Security Target

IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1

Document Version 0.7

April 30, 2012

Security Target: IBM Internet Security Systems GX Series Security Appliances Version 4.1 and SiteProtector Version 2.0 Service Pack 8.1

Prepared For:

IBM Internet Security Systems, Inc.

6303 Barfield Road

Atlanta, GA 30328

www.iss.net

Prepared By:

Apex Assurance Group, LLC

530 Lytton Ave, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ST Revision	0.7
ST Publication Date	April 30, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
Analyzer data	Data collected by the Analyzer functions
Analyzer functions	The active part of the Analyzer responsible for performing intrusion analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.
Assets	Information or resources to be protected by the countermeasures of a TOE.
Attack	An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.

[1] Derived from the IDSPP

TERM	DEFINITION
Audit	The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
Audit Trail	In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
Authentication	To establish the validity of a claimed user or object.
Authorized Administrator	A subset of authorized users that manage an IDS component
Authorized User	A user that is allowed to perform IDS functions and access data
Availability	Assuring information and communications services will be ready for use when expected.
CC	Common Criteria version 3.1
Compromise	An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
Confidentiality	Assuring information will be kept secret, with access limited to appropriate persons.
EAL	Evaluation Assurance Level
Evaluation	Assessment of a PP, a ST or a TOE, against defined criteria.
External IT Product	A device, workstation, or other system used in a trusted environment that interacts with the TOE (e.g., the workstation hosting the Site Protector management application for administration of the TOE)
IDS component	A Sensor, Scanner, or Analyzer
IDSPP	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSPP)
Information Technology (IT) System	May range from a computer system to a computer network
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion	Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection	Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
Intrusion Detection System (IDS)	A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity that may inappropriately affect the IT System's assets and react appropriately.
Intrusion Detection System Analyzer (Analyzer)	The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
Intrusion Detection System Scanner (Scanner)	The component of an IDS that collects 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.

TERM	DEFINITION
Intrusion Detection System Sensor (Sensor)	The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
IT Product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
Network	Two or more machines interconnected for communications.
OSP	Organizational Security Policy
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Sniffer	A device or program that monitors the data traveling between computers on a network
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Remote Trusted IT Product	A device, workstation, or other system used in a trusted environment that interacts with the TOE (e.g., the workstation hosting the Site Protector management application for administration of the TOE)[2]
Scanner data	Data collected by the Scanner functions
Scanner functions	The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
Security	A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE
Sensor data	Data collected by the Sensor functions
Sensor functions	The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data)
SFP	Security Function Policy
SFR	Security Functional Requirement
SiteProtector	SiteProtector Version 2.0 Service Pack 8.1
ST	Security Target
Target of Evaluation (TOE)	An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Threat	The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security
TOE	Target of Evaluation
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

[2] Note that the definitions are the same for External IT Product and Remote Trusted IT Product. These terms were derived from the IDSPP.

TERM	DEFINITION
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
Trojan Horse	An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
TSF	TOE Security Function
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Virus	A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.
Vulnerability	Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Description

1.6.1 Summary

The TOE is an automated real-time intrusion detection system (IDS) designed to monitor and protect IPv4 and IPv6 (simultaneously) network segments with Network Intrusion Protection System (NIPS) or passive mode (IDS) functionality. The TOE unobtrusively analyses and responds to activity across computer networks. The TOE is comprised of two components:

1. The Proventia GX Series Appliances TOE component (hereafter referred to as the appliance(s), GX, GX Series, GX Appliance(s), Sensor, Agent, or as stated) provides IDS security functionality. This component includes the Proventia GX appliance hardware, the appliance resident Red Hat operating system (OS) and the Proventia GX application software image.

2. The SiteProtector Version 2.0 Service Pack 8.1 with Reporting Module component of the TOE (hereafter referred to as SiteProtector or as stated) is a software product that runs on a Microsoft Windows-based workstation and enables administrators to monitor and manage the Sensor components of the TOE.

The Proventia GX Series TOE component provides the IDS functionality; it 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, the Proventia GX Series will create an audit

record. The SiteProtector Version 2.0 Service Pack 8.1 with Reporting Module TOE component provides management, monitoring and configuration functions to administrators. The SiteProtector management workstation connects to the appliance via TLS session, and this workstation is only used by authorized administrators for the management of the appliance.

1.6.2 TOE Functionality Overview

1.6.2.1 Proventia GX Series

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. A single appliance can provide both IDS and IPS functionality.

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.

1.6.2.2 SiteProtector Version 2.0 Service Pack 8.1with Reporting Module

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

- Manages and monitors Sensors and SiteProtector sub-components;
- Enables an administrator to view TOE component configuration data;
- Displays audit and system data records; and
- Monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

The SiteProtector is divided into the following software sub-components:

- 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:
    - Vulnerability Assessment reports
    - Attack Activity reports
    - User Audit reports
    - Content Filtering reports
    - User Permission reports

- 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.
- 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.
- 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.

