IBM Proventia
Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008)
Security Target

Version 1.6

November 25, 2008

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

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

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, Maryland 21046-2587

Prepared For:

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008). 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.

REVISION HISTORY

Rev	Date	Description
1.6	November 25, 2008	Public Release

.

TABLE OF CONTENTS

1. SECURITY TARGET INTRODUCTION 1
1.1 Security Target Reference 1
1.1.1 Security Target 1
1.1.2 TOE Reference 1
1.1.3 Security Target Authors 1
1.1.4 Evaluation Assurance Level 1
1.2 TOE Overview 1
1.2.1 Security Target Organisation 1
1.3 Common Criteria Conformance 2
1.4 Protection Profile Conformance 2

2. TOE DESCRIPTION 3
2.1 TOE Overview 3
2.2 TOE Component Overview 3
2.2.1 Enterprise Scanner Functionality 3
2.2.2 SiteProtector with Reporting Module Functionality 4
2.3 Physical Boundary 4
2.3.1 SiteProtector with Reporting Module Physical Boundary 4
2.3.2 Proventia Network Enterprise Scanner Physical Boundary 4
2.4 Logical Boundary 5
2.4.1 Scanning 5
2.4.2 Audit Data Generation and Viewing 5
2.4.3 System Data Generation 5
2.4.4 System Data Viewing 5
2.4.5 Self Protection 6
2.4.6 Management 6
2.5 TOE Evaluated Configuration 6
2.5.1 TOE Evaluated Configuration Requirements 7
2.5.2 SiteProtector Host Configuration 7
2.5.3 Functionality Not Included in the Evaluation 8
2.6 TOE Data 8
2.7 Rationale for Non-Bypassability and Separation for the TOE 13
2.7.1 SiteProtector with Reporting Module TOE Component 13
2.7.2 Enterprise Scanner TOE Component 14

3. TOE SECURITY ENVIRONMENT 15
3.1 Introduction 15
3.2 Assumptions 15
3.3 Threats 15
3.4 Organizational Security Policies 16

4. SECURITY OBJECTIVES 18
4.1 Security Objectives for the TOE 18
4.2 Security Objectives for the IT Environment 18

5. IT SECURITY REQUIREMENTS 20
5.1 Security Functional Requirements for the TOE 20

5.1.1 Security Audit (FAU) 21
5.1.2 Cryptographic Support (FCS) 25
5.1.3 Identification and authentication (FIA) 26
5.1.4 Security Management (FMT) 31
5.1.5 Protection of the TSF (FPT) 39
5.1.6 IDS Component Requirements (IDS) 40
5.2 Security Functional Requirements for the IT Environment 44
5.2.1 Security Audit (FAU) 45
5.2.2 Cryptographic Support (FCS) 45
5.2.3 Identification and authentication (FIA) 45
5.2.4 Protection of the TSF (FPT) 46
5.2.5 IDS Component Requirements (IDS) 47
5.3 Strength of Function for the TOE 47
5.4 TOE Security Assurance Requirements 47

6. TOE SUMMARY SPECIFICATION 49
6.1 Security Functions 49
6.1.1 Scanning Security Function 49
6.1.2 Management Security Function 51
6.1.3 Audit Data Generation and Viewing Security Function 57
6.1.4 System Data Generation Security Function 58
6.1.5 System Data Viewing Security Function 59
6.1.6 Self Protection Security Function 60
6.2 Assurance Measures 60
6.2.1 TOE Security Assurance Requirements 60
6.2.2 Rationale for TOE Assurance Requirements 62

7. PROTECTION PROFILE CLAIMS 63
7.1 Protection Profile Reference 63
7.2 Protection Profile Refinements 63
7.3 Protection Profile Additions 63

8. RATIONALE 64
8.1 Rationale for IT Security Objectives 64
8.1.1 Rationale Showing Threats to Security Objectives 65
8.2 Rationale for Security Functional Requirements (SFRs) 69
8.2.1 Rationale for Security Functional Requirements of the TOE Objectives 69
8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives 72
8.3 Rationale for TOE Summary Specification 73
8.4 CC Component Hierarchies and Dependencies 77
8.4.1 TOE Security Functional Component Hierarchies and Dependencies 77
8.4.2 IT Environment Security Functional Component Hierarchies and Dependencies 79
8.5 PP Claims Rationale 80
8.6 Strength of Function Rationale 80

LIST OF TABLES

Table 1 - Scanner Hardware 4
Table 2 - SiteProtector Host Minimum Requirements 7
Table 3 - TOE Data 8
Table 4 - Intended Usage Assumptions 15
Table 5 - Physical Assumptions 15
Table 6 - Personnel Assumptions 15
Table 7 - Threats 16
Table 8 - Organizational Security Policies 16
Table 9 - Information Technology (IT) Security Objectives 18
Table 10 - Security Objectives of the IT Environment 18
Table 11 - TOE SFRs 20
Table 12 - TOE Audit Record Generation Detail 21
Table 13 - IT Environment SFRs 25
Table 14 - Group Ownership Details 26
Table 15 - Global Permissions Details 26
Table 16 - Group Permissions Details 27
Table 17 - FMT_MOF.1 Detail 32
Table 18 - FMT_MTD.1 Detail 33
Table 19 - System Analyzer Analysis Events and Details 41
Table 20 - IDS_RDR.1.1 Details 41
Table 21 - IT Environment SFRs 44
Table 22 - IT Environment SFRs 45
Table 23 - TOE Security Assurance Requirements 47
Table 24 - Background Scan Policy Permissions 54
Table 25 - Scan Job States 56
Table 26 - Assurance Measures 60
Table 27 - Assumptions, Threats and Policies to Security Objectives Mapping 64
Table 28 - Assumption, Threat and Policy to Security Objectives Rationale 65
Table 29 - TOE SFRs to Security Objectives Mapping 69
Table 30 - TOE Security Objectives to SFR Rationale 70
Table 31 - IT Environment SFRs to Security Objectives Mapping 72
Table 32 - TOE Security Objectives to SFR Rationale 73

Table 33 - SFRs to TOE Security Functions Mapping 73
Table 34 - SFR to SF Rationale..... 75
Table 35 - TOE SFR Dependency Rationale 77
Table 36 - IT Environment SFR Dependency Rationale 79

ACRONYMS LIST

AD ..... Active Directory
CC ..... Common Criteria
CD ..... Crystal Display
EAL ..... Evaluation Assurance Level
GUI ..... Graphical User Interface
I&A ..... Identification and Authentication
IP ..... Internet Protocol
IT ..... Information Technology
NES ..... Network Enterprise Scanner
NIAP ..... National Information Assurance Partnership
LED ..... Light-emitting Diode
PP ..... Protection Profile
RU ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SOF ..... Strength of Function
SP ..... Service Pack (when SP is followed by a numer)
SP ..... SiteProtector
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TOE Scope of Control
TSF ..... TOE Security Function
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9*, and all international interpretations through March 16, 2007. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target

IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) Security Target, version 1.6, dated November 25, 2008.

1.1.2 TOE Reference

IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) TOE.

1.1.3 Security Target Authors

COACT, Inc.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.2 TOE Overview

This Security Target defines the requirements for the IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) TOE. The TOE is a vulnerability management system designed to scan specified targets for vulnerabilities and includes a management system that provides management and monitoring functionality.

1.2.1 Security Target Organisation

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

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

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

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

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

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

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

This ST is compliant with the Common Criteria (CC) Version 2.3 assurance requirements (Part 3) for EAL2. This ST uses explicitly stated functional requirements in addition to functional requirements drawn from CC Version 2.3 (Part 2). In addition, the cryptographic requirements are not FIPS validated.

1.4 Protection Profile Conformance

This ST does not claim conformance to any Protection Profile.

CHAPTER 2

2. TOE Description

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

2.1 TOE Overview

IBM Proventia Network Enterprise Scanner 1.3 with XPU 1.28 and SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) is a vulnerability management system that scans network devices and identifies and reports known vulnerabilities.

2.2 TOE Component Overview

The TOE is divided into two components: IBM Proventia Network Enterprise Scanner Version 1.3 with XPU 1.28 (hereafter referred to as IBM ISS Network Enterprise Scanner Version 1.3, Network Enterprise Scanner, Enterprise Scanner, or Scanner) and IBM Proventia Management SiteProtector 2.0 SP6.1 with Reporting Module and with Catalog 2.61 (Version 2.684/1/24/008) (hereafter referred to as IBM SiteProtector with Reporting Module Version 2.0 SP 6.1, SiteProtector with Reporting Module, or SiteProtector).

The Enterprise Scanner is an appliance that performs the scanning. All hardware and software included in the Enterprise Scanner is included in the TOE boundary. SiteProtector with Reporting Module is a software distribution running on a Windows based workstation. SiteProtector provides the management and monitoring functionality for the Enterprise Scanner(s). The Reporting Module is separately licensed software in SiteProtector that enables authorized administrators to create and view reports reflecting audit data events and system data events. Scanners support two separate network interfaces: the scanning network and the management network. Scanners communicate with SiteProtector using the management network. The scanning network is used to scan hosts.

2.2.1 Enterprise Scanner Functionality

The Enterprise Scanner scans any Internet Protocol version 4 addressable device connected to the scanning network (operational network) and discovers assets and determines the assets' services and known vulnerabilities. Vulnerabilities are known weaknesses in a system allowing an attacker to violate the integrity, confidentiality, access control, availability, consistency or audit mechanism of the system or the data and applications it hosts. The Enterprise Scanner identifies vulnerabilities such as:

1) improperly configured desktops, servers, Web servers, routers or firewalls;
2) hosts running unauthorized services;
3) weak or no password protection; and
4) unpatched or outdated versions of operating systems.

The complete Scanner is included in the TOE boundary including hardware, OS and IBM ISS software.

2.2.2 SiteProtector with Reporting Module Functionality

SiteProtector with Reporting Module is used as the central controlling point for Enterprise Scanners deployed on the network. The Reporting Module is embedded within SiteProtector, but its functionality must be enabled via a separate license. The SiteProtector performs the following functionality:

1) Manages and monitors Enterprise Scanners;
2) Manages and monitors SiteProtector and
3) displays audit data and system data events.

