IBM
Proventia G 1.3
and
SiteProtector 2.0 Service Pack 6.1 with Reporting Module

Security Target

Version 1.19

May 10, 2010

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:	IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Security Target
ST Version:	Version 1.19
Publication Date:	May 10, 2010
Authors:	Internet Security Systems, Inc.
TOE Identification:	IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module Target of Evaluation
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Protection Profile (PP) Conformance	Intrusion Detection System System Protection Profile Version 1.6, April 2006
Keywords:	Intrusion Detection System, IDS

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 August 2005, version 2.3, CCIMB-2005-08-002.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCIMB-2005-08-002.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCIMB-2005-08-002.
[CEM]	Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, dated August 2005, version 2.3.

1.3 Acronyms and Abbreviations

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
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

1.4 Security Target Overview

The TOE is an automated real-time intrusion detection system designed to protect 10/100/1000 Mbps and 1000 Mbps SX network segments. Proventia G 1.3 detects and reports potential security violations to a software managed central console, the SiteProtector 2.0 Service Pack 6.1 with Reporting Module.

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 2.3.

2 TOE DESCRIPTION

This section provides an overview of the IBM Proventia G 1.3 and SiteProtector 2.0 Service Pack 6.1 with Reporting Module TOE. This section defines the TOE components and describes TOE functionality, presents the physical and logical boundaries of the TOE, provides an overview of the TOE architecture and describes the evaluated configuration of the TOE.

2.1 TOE Product Type

The 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 two components:

a) Proventia G 1.3 appliance (hereafter referred to as Proventia G 1.3, Proventia GX, Sensor or Agent).

b) SiteProtector 2.0 Service Pack 6.1 with Reporting Module. (hereafter referred to as SiteProtector 2.0 Service Pack 6.1 with Reporting Module or SiteProtector)

The Proventia GX TOE component provides the IDS functionality. This Sensor monitors a network or networks and compares incoming packet or packets against known packets and packet patterns that indicate a potential security violation. If a match occurs, Proventia GX will create an audit record. The SiteProtector 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators.

The Sensor monitors one or more 10/100/1000 Mbps copper or 1000 Mbps SX fiber network segments (the sensed, monitored network).

The SiteProtector Version 2.0 Service Pack 6.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation is connects to the appliance via TLS session, and this workstation is only used by authorized administrators for the management of the appliance

2.1.1 TOE Components

The Proventia GX and SiteProtector TOE components are described in the following sections.

2.1.2 Proventia GX TOE Component

The Proventia GX TOE component provides IDS security functionality. The Proventia GX TOE component consists of Proventia G 1.3 firmware and is made up of one of the following appliances GX4002, GX4004, GX5008 C, CF and SFP (Copper, Copper/Fiber and small form factor pluggable port configuration), GX5208 and GX5108 (C, CF and SFP) appliances. The Proventia GX TOE component includes the Proventia GX appliance

hardware, the appliance resident Red Hat operating system (OS) and the Proventia GX application software image.

2.1.3 SiteProtector 2.0 Service Pack 6.1 TOE Component

The SiteProtector 2.0 Service Pack 6.1 with Reporting Module component of the TOE is a software product that runs on a Windows based workstation. The SiteProtector enables administrators to monitor and manage the Sensor components of the TOE. The SiteProtector TOE component includes the SiteProtector 2.0 Service Pack 6.1 with Reporting Module software.

2.2 TOE Functionality Overview

2.2.1 Proventia GX

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

2.2.2 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 and system data records; and

d) monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

The SiteProtector is divided into the following software sub-components and depicted in Figure 1 below.

a) SiteProtector Console – The SiteProtector Console is a graphical user interface (GUI) that provides an interface that enables an Administrator to configure and monitor the Sensors. The add-on Reporting Module provides the ability to generate a wide range of reports in a variety of formats, including the following:

1. Vulnerability Assessment reports
2. Attack Activity reports
3. User Audit reports
4. Content Filtering reports
5. User Permission reports

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 database via the DBMS.

c) SiteProtector Application Server – The SiteProtector Application Server is a software process that is responsible for providing the communication path between the DBMS and all other SiteProtector software components.

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 database (via the SiteProtector Application Server) and sending the command and control information to the Sensors or the SiteProtector Event Collector.

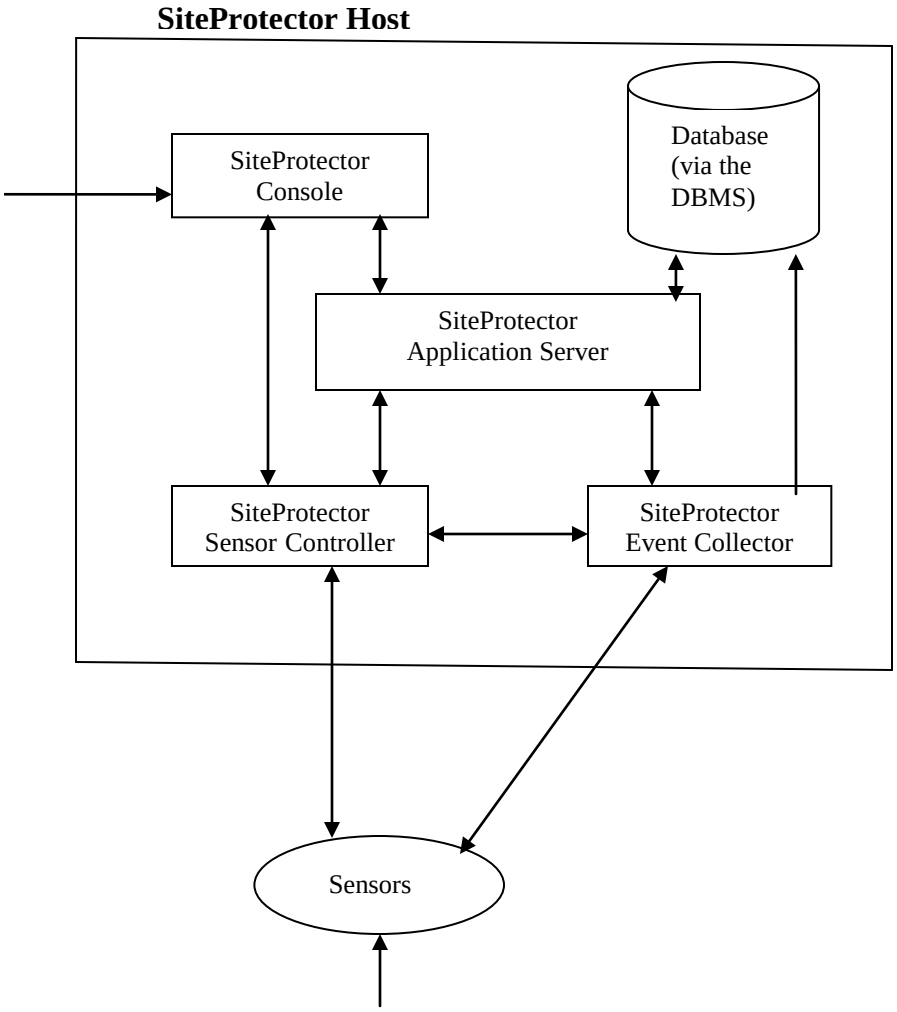

Figure 1 SiteProtector Host TOE Component Relationships

2.3 TOE Physical Boundary

Figure 2 provides a representation of the physical boundary of the TOE. The TOE physical boundary includes the SiteProtector 2.0 Service Pack 6.1 with Reporting Module software distribution and all hardware and software for the Proventia G 1.3 appliance. The subsections below provide details for each of the TOE component.