1.6.3 Physical Boundary

The TOE is a combined hardware/software TOE and is defined as the GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER	
TOE Software	Site Protector	Version 2.0 Service Pack 8.1 with Reporting Module
	Proventia GX	Version 4.3
	Operating System	Red Hat Version 8.0
TOE Hardware	Proventia GX3002, GX4002, GX4004, GX5008, GX5108, GX5208, GX6116	
IT Environment	Common Criteria Evaluated Version of Microsoft Windows[3]	

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below (note that TOE components are shaded):

[3] A list of compatible versions of Windows can be found in Table 4 – Hardware and Software Requirements for IT Environment. A list of Microsoft Windows Common Criteria evaluations can be found at www.commoncriteriaportal.org

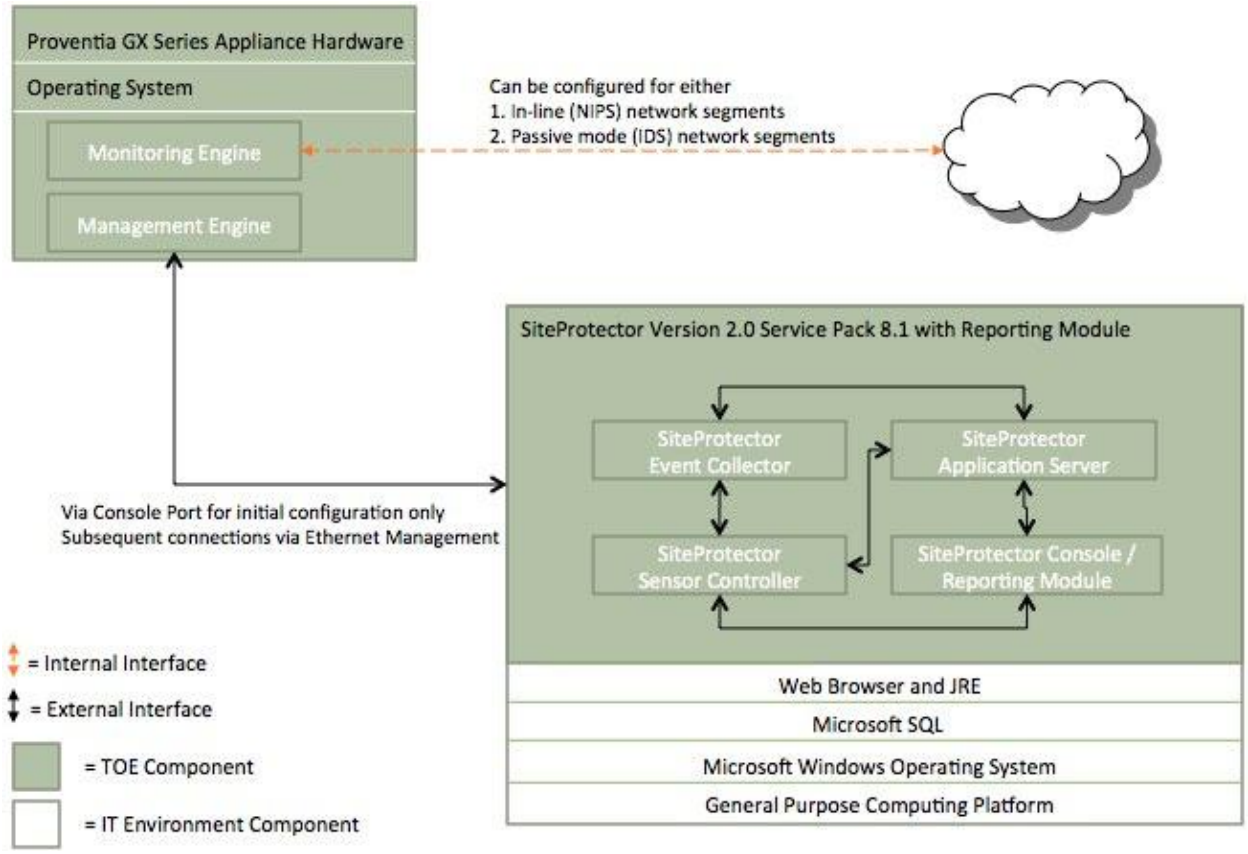

Figure 1 – TOE Boundary

The TOE interfaces are comprised of the following:

1. Network interfaces (also known as monitoring or sensing interfaces) which receive traffic from the monitored interface
2. Management interface through which handle administrative actions. This connection is secured via TLS tunnel, and the GX appliance and SiteProtector component communication is protected by TLS (cryptographic functionality provided by OpenSSL v1.1.2).