2.3 Physical Boundary

The physical boundary of the TOE includes:

1) The IBM ISS Network Enterprise Scanner appliance (hardware and software)
2) The IBM ISS SiteProtector application software
3) The IBM ISS Reporting Module software in SiteProtector
4) TSF Data stored on the SiteProtector platform.
5) TSF Data stored on the Network Enterprise Scanner.

2.3.1 SiteProtector with Reporting Module Physical Boundary

The SiteProtector software executes on a system dedicated to this purpose. The IT Environment supplies the hardware, operating system, DBMS, Java Runtime Environment, and SSL/TLS software required by SiteProtector. Table 2 itemizes the minimum requirements for a SiteProtector platform provided by the IT Environment.

2.3.2 Proventia Network Enterprise Scanner Physical Boundary

The complete hardware, OS (Redhat Linux), and Scanner software is included in the TOE boundary. The Scanner is available in two models, the Proventia ES 750 and the Proventia ES 1500. The models are functionally equivalent, but differ in performance characteristics. The hardware differences are summarized in the following table.

Table 1 - Scanner Hardware

Hardware Specific	ES 750 Detail	ES 1500 Detail
Appliance	Desktop	1-RU form factor
Scanning port	One 10/100/1000 PCI Ethernet port	One 32-bit gigabit PCI-Express Ethernet port (4 additional ports reserved for future use)
Management port	One 32-bit gigabit Ethernet port	One 32-bit gigabit Ethernet port
Console port	One front accessible RJ45 serial port. This interface is not available once the appliance is configured to talk to SiteProtector (after installation)	One front accessible RJ45 serial port. This interface is not available once the appliance is configured to talk to SiteProtector (after installation)
Display	n/a	LCD panel, 2x16 characters

LEDs	LED indicating power status and data access.	LED indicating power status and data access.
Hard drive	Used to store the executable code	Used to store the executable code

2.4 Logical Boundary

The logical boundaries of the TOE are defined by the functions provided by the TOE and are described in the following sections.

2.4.1 Scanning

The TOE performs scanning of designated systems to detect known vulnerabilities on those systems. The TOE is designed to automate the process of cyclically discovering and assessing assets (background scanning), while accommodating ad hoc scans as well. Background scans are well suited to minimize impact on operational systems since their execution can be tailored for times when operational usage of the systems and networks is low.

Scanning is broken into two categories: discovery and assessment. Discovery scans are initially used to discover assets on the network (so that they may subsequently be assessed). On-going discovery scans highlight changes to the assets and detect unauthorized systems on the network. Assessment scans perform in-depth searches for vulnerabilities on previously discovered systems.

Results of the scans are stored in the DBMS (IT Environment) located on the same system as the SiteProtector software.

2.4.2 Audit Data Generation and Viewing

The TOE's Audit Data Generation and Viewing Security Function provides administrator support functionality that records the administrator commands and enables authorized administrators to view audit data records in human readable format via the SiteProtector Console.

The TOE stores audit records into the SiteProtector database via the DBMS supplied by the IT Environment. The audit records are retrieved from the database and saved as a report via the OS file system (IT Environment) for audit viewing.

2.4.3 System Data Generation

The TOE's System Data Generation Security Function provides functionality to generate and store system data related to scans performed by the TOE. The TOE's system data includes three types of system data: scan events; analysis views; and system data reports.

The first two types of system data are saved via the SiteProtector database via the DBMS supplied by the IT Environment, while the system data reports are saved on disk using the OS' file I/O functionality (IT Environment).

2.4.4 System Data Viewing

The TOE's System Data Viewing Security Function provides administrator support functionality that enables authorized administrators to view system data records (e.g., detected vulnerabilities) in human readable format via the SiteProtector Console. Data

included in system data records and available for viewing are the specific vulnerability, associated severity, timestamp, IP name and address of the asset on which the vulnerability was detected, scanner from which the scan was performed, and the service protocol (if applicable) associated with the vulnerability.

The TOE retrieves system data from the SiteProtector database via the DBMS or from a file on disk via the OS' file I/O functionality supplied by the IT Environment.

2.4.5 Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the roles (and therefore permissions) are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC.

Since the SiteProtector component of the TOE consists of a set of applications, the TOE cannot provide complete self-protection for itself. The TOE depends on the operating system and hardware (IT Environment) on the SiteProtector platform to protect the TOE from interference or bypass from users or processes outside the TSC.

TLS is used to protect communication between the TOE components. The TLS functionality is provided by the TOE on the Enterprise Scanners and by the IT Environment on the SiteProtector platform.

2.4.6 Management

Management of the TOE may be performed via SiteProtector Console on the SiteProtector platform. All management of the TOE components is performed via SiteProtector.

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.

2.5 TOE Evaluated Configuration

The evaluated configuration of the TOE consists of:

1) One instance of SiteProtector with Reporting Module enabled on a system dedicated to that purpose. The DBMS, supplied by the IT Environment, is hosted on the same platform.
2) One or more instances of Enterprise Scanners.

2.5.1 TOE Evaluated Configuration Requirements

1) Network Time Protocol support is disabled. The Enterprise Scanner appliance generates its own time stamps and the operating system the SiteProtector resides on generates the timestamps for the SiteProtector.
2) SSH functionality for connecting to the Scanners is disabled.
3) The Authentication Level configured on all Enterprise Scanners is "first time trust."
4) Automatic retrieve of X-Press updates (XPUs) 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.
5) SiteProtector components are resident on one workstation (a remote SiteProtector Console is not supported in the evaluated configuration).
6) SSL/TLS is used for the communication between Scanners and SiteProtector. The IT Environment supplies the SSL/TLS on the SiteProtector Host. SSL/TLS on the Scanner is supplied by the TOE.

2.5.2 SiteProtector Host Configuration

The minimum requirements for the SiteProtector Host (supplied by the IT Environment) are described in the following table.

Table 2 - SiteProtector Host Minimum Requirements

Minimum Requirements	
Processor	1 GHz Pentium III
Memory	1 GB
Disk Space	8 GB
Operating System	Windows 2000 Server with Service Pack 4 or later, or Windows 2000 Advanced Server with Service Pack 4 or later, or Windows Server 2003 with or without Service Pack 1, or Windows Enterprise Server 2003 with Service Pack 1
DBMS	SQL Server 2000 Desktop Engine (MSDE) with Service Pack 3a and Security Patch 03-031 or SQL Server 2000 with Service Pack 3a and SQL Security Patch MS03-031 (The SQL Server version will be 8.00.818 after you apply this patch.) or SQL Server 2000 with Service Pack 4
Additional Software	Microsoft Data Access Components (MDAC) 2.8 or later Sun Java 2 Runtime Environment (J2RE), Standard Edition, Version 1.5.0_06 Adobe Acrobat Reader 6.0 or later

	OpenSSL 0.9.7c
Network Configuration	Static IP address
Disk Partition Formats	NTFS

2.5.3 Functionality Not Included in the Evaluation

The functionality included in the TOE boundary that is not included in the evaluation is described below:

1) Active Directory Import Data - SiteProtector provides authorized users the ability to import assets from Active Directory. If an asset is imported from AD, the group name cannot be modified via SiteProtector. Therefore, the functionality relating to interfacing to Active Directory is not claimed in the ST; all assets must be discovered or created by a SiteProtector administrator.
2) Tickets - The SiteProtector ticketing functionality enables an administrator to generate a ticket that reports a known vulnerability discovered by the Scanners. Administrators are required to input ticket information and status of tickets. SiteProtector follows the ticket's status until the issue is closed. The ST does not claim this functionality as security relevant.
3) Web Access - SiteProtector provides a read-only Web-based interface. This interface provides limited SiteProtector functionality. This interface is not claimed as a monitoring interface in the ST and is disabled at TOE installation.
4) X-Press Update Server - The X-Press Update Server is a means to update the TOE software. This functionality is not used since it would change the TOE from the evaluated version.
5) Proventia Manager - The Proventia Manager is a Network Enterprise Scanner resident web-based interface used for Enterprise Scanner installation configuration and start-up. The interface is not used for an operational TOE; all management and monitoring functionality is performed via the SiteProtector Console.

2.6 TOE Data

The following table identifies and describes the TOE Data.

Table 3 - TOE Data

TOE Data Category	Data	Description
User Information	User Groups and Members List	A list of user groups and associated members (users) who belong to the group. User groups are known only to SiteProtector. Users must be known to the IT Environment.

TOE Data Category	Data	Description
	Global Permissions List	A list of global permissions and user groups and/or users who have been assigned each permission.
	Group Owner	The user who created the group or the current owner.
	Group Permission List	A list of user groups and/or users and the group permission name and level (View, Modify, Control) assigned and not assigned to the user group and/or user. The Group Permission List is managed at the Site Group (the top-most group in a hierarchy, associated with a specific Site) level. An administrator may select to inherit a group's group permissions from the Site Group or may maintain a separate instance of the Group Permission List for each group.
Management Data	Site List	A list of Sites. In the evaluated configuration, only a single site is supported since the management function is co-located with the SiteProtector instance.
	Groups List	A list of the Site Groups and groups.
	Group owner	For each group, the group's owner.
	Group Parameters	For each group, the rules defining membership of assets and agents (e.g., Scanners) in the group (either IP addresses, DNS names, NetBIOS Names, or Operating Systems).
	Site Agent List	A list of agents at the site level.
	Group Agent List	A list of agents at the Site Group and group level.
	Site Asset List	A list of assets (Scanners and devices configured or discovered by scans) at the site level.
	Group Asset List	A list of assets at the Site Group and group level.
	Asset Details	For each asset, the IP address, DNS name and OS name.
	Scanner Agent Policy List	A list of Scanner agent policies.