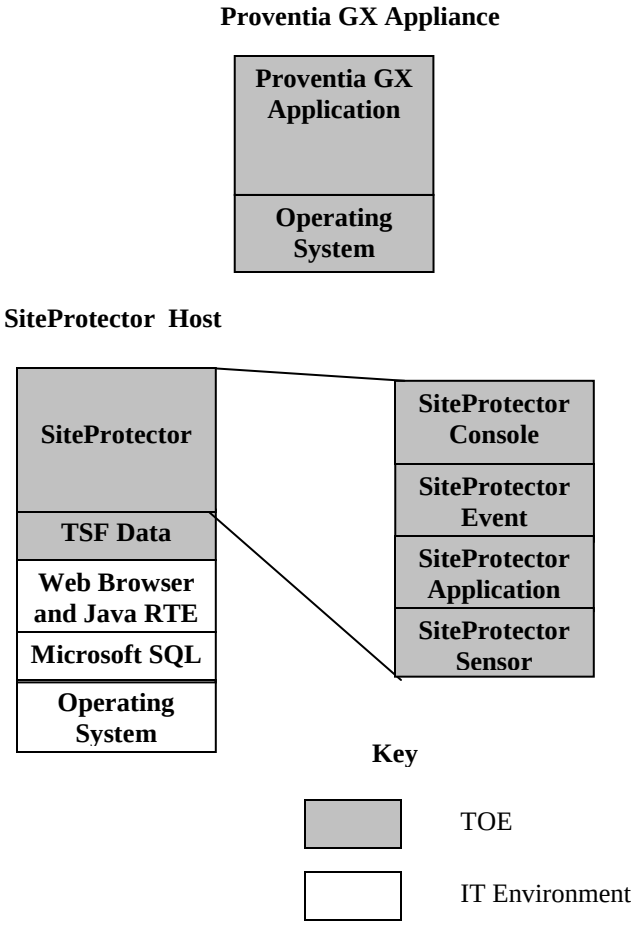

Figure 2 TOE Physical Boundary

2.3.1 Proventia GX

The physical boundary for the Proventia GX includes:

a) Proventia GX hardware appliance Series GX4xxx and GX5xxx models

b) Proventia G 1.3 application software

c) Proventia GX appliance operating system, Red Hat 8.0

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

2.3.2 SiteProtector 2.0 Service Pack 6.1 with Reporting Module

The physical boundary for SiteProtector includes:

a) SiteProtector 2.0 Service Pack 6.1 with Reporting Module software distribution

b) SiteProtector resident default Policy Files and audit data

2.4 IT Environment Supplied Hardware and Software

The following table identifies the minimum hardware and software requirements for components provided by the IT Environment.

Minimum Requirements	
Processor	1 GHz Pentium III
Memory	1 GB
Disk Space	8 GB
Operating System	Windows 2000 Server with Service Pack 4 or later, or Windows 2000 Advanced Server with Service Pack 4 or later, or Windows Server 2003 with or without Service Pack 1, or Windows Enterprise Server 2003 with Service Pack 1
DBMS	SQL Server 2000 Desktop Engine (MSDE) with Service Pack 3a and Security Patch 03-031 or SQL Server 2000 with Service Pack 3a and SQL Security Patch MS03-031 or SQL Server 2000 with Service Pack 4
Additional Software	Microsoft Internet Explorer 5.0 or higher Microsoft Data Access Components (MDAC) 2.8 or later Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.5.0_06 Adobe Acrobat Reader 6.0 or later OpenSSL 0.9.7d[1]
Network Configuration	Static IP address
Disk Partition Formats	NTFS

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.
Intrusion Detection Security Function	The TOE provides Intrusion Detection Security Functionality by continuously

[1] **Note that OpenSSL 0.9.7d is not FIPS validated**

	monitoring network traffic, comparing this traffic to signatures, and reporting any match that may indicate a intrusion.
Self Protection Security Function	The TOE Self Protection 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 an authorized user to manage and monitor the TOE.
Reaction Security Function	The TOE's Reaction Security Function provides the actions taken in response to a detected intrusion attempt.

The TOE's logical scope does not include the intrusion prevention functionality provided by Proventia GX. The Proventia GX appliance is configured as an IDS system at system installation by the administrator selecting to operate in Passive mode only.

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 (removed to maintain compliance with the Protection Profile)
- The Incident and Exception Component (removed to maintain compliance with the Protection Profile)
- Firewall capabilities (removed to maintain compliance with the Protection Profile
- Administrator access to the Proventia GX other than through SiteProtector (required to meet auditing and management requirements of the Protection Profile).

2.5.2 TOE Data

2.5.2.1 TSF Data

The TSF data for the TOE are the policy files, audit records, system data records, and signature data.

2.5.2.2 Security Attributes

The security attributes of the TOE are permissions associated with each authorized user (administrator) of SiteProtector. The permissions of a user define the operations that the user may carry out while having an active user session with the TOE.

2.5.2.3 User Data

The TSC does not control any user data.

2.6 Rational for Non-bypassability and Separation of the TOE

The following sections provide rationale for non-bypassability and separation for the TOE. This rationale describes how the components of the TOE support secure operation of the TSF and how the security architecture of the TOE cannot be compromised or corrupted.

2.6.1 Proventia GX TOE Component

The Proventia GX TOE component consists of hardware and software dedicated to providing IDS functionality to a monitored network. The Proventia GX TOE component provides non-bypassability by mediating its own interfaces and ensuring that the TSP is invoked and successful before allowing any other TSF-mediated action to proceed.

The Proventia GX TOE components have monitoring interfaces (also referred to as sensing interfaces) that are connected to the monitored network. The monitoring interfaces of the Proventia GX component read packets from the monitored network and 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 GX TOE component. No other functionality is available through the Proventia GX monitoring interface. Further, the monitoring interfaces of the Proventia GX 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 GX TOE component is the management interface that communicates 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 GX TOE components to proceed.

The Proventia GX TOE Component maintains a domain for its own execution. The security domain of the Proventia GX TOE Component consists of all hardware and software that makes up the Proventia GX appliance. The Proventia GX TOE components maintain this 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 GX TOE component. The monitoring interfaces of the Proventia GX TOE component 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 GX TOE component to have a security domain that protects it from interference and tampering.

2.6.2 Rationale for the SiteProtector TOE Component

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment for the SiteProtector TOE Component. The SiteProtector TOE component is software only and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The SiteProtector TOE component runs as a service on top of the IT Environment supplied OS.

The SiteProtector TOE component ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: incoming network IP traffic is inspected before the packets are acted upon by higher-level protocol handlers, and management actions are limited to the permissions of the authenticated users. Non-security relevant interfaces do not interact with the security functionality of the TOE. The OS ensures that the security relevant interfaces are invoked: all incoming network packets are delivered to the TOE for inspection.

2.7 TOE Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia G 1.3) and one instance of a workstation running SiteProtector 2.0 Service Pack 6.1 with Reporting Module.

The following list itemizes configuration options for the TOE for the evaluated configuration:

1. Telnet server support in the Sensors is not included. Telnet is disabled on the sensor by default, and it must remain disabled for the evaluated configuration.

2. Incidents and Exceptions are disabled.

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 automatically retrieve and store the updates on the SiteProtector system.

4. Intrusion Prevention and firewall functionality provided by Proventia GX 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 DBMS implementation reside on one workstation.

7. Proventia GX and SiteProtector communicate via TLS (Transport Layer Security).

8. SSL or encrypted SQL is used for the communication between SiteProtector and the DBMS. SSL encryption can be manually configured by the user for each component that connects to the DB. The SiteProtector documentation includes steps to manually configure SSL. Neither data nor database code is encrypted, encryption occurs only in the communications to the DB.

9. Management via local management or web interface directly to the Proventia GX is not included in the evaluated configuration. Local management by the Console port and the Proventia Manager web interface are used for initial installation and configuration only. These two interfaces are not to be used after the TOE has been placed into the evaluated configuration

10. The SiteProtector Reporting Module add-on must be installed and configured. The Reporting Module is licensed to allow viewing of Audit Reports; it does not generate audit data. The Reporting Module requires the end user to purchase a license to unlock this functionality within the TOE.

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) Organizational 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. Policies are identified as P.*policy* with *policy* specifying a unique name.

3.1 Assumptions

The specific conditions listed in Table 1 are assumed to exist in the TOE's 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.