The TOE's evaluated configuration requires one or more instances of a Sensor TOE component (Proventia GX series) and one instance of a workstation running SiteProtector Version 2.0 Service Pack 8.1 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. Incidents and Exceptions are disabled.
2. All TOE updates should be disabled. 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.

3. SiteProtector components are resident on one workstation (a remote SiteProtector Console is not supported in the evaluated configuration).
4. SiteProtector components and the DBMS implementation reside on one workstation.
5. Proventia GX and SiteProtector communicate via TLS.
6. After the initial configuration, management via local console is not included in the evaluated configuration.
7. SiteProtector must run on a Common Criteria evaluated version of Microsoft Windows.
8. The Console Port must not be used after the initial configuration. All subsequent configuration occurs via SiteProtector.
9. Management via Proventia Manager is not included in the evaluation, and Proventia Manager should not be used in evaluated configuration. All management of the TOE occurs through the SiteProtector application.

Note that the SiteProtector runs on a dedicated workstation; applications not essential to the operation of the TOE are not installed on the workstation.

1.6.4 Hardware and Software Supplied by the IT Environment

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

Component	Minimum Requirement
Processor	1 GHz Pentium III Dual 3.0 GHz Pentium 4 (recommended)
Operating system	SiteProtector supports both 32- and 64-bit versions of the following Windows operating systems: • Windows Server 2008 Standard • Windows Server 2008 Enterprise • Windows Server 2003 SP2 Standard Edition • Windows Server 2003 SP2 Enterprise Edition Note: You must run SiteProtector and its components on an NTFS formatted partition. FAT and FAT32 partitions do not allow you to harden your system properly. Note: See Technote #1435194 for more information about Windows Firewall.
RAM	1 GB 2 GB (recommended)
Free hard disk space	8 GB 70 GB (recommended)
Screen resolution	1024 by 768 pixels
Third-party software (included)	IBM Java Runtime Environment (JRE), Version 1.6.0 SR7

Component	Minimum Requirement
Third-party software (not included)	• SQL Server 2008 Enterprise Edition • SQL Server 2008 Standard Edition • SQL Server 2008 64-bit • SQL Server 2005 Enterprise Edition • SQL Server 2005 Standard Edition • SQL Server 2005 64-bit • SQL Server 2008 Express Edition • Internet Explorer 7.0 or later http://www.microsoft.com/windows/internetexplorer/default.aspx • Adobe Reader 8.0 or later http://www.adobe.com/products/acrobat/ readstep2.html • For the latest updates for Windows operating system software and Windows-based hardware, go to the Microsoft Update Web site at http:// www.windowsupdate.com

Table 4 – Hardware and Software Requirements for IT Environment

1.6.5 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	The TOE provides an audit feature for actions related to operator authentication attempts and administrator actions. Audit data is protected from unauthorized viewing, and viewing can be customized.
Identification and Authentication	The TOE requires operators to be successfully authenticated before any actions can be performed. 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.
Security Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Security Audit and Traffic Analysis.
Traffic Analysis	The TOE collects information on traffic flowing from TOE ingress points to egress points and analyzes the data against rules defined by an administrator to determine whether the traffic should be allowed or should be dropped.
Protection of Management Functions	The TOE protects the connection between the SiteProtector and appliance TOE components with a TLS tunnel.

Table 5 – Logical Boundary Descriptions

1.7 Rationale 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.

1.7.1 Proventia GX Series TOE Component

The Proventia GX Series TOE component consists of hardware and software dedicated to providing IDS functionality to a monitored network. The Proventia GX Series 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.

This TOE component has monitoring interfaces (also referred to as sensing interfaces) that are connected to the monitored network. The monitoring interfaces of the appliance 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 appliance TOE component. No other functionality is available through the monitoring interface. Further, the monitoring interfaces of the appliances 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 Series 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 appliance TOE components to proceed.

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

1.7.2 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.

Note that the FCS class requirements included in this evaluation apply only to the Proventia GX Series TOE Component. Though the link between SiteProtector and the appliances is protected via TLS, the IT Environment provides the cryptography from SiteProtector side.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented with ALC_FLR.2.

2.2 Protection Profile Conformance Claim

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (IDSPP).

2.3 Package Claim

The TOE claims conformance to the Interim Basic assurance package as defined by the Consistency Instruction Manual for Interim Basic Robustness Environments and summarized in the IDSPP.

2.4 Conformance Rationale

All applicable Security Functional Requirements and Security Assurance Requirements are satisfied in accordance with the IDSPP and with relevant NIAP Precedents.