TOE Data Category	Data	Description
	Scanner Asset Policy List	A list of asset policies (Scanner policies) The Scanner Asset Policy List is initially managed at the Site Group level. An administrator may select to inherit a group's policy list from the Site Group or may maintain a separate instance of the scanner policies for each group.
Asset Policies (Scanner) The TOE maintains Asset Policies at the Site Group level. Administrators may choose to inherit a group's asset policies from the Site Group or may maintain a separate instance of the policies for each group.	Assessment Checks Policy	The policy enables an authorized administrator to define which assessment checks to run against assets in the group for background scans. An instance of the Assessment Checks Policy may be optionally maintained per ad-hoc scan.
	Assessment Settings Policy	The policy enables an authorized administrator to define common settings that apply to running assessment scans including port ranges and whether to run TCP, UDP or both for background assessment scans.
	Assessment Credentials Policy	The policy enables an authorized user to define log on account information for running checks that require authenticated access. The policy applies to ad-hoc and background assessment scans.
	Discovery Policy	The policy enables an authorized user to define IP address ranges for background discovery scans and parameters that define the TOE's action on discovery.
	Network Locations Policy	The Policy enables an authorized user to define the network locations for scans within a group. The policy applies to ad-hoc and background discovery and assessment scans.
	Network Services Policy	This policy defines which ports services run on and enables an authorized administrator to enable or disable service checks. The policy applies to ad-hoc and background assessment scans.
	Scan Control Policy	The policy enables an authorized administrator to enable or disable background discovery and assessment scans and defines refresh cycles for background discovery and assessment scanning.

TOE Data Category	Data	Description
	Scan Exclusion Policy	The policy enables an authorized user to define IP addresses and ports that should be excluded from ad-hoc and background assessment scans.
	Discovery Scan Windows Policy	The policy enables an authorized administrator to define the allowable windows for ad-hoc and background discovery scanning.
	Assessment Scan Windows Policy	The policy enables an authorized administrator to define the allowable windows for ad-hoc and background assessment scanning.
	Scan Time Windows Policy	The policy enables an authorized administrator to view the current time zone associated with the two scan window policies and modify the time zone.
Scan Job Information	Site Job Status List	A list of jobs at the site level and their completion status.
	Group Job Status List	A list of jobs at the Site Group and group level and their completion status.
	Scan Job Result	For each job, the detailed results of individual scan jobs.
Selective Auditing Event Lists - 7 lists, grouped by topic, that list auditable events by event type and whether the events are enabled or disabled.	Selective Auditing – General	Includes general audit events such as logging into and out of SiteProtector, global permissions and selective auditing modifications.
	Selective Auditing – Group	Includes group related audit events including group management and group permission management.
	Selective Auditing – Agent	Includes agent related audit events.
	Selective Auditing – Asset	Includes asset related audit events.
	Selective Auditing – Policy	Includes policy related audit events.
	Selective Auditing – User Group	Includes user group related audit events.
	Selective Auditing – Report	Includes report related audit events.
Reports	Report Lists	For each of the reports, a list of the created reports.
Audit Data – Events	Audit Events	Events generated as the result of management commands.

TOE Data Category	Data	Description
AuditReports	Audit Detail Report	Displays the audit data generated as the results of management commands.
	User to Group	This report displays, for each Windows user or group defined in SiteProtector, the SiteProtector User Group(s) to which that user or group belongs.
System Data - Events	Scan Events	Events (analytical results) generated by the Scanners as the result of scans.
System Reports	Asset Assessment Detail Report	The report displays a detailed list of vulnerabilities (including remedy information) and services per asset.
	Asset Assessment Summary Report	The report displays a list of discovered assets and for each asset the asset's network services and vulnerabilities.
	Operating System Summary Report	The percentage and number of assets by OS.
	Operating System Summary By Asset Report	A list of assets scanned and their operating system and NetBIOS name.
	Service Summary Report	The report displays a list of services discovered on any asset and a count of the assets on which that service is available.
	Service Summary By Asset Report	The report displays a list of services discovered for each asset scanned.
	Top Vulnerabilities Report	The report displays a list of top vulnerability types by frequency.
	Vulnerability By Asset Report	The report displays, for each asset, a count of the detected vulnerabilities by severity.
	Vulnerability By Group Report	The report displays, for each group and subgroup, a count of the detected vulnerabilities by severity.
	Vulnerability By OS Report	The report displays, for each detected operating system, a count of the detected vulnerabilities by severity.
	Vulnerability Counts Report	The report graphically displays a count of the detected vulnerabilities by severity.
	Vulnerability Counts By Asset Report	The report displays, for each asset, the IP address, operating system, and a count of the detected vulnerabilities by severity.
	Vulnerability Detail By Asset Report	The report displays a detailed list of all vulnerability information available for each asset.

TOE Data Category	Data	Description
	Vulnerability Differential Report	The report displays a summary comparison between two dates of detected vulnerabilities by severity and vulnerability details for each asset.
	Vulnerability Names By Asset Report	The report displays, for each asset, a list of vulnerability names detected along with the severity and a brief desciption.
	Vulnerability Remedies By Asset Report	The report displays, for each asset, a list of detected vulnerabilities and detailed information on their remedies.
	Vulnerability Summary By Asset Report	The report displays, for each asset, a list of detected vulnerabilities and their severity and description.
	Vulnerable Assets Report	The report displays, for each detected vulnerability, a list of assets on which the vulnerability was detected.
	Vulnerability Trend Report	The report displays a count per period (day, week, month, quarter, or year) of the detected vulnerabilities according to the following criteria: total, status (existing, fixed, new), new by severity, fixed by severity, and existing by severity.
	Permission Detail Report	The report displays, for each SiteProtector user or user group, the global and/or group permissions and levels that have been assigned to them.

2.7 Rationale for Non-Bypassability and Separation for the TOE

2.7.1 SiteProtector with Reporting Module TOE Component

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

SiteProtector provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). SiteProtector controls actions carried out by an administrator by controlling a session and the actions carried out during a session. Unauthenticated users may not perform any actions other than I&A within SiteProtector. When multiple administrators are connected simultaneously, the permissions are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a session a user has with SiteProtector, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents SiteProtector from being interfered with or tampered with for those users that are within the TSC.

SiteProtector depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The workstation hardware provides virtual memory and process separation which the workstation OS utilizes to ensure that other (non-SiteProtector) processes may not interfere with SiteProtector; all interactions are limited to the defined TOE interfaces.

2.7.2 Enterprise Scanner TOE Component

The Enterprise Scanner is a device that includes software that executes on top of an underlying hardware system. Together, the software and underlying hardware make up the TOE component.

The Enterprise Scanner is protected from interference. The Enterprise Scanner does not allow generic users to introduce new processes or executable code to the system. The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through defined access control, the TSF is protected from corruption or compromise. Arbitrary entry into the Enterprise Scanner is not possible and therefore the TSF is protected against external interference by untrusted subjects.

CHAPTER 3

3. TOE Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies 1) assumptions about the environment, 2) threats to the assets and 3) organisational security policies.

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

3.2 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 4 - Intended Usage Assumptions

A.Type	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.

Table 5 - Physical Assumptions

A.Type	Description
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.

Table 6 - Personnel Assumptions

A.Type	Description
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 with respect to their roles, permissions and ownership.
A.NOTRST	The TOE can only be accessed by authorized users.

3.3 Threats

The following are threats identified for the TOE and the IT System (i.e., IT Environment) 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 following table identifies threats to the TOE.

Table 7 - Threats

T.Type	TOE Threats
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.
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.FALREC	The TOE may fail to recognize vulnerabilities based on the network data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities based on association of the network data received from all data sources.

3.4 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

Table 8 - Organizational Security Policies

P.Type	Organizational Security Policy
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 vulnerabilities must be applied to incoming Scanner network data and appropriate notification provided.

P.Type	Organizational Security Policy
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 TOE
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.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 9 - Information Technology (IT) Security Objectives

Objective	Definition
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDSCAN	The Scanner must collect and store information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDANLZ	The TOE must accept data from Scanners and then apply analytical processes and information to derive conclusions about vulnerabilities.
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 data and system data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of theTOE functions.
O.INTEGR	The TOE must ensure the integrity of all TSF data.

4.2 Security Objectives for the IT Environment

The TOEs operating environment must satisfy the following objectives.

Table 10 - Security Objectives of the IT Environment

Objective	Definition
O.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
O. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

Objective	Definition
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.INTROP	The TOE is interoperable with the IT System it monitors
OE.TIME	The IT Environment will provide reliable timestamps to the TOE
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE_AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to the TOE allowing access to TOE functions and data.

.

CHAPTER 5

5. IT Security Requirements

This section identifies the security functional requirements for the TOE and for the IT environment. The functional requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of italicised items listed in brackets.

The CC defines four operations on security functional requirements. The font conventions listed below identify the conventions for the operations defined by the CC.

Assignment: *indicated in italics*

Selection: indicated in underlined text

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

Refinement, text added**: indicated with bold text**

Refinement, text deleted: ~~indicated with strikethrough~~

Explicitly stated requirements are included in this ST. FPT_SEP.1 and FPT_RVM.1 pertaining to SiteProtector are split and levied on both the TOE and the IT Environment. These SFRs are identified as FPT_SEP_SFT.1, FPT_SEP_OS.1, FPT_RVM_SFT.1, and FPT_RVM_OS.1. Additionally, explicitly stated SFRs were copied from the IDS System PP to specifically address the data collected and analysed by an IDS. The names of these requirements start with IDS_.

5.1 Security Functional Requirements for the TOE

The functional security requirements for the TOE consist of the following components, summarized below.

Table 11 - TOE SFRs

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SEL.1	Selective audit
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4(1)	Cryptographic Key Generation
FCS_COP.1(1)	Cryptographic Operation
FIA_ATD.1(1)	User attribute definition
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions

Functional Components	
FMT_SMR.1	Security roles
FPT_ITT.1(1)	Basic Internal TSF Data Transfer Protection
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs
FPT_SEP_SFT.1	TSF Domain Separation for Software TOEs
FPT_STM.1(1)	Reliable time stamps
IDS_ANL.1	Analyzer analysis
IDS_RDR.1	Restricted Data Review
IDS_STG.2	Prevention of System data loss

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1: Audit data generation

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

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

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

c) *the audit records specified in the Events Type column in the following table*.

