Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ADV_HLD.1 AGD_ADM.1, AGD_USR.1

5.4 SFRs With SOF Declarations

The overall SOF for this ST is SOF-basic.

None of the TOE functional requirements in this ST deal with computational and permutational mechanisms and therefore none of the functional requirements have their own SOF claim.

6 TOE SUMMARY SPECIFICATION

This chapter identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

6.1 TOE Security Functions

The security functions implemented by the TOE are:

6.1.1 Detection Security Function

The TOE Sensors provide Detection Security Functionality by continuously monitoring network traffic (Network Detection) and monitoring the TOE components (System Detection).

The TOE provides a Detection Security Function in two ways: 1) by monitoring incoming network traffic and reporting potential security violations (Network Detection) and 2) by monitoring the TOE and access to the TOE and detecting abnormal behaviour (System Detection). The TOE's Detection Security Function is described below.

6.1.1.1 Network Detection

Sensors monitor network packets and look for patterns in the traffic that indicate an attack against the system the Sensor is monitoring. Incoming packets are compared against signatures defined in the Sensor's resident Policy File. The Sensors are shipped with a default Policy File that includes pre-defined signatures that detect denial of service, unauthorized access attempts, pre-attack probes, and suspicious activity. The Sensors achieves this function by reading and processing frames that are read from the host IT Environment that the Sensor software executes on. The Sensors invoke an interface to the IT Environment to read the next available network frame that was captured by the IT Environment hosting the Sensor. After the Sensor reads the next network frame the Sensor processes the network frame using the Protocol Analysis Module (PAM). Processing by PAM detects the patterns that are indicative of security violations based on the signature definitions in the resident Policy File on the Sensor. Additionally, users may customize Policy Files by disabling/enabling signatures through an Apply Policy graphical user interface (GUI) by using SiteProtector. The Apply Policy GUI allows for a human user to apply a policy file to a Sensor which affects the security violation patterns that the Sensors will recognize in network frames collected from the monitored network. Human users through SiteProtector are able to selectively enable or disable signatures that are used to help recognize network active as being a security violation.

6.1.1.2 System Detection

The SiteProtector components SiteProtector Sensor Controller and SiteProtector Event Controller monitor communication links between themselves and the Sensors to carry out system detection. System detection monitoring is the reporting of network communication link problems that may occur between the SiteProtector components Sensor Controller and

Event Collector and the Sensors. The SiteProtector components use an IT Environment supplied timer that triggers the SiteProtector components to check for communication path problems between themselves and the Sensors. This is carried out by SiteProtector components periodically querying the Sensors and determining if communication exists between the SiteProtector components and the queried Sensors. The timer is started when SiteProtector has been started. During the operation of SiteProtector and Sensors if there are any communication link problems between the Sensor Controller or Event Controller SiteProtector components and the Sensors an audit record is generated by the SiteProtector component.

Functional requirements for Detection Security Function: FAU_SAA.3, FAU_GEN_EXP.1, FAU_SEL.1

6.1.2 Audit Security Function

The TOE’s Audit Security Functionality provides Event auditing, alert auditing, selective auditing, and selective audit viewing.

The TOE’s Audit Security Function provides the following functionality that is described in the following sections.

6.1.2.1 Network Detection Event Generation

A Sensor detects security violations when incoming packets are matched against a signature defined in a Sensor’s Policy File. Upon detection of a signature match, the Sensor creates an Event (audit record). Data included in the Event is event name, date, source and destination IP address and the IP address of the Sensor that monitored the Event. The Sensors detect security violations by processing and analyzing network frames that it reads from the IT Environment through the protocol analysis module (PAM) which is part of the Sensor. PAM identifies security violations based on the Sensor’s Policy File and will trigger an audit record generation that will create an audit record based on a network frame match against a policy file signature.

6.1.2.2 System Detection Event Generation

The SiteProtector components Sensor Controller and Event Collector generate Events in order to notify a User of abnormal system behaviour (System Detection). Abnormal system behaviour includes detection of loss of network connectivity with a Sensor. The SiteProtector components Sensor Controller and Event Controller detect the loss of network connectivity with a Sensor by querying Sensors on a periodic basis. When the SiteProtector components Sensor Controller and Event Collector query the Sensors and determine if communication can not be established with the Sensors then this causes the generation of an audit record that specifically indicates that communications with a Sensor does not exist and is therefore offline.

6.1.2.3 Management Function Event Generation

Management functions generate events that report the completion of management events, specifically starting and stopping sensors and applying sensor policy files that are initiated through SiteProtector. The SiteProtector Sensor Controller gets the status information resulting from starting a Sensor, stopping a Sensor, and applying sensor policy files. The SiteProtector Sensor Controller gets the completion information, a generated event; from a Sensor and stores the event in the IT environment supplied DBMS. This completion message is then available for the human user using SiteProtector to see that the management function had completed.

6.1.2.4 Selective Auditing

The Sensors and SiteProtector support selective auditing by allowing a User to disable or enable signatures defined in a Sensor's Policy File. The User disables or enables signatures through the SiteProtector Console. The SiteProtector Console uses the SiteProtector Application Server to store the Sensor Policy File in the IT environment supplied DBMS which the SiteProtector Sensor Controller will use to update a Sensor's Policy File that is resident on the Sensor. A human user uses the Apply Policy GUI available thru SiteProector to apply the selected signatures that the user chooses. The selection of signatures (enabling and disabling of signatures) helps implement selective auditing by allowing the user to define what security violations that the Sensor will detect through the use of the PAM module. When a user selects a set of signatures, enables a set of signatures, and applies the policy file that has the enabled signatures to a Sensor this action selects the security violations that the Sensor will trigger on and there by affecting the audit records that will be generated by the Sensor. Through the selection of signatures in the policy file the user has selected for a Sensor the types of audit records the Sensor will generate based on the enabled signatures in the Sensor's Policy File.

6.1.2.5 Audit Data Viewing

Data included in Events is Event name, date, source and destination IP address and the IP address of the Sensor that monitored the Event. Audit data viewing is accomplished using the SiteProtector Console. The SiteProtector Console uses the SiteProtector Application Server to retrieve the audit data from the IT environment supplied DBMS. The audit data is stored in the IT environment supplied DBMS through the use of the SiteProtector Event Collector. The SiteProtector Event Collector collects audit data from sensors and stores the collected audit data in the IT environment supplied DBMS making it available for viewing by the SiteProtector Console. The SiteProtector component of the TOE provides a graphical user interface (GUI) that allows the human user to view the audit data. The viewing of the audit data is provided through the GUI interface by a panel display that is implemented in a table format that is structured into rows and columns. Each row of the display is an audit record and the columns are the attributes of the audit record. The columns of the panel display provide the Event name, date, source and destination IP address and the IP address of the Sensor that monitored the generated event.