2.4.1 Protection Profile Refinements

The TOE is a distributed system – an appliance in one case and application code in another (SiteProtector). IDS_STG.1, FIA_UAU.1 and FIA_UID.1 have been moved to the IT Environment. 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:

- FIA_AFL.1
- FPT_ITA.1
- FPT_ITC.1
- FPT_ITI.1
- O.EXPORT

With the Proventia GX component, functionality defined in FPT_ITT.1(1) 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.

2.4.2 Protection Profile Additions

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 move 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(1) requirement.

IDS_RCT.1 has been iterated to address both IDS and IPS functionality. The former is addressed by IDS_RCT.1 (1), and the latter is addressed by IDS_RCT.1 (2).

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
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.

Table 6 – Threats Addressed by the TOE

The IT System addresses the following threats:

THREAT	DESCRIPTION

THREAT	DESCRIPTION
T.SCNCFG	Improper security configuration settings 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.

Table 7 – Threats Addressed by the IT System

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

THREAT	DESCRIPTION
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.

Table 8 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
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, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

Table 9 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
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, use of the System functions, and the results of the TOE's detection/filtering functions[4]
O.INTEGR	The TOE must ensure the integrity of all audit and System data.

Table 10 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.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.

[4] Objective expanded to include audit capabilities of IPS functionality

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.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.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
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.

Table 11 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREATS/ ASSUMPTION	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.IDAUTH	OE.SD_PROTECTION
A.ACCESS																			✓		
A.DYNMIC																		✓	✓		
A.ASCOPE																			✓		
A.PROTCT																✓					
A.LOCATE																✓					
A.MANAGE																		✓			
A.NOEVIL															✓	✓	✓				
A.NOTRST																✓	✓				
T.COMINT	✓						✓	✓			✓										
T.COMDIS	✓						✓	✓													
T.LOSSOF	✓						✓	✓			✓										
T.NOHALT		✓	✓	✓			✓	✓													
T.PRIVIL	✓						✓	✓													
T.IMPCON						✓	✓	✓							✓						
T.INFLUX									✓												✓
T.FACCNT										✓											
T.SCNCFG		✓																			

OBJECTIVE / THREATS/ ASSUMPTION	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.IDAUTH	OE.SD_PROTECTION
T.SCNMLC		✓																			
T.SCNVUL		✓																			
T.FALACT					✓																
T.FALREC				✓																	
T.FALASC				✓																	
T.MISUSE			✓																		
T.INADVE			✓																		
T.MISACT			✓																		
P.DETECT		✓	✓							✓				✓							
P.ANALYZ				✓																	
P.MANAGE	✓					✓	✓	✓							✓		✓	✓			✓
P.ACCESS	✓						✓	✓				✓								✓	✓
P.ACCACT								✓		✓			✓	✓							
P.INTGTY											✓										
P.PROTCT									✓							✓					

Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The OE.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.ASCOPE	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.NOEVIL	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.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.
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.
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.
T.IMPCON	The OE.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.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
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	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 configuration setting change. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
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. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
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. The Scanner/Monitoring Engine component of the TOE specifically addresses this threat.
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.
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.
P.ANALYZ	The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.MANAGE	The OE.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 OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE_IDAUTH objective by only permitting authorized users to access TOE functions. The OE.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.
P.INTGTY	The O.INTEGR objective ensures the protection of data from modification.
P.PROTCT	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

Table 13 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Definition of Extended Components

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS and to maintain compliance to the aforementioned Protection Profile. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3(1)	Selective Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.4	Prevention of Audit Data Loss
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
Identification and Authentication	FIA_ATD.1(1)	User Attribute Definition
	FIA_UAU.1(1)	Timing of Authentication
	FIA_UID.1(1)	Timing of Identification
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1(1)	Internal TOE TSF Data Transfer
	FPT_STM.1(1)	Reliable Time Stamps
Traffic Analysis	IDS_SDC.1 (EXT)	System Data Collection
	IDS_ANL.1 (EXT)	Analyzer Analysis
	IDS_RCT.1(1) (EXT)	Analyzer React (IDS)
	IDS_RCT.1(2) (EXT)	Analyzer React (IPS)
	IDS_RDR.1 (EXT)	Restricted Data Review
	IDS_STG.2 (EXT)	Prevention of System data loss

Table 14 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 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:

- Start-up and shutdown of the audit functions;
- All auditable events for the *basic* level of audit;
- [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:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- **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 15 – Auditable Events.

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1(1)	All use of the authentication mechanism	User identity, location
FIA_UID.1(1)	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 15 – Auditable Events

].

6.1.1.2 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 Table 15 – Auditable Events] 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.

6.1.1.3 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.