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional information specified in the Audit Record Detail column in the following table.*

Table 12 - TOE Audit Record Generation Detail

Operation		Audit Record	
General	**Specific**	**Event Type**	**Audit Record Detail**
Starting and Stopping Auditing	Starting Auditing (starting the SiteProtector Core agent)	Starting Auditing	Location of Console: *SP hostname*
	Stopping Auditing (stopping the SiteProtector Core agent)	Stopping Auditing	Location of Console: *SP hostname*

Operation		Audit Record	
General	**Specific**	**Event Type**	**Audit Record Detail**
Logging into and out of SiteProtector Console	Log on	Console Login	Location of Console: *SP hostname*
	Log off	Console Logout	Location of Console: *SP hostname*
Manage User Groups and Users	Add a new user group	Add New User Group	User Group added: *User Group Name* Location of Console: *SP hostname*
	Rename user group (complete the add user group operation)	Update User Group	User Group updated: *User Group Name* Location of Console: *SP hostname*
	Delete user group	Delete User Group	User Group removed: *User Group Name* Location of Console: *SP hostname*
	Add a new user to a user group	Add User Group Member	Location of Console: *SP hostname*
	Delete a user from a user group	Delete User Group Member	Location of Console: *SP hostname*
Global Permissions	Add a user group to a global permission	Update Site Level Permissions	Location of Console: *SP hostname*
	Add a user to a global permission		
	Delete a user group from a global permission		
	Delete a user from a global permission		
Groups	Add a group	Add New Group	Group Path*: group path* Location of Console: *SP hostname*
	Modify the default group name (complete the add a group operation)	Update Group	Group Path*: new group path* Old Group Path: *olf group path* Location of Console: *SP hostname*
	Delete a group	Delete Group	Group Path: *group path* Location of Console: *SP hostname*

Operation		Audit Record	
General	**Specific**	**Event Type**	**Audit Record Detail**
Group Permissions	Add user or user group to a group permission	Update Group Permissions	Location of Console: *SP hostname*
	Delete a user or user group from a group permission		
	Modify Permissions		
Agent	Delete an Agent	Delete an Agent	Location of Console: *SP hostname*
Asset	Add an asset	Add Asset	Location of Console: *SP hostname* Asset: *Asset's DNS Name* Group Path: *group path* Asset: *Asset's IP Address/DNS Name*
	Update asset name (complete add asset operation)	Update Asset	Location of Console: *SP hostname* Asset: *Asset's DNS Name*
	Delete an asset	Delete Asset	Group Path: *group path* Location of Console: *SP hostname* Asset: *Asset's DNS Name*
Asset Policies	Update one of 11 asset policies: Assessment Checks Policy, Assessment Settings Policy, Assessment Credentials Policy, Discovery Policy, Network Locations Policy, Network Services Policy, Scan Control Policy, Scan Exclusion Policy, Discovery Scan Windows Policy,	Update Group Policy	Group Path: *group path* Enabled: 1 Namespace: *policy's namespace* Location of Console: *SP hostname* Schema Version: 1.0

Operation		Audit Record	
General	**Specific**	**Event Type**	**Audit Record Detail**
	Assessment Scan Windows Policy or Scan Time Windows Policy.		
Scans	Start an Ad-hoc scan	Start Scan	Group Path: *group path* Scan Arguments *empty* Task Description: *group* Location of Console: *SP hostname*
Reports	Create a report	Create a new report	Group Path: *group path* Type of Action: Create Report Name: *Report Name* Command Scheduled: *scheduled time* Location of Console: *SP hostname* Report Type: *Template name*
	Delete a report	Delete a report	Group Path: *group path* Type of Action: Delete Report Name: *Report Name* Location of Console: *SP hostname* Report Type: *Template name*
	View a report	View a report	Group Path: *group path* Type of Action: View Report Name: *Report Name* Location of Console: *SP hostname* Report Type: *Template name*
Selective auditing	Disable or re-enable an audit record	Update Auditing Setup	Location of Console: *SP hostname*

5.1.1.2 FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide *Administrators assigned the Full Access To All Functionality global permission or Administrators assigned a group's Report/Audit/Audit Detail group permission at either the View or Modify level* with the capability to read *all audit record detail identified in the above table* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_SAR.2: Restricted audit review

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

5.1.1.4 FAU_SEL.1: Selective audit

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

a) event type;

b) *no additional attributes.*

5.1.1.5 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.

Application Note: FAU_STG.4 refers to audit data referred to in FAU_GEN.1

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *random number generator* and specified cryptographic key sizes *168 bits* that meet the following: *X9.31 A.2.4 (TDES) (CAVP Cert TBD).*

5.1.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2 (CMVP Cert TBD).*

5.1.2.3 FCS_COP.1 Cryptographic Operation

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

Table 13 - IT Environment SFRs

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and decryption	Triple-DES (EDE, CBC) (CAVP Cert TBD)	168	FIPS 46-3
Key establishment	RSA (CCTL Tested)	1024 (modulus)	RFC2246
Hashing	SHS (CAVP Cert TBD)	128	FIPS 180-2
Random number generation	X9.31 A.2.4 (TDES) (CAVP Cert TBD)	n/a	X9.31 A.2.4 (TDES)

5.1.3 Identification and authentication (FIA)

5.1.3.1 FIA_ATD.1 User Attribute Definition

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

a) *username;*

b) *User Group membership;*

c) *Group ownership described in Table 14 below.*

d) *user assigned global permissions identified in Table 15 below; and*

e) *user assigned group permissions and group permission level (View, Modify or Control) identified in Table 16 below.*

Table 14 - Group Ownership Details

Group Ownership	Description
Group Ownership	Enables an administrator to view and modify the Group Permission List; and change a group's owner if the user is the owner.

Table 15 - Global Permissions Details

Global Permission	Description
Auditing Setup	Enables an administrator to disable and re-enable generation of audit records (view and modify Selective Auditing –General, Selective Auditing –Group, Selective Auditing –Agent, Selective Auditing –Asset, Selective Auditing – Policy, Selective Auditing –User Group, and Selective Auditing –Report TSF Data).
Full Access To All Functionality	Enables an administrator access to all TOE management functions. This permission supersedes all other global and group permission requirements.
Manage Global Permissions	Enables an administrator to assign and un-assign global permissions (view and modify the Global Permissions List).
Manage User Groups	Enables an administrator to add and delete user groups to/from SiteProtector and to add/delete users to/from user groups (view and modify the Group Permission List).

Table 16 - Group Permissions Details

Group Permission	Group Permission Level (either View, Modify, or Control)	Description
Group	View or Modify	Enables an administrator to log onto SiteProtector; view Agents at the Site and Group levels; view Assets at the Site and Group levels; view Scanner Agent Policy Lists; view Scanner Asset Policy Lists; view job status at the Site and Group levels; view scan job results; view the Analysis Views (Event Analysis – Details; Even Analysis – OS; Event Analysis – Target; Vulnerabilities Analysis – Name; Vulnerabilities Analysis - Asset; Vulnerabilities Analysis - Object; and Vulnerabilities Analysis – Detail).
	Modify	Enables an administrator to add and delete a group.
Assets	Modify	Enables an administrator to add and delete an asset; view and modify asset details.
Agents	Modify	Enables an administrator to delete an agent.
Report/Assessment/Asset Assessment Detail	View or Modify	Enables an administrator to view the list of previously created Asset Assessment Detail Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Asset Assessment Detail Reports.
Report/Assessment/Asset Assessment Summary	View or Modify	Enables an administrator to view the list of previously created Asset Assessment Summary Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Asset Assessment Summary Reports.
Report/Assessment/Operating System Summary	View or Modify	Enables an administrator to view the list of previously created Operating System Summary Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Operating System Summary Reports.

Group Permission	Group Permission Level (either View, Modify, or Control)	Description
Report/Assessment/Operating System Summary By Asset	View or Modify	Enables an administrator to view the list of previously created Operating System Summary By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Operating System Summary By Asset Reports.
Report/Assessment/Service Summary	View or Modify	Enables an administrator to view the list of previously created Service Summary Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Service Summary Reports.
Report/Assessment/Service Summary By Asset	View or Modify	Enables an administrator to view the list of previously created Service Summary By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Service Summary By Asset Reports.
Report/Assessment/Top Vulnerabilities	View or Modify	Enables an administrator to view the list of previously created Top Vulnerabilities Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Top Vulnerabilities Reports.
Report/Assessment/Vulnerability By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability By Asset Reports.
Report/Assessment/Vulnerability By Group	View or Modify	Enables an administrator to view the list of previously created Vulnerability By Group Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability By Group Reports.
Report/Assessment/Vulnerability By OS	View or Modify	Enables an administrator to view the list of previously created Vulnerability By OS Reports and enables administrators to view the individual reports.

Group Permission	Group Permission Level (either View, Modify, or Control)	Description
	Modify	Enables an administrator to create and delete Vulnerability By OS Reports.
Report/Assessment/Vulnerability Counts	View or Modify	Enables an administrator to view the list of previously created Vulnerability Counts Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Counts Reports.
Report/Assessment/Vulnerability Counts By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability Counts By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Counts By Asset Reports.
Report/Assessment/Vulnerability Detail By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability Detail By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Detail By Asset Reports.
Report/Assessment/Vulnerability Differential	View or Modify	Enables an administrator to view the list of previously created Vulnerability Differential Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Differential Reports.
Report/Assessment/Vulnerability Names By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability Names By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Names By Asset Reports.
Report/Assessment/Vulnerability Remedies By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability Remedies By Asset Reports and enables administrators to view the individual reports.