6.1.2.6 Selective Audit Data Viewing

A user may search and sort the Event data, by Event name, source and destination IP address and the IP address of the Sensor that monitored the Event. The User may sort audit data after the SiteProtector Console has retrieved audit data from the IT environment supplied DBMS using the SiteProtector Application Server. Once the SiteProtector Console has pulled audit data from the IT environment supplied DBMS, the audit data is stored by the SiteProtector Console allowing the Console to carry out sorting of the audit data based on a users action on how and what field the user wants to sort on. The SiteProtector component of the TOE implements this functionality by providing the human user a graphical user interface (GUI) that provides the user a list box feature and a panel display that is structured into rows and columns. The list box feature allows the user to selectively choose different types of Event Analysis views. The different types of Event Analysis views when selected will selectively show different information in the panel display that displays one audit record per row and different audit attributes in the columns of the panel. The columns of the panel show different audit attributes based on the selection by the user with respect to the Event Analysis view. Once a user has selected an Event Analysis view they can click on the individual columns in the panel to sort the displayed events, audit records, in different orders based on the column and the audit attribute the column is describing. Since SiteProtector is able to search the IT Environment DBMS for specific audit records and display the audit records in a GUI that allows for the sorting of the records in varying ways allows SiteProtector to provide the functionality to a human user to selectively search and sort the audit records.

Functional requirements for Audit Security Function: FAU_SAA.3, FAU_SAR.1,
FAU_SAR.3, FAU_SEL.1, FAU_GEN_EXP.1

6.1.3 Protect Security Function

The TOE Protect Security Functionality provides functions that help in the protection of TSF Data and TOE functions and self protection of the TOE by implementing roles and requiring user identification along with providing domain separation and non-bypassability for those functions within the TOE's scope of control.

The TOE provides a Protect Security Function that protects the TOE, TSF Data and the invocation of TOE functions. The TOE's Protect Security Function provides the following functionality:

6.1.3.1 Access Control

SiteProtector enforces access control over resources available to human users of SiteProtector. SiteProtector enforces rules for operations of subjects on objects based on the security attributes of the subjects. The security attributes of the subjects used by SiteProtector is the role of the user.

SiteProtector supports three roles: Operator, Analyst and Administrators. The user roles are initially setup during the installation of SiteProtector. The IT Environment Administrator is responsible for assigning users the SiteProtector supported user roles. User roles determine if the user may view audit data and modify policy files. Further, user roles determine if the user may start a sensor, stop a sensor, start a SiteProtector Event Collector, stop a SiteProtector Event Collector, apply Policy Files, and modify the signatures (enable or disable) contained within a Policy File.

A human user is required to identify and authenticate when they use SiteProtector. SiteProtector uses the user name and password credentials supplied by the user to setup the SiteProtector environment so that the user only has access to those features of SiteProtector and the Sensors that the user role supports. SiteProtector carries out giving a user the proper authorizations in several steps. SiteProtector first interacts with the host operating system (OS) to identify and authenticate a user into a specific role of Operator, Analyst or Administrator. The user name and password are OS maintained credentials. The OS performs the identification and authentication of the user and passes the result of either successfully logging in or not successfully logging in to SiteProtector. A user must successfully login to gain access to the SiteProtector functionality. A user that has successfully logged into SiteProtector will have a SiteProtector environment established based on the role of the user. Based on the role of the user, SiteProtector will give the user access to different graphical user interfaces (GUIs). Giving access to different GUIs of SiteProtector based on the role of the user, controls the access a user has to the management and monitoring capabilities of SiteProtector and the sensors.

6.1.3.2 Self Protection

There are non-bypassability and domain separation requirements on the TOE and the IT Environment. The descriptions that follow will first discuss the non-bypassability and domain separation requirements for the TOE and then will discuss the role that the IT Environment plays in non-bypassability and domain separation.

6.1.3.2.1 Non-bypassability and Domain Separation for the TOE

The TOE provides for non-bypassability of functions within the TOE’s scope of control (TSC) and domain separation. The first part of this section discusses the Proventia A, Proventia G, and Network Sensor 7.0 TOE components, and the second part discusses the SiteProtector TOE component.

A) Proventia A, Proventia G, Network Sensor 7.0 TOE Components

This section describes the non-bypassabiltiy and domain separation for the Proventia A, Proventia G, and Network Sensor 7.0 TOE components.

Non-Bypassability

The Proventia A, Proventia G, and Network Sensor 7.0 TOE components play a role in non-bypassability by providing two well defined and restricted interfaces. The interfaces include one to the host IT Environment that collects network frames from the monitored network and one restricted management interface to SiteProtector. The monitoring interface collects network frames from the host IT Environment and immediately applies the TSP enforcement functions that analyze and processes the frames looking for security violations as specified in the sensors policy files. The Proventia A, Proventia G, and Network Sensor 7.0 monitoring interfaces do not provide any other functionality. In addition, the Proventia A, Proventia G, and Network Sensor 7.0 TOE components do not provide any other programmatic interfaces or functions and do not accept commands from users on the monitored network.

The Proventia A, Proventia G, and Network Sensor 7.0 management interface is a well defined interface that controls all communications received from SiteProtector. The management interface ensures that security enforcing functions succeed before allowing any type of management activities with the Proventia A, Proventia G, or Network Sensor 7.0 to proceed..

Domain Separation

The Proventia A, Proventia G, and Network Sensor 7.0 TOE components maintain a security domain by having well defined monitoring and management interfaces and only allowing a strictly controlled set of functions to be carried out through these interfaces. The monitoring interface only allows for the collection of network packets. No other functionality is provided by this interface. The management interface only allows authorized subjects to connect and communicate with the Proventia A, Proventia G, and Network Sensor 7.0 TOE components. The strictly controlled functionality provided by the interfaces allows the Proventia A, Proventia G, and Network Sensor 7.0 TOE components to have a security domain that protects from interference and tampering.

B) SiteProtector TOE Component

This section describes the non-bypassabiltiy and domain separation for the SiteProtector TOE component.

Non-Bypassability

SiteProtector plays a role in non-bypassability by providing well defined and restricted interfaces to human users, Proventia A, Proventia G, and Network Sensor 7.0 TOE sensor components and to the Windows 2000 Server host IT Environment.

The SiteProtector graphical user interfaces (GUI) provide strictly controlled functionality to the users within the TSC. By limiting the functionality, the TSF is protected from corruption or compromise from users within the TSC. SiteProtector interfaces are separated into two categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). Human users must identify and authenticate themselves through the Windows 2000 Server host IT Environment before being allowed to use the features of SiteProtector. Identification and authentication

(I&A) of the user with the Windows 2000 Server IT Environment establishes the user as an authorized user of StieProtector and is necessary before they may carry out any other action within the TSC.

The SiteProtector network and application interfaces are used to collect data from the sensors and the Windows 2000 Server and Microsoft SQL Server IT Environment and to communicate commands to the Proventia A, Proventia G, and Network Sensor 7.0 TOE sensor components and the Windows 2000 Server and Microsoft SQL Server IT Environment. The network and application interfaces are established to communicate only with the Proventia A, Proventia G, and Network Sensor 7.0 TOE sensor components and the Windows 2000 Server and Microsoft SQL Server host IT Environment. Whenever the SiteProtector network or application communication interfaces are used, they invoke the TSP enforcement functions before any other action that is to be carried out by the SiteProtector is allowed to proceed.

Domain Separation

SiteProtector maintains a security domain by having well defined interfaces (GUI, network and application communication), only allowing a strictly controlled set of functionality to be carried out through these interfaces, and not offering any general purpose computing or programming capabilities. The strictly controlled functionality provided by the interfaces allows SiteProtector to have a security domain that is protected from interference and tampering.