Table 1: Assumptions

Assumption	Definition
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

3.2 Threats

Table 2 and Table 3 list the threats addressed by the TOE. The following are threats identified for the TOE and the IT System the TOE monitors. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 TOE Threats

Table 2: TOE Threats

Threat	Definition
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

3.2.2 IT System Threats

Table 3: IT System Threats

Threat	Definition
T.SCNCFG	Improper security configuration setting may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4 identifies the organizational security policies applicable to the TOE.

Table 4: Organizational Security Policies

Policy	Definition
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

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 and IT Environment as O.*objective* or OE.*objective* with *objective* specifying a unique name.

4.1 Security Objectives for the TOE

Table 5 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 5: Security Objectives for the TOE

Objective	Definition
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 6 identifies the security objectives for the environment.

Table 6: Security Objectives for the ITEnvironment

Objective	Definition
O.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
O.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.INTROP	The TOE is interoperable with the IT System it monitors.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to allowing access to TOE functions and data.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived verbatim (including font) from the Intrusion Detection System System Protection Profile, Version 1.6.

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 completed by the ST author are in bold text and surrounded by square brackets: [**assignment completed by ST author**].
>
> Selections completed by the ST author are in underlined text surrounded by square brackets: [selection completed by ST author].
>
> Assignments within selections completed by the ST author are in underlined bold text surrounded by square brackets: [**assignment within a selection completed by the ST author**].
>
> Refinements completed by the ST author are indicated in italicized text surrounded by square brackets: [*added text completed by the ST author*] for added text and italicized text with a strikethrough surrounded by square brackets for the deletion of text: [*~~deletion of text completed by the ST author~~*].

Explicitly stated requirements are included in this ST. Explicitly stated SFRs were copied from the IDS System PP to specifically address the data collected and analysed by an IDS. The names of these requirements start with IDS_.

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 to provide a unique identifier for each SFR.

5.1 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1: Audit data generation

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

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

b) All auditable events for the basic level of audit; and

c) **Access to the System and access to the TOE and System data**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**, the additional information specified in the **Details** column of Table [2] [7] Auditable Events.

Table 7: Auditable Events

Component	Event	Details
FAU_GEN.1	**Start-up and shutdown of audit functions**	**Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event**
FAU_GEN.1	**Access to System**	**All access to the audit and system data by Administrators**
FAU_GEN.1	**Access to the TOE and System data**	**Object IDS, Requested access**
FAU_SAR.1	**Reading of information from the audit records**	**All access to the audit and system data by Administrators**
FAU_SAR.2	**Unsuccessful attempts to read information from the audit records**	**All access to the audit and system data by Administrators**
FAU_SEL.1	**All modifications to the audit configuration that occur while the audit collection functions are operating**	**All changes to the audit event configuration by Administrators**
FMT_MOF.1	**All modifications in the behavior of the functions of the TSF**	**The identity of the authorized administrator and the operation modified**
FMT_MTD.1	**All modifications to the values of TSF data**	**All changes to the behavior of the TOE by Administrators**
FMT_SMR.1	**Modifications to the group of users that are part of a role**	**User identity**

Rationale for Refinement: The SFR refers to Table 2 yet in this ST, the table is Table 7.

5.1.1.2 FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide [**authorized administrators with permission to view reports on management actions**] with the capability to read [**all audit record detail identified in the above table**] 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.

5.1.1.3 FAU_SAR.2: Restricted audit review

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

5.1.1.4 FAU_SAR.3: Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event.

5.1.1.5 FAU_SEL.1: Selective audit

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**].

5.1.1.6 FAU_STG.4: Prevention of audit data loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and send an alarm if the audit trail is full.

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**random number generator**] and specified cryptographic key sizes [**168 bits**] that meet the following: [**(FIPS 46-3)**].

5.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**(No Standard)**].

5.1.2.3 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1(1) The TSF shall perform [**the operations described below**] in accordance with a specified cryptographic algorithm [**multiple algorithms in the modes of operation described below**] and cryptographic key sizes [**multiple key sizes described below**] that meet the following [**multiple standards described below**]:

Table 8: Cryptographic Operations

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and decryption	Triple-DES (EDE, CBC)	168	FIPS 46-3
Key establishment	RSA	1536 (modulus)	RFC2246
Hashing	SHA-1	N/A	FIPS 180-2
Random number generation	The TLS PRF based upon MD5 and SHA-1 is used to generate key material.	N/A	N/A

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1(1): User attribute definition

FIA_ATD.1.1(1) The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) ***[****~~Authentication data;~~****]***

c) Authorizations**;** and

d) [**no other security attributes**].

Rationale for Refinement: FIA_ATD is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.1.3.2 FIA_UAU.1(1): Timing of authentication

FIA_UAU.1.1(1) The [*TSF*] shall allow [**no other TSF-mediated actions**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(1) The [*TSF*] shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Rationale for Refinement: FIA_UAU.1 is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.1.3.3 FIA_UID.1(1): Timing of identification

FIA_UID.1.1(1) The [*TSF*] shall allow [**no other TSF-mediated actions**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(1) The [*TSF*] shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Rationale for Refinement: FIA_UID.1 is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1: Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to <u>modify the behavior of</u> the functions **of System data collection, analysis and reaction** to <u>authorized System administrators</u>.

5.1.4.2 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add System and audit data, and shall restrict the ability to query and modify all other TOE data** to [**authorized administrators with explicit permissions to perform these actions**].

5.1.4.3 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the **following *roles*: authorized administrator, authorized System administrators, and [no other roles**].

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

Application Note: The only distinction between the 2 specified roles in the PP are in FIA_AFL.1, FMT_MTD.1 and FMT_MOF.1. In this ST, FIA_AFL.1 has been deleted per PD-0097. Therefore, in this ST, the role "authorised administrator" refers to any authorised user of SiteProtector and the role "authorised system administrator" refers to authorised users of SiteProtector whose permissions explicitly include view and configure assets, agents and policies as well as start and stop agents.

5.1.5 Protection of the TOE Security Functions (FPT)

5.1.5.1 FPT_ITT.1: Internal TOE TSF data transfer

FPT_ITT.1(1) The TSF shall protect TSF data from disclosure **and** modification when it is transmitted between separate parts of the TOE.

Protection Profile Claim: In accordance with NIAP Precedent PD-0097, FPT_ITT.1 has been added. With the Proventia GX component, this functionality is provided by the TOE. With the SiteProtector component, the functionality is provided by the IT Environment. Therefore, iterations have been levied on both the TOE and IT Environment with refinements to clarify the scope of each. On the SiteProtector Host, this functionality is provided by a third-party package (OpenSSL) that is not modified in any way by the vendor. The OpenSSL package executes as a DLL that is called from the TOE.

5.1.5.2 FPT_RVM.1: Non-bypassability of the TSP

FPT_RVM.1.1(1) The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC *[on the Proventia GX]* is allowed to proceed.

5.1.5.3 FPT_SEP.1: TSF domain separation

FPT_SEP.1.1(1) The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects *[on the Proventia GX]*.

FPT_SEP.1.2(1) The TSF shall enforce separation between the security domains of subjects in the TSC *[on the Proventia GX]*.

5.1.5.4 FPT_STM.1: Reliable Time Stamps

FPT_STM.1.1(1) The TSF shall be able to provide reliable time stamps for its own use.

5.1.6 IDS Component Requirements (IDS)

5.1.6.1 IDS_SDC.1: System data collection (EXP)

IDS_SDC.1.1 **The System shall be able to collect the following information from the targeted IT System resource(s):**
a) [network traffic] **and**
b) [**no other specifically defined events**].

IDS_SDC.1.2 **At a minimum, the System shall collect and record the following information:**

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the *Details* column of Table [*9*] [~~3~~]System Events.

Table 9: System Events

Component	Event	Details
IDS_SDC.1	Network traffic	**Protocol, source address, destination address**

Rationale for Refinement: The SFR refers to Table 3 yet in this ST, the table is Table 8.