Group Permission	Group Permission Level (either View, Modify, or Control)	Description
	Modify	Enables an administrator to create and delete Vulnerability Remedies By Asset Reports.
Report/Assessment/Vulnerability Summary By Asset	View or Modify	Enables an administrator to view the list of previously created Vulnerability Summary By Asset Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Summary By Asset Reports.
Report/Assessment/Vulnerable Assets	View or Modify	Enables an administrator to view the list of previously created Vulnerable Assets Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerable Assets Reports.
Report/Audit/Audit Detail	View or Modify	Enables an administrator to view the list of previously created Audit Detail Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Audit Detail Reports.
Report/Audit/User to Group	View or Modify	Enables an administrator to view the list of previously created User to Group Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete User to Group Reports.
Report/Management/Vulnerability Trend	View or Modify	Enables an administrator to view the list of previously created Vulnerability Trend Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Vulnerability Trend Reports.
Report/Permissions/Permission Detail	View or Modify	Enables an administrator to view the list of previously created Permission Detail Reports and enables administrators to view the individual reports.
	Modify	Enables an administrator to create and delete Permission Detail Reports.

Group Permission	Group Permission Level (either View, Modify, or Control)	Description
Agent/Network Enterprise Scanner/Ad Hoc Scan	Control	Enables an administrator to invoke ad-hoc discovery and assessment scans.
Agent/Network Enterprise Scanner/Assessment Policy	View	Enables an administrator to view the Assessment Checks Policy or the Assessment Setting Policy.
	Modify	Enables an administrator to view and modify the Assessment Checks Policy or the Assessment Setting Policy.
Agent/Network Enterprise Scanner/Assessment Credentials Policy	View	Enables an administrator to view the Assessment Checks Policy.
	Modify	Enables an administrator to view and modify the Assessment Checks Policy.
Agent/Network Enterprise Scanner/Discovery Policy	View	Enables an administrator to view the Discovery Policy.
	Modify	Enables an administrator to view and modify the Discovery Policy.
Agent/Network Enterprise Scanner/Network Locations Policy	View	Enables an administrator to view the Network Locations Policy.
	Modify	Enables an administrator to view and modify the Network Locations Policy.
Agent/Network Enterprise Scanner/Policy	Modify	Enables an administrator to view and modify the Network Services Policy; the Scan Control Policy and the Scan Exclusion Policy.
Agent/Network Enterprise Scanner/Scan Window Policy	View	Enables an administrator to view the Discovery Scan Window Policy, the Assessment Scan Window Policy and the Scan Time Policy.
	Modify	Enables an administrator to view and modify the Discovery Scan Window Policy, the Assessment Scan Window Policy and the Scan Time Policy.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **perform the operation identified in column 1 in the following table** the functions *identified in column 3 in the following table* to *administrators assigned the Full Access To All*

Functionality global permission or the group permission for the group identified in column 4 in the following table.

Table 17 - FMT_MOF.1 Detail

Operation	***Application note:*** scan job	Function	Permission
Disable and Enable	All discovery background scanning jobs for a group	Administrators may disable and enable discovery background and ad-hoc scanning jobs for a group.	Global Administrator, Group Owner, Group Member
Disable and Enable	All assessment background scanning for a group	Administrators may disable and enable assessment background and ad-hoc scanning jobs for a group	Global Administrator, Group Owner, Group Member
Modify the behaviour of	Ad-hoc scanning	Administrators may start ad-hoc discovery and assessment scans.	Global Administrator, Group Owner, Group Member
Modify the behaviour of	Previously invoked scan jobs	Administrators may cancel, pause, rerun and resume previously invoked individual scan jobs.	Global Administrator, Group Owner, Group Member
Modify the behaviour of	Ad-hoc and background discovery scan job.	Administrators may limit or augment discovery scan's network scope by defining the IP address ranges of the scans.	Global Administrator, Group Owner, Group Member
Modify the behaviour of	Ad-hoc and background assessment scans jobs.	Administrators may limit or augment assessment scan's scope by defining a set of IP addresses to exclude from scanning and defining the networks to scans.	Global Administrator, Group Owner, Group Member
Modify the behaviour of	Ad-hoc and background assessment scans jobs.	Administrators may limit or augment the scope of assessment scan jobs by defining which assessment checks to run; defining the UDP and TCP port ranges to perform assessment checks; defining which service checks to run; and defining service checks	Global Administrator, Group Owner, Group Member

Operation	*Application note:* scan job	Function	Permission
		for TCP or UDP ports or both.	
Modify the behaviour of	Ad-Hoc and background discovery and assessment scans.	Administrators may define the time window scans run.	Global Administrator, Group Owner, Group Member

Rationale for SFR refinement: The TOE supports multiple management functions pertaining to security function behaviour. Therefore, these functions are presented in a table. The operations listed in column one are valid FMT_MOF.1 selection operation options.

5.1.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *perform the operation identified in column 2 in the following table* the *TSF Data identified in column 1, in the following table* to *administrators identified in column 3 in the following table.*

Table 18 - FMT_MTD.1 Detail

Specific	Operation	Administrator
Site List	View	Global Administrator, Group Owner, Group Member
User Groups and Members List	View, Add a User Group to SiteProtector, Remove a User Group from SiteProtector, Add a User to a SiteProtector User Group, and Remove a User from a SiteProtector User Group	Global Administrator
Global Permissions List	View, Add a User Group or a User to a global permission and Remove a User Group or a User from a global permission	Global Administrator
Site Group List	View	Global Administrator, Group Owner, Group Member
Groups List	View	Global Administrator, Group Owner, Group Member
	Add a group, delete a group	Global Administrator, Group Owner, Group Member

Specific	Operation	Administrator
Group Permission List	View, Add a User Group or a user to a group's group permission list, Remove a user group or a user from a group's group permission list, Enable a permission level (View, Modify, Control) for a user group and/or user, and Remove a permission level (View, Modify, Control) from a user group and/or user;.	Global Administrator, Group Owner
	Inherit or Override from Site Group (group level only)	
Group ownership	View, Modify	Global Administrator, Group Owner
Group Parameters	View, Modify	Global Administrator, Group Owner
Site Agent List	View List	Global Administrator, Group Owner, Group Member
Group Agent List	View List	Global Administrator, Group Owner, Group Member
	Delete an entry (Scanner only)	Global Administrator, Group Owner, Group Member
Scanner Agent Policy List	View	Global Administrator, Group Owner, Group Member
Site Asset List	View	Global Administrator, Group Owner, Group Member
Group Asset List	View	Global Administrator, Group Owner, Group Member
	Add an entry (Asset), delete an entry (an asset), move an asset	Global Administrator, Group Owner, Group Member
Asset Details	View, Modify	Global Administrator, Group Owner, Group Member
Scanner Asset Policy List	View	Global Administrator, Group Owner, Group Member
Assessment Checks Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Assessment Settings Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner,

Specific	Operation	Administrator
	Inherit or Override from Site Group (group level only)	Group Member
Assessment Credentials Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Discovery Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Network Locations Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Network Services Policy	View, Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Scan Control Policy	View, Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Scan Exclusion Policy	View, Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Discovery Scan Window Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Assessment Scan Window Policy	View	Global Administrator, Group Owner, Group Member
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Scan Time Policy	View	Global Administrator, Group Owner, Group Member

Specific	Operation	Administrator
	Modify	Global Administrator, Group Owner, Group Member
	Inherit or Override from Site Group (group level only)	
Site Job Status List	View	Global Administrator, Group Owner, Group Member
Group Job Status List	View	Global Administrator, Group Owner, Group Member
Scan Job Result	View	Global Administrator, Group Owner, Group Member
Report Lists	View	Global Administrator, Group Owner, Group Member
Audit Detail Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
User to Group Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Operating System Summary Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Operating System Summary By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Asset Assessment Detail Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Asset Assessment Summary Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Service Summary Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member

Specific	Operation	Administrator
Service Summary By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Top Vulnerabilities Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group
Vulnerability By Group Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability By OS Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Counts Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Counts By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Detail By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Differential Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Names By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member

Specific	Operation	Administrator
Vulnerability Remedies By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Summary By Asset Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerable Assets Report	Create, Delete	Global Administrator, Group Owner, Group Member
	View	Global Administrator, Group Owner, Group Member
Vulnerability Trend Report	Create, Delete	Global Administrator, Group Owner, Group
	View	Global Administrator, Group Owner, Group Member
Permission Detail Report	Create, Delete	Global Administrator, Group Owner, Group Member
	Create, Delete	Global Administrator, Group Owner, Group Member
Event Analysis – Details	View	Global Administrator, Group Owner, Group Member
Event Analysis – OS	View	Global Administrator, Group Owner, Group Member
Event Analysis - Target	View	Global Administrator, Group Owner, Group Member
Vulnerability Analysis - Vulnerability Name	View	Global Administrator, Group Owner, Group Member
Vulnerability Analysis – Asset	View	Global Administrator, Group Owner, Group Member
Vulnerability Analysis – Object	View	Global Administrator, Group Owner, Group Member
Vulnerability Analysis - Detail	View	Global Administrator, Group Owner, Group Member
Selective Auditing - General	View and Modify	Global Administrator
Selective Auditing – Group	View and Modify	Global Administrator
Selective Auditing – Agent	View and Modify	Global Administrator

Specific	Operation	Administrator
Selective Auditing – Asset	View and Modify	Global Administrator
Selective Auditing – Policy	View and Modify	Global Administrator
Selective Auditing – User Group	View and Modify	Global Administrator
Selective Auditing – Report	View and Modify	Global Administrator

5.1.4.3 FMT_SMF.1 Specification of Management Functions

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

1. Perform the TSF Data management operations identified in Table 18 above;

2. perform the security function behaviour management functions identified in Table 17 above.

5.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles*:*

1) Global Administrator;

2) Group Owner;

3) Group Member.

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

Rationale for SFR refinement: The TOE is responsible for protecting communication originating from a Scanner. The IT Environment is responsible for protecting information sent from SiteProtector. FPT_ITT.1(1) and FPT_ITT.1(2), levied on the IT Environment, together address TSF data transfer protection.

5.1.5.2 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

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

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE; this applies to the entire Enterprise Scanner appliance as well as the SiteProtector application. See FPT_RVM_OS (levied on the IT Environment) for the remaining functionality.