6.1.3.2.2 Role of IT Environment in Non-Bypassability and Domain Separation

This section describes the non-bypassability and domain separation offered by the IT Environment. The section is divided into three parts, Proventia A and Proventia G TOE components, the Network Sensor 7.0 component, and the SiteProtect TOE component. The breakdown of the different TOE components is necessary as the components operate in different IT Environments. Proventia A and Proventia G operate in a Red Hat 8.0 environment, Network Sensor 7.0 operates in a Windows 2000 or Red Hat 7.3 environment, and SiteProtector operates in a Windows 2000 server environment.

A) Proventia A, Proventia G TOE Components IT Environment

The host IT Environment for the Proventia A and Proventia G TOE components is composed of the Red Hat 8.0 operating system (OS), ISS device drivers, and the hardware appliances which provide the CPU, memory, hard disk, and network resources on which the components execute. This section describes the non-bypassabiltiy and domain separation for the Proventia A and Proventia G TOE components provided by the IT Environment.

Non-Bypassability

Red Hat 8.0 provides an architecture which supports non-bypassability. Red Hat 8.0 provides identification and authentication functionality along with mediating all interfaces including the networking interfaces that connect the hardware appliances to the monitored network and the management network. A network driver interface uses the ISS device drivers supplied by the IT Environment to support the collection of packets from the monitored network. The network driver only provides the capability to collect data from the monitored network. Red Hat 8.0 also ensures that the management interfaces of the TOE components are used. This is accomplished by providing for administratively configured encrypted links between the Proventia A and Proventia G management interfaces and the SiteProtector management interface. By mediating the access to the system and interfaces, Red Hat 8.0 provides the capability to help ensure the TSP enforcing interfaces of the Proventia A and Proventia G TOE components are used and not bypassed.

Domain Separation

The Red Hat 8.0 OS provides process isolation. The process isolation provided by Red Hat 8.0 to the Proventia A and Proventia G applications helps provide a separate execution domain for these TOE components. Red Hat 8.0 along with the memory provided by the hardware appliances provides the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for the Proventia A and Proventia G applications running on their respective hardware appliances. With the Red Hat 8.0 OS and the hardware appliances working together, the IT Environment is supplying an execution domain for the Proventia A and Proventia G TOE components that helps protect these TOE components from interference and tampering.

B) Network Sensor TOE Component IT Environment

The host IT Environment for the Network Sensor TOE component is composed of either the Red Hat 7.3 OS or the Windows 2000 OS, network drivers, and the hardware which provides the CPU, memory, and network resources on which the components execute. This section describes the non-bypassabiltiy and domain separation for the Network Sensor TOE component provided by the IT Environment.

Non-Bypassability

Red Hat 7.3 and Windows 2000 provide architectures which support non-bypassability. Both operating systems provide identification and authentication functionality along with mediating all interfaces to include the networking interfaces that connect the component hardware to the monitored network and the management network. A network driver interface uses the ISS device drivers supplied by the IT Environment to support the collection of packets from the monitored network. The network driver only provides the capability to collect data from the monitored network. Red Hat 7.3 and Windows 2000 also ensure that the management interfaces are of the TOE components are used. This is accomplished by providing for administratively configured encrypted links between the Network Sensor's management interfaces and the SiteProtector management interface. By mediating the access to the system and interfaces, the operating systems provide the capability to help ensure the TSP enforcing interfaces of the Network Sensor TOE component are used and not bypassed.

Domain Separation

The Red Hat 7.3 OS and the Windows 2000 OS provide process isolation. The process isolation provided by either Red Hat 7.3 OS or the Windows 2000 OS isolates the Network Sensor TOE component while it is executing on the host OS. This helps provide a separate execution domain for the Network Sensor. Red Hat 7.3 OS or the Windows 2000 OS along with the memory provided by the hardware the OS is loaded on provides the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for the Network Sensor TOE component. With either Red Hat 7.3 or Windows 2000, and the hardware supplied by the workstation working together the IT Environment is supplying an execution domain for the Network Sensor TOE component that helps protect it from interference and tampering.

C) SiteProtector TOE Component IT Environment

The host IT Environment for the SiteProtector TOE component is composed of the Windows 2000 Server OS, ISS device drivers, Microsoft SQL Server, and the hardware which provides the CPU, memory, hard disk, and network resources which SiteProtector executes on. This section describes the non-bypassabiltiy and domain separation for the SiteProtector TOE component provided by the IT Environment.

Non-Bypassability

Windows 2000 Server provides an architecture which supports non-bypassability. Windows 2000 Server provides identification and authentication functionality along with mediating all interfaces to include the networking interfaces that connect the hardware platform to the management network.

Windows 2000 Server ensures that the management interface of SiteProtector is used by providing for administratively configured encrypted links between the Proventia A, Proventia G, and Network Sensor TOE component management interfaces and the SiteProtector management interface. Further, Windows 2000 Server supports the non-bypassability of SiteProtector management interfaces by controlling access to the SiteProtector GUI. Access to the management capabilities is only permitted after successful identification and authentication through the TSP enforcing GUI supplied to human users of SiteProtector.

The IT Environment supplies a database management system (DBMS) implementation which in this case is Microsoft SQL Server. The DBMS provides protected storage of TSF data and requires identification and authentication of users which helps in providing and supporting non-bypassability of SiteProtector.

By mediating access to the system and mediating the interfaces Windows 2000 Server provides the capability to help make sure that the TSP enforcing interfaces of SiteProtector are used and are not bypassed.

Domain Separation

Windows 2000 Server provides for process isolation. This process isolation provided by Windows 2000 Server isolates the SiteProtector TOE component while it is executing on the host OS. This helps provide a separate execution domain for this TOE component. Windows 2000 Server along with the memory provided by the hardware the OS is loaded on provides the virtual memory capabilities and the separation of memory regions of running processes which further helps in supplying a separate execution domain for SiteProtector.

Functional requirements: FDP_ACC.1(1), FDP_ACF.1(1), FMT_MOF.1, FMT_MTD.1, FMT_SMR.1(1), FPT_RVM_SFT_EXP.1, FPT_SEP_SFT_EXP.1

6.1.4 Management Security Function

The SiteProtector and Sensor's management security functions provide interfaces that enable a human user to manage and monitor the Sensors. This functionality includes starting and stopping the sensing capability of the Sensors and SiteProtector by starting and stopping the Sensors and/or the Event Collector and applying Sensor Policy Files which define the enabled and disabled signatures for a Sensor. The management interface is the SiteProtector Console. The SiteProtector Console allows a user to manage and monitor Sensors by communicating with the SiteProtector Application server which communicates with the IT environment supplied DBMS. The IT environment DBMS is the storage resource for storing management commands and storing status information of the Sensors. The SiteProtector Sensor Controller supports the management and monitoring of the Sensors by taking management commands that are stored in the IT environment supplied DBMS and applying them to a Sensor and returning status information from a Sensor to the IT environment supplied DBMS. The SiteProtector Application Server then sends the information to the SiteProtector Console for display. SitProtector restricts the use of the management security functions by the use of roles and requiring the user to successfully identify and authenticate to the host IT Environment before allowing the access to the management security functions that the role the user operates in supports. The user roles are initially setup during the installation of SiteProtector. The host IT Environment Administrator is responsible for assigning users the SiteProtector supported User Roles. For a user to access any of the management security functions they must be in the Analyst or Administrator role and have successfully identified and authenticated themselves to the host IT Environment into one of the roles of Analyst or Administrator that SiteProtector supports.