6.1.1.4 FAU_SAR.3(1) – Selectable Audit Review

FAU_SAR.3.1 (1)	The TSF shall provide the ability to apply [sorting] of audit data based on [date and time, subject identity, type of event, and success or failure of related event].

6.1.1.5 FAU_SEL. – Selective Audit

FAU_SEL.1.1	The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes: a) *event type* b) [no additional attributes].

Application Note: "event type" is defined by one of the following categories of events: ***Audit events*** *match network traffic that seeks information about the network, and* ***Attack events*** *match network traffic that seeks to harm the network.*

6.1.1.6 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.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 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: [X9.31 A.2.4 (TDES) and CAVP certificate 652].

6.1.2.2 FCS_CKM.4 –Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [FIPS 140-2 and CMVP certificate 1402] .

6.1.2.3 FCS_COP.1 –Cryptographic Operation

FCS_COP.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]:

Operation	Algorithm (mode)	Key Size in Bits	Standard
Encryption and decryption	AES	256	FIPS 197 (CAVP certificate 1181)
Key establishment	RSA	1024 (modulus)	RFC2246 (CAVP certificate 562)
Hashing	SHS	128	FIPS 180-2 (CAVP certificate 1090)
Random number generation	X9.31 A.2.4 (TDES)	n/a	X9.31 A.2.4 (TDES) (CAVP certificate 652)

Table 16 – Cryptographic Operations

6.1.3 Identification and Authentication (FIA)

6.1.3.1 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*;

d) [User group memberships;

e) User assigned group permissions and group permission level].

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). It is also the groups and permissions terms used by the vendor.

6.1.3.2 FIA_UAU.1(1) – Timing of Authentication

FIA_UAU.1.1 (1) The TSF shall allow [no administrative 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.

6.1.3.3 FIA_UID.1(1) – Timing of Identification

FIA_UID.1.1 (1) The TSF shall allow [no administrative 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.

6.1.4 Security Management

6.1.4.1 FMT_MOF.1 – Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behavior of* the functions [of System data collection, analysis and reaction] to [system administrators and authorized administrators with explicit permissions to perform these actions].

6.1.4.2 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].

6.1.4.3 FMT_SMR.1 – Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [authorized administrator (which can be either a Global Administrator, Group Owner, or Group Member depending on the

associated permissions; see Section 7.4 – Security Management for more details)].

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 and FMT_MOF.1. In this ST, FIA_AFL.1 has been deleted per PD-0097. Therefore, in this ST, the role "authorized administrator" refers to authorized users of SiteProtector whose permissions explicitly include view and configure assets, agents and policies as well as start and stop agents.

6.1.5 Protection of the TOE Security Functions

6.1.5.1 FPT_ITT.1(1) – Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1(1) The TSF shall protect TSF data from *disclosure* **and** *modification* when it is transmitted between separate parts of the TOE.

6.1.5.2 FPT_STM.1(1) – Reliable Time Stamps

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

6.1.6 Traffic Analysis Component Requirements

6.1.6.1 IDS_SDC.1 – System Data Collection (EXT)

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 17 – System Events. (EXT)

COMPONENT	EVENT	DETAILS
IDS_SDC.1	Network traffic	Protocol, source address, destination address

Table 17 – System Events

6.1.6.2 IDS_ANL.1 – Analyzer Analysis (EXT)

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

a) *signature* and

b) [matching to limited traffic flow rules].

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, identification of data source; and

b) [no other security relevant information about the result].

6.1.6.3 IDS_RCT.1(1) – Analyzer React (IDS Functionality)

IDS_RCT.1.1(1) The System shall send an alarm to [the Site Protector Console] and take [the following actions: notify the administrator's designated personnel via email and/ or generate an SNMP trap message] when an intrusion is detected.

6.1.6.4 IDS_RCT.1(2) – Analyzer React (IPS Functionality)

IDS_RCT.1.1(2) The System shall send an alarm to [the Site Protector Console] and take [the following actions: notify the administrator's designated personnel via email, quarantine the network against attacks by blocking the originating IP address, and/ or generate an SNMP trap message] when an intrusion is detected.

6.1.6.5 IDS_RDR.1 – Restricted Data Review

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.

6.1.6.6 IDS_STG.2 – Prevention of System data loss (EXT)

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

6.2 IT Environment Security Functional Requirements

6.2.1 Security Audit

6.2.1.1 FAU_SAR.3(2) – Selectable Audit Review

FAU_SAR.3.1 (2)	The ~~TSF~~ **IT Environment** shall provide the ability to apply [sorting] of audit data based on [date and time, subject identity, type of event, and success or failure of related event].

6.2.1.2 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* modifications to the audit records.
FAU_STG.2.3	The ~~TSF~~ **IT Environment** shall ensure that [stored] audit records will be maintained when the following conditions occur: *failure*.