5.1.6.2 IDS_ANL.1: Analyser analysis (EXP)

IDS_ANL.1.1 **The System shall perform the following analysis function on all IDS data received:**

a) [signature]; **and**

b) **[no other analytical functions].**

IDS_ANL.1.2 **The System shall record within each analytical result at least the following information:**

a) Date and time of the result, type of result, and identification of data source; and
b) [no other security relevant information about the result].

5.1.6.3 IDS_RCT.1: Analyzer react (EXP)

IDS_RCT.1.1 **The System shall send an alarm to** [**the SiteProtector Console**] **and take** [**the following actions: generate email to the System Administrator and/ or generate an SNMP trap message**] **when an intrusion is detected**.

5.1.6.4 IDS_RDR.1: Restricted data review (EXP)

IDS_RDR.1.1 **The System shall provide** [**administrators with permission to view reports for IDS events] with the capability to read** [**event data] from the System data.**

IDS_RDR.1.2 **The System shall provide the System data in a manner suitable for the user to interpret the information.**

IDS_RDR.1.3 **The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.**

5.1.7 IDS Component Requirements (IDS)

5.1.7.1 IDS_STG.2: Prevention of system data loss (EXP)

IDS_STG.2.1 **The System shall** [overwrite the oldest stored System data**] and send an alarm if the storage capacity has been reached.**

5.2 IT Environment Security Functional Requirements

This section identifies the Security Functional Requirements for the IT Environment.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1 The [~~*TSF*~~] *[IT Environment*] shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The [~~*TSF*~~] [*IT Environment*] shall be able to detect unauthorized modifications to the audit records.

FAU_STG.2.3 The [~~*TSF*~~] [*IT Environment*] shall ensure that [**all but the oldest records of sufficient size to accommodate the new**] audit records will be maintained when the following conditions occur: [audit storage exhaustion].

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**No Standard**].

5.2.2.2 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1(2) The TSF shall perform [**the operations described below**] in accordance with a specified cryptographic algorithm [**multiple algorithms in the modes of operation described below**] and cryptographic key sizes [**multiple key sizes described below**] that meet the following [**multiple standards described below**]:

Table 10: Cryptographic Operations

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and decryption	Triple-DES (EDE, CBC)	168	FIPS 46-3
Key establishment	RSA	1536 (modulus)	RFC2246
Hashing	SHA-1	N/A	FIPS 180-2

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_ATD.1(2): User attribute definition

FIA_ATD.1.1(2) The [~~*TSF*~~] [*IT Environment*] shall maintain the following list of security attributes belonging to individual users:

a) User identity;

b) Authentication data;

c) *[~~Authorizations;~~]* and

d) [**no other security attributes**]**.**

Rationale for Refinement: FIA_ATD is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.2.3.2 FIA_UAU.1(2): Timing of authentication

FIA_UAU.1.1(2) The [*~~TSF~~*] [*IT Environment*] shall allow [**no other TSF-mediated actions**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(2) The [*~~TSF~~*] [*IT Environment*] shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Rationale for Refinement: FIA_UAU.1 is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.2.3.3 FIA_UID.1(2): Timing of identification

FIA_UID.1.1(2) The [*~~TSF~~*] [*IT Environment*] shall allow [**no other TSF-mediated actions**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(2) The [*~~TSF~~*] [*IT Environment*] shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Rationale for Refinement: FIA_UID.1 is iterated with one instance levied on the TOE and the other on the IT Environment. The IT Environment validates the logon information (user identity and password (authentication data), after which the TOE associates permission (authorizations) with the user identity).

5.2.4 Protection of the TOE Security Functions (FPT)

5.2.4.1 FPT_ITT.1: Internal TOE TSF data transfer

FPT_ITT.1(2) The [~~*TSF*~~] [*IT Environment*] shall protect TSF data from disclosure **and** modification when it is transmitted between separate parts of the TOE.

5.2.4.2 FPT_RVM.1: Non-bypassability of the TSP

FPT_RVM.1.1(2) The [~~*TSF*~~] [*IT Environment*] shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC *[on the SiteProtector Host]* is allowed to proceed.

5.2.4.3 FPT_SEP.1: TSF domain separation

FPT_SEP.1.1(2) The [~~*TSF*~~] [*IT Environment*] shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects *[on the SiteProtector Host]*.

FPT_SEP.1.2(2) The [~~*TSF*~~] [*IT Environment*] shall enforce separation between the security domains of subjects in the TSC *[on the SiteProtector Host]*.

5.2.4.4 FPT_STM.1: Reliable Time Stamps

FPT_STM.1.1(2) The [~~*TSF*~~] [*IT Environment*] shall be able to provide reliable time stamps for ~~its own~~ the TOE's use.

5.2.5 IDS Component Requirements (IDS)

5.2.5.1 IDS_STG.1: Guarantee of system data availability (EXP)

IDS_STG.1.1 **The [~~*System*~~]** [*IT Environment*] **shall protect the stored System data from unauthorized deletion.**

IDS_STG.1.2 **The [~~*System*~~]** [*IT Environment*] **shall protect the stored System data from modification.**

IDS_STG.1.3 **The [~~*System*~~]** [*IT Environment*] **shall ensure that [all but the oldest records of sufficient size to accommodate the new] System data will be maintained when the following conditions occur:** [System data storage exhaustion]**.**

5.3 TOE Security Assurance Requirements

The following table 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 11: 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 claimed minimum strength of function for the TOE is SOF-basic. No TOE SFRs include a permutational or probabilistic mechanism.

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 described below.

6.1.1 Intrusion Detection Security Function

The TOE provides Intrusion Detection Security Functionality by continuously monitoring network traffic and comparing the packets to signatures identified in the Sensor's Policy File. Signatures identify packet and packet patterns that indicate a potential security violation to a device accessible by the Sensor's monitored network. The Sensors are shipped with a default Policy File that includes pre-defined signatures that include detection of denial of service, unauthorized access attempts, pre-attack probes, and suspicious activity.

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 a system data record (event). Data included in the Event is date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, protocol and source and destination IP address.

Authorized 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 traffic as being a security violation. The reactions (generating an email and/or SNMP trap) taken for specific events are also configured via the Policy Files.

6.1.2 Audit Security Function

The TOE's Audit Security Functionality combines both audit data record and system data records functionality. The Audit Security Function includes audit and system data generation; audit data selective generation; audit and system data viewing; audit and system data selective viewing; audit and system data storage; and viewing of TOE generated alerts.

6.1.2.1 Audit Data Generation

Audit records are generated as the result of administrator functions. Management functions, defined in the Management Security Function, generate audit records that report the completion of administrator actions. These events include:

a) Startup and shutdown of the TOE (the audit function is always running when the TOE is running, so these events correspond to start-up and shutdown of the audit function).

b) Results of all I&A actions taken by the operating system on behalf of the TOE.

c) All access to the audit and system data by Administrators.

d) All changes to the audit event configuration by Administrators (selective audit).

e) All changes to the behavior of the TOE by Administrators.

f) All changes to the IDS configuration of the TOE by Administrators.

g) All changes to the associations of users to user groups inside SiteProtector and user's permissions.

The above audited management commands are all generated locally on the SiteProtector host with the exception of item e) changes to the behavior of the TOE. Theses management commands include starting and stopping Sensors and applying sensor policy files. The SiteProtector Sensor Controller receives completion indication (audit records) from the Sensor reporting the completion of these events. (Sensors remain in an idle state when stopped and therefore can send and receive commands and report the success of a stop and start Sensor command).

6.1.2.2 System Data Generation

The System Data Generation functionality of the Audit Security Function provides the capability of the TOE to report a possible security violation as the result of collecting and analyzing network traffic. System data is generated as the result of the Intrusion Detection Security Function. 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 a system data record (event). Data included in the Event is date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, protocol and source and destination IP address.

6.1.2.3 Viewing – Audit Data and System Data

The TOE provides equivalent functionality for viewing audit data and viewing system data. Audit and system data viewing is accomplished using the SiteProtector Console. The SiteProtector Console uses the SiteProtector Application Server to retrieve the audit and system data from the database via the DBMS. Data included in the records includes date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, protocol, and source and destination IP address (if applicable).