Functional requirements: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1(1)

6.2 Assurance Measures

The TOE satisfies CC EAL2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by ISS to satisfy the CC EAL2 assurance requirements.

Table 9: Assurance Measures

Assurance Component	How requirement will be met
ACM_CAP.2 Configuration items	ISS performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE. The configuration items are uniquely identified and each release of the TOE has a unique reference.
ADO_DEL.1 Delivery procedures	ISS documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the ISS website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ADO_IGS.1 Installation, generation and startup procedures	ISS documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ADV_FSP.1 Informal functional specification	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by ISS development evidence.
ADV_HLD.1 Descriptive high-level design	The subsystems and the communication between the subsystems of the TOE are documented in ISS development evidence.
ADV_RCR.1 Informal correspondence demonstration	The correspondence is contained in the documents used for ADV_FSP.1 and ADV_HLD.1.
AGD_ADM.1 Administrator Guidance	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.

Assurance Component	How requirement will be met
AGD_USR.1 User guidance	User guidance is provided for those roles defined in the TOE that do not have all the authorizations as the administrative role.
ATE_COV.1 Evidence of coverage	ISS demonstrates the interfaces tested during functional testing using a coverage analysis.
ATE_FUN.1 Functional testing	ISS functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2 Independent testing - sample	ISS will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_SOF.1 Strength of TOE security function evaluation	ISS documented the strength of functions in the vulnerability analysis documentation.
AVA_VLA.1 Developer vulnerability analysis	ISS carried out a vulnerability analysis search for obvious flaws and weaknesses in the TOE.

7 PROTECTION PROFILE CLAIMS

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 claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

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

7.4 Protection Profile Rationale

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

8 RATIONALE

8.1 Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective. Table 9 demonstrates the correspondence between the security objectives identified in Chapter 4 to the assumptions and threats identified in Chapter 3. Table 10 provides the rationale proving that each threat and assumption is addressed.

Table 10: Threats and Assumptions to Security Objectives Mapping

Threats and Assumptions	Security Objectives														
	O.ACCESS	O.AUDIT	O.NETMON	O.MONITOR	O.PSELF_PROTECT	O.E.AUDIT	O.E.DBASE	O.E.DEDICATE	O.E.ENFORCE	O.E.ENVIRON	O.E.I&A	O.E.ITACCESS	O.E.NETWORK	O.N.INSTALL	O.N.NOEVIL
T.DELIVFAIL	X	X	X	X	X	X					X	X			
T.MALICE		X		X		X									
T.UNAUTH	X				X				X		X	X			
T.TSF_COMPROMISE					X				X						
A.DBASE							X								
A.DEDICATE								X							
A ENVIRON										X					
A.I&A											X				
A.INSTALL														X	
A.NETWORK													X		
A.NOEVIL															X

Table 11: Threats and Assumptions to Security Objectives Rationale

Threat/ Assumption	Security Objectives Rationale
T.DELIVFAIL	O.MONITOR – addresses this threat by monitoring the sensor's sensed, monitored network and comparing incoming traffic to signatures known to indicate a potential security violation and therefore detecting malicious agent access. O.E.AUDIT – this objectives addresses this threat by requiring the IT environment generate an audit record on the stopping and starting of the SiteProtector Sensor Controller, SitProtector Event Collector, and the SiteProtector Application Server which helps in determining if the audit functions of the TOE have been started up or shutdown which helps users of the TOE know if the TOE can create an audit record notifying users of the detection of a potential suspicious network activity. Further, this objective requires the IT environment to generate audit records dealing with user logging into the host IT environment, failing to log into the host IT environment, and activities dealing with assigning or modify a user role dealing with the Administrator, Operator, or Analyst role which allows for the potential detection of an event that may cause an interruption to the operation of the TOE. O.E.I&A - this objective addresses this threat by addressing unauthorized user access by requiring users to identify and authenticate themselves to the IT Environment before attempting to access TSF data or functions. O.NETMON - this objective addresses this threat by monitoring the secure network to detect a loss in communication between TOE components. O.ACCESS – this objective builds on O.E.I&A and addresses this threat by implementing roles for Users and implementing Access Control SFP rules that restrict the Users (subject) access to objects based on the subject's role. O.E.ITACCESS – this objective builds on O.E.I&A and addresses this threat by implementing IT Environment SFP rules that restrict the Users (subject) access to objects based on the subject's role. O.AUDIT – this objective builds on the O.MONITOR and O.NETMON objectives and addresses this threat by creating an audit record notifying users of the detection of a potential suspicious network activity or a loss in communication between TOE components. O.PSELF_PROTECT – this objective helps in addressing this threat by requiring the TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces thereby helping in preventing an interruption to the operation of the TOE that could result in delivery failure of events or the loss of stored event data.
T.MALICE	O.E.AUDIT – this objective helps address this threat by allowing the users of the TOE to determine if the TOE is in a state that will allow the TOE to generate an audit record notifying a user of a potential security violation because the IT environment will generate audit records that show certain components of the TOE are running or not running which indicates if the TOE's audit capability is shutdown or started up.

Threat/ Assumption	Security Objectives Rationale
	O.MONITOR – this objective addresses this threat by the sensor's monitoring network traffic on the sensed, monitor network and comparing network traffic to signatures. The signatures identify suspicious network activity including an influx of data sent by an agent. O.AUDIT – this objective builds on the O.MONITOR objective and addresses this threat by creating an audit record notifying a user of a potential security violation.
T.UNAUTH	O.E.I&A - this objective addresses this threat by requiring Users to identify and authenticate themselves to the IT Environment before attempting to access TSF data or functions. O.ACCESS – this objective builds on O.E.I&A and addresses this threat by implementing roles for Users and implementing SFP rules that restrict the Users (subject) access to objects based on the subject's role. O.E.ITACCESS – this objective builds on O.E.I&A and addresses this threat by implementing IT Environment SFP rules that restrict the Users (subject) access to objects based on the subject's role. O.E.ENFORCE – this objective addresses threat by ensuring that a user will be allowed to proceed only if successfully identified and authenticated. O.PSELF_PROTECT – this objective helps in addressing this threat by requiring the TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces thereby helping in preventing the discloser, the removing, deleting or modifying of TSF data and preventing the unauthorized access to TSF management functions.
T.TSF_COMPROMISE	O.PSELF_PROTECT - contributes to countering this threat by ensuring that the TSF can protect itself from users within the TSC. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the audit trail. Ensuring that the TSF is always invoked is also critical to the mitigation of this threat. O.E.ENFORCE – this objective addresses threat by ensuring that a user will be allowed to proceed only if successfully identified and authenticated.
A.DBASE	O.E.DBASE – The IT Environment provides a reliable DBMS
A.DEDICATE	O.E.DEDICATE – The IT environment ensures the operating system of the computers the TOE is installed on will operate only TOE software and any required third-party software.
A ENVIRON	O.E.ENVIRON – The IT Environment provides for an adequate facility for the operation of the systems and restricts access to the systems.
A.I&A	O.E.I&A – The operating system of the computers the TOE is installed on and the DBMS implementation provided by the IT Environment requires users to identify themselves and authenticate themselves.
A.INSTALL	O.N.INSTALL – the TOE and the IT environment software will be installed by the authorized administrator in accordance with the IT security procedures.
A.NETWORK	O.E.NETWORK - The IT environment will provide a secure, trusted network

Threat/ Assumption	Security Objectives Rationale
	dedicated to communication between the SiteProtector, it's sub components, and the Sensors
A.NOEVIL	O.N.NOEVIL - The authorised administrators of the TOE will not be careless, willfully negligent, or hostile

8.2 Rationale for Security Functional Requirements

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. Table 11 identifies for each Security Functional Requirement identified in Section 5.1, the TOE security objective(s) identified in Section 4.1 that address it. Table 12 provides the rationale proving that each security objective is addressed by a Security Functional Requirement.