5.1.5.3 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

FPT_SEP_SFT.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

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

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE; this applies to the entire Enterprise Scanner appliance as well as the SiteProtector application. See FPT_SEP_OS (levied on the IT Environment) for the remaining functionality.

5.1.5.4 FPT_STM.1 Reliable time stamps

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

Rationale for SFR refinement: The TOE is responsible for generating time stamps on Scanners. The IT Environment is responsible for generating time stamps on SiteProtector. FPT_STM.1(1) and FPT_STM.1(2), levied on the IT Environment, together address reliable time stamps.

5.1.6 IDS Component Requirements (IDS)

Rationale for explicitly stated SFRs: This family of IDS requirements is copied from the IDS System PP to specifically address the data collected and analysed by an IDS. 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.

5.1.6.1 IDS_ANL.1 Analyser analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on network traffic received from targeted IT systems in response to network packets sent by the Scanner:

- **a)** signature; and
- **b)** *host discovery, and*
- **c)** *service discovery.*

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.*** *The additional information specified in the Details column of the table below.*

Table 19 - System Analyzer Analysis Events and Details

Component	Analysis	Details
IDS_ANL.1	Known vulnerabilities	Result, identification of the known vulnerability
IDS_ANL.1	Host discovery	IP address, MAC address, OS name/version, and NetBIOS domain and name of each discovered asset
IDS_ANL.1	Service discovery	Service identification (name and port), protocol

Application Note: During assessment scans, the network traffic received by the Scanner from each targeted IT System is compared to signatures to determine if each known vulnerability being checked for is present on each system.

5.1.6.2 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide *authorized administrators assigned the Full Access To All Functionality global permission or the group permission identified in column 3 in the following table* with the capability to read *the system data identified in column 1 in the following table for all groups if the administrator has been assigned the Full Access To All Functionality global permission or the system data identified in column 1 in the following table for the group associated with the administrator's group permission* 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.

Table 20 - IDS_RDR.1.1 Details

System Data View	System Data Contents	Permission
Event Analysis – Details	The iss-host-scan events display the timestamp of each event, the target (scan) IP address, services (ports) available on the asset, MAC address, NetBIOS domain and name, operating system (as this information is determined)	Group View

System Data View	System Data Contents	Permission
Event Analysis – OS	The operating system detected on one or more assets, the number of assets using that operating system, the number of events referencing that operating system, and the count of vulnerabilities by severity detected on assets using that operating system.	Group View
Event Analysis - Target	For each asset, the IP address, count of detected vulnerabilities by severity, and the timestamps of the earliest and latest events.	Group View
Vulnerability Analysis- Vulnerability Name	For each detected vulnerability, the name of the vulnerability, its severity, the number of events referencing the vulnerability (Event Count), the number of assets on which the vulnerability was detected (Target Count), the number of unique objects (e.g., ports) detected (Object Count), and the timestamp of the latest event.	Group View
Vulnerability Analysis- Asset	For each asset, displays the IP address (Target IP), count of the detected vulnerabilities by severity, count of the associated tags (event types), count of the associated objects (e.g., ports), and the timestamp of the most recent event.	Group View
Vulnerability Analysis - Object	For each object type/name combination, displays the count of the detected vulnerabilities by severity, count of the associated tags (event types), count of the assets on which the object was detected, and the timestamp of the most recent event.	Group View
Vulnerability Analysis- Detail	For each event indicating a detected vulnerability, service or new asset information, displays the event type, severity, associated asset IP address, object type and name (e.g., specific port), scanner, and event-specific information.	Group View
Operating System Summary Report	The percentage and number of assets by OS.	Report/Assessment/Operating System Summary View or Modify group permission
Operating System Summary By Asset Report	A list of assets scanned and their operating system and NetBIOS name.	Report/Assessment/ Operating System Summary By Group View or Modify group permission

System Data View	System Data Contents	Permission
Asset Assessment Detail Report	The report displays a detailed list of vulnerabilities and services for each asset.	Report/Assessment/Asset Assessment Detail View or Modify group permission
Asset Assessment Summary Report	The report displays a list of discovered assets and for each asset the asset's network services and vulnerabilities.	Report/Assessment/Asset Assessment Summary View or Modify group permission
Service Summary Report	The report displays a list of services discovered along with a count of the number of assets providing each service.	Report/Assessment/Service Summary View or Modify group permission
Service Summary By Asset Report	The report displays the operating system and a list of services discovered for each asset scanned.	Report/Assessment/Service Summary By Asset View or Modify group permission
Top Vulnerabilities Report	The report displays a list of top vulnerability types by frequency.	Report/Assessment/Top Vulnerabilities View or Modify group permission
Vulnerability By Asset Report	The report displays, for each asset, a count of the detected vulnerabilities by severity.	Report/Assessment/Vulnerability By Asset View or Modify group permission
Vulnerability By Group Report	The report displays, for each group and subgroup, a count of the detected vulnerabilities by severity.	Report/Assessment/Vulnerability By Group View or Modify group permission
Vulnerability By OS Report	The report displays, for each detected operating system, a count of the detected vulnerabilities by severity.	Report/Assessment/Vulnerability By OS View or Modify group permission
Vulnerability Counts Report	The report graphically displays a count of the detected vulnerabilities by severity.	Report/Assessment/Vulnerability Counts View or Modify group permission
Vulnerability Counts By Asset Report	The report displays, for each asset, the IP address, operating system, and a count of the detected vulnerabilities by severity.	Report/Assessment/Vulnerability Counts By Asset View or Modify group permission
Vulnerability Detail By Asset Report	The report displays a detailed list of all vulnerability information available for each asset.	Report/Assessment/Vulnerability Detail By Asset View or Modify group permission
Vulnerability Differential Report	The report displays a summary comparison between two dates of detected vulnerabilities by severity and vulnerability details for each asset.	Report/Assessment/Vulnerability Differential View or Modify group permission
Vulnerability Names By Asset Report	The report displays, for each asset, a list of vulnerability names detected along with the severity and a brief desciption.	Report/Assessment/Vulnerability Names By Asset View or Modify group permission

System Data View	System Data Contents	Permission
Vulnerability Remedies By Asset Report	The report displays, for each asset, a list of detected vulnerabilities and detailed information on their remedies.	Report/Management/Vulnerability Remedies By Asset View or Modify group permission
Vulnerability Summary By Asset Report	The report displays, for each asset, a list of detected vulnerabilities and their severity and description.	Report/Management/Vulnerability Summary By Asset View or Modify group permission
Vulnerable Assets Report	The report displays, for each detected vulnerability, a list of assets on which the vulnerability was detected.	Report/Management/Vulnerable Assets View or Modify group permission
Vulnerability Trend Report	The report displays a count per period (day, week, month, quarter, or year) of the detected vulnerabilities according to the following criteria: total, status (existing, fixed, new), new by severity, fixed by severity, and existing by severity.	Report/Management/Vulnerability Trend View or Modify group permission

5.1.6.3 IDS_STG.2 Prevention of System data loss

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

Application Note: IDS_STG.2 system data refers to scan data referred to in IDS_ANL.1

5.2 Security Functional Requirements for the IT Environment

The functional security requirements for the IT Environment consist of the following components, summarized below.

Table 21 - IT Environment SFRs

Functional Components	
FAU_STG.1	Protected Audit Trail Storage
FCS_CKM.4(2)	Cryptographic Key Destruction
FCS_COP.1(2)	Cryptographic Operation
FIA_ATD.1(2)	User Attribute Definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of Identification
FPT_ITT.1(2)	Basic Internal TSF Data Transfer Protection
FPT_RVM_OS.1	Non-bypassability of the TSP
FPT_SEP_OS.1	TSF domain separation
FPT_STM.1(2)	Reliable time stamps

Functional Components	
IDS_STG.1	Guarantee of System Data Availability

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1 Protected Audit Trail Storage

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

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

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1(2) The **IT Environment** ~~TSF~~ shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroization* that meets the following: *FIPS 140-2*.

5.2.2.2 FCS_COP.1 Cryptographic Operation

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

Table 22 - IT Environment SFRs

Operation	Algorithm (mode)	Key Size in Bits	Standards
Encryption and decryption	Triple-DES (EDE, CBC)	168	FIPS 46-3
Key agreement	RSA	1024 (modulus)	RFC2246
Hashing	SHS	128	FIPS 180-2

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_ATD.1 User Attribute Definition

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

a) username,

b) password.

5.2.3.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The **IT Environment** ~~TSF~~ shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

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

5.2.3.3 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The **IT Environment** ~~TSF~~ shall allow *no actions* on behalf of the user to be performed before the user is identified.

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

5.2.4 Protection of the TSF (FPT)

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

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

Rationale for SFR refinement: The TOE is responsible for protecting information sent from a Scanner. The IT Environment is responsible for protecting information sent from SiteProtector. Together FPT_ITT.1(1) and FPT_ITT.1(2) address TSF Data transfer protection.

5.2.4.2 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs

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

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM_SFT (levied on the TOE) for the remaining functionality.

5.2.4.3 FPT_SEP_OS.1 TSF Domain Separation for OSs

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

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

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP_SFT (levied on the TOE) for the remaining functionality.

5.2.4.4 FPT_STM.1 Reliable time stamps

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

5.2.5 IDS Component Requirements (IDS)

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

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

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

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

5.3 Strength of Function for the TOE

The minimum SOF claimed is SOF-Basic. None of the TOE SFRs utilize a probabilistic or permutational mechanism.

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the following table:

Table 23 - TOE Security Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration management	ACM_CAP.2	Configuration Items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High Level Design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 Scanning Security Function

6.1.1.1 Overview

The TOE scanners perform scanning on designated networks in order to discover assets, services, and vulnerabilities. The TOE's scanning is broken into two categories: discovery scans and assessment scans. Discovery scans are used to discover assets so that they may subsequently be assessed. Assessment scans perform in-depth searches for services and vulnerabilities on assets. Both types of scans can be managed separately and invoked separately.