6.2.2 Identification and Authentication

6.2.2.1 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).

6.2.2.2 FIA_UAU.1(2) – Timing of Authentication

FIA_UAU.1.1 (2)	The ~~TSF~~ **IT Environment** shall allow [no 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).

6.2.2.3 FIA_UID.1(2) – Timing of Identification

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

FIA_UID.1.2 (2) The T~~SF~~ **IT Environment** SF 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).

6.2.3 Protection of the TOE Security Functions

6.2.3.1 FPT_ITT.1(2) – Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 (2) The ~~TSF~~ **IT Environment** shall protect TSF data from *disclosure* **and** *modification* when it is transmitted between separate parts of the TOE.

6.2.3.2 FPT_STM.1(2) – Reliable time stamps

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

6.2.4 Traffic Analysis Component Requirements

6.2.4.1 IDS_STG.1 – Guarantee of System Data Availability

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

IDS_ STG.1.2 The ~~TSF~~ **IT Environment** shall protect the stored System data from modification.

IDS_ STG.1.3 The ~~TSF~~ **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*.

6.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-Enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 18 – Security Assurance Requirements at EAL2

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.TIME
FAU_GEN.1										✓				
FAU_SAR.1						✓								
FAU_SAR.2							✓	✓						
FAU_SAR.3(1)						✓							✓	
FAU_SEL.1						✓				✓				
FAU_STG.4									✓	✓				
FCS_CKM.1	✓													
FCS_CKM.4	✓													

SFR \ OBJECTIVE	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.TIME
FCS_COP.1	✓													
FIA_ATD.1(1)								✓						
FIA_UAU.1(1)							✓	✓						
FIA_UID.1(1)							✓	✓						
FMT_MOF.1	✓						✓	✓						
FMT_MTD.1	✓						✓	✓			✓			
FMT_SMR.1								✓						
FPT_STM.1(1)										✓				✓
FPT_ITT.1(1)	✓													
IDS_SDC.1 (EXT)		✓	✓											
IDS_ANL.1 (EXT)				✓										
IDS_RCT.1(1) (EXT)					✓									
IDS_RCT.1(2) (EXT)					✓									
IDS_RDR.1 (EXT)						✓	✓	✓						
IDS_STG.2 (EXT)									✓					

Table 19 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.PROTCT	The System 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]. 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]. 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, FCS_COP.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].

OBJECTIVE	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(1) for IDS functionality and IDS)RCT.1(2) for IPS functionality].
O.EADMIN	The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.2, FAU_SAR.3(1), FAU_SEL.1]. The System must provide the ability for authorized administrators 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)].
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]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.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]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1(1), FIA_UAU.1(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]. The System 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 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 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]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

OBJECTIVE	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 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]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].
O.AUDITS	[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]. Time stamps associated with an audit record must be reliable [FPT_STM.1(1)].
O.INTEGR	System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1].

Table 20 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Functional Requirements for the IT Environment

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.

OBJECTIVE / SFR	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.SD_PROTECTION	OE.TIME	OE.IDAUTH
FAU_SAR.3(2)		✓			
FAU_STG.2	✓				
FIA_ATD.1(2)					✓
FIA_UAU.1(2)					✓
FIA_UID.1(2)					✓
FPT_STM.1(2)				✓	
IDS_STG.1			✓		
FPT_ITT.1(2)			✓		

Table 21 – Mapping of IT Environment SFRs to Security Objectives

The following table provides detailed evidence of coverage for each IT Environment security objective:

OBJECTIVE	RATIONALE
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]. The IT Environment must prevent the loss of audit data in the event the audit trail is full [FAU_STG.4].
OE.AUDIT_SORT	The IT environment must provide the ability to review and manage the audit trail of the System to include sorting the audit data [FAU_SAR.3(2)].
OE.TIME	The IT Environment will provide reliable time stamp to the TOE. Time stamps associated with an audit record must be reliable [FPT_STM.1(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]. Data must be protected from disclosure and modification as it travels to and from distributed TOE components [FPT_ITT.1(2)].
OE.IDAUTH	Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The IT Environment is able to associate a password with specific userids in order to perform authentication [FIA_ATD.1(2)].