Table 12: TOE Security Functional Requirement to TOE Security Objectives Mapping

TOE Security Functional Requirements	TOE Security Objectives				
	O.ACCESS	O.AUDIT	O.NETMON	O.MONITOR	O.PSELF_PROTECT
FAU_SAA.3		X		X	
FAU_SAR.1		X			
FAU_SAR.3		X			
FAU_SEL.1		X		X	
FDP_ACC.1(1)	X				

TOE Security Functional Requirements	TOE Security Objectives				
	O.ACCESS	O.AUDIT	O.NETMON	O.MONITOR	O.PSELF_PROTECT
FDP_ACF.1(1)	X				
FMT_MOF.1	X				
FMT_MTD.1	X				
FMT_SMF.1(1)	X				
FMT_SMR.1(1)	X				
FAU_GEN_EXP.1		X	X		
FPT_RVM_SFT_EXP.1					X
FPT_SEP_SFT_EXP.1					X

Table 13: TOE Security Functional Requirement to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement Rationale
O.ACCESS	FDP_ACC.1(1) – defines the subjects, objects and operations used by the TOE's Access Control SFP. FDP_ACF.1(1) – defines the Access Control SFP rules for access to objects by subjects. FMT_MOF.1 – Identifies the security functions under control of the role based Access Control SFP. FMT_MTD.1 – Identifies the TSF data management functions under control of the role based Access Control SFP. FMT_SMF.1(1) – Identifies the TSF management functions available to authorized users. FMT_SMR.1(1) – Identifies the User roles supported by the TOE and used as the subject security attribute to enforce the TOE's Access Control SFP.

Security Objective (TOE)	Security Functional Requirement Rationale
O.AUDIT	FAU_SAA.3 – specifies that the TOE will compare incoming network packets against signature events and indicate a violation in the TSP if a signature match occurs. FAU_GEN_EXP.1 – defines the level of auditing provided by the TOE, the contents of the audit records, and the generation of audit records upon detection of a potential security violation. FAU_SAR.1- specifies the audit data information available for viewing by users. FAU_SAR.3 – specifies the selective audit viewing supported by the TOE by enabling a User to search and sort audit data. FAU_SEL.1 – defines the selective auditing fields available to a User.
O.NETMON	FAU_GEN_EXP.1 – defines the level of auditing provided by the TOE including supporting detecting network outage and generation of an audit record upon detection of a potential security violation.
O.MONITOR	FAU_SAA.3 – defines the signature events provided by the TOE that will trigger an audit event. FAU_SEL.1 – defines the selective auditing fields available to a User.
O.PSELF_PROTECT	FPT_RVM_SFT_EXP.1 – The TOE is composed of multiple software components. The software components of the TOE are not able to provide complete non-bypassability (FPT_RVM) by themselves. The TOE relies on IT environment supplied OSs, hardware and a DBMS to help in completely implementing non-bypassability. This SFR states the portion of the FPT_RVM (non-bypassability of the TSP) requirement that is addressed by the TOE. FPT_SEP_SFT_EXP.1 – The TOE is composed of multiple software components. The software components of the TOE are not able to provide complete domain separation (FPT_SEP) by themselves. The TOE relies on IT environment supplied OSs and hardware to help in completely implementing domain separation. This SFR states the portion of the FPT_SEP (domain separation) requirement that is addressed by the TOE.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

This section provides rationale for the IT Environment's Security Functional Requirements demonstrating that the IT Environment's Security Functional Requirements are suitable to address the IT Environment's security objectives. Table 13 identifies for each IT Environment Security Functional Requirement identified in Section 5.2, the IT Environment's security objective(s) identified in Section 4.2 that address it. Table 14 provides the rationale proving that each IT Environment security objective is addressed by an IT Environment Security Functional Requirement.

Table 14: IT Environment Security Functional Requirements to IT Environment Security Objectives Mapping

IT Environment Security Functional Requirements	IT Environment Security Objectives							
	O.E.AUDIT	O.E.DBASE	O.E.DEDICATE	O.E.ENFORCE	O.E.ENVIRON	O.E.I&A	O.E.ITACCESS	O.E.NETWORK
FAU_GEN.1-NIAP-0347	X							
FAU_STG.1		X			X	X		
FDP_ACC.1(2)							X	
FDP_ACF.1(2)							X	
FIA_UAU.2		X			X	X		
FIA_UID.2		X			X	X		
FMT_MSA.1							X	
FMT_MSA.3							X	
FMT_SMF.1(2)							X	
FMT_SMR.1(2)						X		
FPT_ITT.1					X			X
FPT_RVM_OS_DBMS_EXP.1				X				
FPT_SEP_OS_EXP.1			X		X			
FPT_STM.1					X			

Table 15: IT Environment Security Functional Requirements to IT Environment Security Objectives Rationale

Security Objective (IT Environment)	Security Objectives Rationale
O.E.AUDIT	FAU_GEN.1-NIAP-0347 – The host IT Environment will produce audit records that show when the SiteProtector Sensor Controller, SiteProtector Event Collector, or the SiteProtector Application Server have been stopped or started which indicative if the audit functionality of the TOE has been shutdown or started up. Further, this objective requires the IT environment to generate audit records dealing with user logging into the host IT environment, failing to log into the host IT environment, and activities dealing with assigning or modify a user role dealing with the Administrator, Operator, or Analyst role.
O.E.DBASE	FAU_STG.1 - The properly installed, configured and protected DBMS protects against unauthorized audit record modification and deletion. FIA_UAU.2 - The properly installed, configured and protected hardware and software ensures user authentication before any actions. FIA_UID.2 - The properly installed, configured and protected hardware and software ensures user authentication before any actions.
O.E.DEDICATE	FPT_SEP_OS_EXP.1 – The TOE trusts the underlying operating system to provide its domain for execution. Also, no other applications, other than the Sensors and SiteProtector applications and required third-party applications are executed on the platforms.
O.E.ENFORCE	FPT_RVM_OS_DBMS_EXP.1 - The IT Environment ensures that all functions are invoked and succeed before the next function may proceed.
O.E.ENVIRON	FAU_STG.1 - The properly installed, configured and protected DBMS protects against unauthorized audit record modification and deletion. FIA_UAU.2 - The properly installed, configured and protected hardware and software ensures user authentication before any actions. FIA_UID.2 - The properly installed, configured and protected hardware and software ensures user authentication before any actions. FPT_ITT.1 - The properly installed, configured and protected hardware and software ensures proper implementation of the protected network. FPT_SEP_OS_EXP.1 - The properly installed, configured and protected hardware and software ensures proper implementation of the operating system. FPT_STM.1 – The properly installed, configured and protected hardware and software ensures an accurate time-stamp.