Discovery scans attempt to discover systems on the network and information about these systems. Specifically, discovery scans attempt to discover the following information about network systems: the IP addresses of operational systems; the Operating System Identifier (OSID) for each of the operational systems; and the NetBIOS name for each of the operational systems.

Assessment scans attempt to identify the services running on discovered assets and discover known vulnerabilities.

6.1.1.2 Scanning Invocation

The TOE supports two types of scan invocations: background scans and ad-hoc scans. Background scans are scans that are periodically scheduled to run according to administrator configured parameters. The lowest granularity of background scans is to run once a day. Ad-hoc scans provide a means to run a scan immediately. The TOE enables an administrator to invoke discovery and assessment background scans and discovery and assessment ad-hoc scans.

6.1.1.3 Scanning Scope

Scans are defined by the group they are associated with which in turn designates assets to scan and Scanners (agents) to perform scans. In order to be able to delegate management of scanning to appropriate groups, the TOE supports a hierarchical organization consisting of a Site Group and one or more groups (sub-groups). Within a group, policies controlling the scans are inherited by default from the Site Group or may be customized for each group as necessary. Inheritance simplifies management of scans by permitting many assets to be managed as a single entity.

SiteProtector may (and typically does) operate in conjunction with multiple Scanners. SiteProtector allocates scanning tasks to individual Scanners based on configuration parameters of the scan policies. A single scan may be load shared between multiple Scanners for efficiency.

Assets discovered by a discovery scan may be configured to be automatically added to the Site Group or the groups associated with the scan. This simplifies the task of associating assets with assessment scans. Discovery scans attempt to determine the

operating identification (OSID) of each asset; this information is saved in the DBMS for later use in assessments.

6.1.1.4 Discovery Scans

Discovery scans may be invoked either by configuring a background discovery scan or an ad-hoc discovery scan. Discovery scans attempt to discovery assets and information about these assets. Specifically, discovery scans attempt to discover the following information about assets:

1) IP addresses of operational systems
2) MAC addresses of operational systems
3) Operating System Identifier (OSID) for each of the operational systems
4) NetBIOS domain and name for each of the operational systems.

The TOE uses the following four asset (scanner) policies to perform discovery scans:

1) Network Location Policy - The policy defines the network locations for scans within a group.
2) Scan Control Policy - The policy defines whether discovery scans are enabled or disabled. Additionally, the policy defines the occurrence rate (refresh cycle) for background discovery scans.
3) Discovery Scan Window Policy - The policy defines the allowable time windows to run background discovery scans. An administrator may optionally select to run ad-hoc discovery scans during the time windows defined in the Discovery Scan Window Policy or to run ad-hoc scans immediately.
4) Discovery Policy - The policy defines IP address ranges on which to perform discovery scans. The policy also enables an administrator to select whether discovered assets should be automatically added to a group (subsequently included in assessment scans).

The TOE transmits packets to each IP address included in the Discovery Policy and analyzes the responses to determine the IP address, MAC address, operating system identification (OSID), operating system version, and NetBIOS name of each asset. When new information about a system is discovered, a Scan Event is generated. Each event includes the date and time of the result, type of result, and identification of data source. The event also includes event-specific information as specified in Table 19. This information is saved in the DBMS and used in subsequent assessment scans.

6.1.1.5 Assessment Scans

Assessment scans are associated with assets within the Site Group or group(s) and may be performed either in background (periodic) or ad-hoc modes. The OSID and version associated with each asset is used to determine which checks (vulnerabilities) are applicable to each asset.

The Scanner can identify the following information in an assessment scan:

1) Services running on each asset

2) Known vulnerabilities on each asset.

Scanners perform assessments by sending packets to each target system and analyzing the responses. Incoming packets are compared against signatures. If the received network traffic indicates a scan response, the Scanners analyze the network packets returned by the target systems and generate a scan event that reports the result of a scan. Scan events include source system, date and time, type of service or vulnerability, severity (vulnerabilities only) and success or failure of the check. Scan events report services and vulnerabilities found as well as vulnerabilities not found. Scan events are sent to SiteProtector and stored in the IT Environment supplied DBMS.

The TOE uses the following asset (scanner) policies to perform assessment vulnerability scans:

1) Network Location Policy - The policy defines the network locations for scans within a group.
2) Scan Control Policy - The policy defines whether assessment scans are enabled or disabled. Additionally, the policy defines the occurrence rate (refresh cycle) for background assessment scans.
3) Scan Exclusion Policy - The policy defines IP addresses and ports to exclude from assessment scans.
4) Assessment Policy - Checks - The policy defines which assessment checks (vulnerabilities) to run.
5) Assessment Policy - Settings - The policy defines TCP and UDP port ranges to perform assessment scans.
6) Assessment Credential Policy - The policy contains login credential used for assessment checks that require authenticated access.
7) Assessment Scan Window Policy - The policy defines the allowable time windows to run background assessment scans. An administrator may optionally select to run ad-hoc assessment scans during the time windows defined in the Assessment Scan Window Policy or to run ad-hoc scans immediately.
8) Network Services Policy – The policy defines which ports services run on.

6.1.2 Management Security Function

The TOE's Management Security Function provides administrator support functionality that enables a user to manage and monitor the TOE via a GUI interface (SiteProtector Console). After installation, all management and monitoring of the TOE occurs through SiteProtector. The following sections describe the management functionality provided by the TOE.

6.1.2.1 Site, Site Group, and Groups Management

SiteProtector manages SiteProtector, Scanners, discovered assets, and TSF data in a hierarchical tree format of: Site, Site Group and Groups. A site is an instance of a SiteProtector. For this TOE, one site exists. The site is automatically created at SiteProtector installation. The next level of management is the Site Group. The Site

Group is also automatically created at SiteProtector installation. Each site contains one Site Group. The Site Group maintains an instance of scan policies, group permissions, assets, agents, and jobs. The next level of management is groups. Groups are created by an administrator but are not required in the TOE management infrastructure. Groups enable an administrator to group assets; configure policies (scan policies) specific to those assets; configure group permissions specific to the group; and to run scans for the group only. Groups aid in scanning management. Rather than run all assessment checks for all assets, groups enable an administrator to refine a scan's scope based on assets.

The Site can be viewed but cannot be deleted and there are no management parameters associated with a Site. Likewise, the Site Group can be viewed but cannot be deleted. Groups however can be created and deleted and parameters can be modified for the group. By default, a group is created and is empty. However, assets and agents can be moved into a group. Policies and group permissions can be configured specifically for the group. The TOE maintains a copy of the asset policies and the group permissions at the Site Group level. A group's asset policies and group permissions may be configured to be inherited or overridden. Inherited means the group uses the data (policy or group permissions) at the Site Group level. Override means the group maintains an individual copy of the data and modifications made at the Site Group level do not affect the group. Defining a group's policies and parameters refines scans and determines which assets are automatically included in the group.

6.1.2.2 Agents and Assets Management

TOE Agents are IBM ISS products. The agents included in the TOE are the all scanners and the SiteProtector. The TOE identifies SiteProtector as four separate agents: SiteProtector Database, Event Collector, SiteProtector Core and Agent Manager. Agents are known to the TOE at the site level and at the group level. Site level agents include the SiteProtector agents. Group level agents include the same set of SiteProtector TOE component modules and also include any Network Enterprise Scanners.

An asset is an individual computer or device on a network. Assets are known to the TOE at the site level and the group level. Assets of the TOE on the site level display the SiteProtector Host. Assets of the TOE at the group level display the SiteProtector Host; all Network Enterprise Scanners in the group; and the systems discovered during scanning.

Agents are viewed using the Site Agent List and the Group Agent Lists. Agents are automatically added to SiteProtector. The management functions provided by SiteProtector pertaining to agents is an administrator may delete a Scanner and an administrator may move a Scanner from the Site group to a group. An administrator must be assigned the Agents group permission at the Modify level in order to move or delete a scanner.

Assets known by the TOE are SiteProtector, any Scanners and any configured or discovered hosts. Assets are viewed using the Site Asset List and the Group Asset Lists. The management functions provided by SiteProtector pertaining to assets is an administrator may delete an asset other than SiteProtector, and an administrator may move an asset from the Site group to a group. An administrator must be assigned the Assets group permission at the Modify level to delete or move a scanner.

6.1.2.3 Group Ownership, Global Permissions, and Group Permissions Management

The TOE enforces three types of permissions that enable administrators to perform management and monitoring operations: global permissions, group ownership and group permissions. Global permissions are permissions that apply at the Site level. Global permissions are assigned to a user either by userid or by user group. A user must be assigned a global permission or belong to a user group that has been assigned a global permission in order to perform any global permission related function. Global permissions include which administrators can view and modify user groups and users; which administrators can view and assign global permissions; and which administrators can enable and disable audit data generation. Additionally, the global permissions include the Full Access To All Functionality permission. If an administrator is assigned this permission or belongs to a user group who has been assigned this permission, the administrator may perform any TOE management or monitoring function.

The second type of permission enforced by SiteProtector is group ownership. Group ownership is required and enforced to configure Group Permissions. A group owner or a user who has been assigned Full Access To All Functionality permission may change a group's owner.

The third type of permission enforced by the TOE is group permissions. Group permissions apply to groups. The Site Group maintains a copy of group permissions. All groups defined beneath the Site Group may be configured to use the Site Group's Group Permissions copy or may be configured to maintain a unique copy of the group permissions. This unique copy may be modified by an administrator. Group permissions are assigned to a user either by userid or by user group. A user must be assigned a group permission or belong to a user group that has been assigned a group permission in order to perform any group-level functions. The TOE includes 30 group permissions. Each group permission includes a group permission level (View, Modify or Control, or a combination of the three levels). Not all group permission levels apply to each group permission. Group permissions include which administrators may manage scanner policies; invoke ad-hoc scans; manage groups, agents and assets; and create, view and delete reports. Only users who are the group owner or a user who has been assigned Full Access To All Functionality permission may assign group permissions to a user or user group.