Users who are allowed access to audit and system data must be explicitly configured by a SiteProtector Administrator and therefore, known to SiteProtector. First, a user must be defined by the Windows OS (IT Environment) and log on. Once logged onto Windows, the

user then logs into SiteProtector via a SiteProtector logon GUI. SiteProtector collects the user's userid and password information through the GUI and passes the information to Windows to authenticate the user. If Windows indicates that the user is invalid, SiteProtector terminates the session. Otherwise, if Windows indicates that the user is valid (and authenticated), SiteProtector looks up that userid in its database to determine the TOE managed permissions associated with the user. If the user is not defined in the SiteProtector database, SiteProtector terminates the session. Otherwise, the user has access to view audit and system data. SiteProtector users must be explicitly configured to enable viewing of audit and system data either by specific user permissions or by belonging to a group that has viewing permissions.

Audit Detail Reports are supported via the SiteProtector Reporting Module. This report enables an administrator to view the DBMS stored audit events in human readable format. The Audit Detail Report is the only means to view audit events. Audit Detail Reports are not automatically generated; an authorized administrator must create reports (Management Security Function). When a report is generated, the TOE fetches the Audit Events from the DBMS, formats the Audit Events in human readable format, formats the complete report, and stores the Audit Data Reports on disk using the OS' file I/O functionality (supplied by the IT Environment). An administrator must be assigned the Full Access To All Functionality or the group's Report/Audit/Audit Detail group permission at the Modify level in order to create or delete Audit Detail Reports. Once created, an administrator assigned the Full Access To All Functionality or the group's Report/Audit/Audit Detail group permission at the View or Modify level may view a list of all previously created reports and open each report.
An administrator may disable and re-enable generation of individual Audit Events. Audit Events are enabled and re-enabled by modifying one of seven selective auditing lists, referred to as Selective Auditing lists. These lists are organized according to audit record categories: General, Group, Agent, Asset, Policy, User Group and Report and modified based on event type. An administrator must be assigned the Full Access To All Functionality global permission or the Auditing Setup global permission in order to view and/or modify audit records generation lists.

An authorized user who has permission to view audit and system data may sort data, by event, type of event, subject identity, and the outcome (success or failure) of the event. This sorting is performed by the TOE once the SiteProtector has retrieved the information from the database via the DBMS.

6.1.2.4 Viewing – Alerts

Alarms are messages generated by the TOE, sent to the SiteProtector Console, and displayed in a SiteProtector Console window. Alarms are generated by the TOE under two conditions: 1) the TOE attempts to store audit records and the DBMS is full and 2) a potential intrusion is detected (Intrusion Detection Security Function). Alarms are displayed in a SiteProtector Console's window and therefore, any user who has successfully logged onto the SiteProtector Console may view alerts.

6.1.2.5 Selective Auditing – Audit Data

The Sensors and SiteProtector support selective auditing by allowing an Administrator to include or exclude auditable events from the set of auditable events based on event type. All of management actions defined in the Management Security Function are auditable and all audits may be disabled or enabled based on event type.

6.1.2.6 Audit Data and System Data Storage

Audit and system data are stored in the database via the DBMS through the use of the SiteProtector Event Collector and SiteProtector Sensor Controller components. Both subsystems collect events generated by the Sensors and store the data in the database via the DBMS. The IT Environment provides protection for the audit records stored in the DBMS from unauthorized deletion and unauthorized modification through interfaces outside the TSC. The TOE does communicate with the DBMS and receive indication of unsuccessful store attempts. If the database becomes full, the TOE receives a notification from the DBMS, and send an alarm to the SiteProtector Console. If the DBMS is full, the TOE will continue to store audit records by overwriting the oldest records in the database.

6.1.3 Management Security Function

The TOE's Management Security Function provides administrator support functionality that enables a human user to manage the TOE via a GUI interface (SiteProtector Console). After installation, all management of the TOE components occurs through SiteProtector.

User accounts must be defined in Windows (in the IT Environment). SiteProtector collects userid and password information through a GUI and passes that information to Windows to authenticate the user. If Windows indicates that the user is authenticated, SiteProtector looks up that userid in its database to determine the permissions associated with the user. If Windows indicates that the user is not authenticated, SiteProtector terminates the session.

Administrator permissions are individually configurable. User Accounts may also be associated with one or more groups, which may be used for efficiency to assign permissions to all members of a group rather than individual users.

The functions that administrators may perform are listed in the table below, along with the required permission.

Table 12: Permissions for Management Functions

Function	Permission
View user groups	View permission for the user group
Configure user groups	Modify permission for the user group
View user permissions	View permission for the object you want to grant permission to
Configure user permissions	Modify permission for the object you want to grant permission to
View groups	View permission for the groups
Configure groups	Modify permission for the groups
View assets	View permission for the assets
Configure assets	Modify permission for the assets

Function	Permission
View agents	View permission for the agents
Configure agents	Modify permission for the agents
View policies	View permission for the policies
Configure policies	Modify permission for the policies
Start and stop Agents	Control permission for the agents

The capabilities to perform these actions are enabled by the TSF based on the individual user's permissions. If the user is authorized to perform an action, then access to a GUI is allowed or fields within a GUI are not grayed out. Grayed out capabilities in the SiteProtector Console GUI are disabled and are therefore not available for use.

Authorized 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 traffic as being a security violation. The reactions (generating an email and/or SNMP trap) taken for specific events are also configured via the Policy Files.

SiteProtector provides GUI screens that enable an authorized user to control the Sensors. This functionality includes starting and stopping the sensing capability of the Sensors and applying Sensor Policy Files which define the enabled and disabled signatures for a Sensor. The Management Security Function also includes the modification of the system data collection, analysis and reaction capabilities of the TOE. These capabilities manage how the TOE collects, analyzes and reacts to data collected from the monitored network. Only an authorized Administrator (e.g., modify permission for the signatures) has the ability to modify or add system data (i.e., enable signatures in a policy files). An administrator with view permission for reports is allowed to query TSF data (i.e., view the audit trail).

6.1.4 Self Protection Security Function

The TOE's Self Protection Security Functionality provides self protection of the TOE by providing domain separation and non-bypassability for those functions within the TOE's scope of control. The TOE also provides a portion of the protection mechanism for communication between SiteProtector and Sensors.

The Proventia GX TOE component consists of hardware and software dedicated to providing IDS functionality to a monitored network. The Proventia GX TOE component provides non-bypassability by mediating its own interfaces and ensuring that the TSP is invoked and successful before allowing any other TSF-mediated action to proceed.

The Proventia GX TOE components have monitoring interfaces (also referred to as sensing interfaces) that are connected to the monitored network. The monitoring interfaces of the

Proventia GX component read packets from the monitored network and 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 GX TOE component. No other functionality is available through the Proventia GX monitoring interface. Further, the monitoring interfaces of the Proventia GX 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 GX TOE component is the management interface that communicates 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 GX TOE components to proceed.

TLS 1.0 is used to protect communication between the Sensors and SiteProtector. The TLS implementation is included in the TOE boundary in the Sensors and is part of the IT Environment with SiteProtector. The cipher suite used for the TLS session is TLS_RSA_WITH_3DES_EDE_CBC_SHA. The Sensors initiates the connection with SiteProtector. SiteProtector responds with its RSA certificate; the Sensors authenticate the server (SiteProtector) by comparing the SiteProtector-supplied certificate to the certificate saved on the Server during installation. The pre-master secret is generated with the Sensor's random number generator and sent back to SiteProtector encrypted with the public key from the certificate, and then both sides complete the key establishment phase. Subsequent data traffic is encrypted with 3DES operating with 168 bit keys in CBC mode. SHA-1 is used for message integrity checking. Session keys held in memory are zeroized (overwritten with all zeros) when a session ends. RSA certificates are generated by the IT Environment during installation of the TOE.

Also in accordance with NIAP Precedent PD-0097, FPT_ITT.1 has been added. With the Proventia GX component, this functionality is provided by the TOE. With the SiteProtector component, the functionality is provided by the IT Environment. Therefore, iterations have been levied on both the TOE and IT Environment with refinements to clarify the scope of each. On the SiteProtector Host, this functionality is provided by a third-party package (OpenSSL 0.9.7d[2]) that is not modified in any way by the vendor. The OpenSSL package executes as a DLL that is called from the TOE.