Security Objective (IT Environment)	Security Objectives Rationale
O.E.I&A	FAU_STG.1 - The operating system and the DBMS implementation both require a login name and password to have access and therefore the audit records stored in the database are secure from unauthorised user modification. FIA_UAU.2 - The operating system and the DBMS implementation both require a login name and password to have access before any actions can be performed. FIA_UID.2 - The operating system and the DBMS implementation both require a login name and password to have access before any actions can be performed. FMT_SMR.1(2) – The operating system hosting the SiteProtector TOE component maintains the three roles of Administrator, Analyst and Operator.
O.E.ITACCESS	FDP_ACC.1(2) and FDP_ACF.1(2) – Only IT Environment users assigned the IT Environment supported role of Administrator may access TSF data held in the DBMS via the SiteProtector Host's human user interface. Access includes viewing, modifying and deleteting TSF data... Only IT Environment users assigned the role of Administrator may assign a user a SiteProtector supported User Role of Operator, Analyst or Administrator. FMT_MSA.1 – ... Only IT Environment users assigned the role of Administrator may assign a user a SiteProtector supported User Role of Operator, Analyst or Administrator. FMT_MSA.3 – All users must be explicitly assigned a SiteProtector User Role. There are no default users defined. FMT_SMF.1(2) – Specifies the IT Environment's security management function that enable users assigned an Administrator role to assign SiteProtector supported User Roles.
O.E.NETWORK	FPT_ITT.1 - The IT Environment protects confidentially and integrity of all TSF Data by implementing a secure network between different parts of the TOE by using the encryption capabilities of SSL.

8.3 TOE Security Functions

This section demonstrates the suitability of the security functions defined in section 6.1 of meeting the TOE's Security Functional Requirements identified in Section 5.1 and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in Sections 6.1.

Table 16 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements (SFRs). Table 17 provides descriptions of how security functions are helping in implementing the SFRs they are tracing to. After Table 17 are paragraphs that describe as a whole how the TOE's security functions are being used to satisfy the SFRs. With the demonstration of correspondence given in Table 16 and the descriptions of how security functions are meeting individual SFRs and how the security functions of the TOE are meeting the combined SFRs this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in Section 5.1.

Table 16: TOE Security Functional Requirement to TOE Security Functions Mapping

TOE Security Functional Requirement	Audit Security Function	Detect Security Function	Management Security Function	Protect Security Function
FAU_SAA.3	X	X		
FAU_SAR.1	X			
FAU_SAR.3	X			
FAU_SEL.1	X	X		
FDP_ACC.1(1)				X
FDP_ACF.1(1)				X
FMT_MOF.1			X	X
FMT_MTD.1			X	X
FMT_SMF.1(1)			X	
FMT_SMR.1(1)				X
FAU_GEN_EXP.1	X	X		
FPT_RVM_SFT_EXP.1				X
FPT_SEP_SFT_EXP.1				X

Table 17 Rationale of how the SF(s) meet the SFR(s)

SFR	SF and Rationale
FAU_SAA.3	Audit Security Function – Audit records are generated when the incoming network packets match against a signature maintained by the Sensors which may indicate a potential security violation. Detect Security Function – The Sensors use signature based security audit analysis of incoming network packets. The Sensors

	analyzes incoming network packets that the host IT Environment collects looking to detect security violations through the use of various signatures defined with the Sensors policy file.
FAU_SAR.1	Audit Security Function – The TSF maintains a User Type in the SiteProtector component of the TOE in a User Profile that identifies the role the user operates in and therefore the privilege level of the user. The TSF restricts the ability to conduct audit review to those that operate in the Administrator, Analyst and Operator roles. The TSF provides the capability to perform audit review through a Console that is provided by the SiteProtector component of the TOE. The SiteProtector Console provides the capability to supply audit records in human readable format that allows the user to read event type, date, time, source and destination IP addresses, and sensor host IP addresses that are maintained in the audit records. The SiteProtector Console provides this information in a tabular format to the users.
FAU_SAR.3	Audit Security Function – The TSF provides searching and sorting capabilities to users through the SiteProtector Console discussed in FAU_SAR.1. The SiteProtector Console provides a tabular representation of audit records. Each row of the tabular view is an audit record. Each column represents an attribute of the audit record. The columns are sortable by increasing and decreasing order by clicking on the column heading. The column attributes are the attacker, time and date, Event name, Sensor that generated the event, Target Object and Target. The Console maintains the audit data within its own application space after a pull from the database to retrieve the data. It is this local copy of audit data to the TOE that the searches and sorting are carried out on.
FAR_SEL.1	Audit Security Function – The audit records generated by the Sensors are driven by what signature event (intrusion event signatures) a user enables or disables in a Sensor's Policy File. A user controls what audit records a Sensor will generate by selectively enabling or disabling signatures in the Policy File by using SiteProtector. This selection of audit events refers to the sensing capabilities of the TOE and is meant to show that the TOE can selectively record incidents (intrusions) it monitors on networks based on the signatures that have been chosen by a user and applied to a Sensor. Detect Security Function – A user is able to enable or disable signature events in a Sensor's Policy File. The signatures that are enabled in a Sensor's Policy File determine what type of events that the Sensor will detect in the incoming network packets that the Sensor analyzes. In this way a user is given the ability to

	selectively determine what event types the Sensor will detect by enabling and disabling various signatures in a Sensor's Policy File.
FDP_ACC.1(1)	Protect Security Function – The TSF controls what users may apply, view, and modify Policy Files along with what users may view, search and sort Audit data (audit records). The TSF maintains a user profile that defines the role a user is assigned to and the privileges the role has within the TOE. The TOE only understands the three roles of Administrator, Analysts and Operator. SiteProtector works in conjunction with the host OS of the SiteProtector component to only allow successfully identified and authenticated users that belong to one of the three roles to access and carry out specific operations on Policy Files and Audit Data. SiteProtector communicates with the host IT Environment to make sure that the user has successfully identified and authenticated through the login screen of SiteProtector as an authorized user to one of the three roles. Once this has occurred the SiteProtector maintains the user state while the user has an active session with the TOE. SiteProtector monitors the users operation requests during a session and only allows the user the access to those operations that are supported by the role the user is operating in. SiteProtector controls access to the operations of apply, view, and modify that may be done on Policy Files. SiteProtector controls access to the operations view, sort, and search that may be done against Audit Data. This access is enforced against users of SiteProtector. The enforcement is done by SiteProtector graying out (disabling) or enabling those operations that the user's role (Operator, Analyst, or Administrator) does not or does support.
FDP_ACF.1(1)	Protect Security Function – The TSF controls access to Policy Files and Audit Data by only enabling those operations that are supported by the role that the user is operating in. If a user is in the role of Operator, Analyst or Administrator the TSF will enable the ability of the user to view Policy Files and to view, search and sort Audit Data. If a user is in the role of Analyst or Administrator the TSF will enable the capability of the user to modify and apply policy files. Enabling a capability means the TSF does not gray out the capability in the Console so that it is present to the user for use. Capabilities that are grayed out are not enabled capabilities and are therefore not available for access by the user. SiteProtector controls the access to the commands/operations that a user may carry out through the Console. SiteProtector controls