Table 22 – Rationale for Mapping of IT Environment SFRs to IT Environment Objectives

6.4.3 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Security Architecture Description: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ADV_FSP.2: Security-Enforcing Functional Specification	Function Specification: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ADV_TDS.1: Basic Design	Basic Design: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1

SECURITY ASSURANCE REQUIREMENT	ASSURANCE EVIDENCE TITLE
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ALC_DEL.1: Delivery Procedures	Secure Delivery Processes and Procedures: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ALC_FLR.2: Flaw Reporting Procedures	Flaw Reporting Procedures: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ATE_COV.1: Evidence of Coverage	Test Plan and Coverage Analysis: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ATE_FUN.1: Functional Testing	Test Plan and Coverage Analysis: IBM Internet Security Systems GX Series Security Appliances Version 4.3 and SiteProtector Version 2.0 Service Pack 8.1
ATE_IND.2: Independent Testing – Sample	N/A
AVA_VAN.2: Vulnerability Analysis	N/A

Table 23 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Security Management
- Traffic Analysis
- Protection of Management Functions

7.2 Security Audit

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.

When a packet arrives, it is timestamped via the network processing unit in the appliance. If an event is triggered, it is tagged with the timestamp of the packet, and the event is sent to SiteProtector with this timestamp. Audit events (such as the ones listed in Section 7.2.1 – Audit Data Generation are timestamped via the host operating system in the IT environment; system events (discussed in 7.5.1 – System Data Generation) are timestamped with the NPU clock on the appliance.

7.2.1 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. These 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).

7.2.2 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 the selective auditing lists. These lists are organized according to audit event types: General, Group, Agent, Asset, Policy, User Group License, Analysis,

Report, Ticketing, Notification and Health. 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.

7.2.3 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.

7.2.4 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. *Event type* is defined by one of the following categories of events:

- *Audit events* match network traffic that seeks information about the network
- *Attack events* match network traffic that seeks to harm the network.

7.2.5 Audit Data Storage

Audit data is stored in the SQL database via the DBMS through the use of the SiteProtector Event Collector. 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 overwrite the oldest stored records. In the event of a system failure, the IT environment may lose some audit data (such as data stored in a buffer) depending on the severity and type of failure.

The Security Audit security function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3(1)

- FAU_SEL.1
- FAU_STG.4
- FPT_STM.1(1)

7.3 Identification and Authentication

The TOE requires operators to be successfully authenticated before any actions can be performed. 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.

This ensures that operators are identified and authenticated before they can access any TSF-mediated functions in the TOE that are not associated with execution of IDS policies.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1(1)

7.4 Security Management

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.

The TOE supports an Administrator role the following roles:

- Global Administrator
- Group Owner
- Group Member

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. Administrator permissions are individually configurable, and options for permissions are describes below:

PERMISSION	DESCRIPTION
Active Directory	This permission allows users to do the following: • import assets and groups from Active Directory • retrieve login information for agents
Auditing Setup	This permission allows user to enable/disable auditing for most actions in the console

PERMISSION	DESCRIPTION
Central Responses	This permission allows user to create/edit central response rules and create/edit network objects and response objects policies
Clear/Restore Events	This permission allows users to clear and restore security events on the Analysis view.
Database Maintenance Setup	On the Agent view at the Site level, set Database maintenance options, including the following: • schedule regular maintenance • set database purge options • set database backup options
Export Analysis Data	This permission allows users to do the following on the Analysis view: • print data • export data • schedule data export job
Full Access to All Functionality	This permission allows users to perform all SiteProtector system functions.
Import Policy/Response	This permission allows the user to import policies and/or responses. Note: The SiteProtector system allows you to grant the Import Policy/Response global permission to non-administrative users, however, IBM ISS strongly advises against this. In some cases restricted permissions are circumvented when you grant non-administrative users the Import Policy/Response global permission.
Launch Event Viewer	On the Agent view at the Site level, open the Event Viewer.
Manage Global Permissions	This permission allows users to assign and remove global permissions to users and groups.
Manage Global Responses	This permission allows users to manage global responses.
Manage Health	This permission allows users to manage system health settings.
Manage Incidents and Exceptions	This permission allows users to create and edit incidents and exceptions on the Analysis view.
Manage Licenses	At the Site level, do the following: • Add and remove products licenses • View license information, including warnings and summary information • View available OneTrust tokens and license information for Proventia OneTrust Licensing
Manage SecureSync	At the Site level, use the SecureSync features, including the following: • Use the Site Management Transfer Wizard • Distribute keys • Manage agents • Release agents

PERMISSION	DESCRIPTION
Manage Ungrouped Assets	This permission allows you to do the following: • see ungrouped assets, agents, and analysis events in the site ranges. • add or delete site ranges • perform the Auto Group Hosts function on ungrouped items.
Manage User Groups	This permission allows users to do the following: • create SiteProtector system user groups • delete SiteProtector system user groups • add members to SiteProtector system user groups • remove members from SiteProtector system user groups
Ticketing Setup	At the Site level, set and change ticketing options, including the following: • Email notification settings, including when to send emails and the email addresses of recipients • Ticket status categories • Ticket priority categories • Custom categories for tickets
Audit Detail Reporting	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.