The Proventia GX TOE component maintains a domain for its own execution. The security domain of the Proventia GX TOE component consists of all hardware and software that makes up the Proventia GX appliance. The Proventia GX TOE components maintain this 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 GX TOE component. The monitoring interfaces of the Proventia GX TOE component only allows for the collection of

[2] **Note that OpenSSL 0.9.7d is not FIPS validated**

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 GX TOE component to have a security domain that protects it from interference and tampering.

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 an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the permissions are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a user session 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 by those users that are within the TSC. The TOE relies on the operating system to protect SiteProtector from interference from users outside the TSC.

SiteProtector provides graphical user interfaces (GUIs) used by users to manage and monitor the Sensor(s). 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. Human users must identify and authenticate themselves before being allowed to use the features of SiteProtector. Identification and authentication (performed by the IT Environment) establishes the user as an authorized user of SiteProtector and is necessary before they may carry out any action within the TSC.

The network and application interfaces of SiteProtector are interfaces that are used to collect data from and communicate with Proventia GX. The network and application interfaces are used to communicate only with the Proventia GX Sensors. Whenever the network and application communication interfaces of SiteProtector are used they invoke the TSP nenforcement functions before any other action that is to be carried out by the SiteProtector is allowed to proceed. The TOE provides protected storage of TSF data and requires identification and authentication of users which helps in providing and supporting non-bypassability of SiteProtector.

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.

6.1.5 Reaction Security Function

The Reaction Security Function provides the TOE's reaction capabilities when the analysis capability of the TOE has detected an intrusion (Intrusion Detection Security Function). When an intrusion is detected, the TOE will send an alarm to the SiteProtector Console where it can be viewed by an authorized user. The TOE can be configured to take several

additional actions on detected intrusions. These include generating an email to the System Administrator or generating an SNMP trap message. Delivery of the email or SNMP trap message is the responsibility of the IT Environment.

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 13: 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.
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.

Assurance Component	How requirement will be met
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 claims conformance to the Intrusion Detection System System Protection Profile Version 1.6, April 2006.

7.2 Protection Profile Refinements

In accordance with the errata sheets of the PP, the following SFRs have been moved to the IT Environment:

A) FPT_STM.1

B) FAU_STG.2

The TOE is a distributed system – an appliance in one case (Proventia GX) and application code in another (SiteProtector). FPT_SEP.1 and FPT_RVM.1 are levied on the TOE but have been iterated and refined to indicate that they only pertain to the Proventia GX component. These same SFRs are levied on the IT Environment as well and refined to indicate that they only pertain to the SiteProtector component.

In keeping with the rationale expressed in the errata sheets of the PP, IDS_STG.1 has been moved to the IT Environment.

An iteration of FIA_UAU.1 and FIA_UID.1 has been included in the IT Environment for the IT environment I&A functionality. The TOE collects the userid and password from the SiteProtector user, but this information is passed to Windows (the IT Environment) for authentication. The TOE prevents any other TSF-mediated actions if the authentication with Windows is not successful.

In accordance with NIAP Precedent PD-0097, the following items have been deleted:

A) FIA_AFL.1

B) FPT_ITA.1

C) FPT_ITC.1

D) FPT_ITI.1

E) O.EXPORT

Also in accordance with NIAP Precedent PD-0097, FPT_ITT.1 has been added. With the Proventia GX component, this functionality is provided by the TOE. With the SiteProtector component, the functionality is provided by the IT Environment. Therefore, iterations have been levied on both the TOE and IT Environment with refinements to clarify the scope of each. On the SiteProtector Host, this functionality is provided by a third-party package (OpenSSL) that is not modified in any way by the vendor. The OpenSSL package executes as a DLL that is called from the TOE.

7.3 Protection Profile Additions

In accordance with the errata sheets of the PP, the following IT Environment objectives have been added to the ST:

A) OE.TIME

B) OE.PROTECT

C) OE.AUDIT_PROTECTION

The mappings to threats, assumptions, and policies for these added objectives are also in accordance with the errata sheets of the PP.

OE.SD_PROTECTION has been added to the IT Environment objectives, corresponding to the move of IDS_STG.1 to the IT Environment.

OE.IDAUTH has been added to the IT Environment objectives, corresponding to the inclusion of of FIA_UAU.1 and FIA_UID.1 to the IT Environment.

FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 have been added to specify the cryptographic functionality of the TOE utilized to satisfy the FPT_ITT.1 requirement.

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 14 and Table 15 provide the mapping and rationale for the security objectives identified in Chapter 4 and the assumptions, threats and policies identified in Chapter 3.

Table 14: Threats, Assumptions, and Policies to Security Objectives Mapping

Threats, Assumptions, and Policies	**Security Objectives**																				
	O. PROTCT	**O.IDSCAN**	**O.IDSENS**	**O.IDANLZ**	**O.RESPON**	**O.EADMIN**	**O.ACCESS**	**O.IDAUTH**	**O.OFLOWS**	**O.AUDITS**	**O.INTEGR**	**O.INSTAL**	**O.PHYCAL**	**O.CREDEN**	**O.PERSON**	**O.INTROP**	**OE.TIME**	**OE.PROTECT**	**OE.AUDIT_PROTECTION**	**OE.SD_PROTECTION**	**OE.IDAUTH**
A.ACCESS																X					
A.DYNMIC															X	X					
A.ASCOPE																X					
A.PROTCT													X								
A.LOCATE													X								
A.MANAGE															X						
A.NOEVIL												X	X	X							
A.NOTRST													X	X							
T.COMINT	X						X	X			X							X			
T.COMDIS	X						X	X										X			
T.LOSSOF	X						X	X			X										
T.NOHALT		X	X	X			X	X													
T.PRIVIL	X						X	X													
T.IMPCON						X	X	X				X									
T.INFLUX									X											X	
T.FACCNT										X											
T.SCNCFG		X																			
T.SCNMLC		X																			
T.SCNVUL		X																			
T.FALACT					X																
T.FALREC				X																	
T.FALASC				X																	
T.MISUSE			X																		

Threats, Assumptions, and Policies	Security Objectives																			
	O. PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
T.INADVE			X																		
T.MISACT			X																		
P.DETECT		X	X							X							X				
P.ANALYZ				X																	
P.MANAGE	X					X	X	X				X		X	X						X
P.ACCESS	X						X	X											X	X	
P.ACCACT								X		X							X				
P.INTGTY											X										
P.PROTCT									X				X					X			

Table 15: Threats, Assumptions, and Policies to Security Objectives Rationale

Threats, Assumptions, and Policies	Security Objectives Rationale
A.ACCESS	The O.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will manage appropriately.
A.ASCOPE	The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The O.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

Threats, Assumptions, and Policies	Security Objectives Rationale
A.NOEVIL	The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
T.COMINT	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMDIS	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.LOSSOF	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.
T.PRIVIL	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

Threats, Assumptions, and Policies	Security Objectives Rationale
T.IMPCON	The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the audit trail.
T.FACCNT	The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
T.SCNMLC	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.
T.FALACT	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

Threats, Assumptions, and Policies	Security Objectives Rationale
T.INADVE	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISACT	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
P.DETECT	The O.AUDITS , O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data. The OE.TIME objective supports this policy by providing a time stamp on the SiteProtector Host for insertion into the audit records.
P.ANALYZ	The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.MANAGE	The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCESS	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives counter this threat via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.PROTECT objective supports the TOE protection from the IT Environment.
P.INTGTY	The O.INTEGR objective ensures the protection of data from modification.

Threats, Assumptions, and Policies	Security Objectives Rationale
P. PROTCT	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment.

8.2 Security Functional Requirements Rationale

The purpose of this section is to show that the identified security functional requirements are suitable to meet the security objectives.

Table 16 identifies each Security Functional Requirement and the security objective(s) that address it. Table 17 provides the mapping and rationale for inclusion of each requirement in this ST.