	a user access by graying out (disabling) those commands/operations that the user is not suppose to have access to. SiteProtector enables the viewing operation/command for Policy Files for any user with a role of Operator, Analyst, or Administrator. SiteProtector disables the apply and modify command/operations for Policy Files for user operating in the Operator role and enables them for users operating in the Analyst or Administrator roles. SiteProector enables the view, sort, and search commands/operations for Audit Data for users operating in the Operator, Analyst, or Administrator roles.
FMT_MOF.1	Management Security Function – The TSF provides for the capability to manage security functions by providing the SiteProtector component which provides a GUI for a human user to initiate management commands and by providing the Sensors with the capability to receive management commands and act upon the management commands. Included in the set of management commands is enabling users to stop and start the TOE's sensing functionality and to stop and start the TOE's audit record collection functionality. Protect Security Function – The TSF ensures that a human user with a session with the TOE is operating within one of the three defined roles of Administrator, Analyst or Operator. The TSF interacts with the host OS that the SiteProtector component is running on to determine if a human user has properly identified and authenticated through the SiteProtector logon screen. The TSF maintains an internal representation of a user profile after the user has successfully logged into the host OS IT Environment and the SiteProtector logon screen. The user profile defines the role the user is operating in and the privileges the user has with respect to that role. The TSF uses this user profile to determine what management functions a user has or does not have access to. For those users operating in the Analyst or Administrative role the TSF enables the capability of the user to be able to disable or enable the sensing and collecting of audit records functions of the TOE. The capabilities are enable by the TSF not graying those capabilities out in the Console GUI. Grayed out capabilities in the SiteProtector Console GUI are disabled and are there for not available for use. The TSF grays out, disables, the use of being able to disable or enable the sensing and collecting of audit records to those users operating in the Operator role.
FMT_MTD.1	Management Security Function – The TSF provides for the capability to modify Sensor Policy Files to Sensor components of the TOE. Modifying a Policy File is a management activity that allows a human user to enable and disable different signatures for

	the Sensor. The TSF provides the GUI Console interface through the SiteProtector TOE component to give the user the capability to modify Policy Files. Protect Security Function – The TSF ensures that a human user with a session with the TOE is operating within one of the three defined roles of Administrator, Analyst or Operator. The TSF interacts with the host OS that the SiteProtector component is running on to determine if a human user has properly identified and authenticated through the SiteProtector logon screen. The TSF maintains an internal representation of a user profile after the user has successfully logged into the host OS IT Environment and the SiteProtector logon screen. The user profile defines the role the user is operating in and the privileges the user has with respect to that role. The TSF uses this user profile to determine what management functions a user has or does not have access to. For those users operating in the Analyst or Administrative role the TSF enables the capability of the user to be able to modify Policy Files. The capabilities are enabled by the TSF not graying those capabilities out in the SiteProtector Console GUI. Grayed out capabilities in the SiteProtector Console GUI are disabled and are there for not available for use. The TSF grays out, disables, the use of being able to modify Policy Files to those users operating in the Operator role.
FMT_SMF.1(1)	Management Security Function – The TSF provides management functions to human users by providing a GUI Console to users through the SiteProtector component of the TOE. Through the SiteProtector Console a user is able to start management commands that can start a Sensor, stop a Sensor, apply a Policy File and modify TSF data. The TSF transmit the management command started by a management function to the appropriate TOE component. The TOE component receives the management commands and carries the commands.
FMT_SMR.1(1)	Protect Security Function – The TSF maintains an internal user profile that defines the role a user operates at and the privileges of the role. The privileges of a role define what capabilities the user has to them when using the GUI Console provided by the SiteProtector TOE component.
FAU_GEN_EXP.1	Audit Security Function – As security relevant events occur, the TSF generates audit records. As potential security violation are identified from network traffic being collected by the host IT Environment the Sensors read these frames and analyze the network frames and create audit records when a security violation it detected.

	Detect Security Function – The different components of the TOE maintain a monitoring of the other components to determine if communication is lost with any of the components. When communication is lost to a TOE component this is detected as a security relevant event.
FPT_RVM_SFT_EXP.1	Protect Security Function – The TSF has the ability to be non-bypassable when it is invoked and for those operations that are under the control of the TSF. The TSF monitors user actions and only provides and executes those actions that are appropriate for the user and the role the user is operating in. Further, the TSF is non-bypassable by providing well defined interfaces that need to be used and invoked before allowing any user action to proceed.
FPT_SEP_SFT_EXP.1	Protect Security Function – The TSF implements domain separation by having an architecture that implements several subsystems with well defined functions that help carry out the overall TSP defined in this ST. The subsystems have well defined interfaces that control the flow of information into and out of the subsystems that are only used to carry out the functionality that the subsystem helps implement. Thru this architecture the TSF is maintaining a domain for itself that is protected from interference and tampering by un-trusted users within the TSC. Further, the TSF maintains security domains for users within the TSC by requiring the use of well defined interfaces of the TOE and providing user profiles for users of the TOE.

The **Detect Security Function** has Sensors monitor network packets and that look for patterns in the network traffic that indicate an attack against the system the TOE is monitoring. Incoming packets are compared against signatures defined in the Sensor's resident Policy File (FAU_SAA.3). The Sensors are shipped with a default Policy File that includes pre-defined signatures that detect denial of service, unauthorized access attempts, pre-attack probes, suspicious activity (FAU_SAA.3). Additionally, users may customize Policy Files by disabling/enabling signatures (FAU_SEL.1). The TOE components monitor the communication link between individual TOE components. Included in the System Detection monitoring is reporting network communication problems with other TOE components (FAU_GEN_EXP.1). The TOE uses an IT Environment supplied timer that triggers the TOE to check for communication path problems. The timer is invoked when the TOE components have been started.

The **Audit Security Function** allows the TOE to detect security violations when incoming packets are matched against a signature defined in a Sensor's Policy File. Upon detection of a signature match, the TOE creates an Event (audit record) (FAU_GEN_EXP.1, FAU_SAA.3). Data included in the Event is event name, date, source and destination IP address and the IP address of the Sensor that monitored the Event (FAU_GEN_EXP.1). The TOE generates Events in order to notify a User of abnormal system behaviour. Abnormal system behaviour includes detection of loss of network connectivity with TOE components (FAU_GEN_EXP.1). The management functions of the TOE generate events that report the completion of management events, specifically starting and stopping sensors and applying sensor policy files (FAU_GEN_EXP.1). The TOE supports selective auditing by allowing a User to disable or enable signatures defined in a Sensor's Policy File (FAU_SEL.1). Data included in Events is Event name, date, source and destination IP address and the IP address of the Sensor that monitored the Event (FAU_SAR.1). A user may search and sort the Event data by Event name, source and destination IP address and the IP address of the Sensor that monitored the Event (FAU_SAR.3).