Table 24 – Available Permissions

The group owner sets and manages group-level permissions for a specific group. You specify the group owner at the time you create the group or in the group properties after you create the group. The group owner can perform the following tasks:

- Grant and remove group-level permissions
- Change the group owner

By default, the user or user group that creates the group is the group owner. The group owner can be any of the following:

- An individual local user
- A local user group
- An individual domain user
- A domain user group
- A SiteProtector system user group

Group-level permissions provide very specific control over users actions in the SiteProtector system. For example, group-level permissions control users ability to perform actions such as the following:

- Log on to the Site
- Change group properties, such as name and membership rules
- Add, modify, and remove assets in a group
- Add, modify, and remove agents in a group
- Apply updates and policies to agents in a group
- View properties and log files for assets and agents in a group
- Print report about the assets and agents in a group
- Start, stop, restart, and refresh agents in a group

Each permission controls a very specific action in the SiteProtector system. 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[5] 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

[5] Note that the TOE supports SNMPv1, SNMPv2c, and SNMPv3.

the monitored network. Only a system administrators and authorized administrators have the ability to modify or add system data (i.e., enable signatures in a policy files). An authorized administrator with view permission for reports is allowed to query TSF data (i.e., view the audit trail).

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1
- FMT_MTD.1
- FMT_SMR.1

7.5 Traffic Analysis

The TOE continuously monitors network traffic and compares 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.

The Traffic Analysis 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. Additionally, simple firewall rules can deny traffic based on IP address, TCP port, and/or TCP destination. These packets won't be analyzed by the TOE for Intrusions. Further analysis of the detected events may be accomplished by applying event detail filters while in the Analysis View. The detected events may further be filtered by the agent, attacker, detail, detail time, event name, incidents, OS analysis, target, and target object. Each data column in these filtered views may be sorted in ascending or descending order.

A response filter allows the administrator to refine the security policy by controlling the number of events to which the appliance responds and the number of events reported to the SiteProtector. Response filters have the following configurable attributes:

- Adapter
- Virtual LAN (VLAN)
- Source or target IP address
- Source or target port number (all ports or a port associated with a particular service) or ICMP type/code (one or the other will be used)

When the appliance detects traffic that matches a response filter, the appliance executes the responses specified in the filter. Otherwise, the appliance executes the security event as specified in the event

itself. The response policy determines how the appliance acts when it detects intrusions or other important events, such as those described in Section 7.2 – Security Audit. The administrator creates responses and then applies them to events as necessary. The TOE supports the following response types for both IDS and IPS configurations:

- Email: Send email alerts to an individual address or email group
- SNMP: Send SNMP traps to a consolidated SNMP server.

Captured packets can be viewed in SiteProtector.

For IPS configurations, the TOE supports the three response types above and additionally supports a quarantine function to quarantine the network against attacks by blocking the originating IP address. The appliance also includes an interface that provides TCP Reset functionality, which effectively blocks a configured originating IP address.

7.5.1 System Data Generation

The System Data Generation functionality 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 function related to intrusion detection and intrusion prevention. 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.

Each signature match can be sorted by the following attributes:

- Time
- Tag Name
- Event count
- Status
- Severity
- Source IP
- Source Port
- Target IP
- Agent IP
- Event-type
    - Audit Events
    - Attack Events

The detection signatures selected to create the user policies are selected from the policy Global Protection Domain. The signatures are selectable from two event types. Audit Event types identify the signatures that match network traffic that seeks information about the network, and Attack event types

identify signatures that match network traffic that seeks to harm the network. The administrator may customize the policy to include or exclude any signatures from the two event type categories.

7.5.2 System Data Storage

System data is stored in the SQL database via the DBMS through the use of the SiteProtector Sensor Controller component. The subsystem 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 overwrite the oldest stored records. In the event of a system failure, the IT environment may lose some audit data (such as data stored in a buffer) depending on the severity and type of failure.

The Traffic Analysis function is designed to satisfy the following security functional requirements:

- IDS_SDC.1
- IDS_ANL.1
- IDS_RCT.1(1)
- IDS_RCT.1(2)
- IDS_RDR.1
- IDS_STG.2

7.6 Protection of Management Functions

TLS 1.0 is used to protect communication between the Sensors and SiteProtector. The TLS implementation (via OpenSSL 1.1.2) is included in the TOE boundary. 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 (CAVP certificate 562); 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, then both sides complete the key establishment phase. Subsequent data traffic is encrypted with AES operating with 256-bit keys (CAVP certificate 1181). SHA-1 (CAVP certificate 1090) is used for message integrity checking. Session keys held in memory are zeroized (CMVP certificate 1402) when a session ends. RSA certificates are generated by the IT Environment during installation of the TOE.

The Protection of Management Functions function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1