Table 16: TOE Security Functional Requirements to TOE Security Objectives Mapping

Security Functional Requirements (TOE)	Security Objectives (TOE)										
	O. PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_GEN.1										X	
FAU_SAR.1						X					
FAU_SAR.2							X	X			
FAU_SAR.3						X					
FAU_SEL.1						X				X	
FAU_STG.4									X	X	
FCS_CKM.1	X										
FCS_CKM.4(1)	X										
FCS_COP.1(1)	X										
FIA_ATD.1(1)								X			
FIA_UAU.1(1)						X	X				
FIA_UID.1(1)						X	X				
FMT_MOF.1	X						X	X			
FMT_MTD.1	X						X	X			X
FMT_SMR.1								X			

Security Functional Requirements (TOE)	Security Objectives (TOE)										
	O. PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FPT_ITT.1(1)	X										
FPT_RVM.1(1)	X					X		X		X	X
FPT_SEP.1(1)	X					X		X		X	X
FPT_STM.1(1)										X	
IDS_SDC.1		X	X								
IDS_ANL.1				X							
IDS_RCT.1					X						
IDS_RDR.1						X	X	X			
IDS_STG.2									X		

Table 17: TOE Security Functional Requirements to TOE Security Objectives Rationale

Security Objective (TOE)	Security Functional Requirement (TOE) Rationale
O.PROTCT	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE and modification of TSF data to authorized users of the TOE [FMT_MOF.1, FMT_MTD.1]. Only authorized users of the TOE may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Data must be protected from disclosure and modification as it travels to and from distributed TOE components [FPT_ITT.1(1)]. This protection is provided by cryptographic functionality [FCS_CKM.1, FCS_CKM.4(1), FCS_COP.1(1)].
O.IDSCAN	A system containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1].

Security Objective (TOE)	Security Functional Requirement (TOE) Rationale
O.IDSENS	A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].
O.IDANLZ	The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.RESPON	The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.EADMIN	The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized users to view all System data collected and produced [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1(1), FIA_UAU.1(1)]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1(1), FIA_UAU.1(1)]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1(1)]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized system administrators of the System may query and add System and audit data, and may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)].

Security Objective (TOE)	Security Functional Requirement (TOE) Rationale
O.OFLOWS	The TOE must prevent the loss of audit data in the event the audit trail is full [FAU_STG.4]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].
O.AUDITS	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Time stamps associated with an audit record must be reliable [FPT_STM.1(1)].
O.INTEGR	Only authorized users of the System may query or add audit and System data [FMT_MTD.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)].

The following tables identify each Security Functional Requirements levied on the IT Environment security objective(s) that address it and the rationale for inclusion of each security functional requirement in this ST.

Table 18: IT Environment Security Functional Requirements to IT Environment Security Objectives Mapping

Security Functional Requirements (IT Environment)	Security Objectives (IT Environment)				
	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
FAU_STG.2			X		
FCS_CKM.4(2)		X			
FCS_COP.1(2)		X			
FIA_ATD.1(2)					X

Security Functional Requirements (IT Environment)	Security Objectives (IT Environment)				
	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
FIA_UAU.1(2)					X
FIA_UID.1(2)					X
FPT_ITT.1(2)		X			
FPT_RVM.1(2)		X			
FPT_SEP.1(2)		X			
FPT_STM.1(2)	X				
IDS_STG.1				X	

Table 19: IT Security Objectives to IT SFR Rationale

Security Objectives (IT Environment)	Security Functional Requirement (IT Environment) Rationale
OE.TIME	Time stamps associated with an audit record must be reliable [FPT_STM.1(2)].
OE.PROTECT	The IT Environment must ensure that all functions are invoked and succeed on the SiteProtector Host before each function may proceed [FPT_RVM.1(2)]. The TSF must be protected from interference that would prevent it from performing its functions on the SiteProtector Host [FPT_SEP.1(2)]. The IT Environment also protects information being exchanged between distributed TOE components, which would be another attack vector for interference or tampering [FPT_ITT.1(2)]. This protection is provided by cryptographic functionality [FCS_CKM.4(2), FCS_COP.1(2)].
OE.AUDIT_PROTECTION	The IT Environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2].
OE.SD_PROTECTION	The IT Environment is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1].

Security Objectives (IT Environment)	Security Functional Requirement (IT Environment) Rationale
OE.IDAUTH	Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1(2), FIA_UAU.1(2)]. The IT Environment is able to associate a password with specific userids in order to perform authentication [FIA_ATD.1(2)].

8.2.1 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.

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 20: TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components	FPT_STM.1	Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components	FAU_SAR.1	Satisfied
FAU_SEL.1	No other components	FAU_GEN.1, FMT_MTD.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied
FCS_CKM.1	No other components	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	Satisfied Satisfied Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FCS_CKM.4	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Satisfied Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FCS_COP.1	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied Satisfied Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FIA_ATD.1(1)	No other components	None	N/A
FMT_MOF.1	No other components	FMT_SMF.1, FMT_SMR.1	See the note following the table, Satisfied
FMT_MTD.1	No other components	FMT_SMF.1, FMT_SMR.1	See the note following the table Satisfied
FMT_SMR.1	No other components	FIA_UID.1	Satisfied by FIA_UID.1(1)
FPT_ITT.1(1)	No other components	None	N/A
FPT_RVM .1(1)	No other components	None	N/A
FPT_SEP.1(1)	No other components	None	N/A
FPT_STM.1(1)	No other components	None	N/A
IDS_SDC.1	N/A	N/A	N/A
IDS_ANL.1	N/A	N/A	N/A
IDS_RCT.1	N/A	N/A	N/A
IDS_RDR.1	N/A	N/A	N/A
IDS_STG.2	N/A	N/A	N/A

Note concerning FMT_SMF.1 - Prior to the publication and verification of the IDS System PP, International Interpretation #65 was finalized. This interpretation introduced a new family of Security Management requirements, Specification of Management Functions (FMT_SMF). While this should not normally affect dependency rationale, that interpretation introduces dependencies from FMT_MOF.1 and FMT_MTD.1, both contained in this Security Target. Hence, it seems as though some FMT_MSA security requirements should be added to this Security Target to fulfil those dependencies. However, while the IDS System PP is clearly intended to ensure that certain security management functions are controlled if they are made available, it is not evident from the IDS System PP which, if any, of those security management functions must be present in the first place. This Security Target identifies all applicable security management functions in the TOE and explains how they are appropriately controlled and it is effectively unnecessary to introduce a security functional requirement to demand that certain security management functions must be present.

Table 21: IT Environment Security Functional Requirements Dependency Rationale

Security Functional Requirement (IT Environment)	Hierarchical To	Dependency	Rationale
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied by the TOE
FCS_CKM.4	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Satisfied Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FCS_COP.1	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Satisfied Satisfied Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FIA_ATD.1(2)	No other components	None	N/A
FIA_UAU.1(1)	No other components	FIA_UID.1	Satisfied by FIA_UID.1(1)
FIA_UID.1(1)	No other components	None	N/A
FPT_ITT.1(2)	No other components	None	N/A
FPT_RVM .1(2)	No other components	None	N/A
FPT_SEP.1(2)	No other components	None	N/A
FPT_STM.1(2)	No other components	None	N/A
IDS_STG.1	N/A	N/A	N/A

8.2.2 TOE Security Assurance Component Dependencies

The following table identifies the Security Assurance Components and the Security Assurance Components each are dependent upon and any necessary rationale.

Table 22: EAL2 Assurance Requirement Dependency Satisfaction

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
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, ADV_HLD.1 AGD_ADM.1, AGD_USR.1	Yes

8.3 TOE Security Functions

This section demonstrates the suitability of the security functions of meeting the TOE's Security Functional Requirements and that the Security Functions are completely and accurately met by the Security Functional Requirements.