The **Protect Security Function** of the TOE enforces an Access Control SFP. This SFP enforces rules for operations of subjects on objects based on the security attribute of the subjects (FDP_ACC.1(1)). The security attribute of the subjects used by the TOE's Access Control SFP is User Role (FDP_ACF.1(1)). The TOE supports three roles: Operator, Analyst and Administrators (FMT_SMR.1(1)). User roles determine what TSF data a user may view and what TSF functions the user may perform (FMT_MOF.1, FMT_MTD.1). The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by a user by controlling a user session and the actions carried out during a user session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC (FPT_RVM_SFT_EXP.1, FPT_SEP_SFT_EXP.1).

The **Management Security Function** of the TOE provides an interface that enables a user to manage and monitor the TOE. This functionality includes starting and stopping the sensing capability of the TOE by starting and stopping the Sensors and/or the Event Collector and applying Sensor Policy Files which define the enabled and disabled signatures for a Sensor. (FMT_MOF.1, FMT_MTD.1, FMT_SMF.1(1))

8.4 Rationale for Assurance Requirements

EAL2 was chosen because:

A) EAL2 is consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

8.5 Rationale for Strength of Function

The overall strength of function (SOF) for this ST is SOF-basic. SOF-basic was chosen because the threats defined in part 3 of the ST describe threats that are based on an attacker that will attempt casual breaches of the TOE security, those attackers possessing a low attack potential.

8.6 TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 17 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale. Table 18 lists the IT Environment Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 18: TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_SAA.3	FAU_SAA.1	None	N/A
FAU_SAR.1	Nothing	FAU_GEN.1	See below.
FAU_SAR.3	Nothing	FAU_SAR.1	Satisfied
FAU_SEL.1	Nothing	FAU_GEN.1 FMT_MTD.1	See below. The FMT_MTD.1 dependency is satisfied.
FDP_ACC.1(1)	Nothing	FDP_ACF.1	Satisfied by FDP_ACF.1(1)
FDP_ACF.1(1)	Nothing	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(1) The FMT_MSA.3 dependency is satisfied because FMT_MSA.3 is provided by the IT Environment.
FMT_MOF.1	Nothing	FMT_SMF.1 FMT_SMR.1(1)	Satisfied Satisfied
FMT_MTD.1	Nothing	FMT_SMF.1 FMT_SMR.1(1)	Satisfied Satisfied
FMT_SMF.1(1)	Nothing	None	N/A
FMT_SMR.1(1)	Nothing	FIA_UID.1	The FIA_UID.1 dependency is satisfied because FIA_UID.2 is provided by the IT Environment.

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN_EXP.1	Nothing	FPT_STM.1	FPT_STM.1 is satisfied because the SFR is included in the IT Environment's SFRs.
FPT_RVM_SFT_EXP.1	Nothing	None	N/A
FPT_SEP_SFT_EXP.1	Nothing	None	N/A

Table 19: IT Environment Security Functional Requirements Dependency Rationale

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0347	Nothing	FPT_STM.1	Satisfied
FAU_STG.1	Nothing	FPT_STM.1	Satisfied
FAU_STG.1	Nothing	FAU_GEN.1	See below.
FDP_ACC.1(2)	Nothing	FDP_ACF.1	Satisfied by FDP_ACF.1(2)
FDP_ACF.1(2)	Nothing	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1(2) Satisfied by FMT_MSA.3
FIA_UAU.2	Nothing	FIA_UID.1	Satisfied
FIA_UID.2	Nothing	None	N/A
FMT_MSA.1	Nothing	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1(1)	[Satisfied by FDP_ACC.1(2) or N/A] Satisfied by FMT_SMF.1(2) Satisfied by the TOE's SFRs
FMT_MSA.3	Nothing	FMT_MSA.1 FMT_SMR.1(1)	Satisfied Satisfied by the TOE's SFRs
FMT_SMF.1(2)	Nothing	None	N/A
FMT_SMR.1(2)	Nothing	FIA_UID.1	Satisfied
FPT_ITT.1	Nothing	None	N/A
FPT_RVM_OS_DMBS_EXP.1	Nothing	None	N/A
FPT_SEP_OS_EXP.1	Nothing	None	N/A
FPT_STM.1	Nothing	None	N/A

SFR FAU_GEN.1 dependency could not be met because the TOE cannot satisfy the requirement of stopping and starting of audit functions of the FAU_GEN.1. Because of this, FAU_GEN_EXP.1 was created. Although the TOE does report network outages which indicates a halt of auditing functionality, the TOE could not claim the requirement of FAU_GEN.1 for creating an event that indicates complete stopping and starting of audit functions. Since FAU_GEN_EXP.1 is an explicit requirement it is not an allowable dependency for other requirements so it can not satisfy the FAU_GEN.1 dependencies that FAU_SAR.1 and FAU_SEL.1 have on FAU_GEN.1. Even though FAU_GEN_EXP.1 is not an allowable dependency for other requirements it specifies auditable event generation that is necessary for the requirements FAU_SAR.1 and FAU_SEL.1 need to be able to carry out the audit review and selective auditing that are specified in those two requirements.

8.7 Rationale for Explicitly Stated SFR for the TOE

The TOE cannot satisfy the FAU_GEN.1 SFR because of the requirements to generate an audit record to record the stopping and starting of audit functions or the outcome (success or failure) of the event. Therefore, FAU_GEN_EXP.1 was created. FAU_GEN_EXP.1 is identical to FAU_GEN.1 except for the absence of the requirements to create an audit record to record stopping and starting audit functions and to record the outcome (success or failure) of the event. Although the TOE reports network outages which indicates a halt of auditing functionality, the TOE could not claim the requirement of FAU_GEN.1 for creating an audit record that indicates complete stopping and starting of audit functions nor being able to record the outcome (success or failure) of all events for which an audit record is generated.

Software TOEs are unable to fully satisfy FPT_RVM by themselves. The explicitly stated SFR FPT_RVM_SFT_EXP.1 states the portion of FPT_RVM that can be addressed by the TOE.

Software TOEs are unable to fully satisfy FPT_SEP by themselves. The explicitly stated SFR FPT_SEP_SFT_EXP.1 states the portion of FPT_SEP that can be addressed by the TOE.

8.8 Rationale for Explicitly Stated SFR for the IT Environment

Software TOEs are unable to fully satisfy FPT_RVM by themselves. The explicitly stated SFR FPT_RVM_OS_DBMS_EXP.1 states the portion of FPT_RVM supplied by the OS, DBMS and hardware in support of the overall FPT_RVM functionality.

Software TOEs are unable to fully satisfy FPT_SEP by themselves. The explicitly stated SFR FPT_SEP_OS_EXP.1 states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality.

FAU_GEN-NIAP-0347 is an explicitly stated requirement because it is a requirement based on a US Interpretation, NIAP-0347.

8.9 Assurance Measures Rationale for TOE Assurance Requirements

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

Table 19 provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement. N/A means not applicable because the Assurance Component does not have any dependencies.

Table 20: EAL2 SAR Dependencies

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	N/A
ADO_DEL.1	Delivery procedures	None	N/A
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	Yes
ADV_FSP.1	Informal functional specification	ADV_RCR.1	Yes
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	Yes
ADV_RCR.1	Informal correspondence demonstration	None	N/A
AGD_ADM.1	Administrator guidance	ADV_FSP.1	Yes
AGD_USR.1	User guidance	ADV_FSP.1	Yes
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	Yes
ATE_FUN.1	Functional testing	None	Yes

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	Yes
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	Yes
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	Yes