Table 23: TOE Security Functional Requirement to Security Functions Mapping

Security Functional Requirements (TOE)	Security Functions				
	Audit Security Function	Intrusion Detection Security Function	Management Security Function	Self Protection Security Function	Reaction Security Function
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.4	X				
FCS_CKM.1				X	
FCS_CKM.4(1)				X	
FCS_COP.1(1)				X	
FIA_ATD.1(1)	X		X		
FIA_UAU.1(1)			X		
FIA_UID.1(1)			X		
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMR.1			X		
FPT_ITT.1(1)				X	
FPT_RVM.1(1)				X	
FPT_SEP.1(1)				X	
FPT_STM.1(1)	X				
IDS_SDC.1	X	X			
IDS_ANL.1	X	X			
IDS_RCT.1	X				X
IDS_RDR.1	X				

Security Functional Requirements (TOE)	Security Functions				
	Audit Security Function	Intrusion Detection Security Function	Management Security Function	Self Protection Security Function	Reaction Security Function
IDS_STG.2	X				

Table 24: TOE Security Functional Requirement to TOE Security Functions Rationale

Security Functional Requirements (TOE)	Security Function Rationale
FAU_GEN.1	Audit Security Function – The TOE generates audit records reporting the security relevant management actions including modification of TSF Data, modification of user permissions, and modification of TOE system behavior. All management functions defined in the Management Security Function are audited. Included in each audit record is date and time, type of event, identity of the system that generated the record, and outcome of event.
FAU_SAR.1	Audit Security Function – The TOE enables authorized administrators to view all audit records generated as the result of a management event including modification to TSF data and modification of TSF behavior. Only authorized users who have successfully authenticated to the SiteProtector OS (IT Environment supplied Windows OS) and who have been configured as a valid user in SiteProtector and have permission to view audit records may view audit records. Permissions are configured on a user or group bases. All audit record viewing is done via the SiteProtector Console which supplies a GUI interface for human users.
FAU_SAR.2	Audit Security Function – Only authorized users who have successfully authenticated to the SiteProtector OS (IT Environment supplied Windows OS) and who have been configured as a valid user in SiteProtector (via the TOE's Management Security Function) and who have been configured to view audit records may view audit records. Audit data is not available to users who have not met the above criteria.
FAU_SAR.3	Audit Security Function – The TSF provides users sorting capabilities of

Security Functional Requirements (TOE)	Security Function Rationale
	audit data via the SiteProtector Console. Audit data is retrieved by the TOE from the DBMS. Once retrieved, authorized users may sort audit data based on all fields displayed including date and time, type of event, success or failure of event and identify of the system that generated the event.
FAU_SEL.1	Audit Security Function – The audit records generated by the TOE as the result of any management activity may be disabled according to event type. Event types include starting and stopping auditing, logging into and out of SiteProtector; viewing audit and system data; any modifications to disable or enable audit records and system data; and any modifications to the behavior of the TOE including starting and stopping Sensors.
FAU_STG.4	Audit Security Function – The SiteProtector Event Collector communicates with the DBMS to store audit records. When the DBMS becomes full, the DBMS sends a message to the TOE. The TOE in turn will generate an alarm and send it for display to the SiteProtector Console. Once full, the TOE will instruct the DBMS to store new audit records, overwriting the old audit records.
FCS_CKM.1	Self Protection Security Function – The TOE's Sensors protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by using TLS. The TOE generates a session key for the TLS session.
FCS_CKM.4(1)	Self Protection Security Function – The TOE's Sensors protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by using TLS. When a session ends, the key is zeroized.
FCS_COP.1(1)	Self Protection Security Function – The TOE's Sensors protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by using TLS. The encryption algorithm is 3DES (EDE CBC), RSA is used for key establishment, and message integrity uses SHA-1.
FIA_UAU.1(1)	Management Security Function – The SiteProtector collects username and password information through the SiteProtector GUI and passes that information to Windows to authenticate/authenticate the user.
FIA_UID.1(1)	Management Security Function - The SiteProtector collects username and password information through the SiteProtector GUI and passes that information to Windows to identify/authenticate the user.
FIA_ATD.1(1)	Management Security Function – SiteProtector interacts with the OS to determine if a 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 on through the SiteProtector logon screen. The user profile defines the permissions of the user. The TSF uses this user profile to determine what management functions a user has or does not have access to.

Security Functional Requirements (TOE)	Security Function Rationale
	Audit Security Function – SiteProtector interacts with the OS 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 on through the SiteProtector logon screen. The user profile defines the permissions of the user. The TSF uses this user profile to determine what audit data and system data a user has access to or does not have access to.
FMT_MOF.1	Management Security Function – The TSF provides for the capability of authorized users to manage the TOE. Management access is via the SiteProtector Console GUI. Management actions include enabling and disabling signatures, starting and stopping Sensors, and publishing policies.
FMT_MTD.1	Management Security Function – The TSF provides the capability for authorized users to modify TSF data. . Management access is via the SiteProtector Console GUI. Data that can be modified includes enabling and disabling signatures pointed to by a Policy File, assigning permissions to users, assigning users to groups, and configuring reaction to IDS events.
FMT_SMR.1	Management Security Function - The TSF maintains an internal user profile that defines the permissions of a user. The permissions define what capabilities the user has when using the SiteProtector Console. An authorized administrator is any user who has defined within SiteProtector and been assigned permissions.
FPT_ITT.1(1)	Self Protection Security Function - The TOE's Sensors protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. This refers to information that is communicated between SiteProtector and Proventia GX that is protected by TLS.
FPT_RVM .1(1)	Self Protection Security Function - The TOE's Sensors ensures that the TSP enforcement functions are invoked and succeed before any other TSF-mediated actions occur.
FPT_SEP.1(1)	Self Protection Security Function - The TOE's Sensors maintains a domain for their own execution that is protected from tampering and corruption by untrusted subjects.
FPT_STM.1(1)	Audit Security Function - The TOE's Sensors generate and maintains reliable timestamps for used for auditing and system data.
IDS_SDC.1	Intrusion Detection Security Function – The TOE collects network traffic for analysis in support of the IDS functionality. The TOE compares this traffic to packets and packet patterns (signatures) that indicate a potential security violation. Audit Security Function - The TOE will generate a system data record if the analysis of network traffic indicates a potential security violation.

Security Functional Requirements (TOE)	Security Function Rationale
	Included in the result is event type, date and time, source IP address.
IDS_ANL.1	Intrusion Detection Security Function - The TOE provides signature analysis capability in support of identification of malicious activity on the monitored network Audit Security Function - The TOE will generate an audit record if the analysis of network traffic indicates a potential security violation. Included in the result is event type, date and time, source IP address.
IDS_RCT.1	Reaction Security Function - The TOE generates an alert upon detection of a potential security violation as the result of collecting and analyzing network traffic. The TOE sends the alert to the SiteProtector Console where it can be viewed by any logged on administrator. The TOE can be configured to take additional actions in response to a signature match including generating an e-mail and/or generating an SNMP trap. Audit Security Function – Alerts are available for viewing via the SiteProtector Console by an authorized Administrator. Alerts are displayed in a SiteProtector Console window and available for reading by any Administrator who is logged onto the SiteProtector Console.
IDS_RDR.1	Audit Security Function - The TOE enables Administrators to view system data (events) generated by the TOE as the result of collecting network data and comparing this data to signatures. This system data is viewable via the SiteProtector Console by authorized Administrators who have explicit read permissions to system data.
IDS_STG.2	Audit Security Function – The TOE stores system data in the TOE's database via the IT Environment supplied DBMS. When the system data storage has reached capacity in the DBMS, the TOE will generate and send an alert to the SiteProtector Console and direct the DBMS to overwrite the oldest stored system data for further store system data requests. Alerts are displayed in a SiteProtector Console window and available for reading by any Administrator who is logged onto the SiteProtector Console.

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. This is consistent with the security objectives defined in the Intrusion Detection System System Protection Profile Version 1.6 April 2006, which is the PP to which this ST claims compliance.

8.6 Rationale for Explicitly Stated SFR for the TOE

The IDS class FAU_GEN.1 was created to include functionality appropriate for the TOE to audit according to the technology being evaluated.

8.7 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.