6.1.2.4 User Groups and Users Management

To access SiteProtector, a user invokes the SiteProtector Console. The SiteProtector Console requests a userid and password from the user. Once entered, SiteProtector passes the information to Windows (IT Environment) to authenticate the user. If Windows indicates that the user is not authenticated, SiteProtector terminates the session. If Windows indicates that the user is authenticated, SiteProtector looks up the userid in its database (IT Environment supplied DBMS) to determine the user group(s), global permissions, group permissions, and group ownership associated with the user. At the minimum, a user must be assigned the Site Group's Group group permission at the View level or be a member of a user group that has been assigned the Site Group's Group

group permission at the View level in order to log on to SiteProtector. If the user does not have the minimum permission to log on, SiteProtector will terminate the session.

Global permissions and group permissions are assigned to users by userid or user group. Additionally, groups' ownerships are identified and modified by userid. User groups are specific to SiteProtector; a user group does not need to be known by the IT Environment to be created by a SiteProtector administrator. However, userids do need to be known to the IT Environment. Userids are entered when added to a user group; assigned a global permission or group permission; and when entered as a new group owner. When an administrator enters a userid, the TOE interfaces to the IT Environment and determines if the userid is known to the IT Environment. If the userid is not known to the IT Environment, the TOE will reject the operation. If the userid is known to the IT Environment, the operation is allowed.

6.1.2.5 Modification of Scan Behavior

The following sections describe scan management.

6.1.2.5.1 Disabling and Enabling Scanning

Scanning is enabled and disabled using the group's Scan Control Policy. A group's Scan Control Policy effects both background and ad-hoc scanning. The policy enables an administrator to enable or disable both discovery and assessment scans separately and enables an administrator to define the reoccurrence rate of background scans (refresh cycle). Disabling and enabling scanning is a privileged operation and can only be performed by an administrator assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Policy Control group permission for the group.

6.1.2.5.2 Managing Background Scans

The TOE enables an administrator to start a discovery background scan job, an assessment background scan job, or a background scan that performs both types of scans. Invoking background scans is a privileged operation. An administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Modify group permission specified in the following table in order to modify any of the background scan's policies.

Table 24 - Background Scan Policy Permissions

Group Permission	Applies To These Policies
Assessment Credentials Policy	Assessment Credentials Policy
Assessment Policy	Assessment Policy
Discovery Policy	Discovery Policy
Policy	Scan Control Policy, Scan Exclusion Policy
Scan Window Policy	Scan Window Policy

In order to launch a new background scan or modify an existing background scan, the administrator must have permission to modify the Scan Control Policy.

6.1.2.5.3 Managing Ad-Hoc Scans

The TOE enables an administrator to start a discovery ad-hoc scan job, an assessment ad-hoc scan job, or an ad-hoc scan that performs both types of scans. When an ad-hoc scan is invoked, the scan inherits the group's existing policies. However, the TOE enables an administrator to modify a subset of policies related to the scan. This scan-job-specific copy of the policies is maintained for the life of the scan job (until the scan job is deleted) and is reused if the scan job is rerun. The scan-job-specific policies are the Discovery Policy used for discovery scans and the Assessment Checks Policy and Assessment Setting Policy used for assessment scans.

Invoking ad-hoc scans is a privileged operation. An administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Ad Hoc Scan Control user group permission in order to start ad-hoc scans. Additionally, an administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Discovery Policy Modify group permission in order to modify an ad-hoc scan's Discovery Policy. An administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Assessment Policy Modify group permission in order to modify any of the ad-hoc scan's assessment policies.

6.1.2.5.4 Defining the Scope of Discovery Scans

Discovery scans are, by default, run against all hosts defined in the group's Network Location Policy. However, the TOE provides an administrator the ability to refine discovery scans based on IP address ranges. This functionality is provided by enabling an administrator to modify the Scanner's Discovery Policy (TSF Data). Modifying the Discovery Policy is a privileged operation. An administrator must be assigned the Full Access To All Functionality global permission or the group's Agent/Network Enterprise Scanner/Discovery Policy group permission at the Modify level in order to modify the Discovery Policy.

6.1.2.5.5 Defining the Scope of Assessment Scans

Assessment scans by default run all assessment checks, for both TCP and UDP ports, and all service checks defined in the Assessment Checks Policy, the Assessment Settings Policy, and Network Services Policy. However, the TOE provides an administrator with the ability to refine which assessment checks to run (Assessment Checks Policy); define the UDP and TCP port ranges to perform assessment checks (Assessment Setting Policy); define whether service checks should be run for TCP ports, UDP ports or both (Assessment Setting Policy); define which services to check (Network Services Policy); and define hosts and ports to exclude from a scan (Scan Exclusion Policy). Refining the scope of an assessment scan is a privileged operation. An administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Assessment Policy Modify group permission for the group in order to modify the Assessment Checks Policy or the Assessment Settings Policy. An administrator must be assigned the Full Access To All Functionality global permission or the Agent/Network Enterprise Scanner/Policy Control group permission for the group in order to modify the Network Services Policy or the Network Exclusion Policy.

6.1.2.5.6 Managing Scan Jobs

Scan jobs may be run at the Site Group level and at the group level. Scans run at the Site Group level are listed in the Site Job Status List. Scans run at the group level are listed in the group's job status list. Once a scan job (background or ad-hoc) is invoked, the job is listed as an entry in the group's job status list. The Site Job Status List and the group's job status list display the status of individual scan jobs. Available statuses are:

1) Pending – the scan job is starting and collecting policies.
2) Idle – the scan job is idle (waiting for an open scan window).
3) Processing – the scan job is currently running.
4) Paused – the scan job was paused.
5) Completed – the scan job has completed.
6) Cancelled – the scan job was cancelled.
7) Expired – a cancelled job has not been resumed or rerun in seven days.

Jobs enter the idle, processing, completed, and expired states without any interaction from an administrator. Jobs enter the pending, paused, and cancelled states with interaction due to administrators' actions. Jobs enter the pending state when invoked; the paused state when paused; and the cancelled state when canceled by an administrator.

On an individual scan job basis, an administrator may cancel, rerun, pause and resume scan jobs. These management functions apply only when a scan job is in a specific state (status) (for example, a canceled scan job cannot be canceled). The following table specifies the specific management function that is allowed given a scan job's state. An entry in the table means the management function is available for the state listed in the column. Each entry identifies the next state the scan job will enter based on the management command. Managing a scan job is considered an ad-hoc scan function and therefore, an administrator must be assigned the Full Access to All Functionality global permission or the Agent/Network Enterprise Scanner/Ad Hoc Scan Control group permission in order to perform the following management functions.

Table 25 - Scan Job States

Scan Job Management Function	Scan Job State (status)						
	Pending Scan	**Idle Scan**	**Processing Scan**	**Paused Scan**	**Canceled Scan**	**Completed Scan**	**Expired Scan**
Rerun	Next state = pending	Next state = pending	Next state = pending	Next state = pending	Next state = pending	Next state = pending	Next state = pending
Pause	Next State = Paused	Next State = Paused	Next State = Paused	N/A	N/A	N/A	N/A
Resume	N/A	N/A	N/A	Next state = previous	N/A	N/A	N/A

Scan Job Management Function	Scan Job State (status)						
	Pending Scan	**Idle Scan**	**Processing Scan**	**Paused Scan**	**Canceled Scan**	**Completed Scan**	**Expired Scan**
				state either pending, idle or processing			
Cancel	Next state = Canceled	Next state = Canceled	Next state = Canceled	Next state = Canceled	N/A	N/A	N/A

6.1.3 Audit Data Generation and Viewing Security Function

The TOE's audit data include two types of audit data: Audit Events and Audit Data Reports. Audit Events are generated as the result of administrator commands, stored in the DBMS (IT Environment), and available for viewing by generating an Audit Data Report. Audit Data Reports are files that contain a human readable representation of the Audit Events. Audit Data Reports provide the only means to view Audit Events. These reports, available due to the SiteProtector Reporting Module, are not automatically created and must be created by an authorized administrator.

Audit Events are generated as the result of administrator commands. These events include recording SiteProtector Console log ins and outs; policy modifications; group, agent and asset management operations; user group and user management operations, user group and user permission management operations, and starting ad-hoc scans. Table 12 identifies the Audit Events generated by the TOE. Audit Events are stored in the IT Environment supplied disk using the IT Environment supplied DBMS interface. The SiteProtector relies on the timestamps that is derived from the resident operating system. If the TOE attempts to store an Audit Event and the disk is full, the DBMS will return a response indicating storage exhaustion. Upon receipt of a storage exhaustion response, the TOE will generate an alarm (SNMP trap) indicating the DBMS is full. If the DBMS enters this state, the TOE directs the DBMS to store new Audit Events by overwriting the oldest Audit Events. In this state, a DBMS administrator (IT Environment) is required to correct the situation (back-up or delete old data).

The second type of TOE audit data is the Audit Detail Report. This report, available via the SiteProtector Reporting Module, 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. The IT Environment is responsible for managing Audit Data Reports and notifying the administrator if storage exhaustion is reached. If the Audit Data Reports exhaust the OS' storage space, the OS will ignore any new requests to store reports (audit data) and generate an alarm (displayed on the console). In this state, an OS administrator (IT Environment) is required to correct the situation (back-up or delete old data).

An administrator may disable and re-enable generation of individual Audit Events. Audit Events are enabled and re-enabled by modifying one of seven selective auditing lists, referred to as Selective Auditing lists. These lists are organized according to audit record categories: General, Group, Agent, Asset, Policy, User Group and Report and modified based on event type. An administrator must be assigned the Full Access To All Functionality global permission or the Auditing Setup global permission in order to view and/or modify audit records generation lists.

6.1.4 System Data Generation Security Function

Scanners initiate scans by sending network packets to targeted IT systems. Incoming network data sent by the remote systems in response to scan traffic are received by the Scanners and compared against signatures. If the network traffic indicates a scan response, the Scanners generate Scan Events that report the results of a scan; the contents of each type of Scan Event are specified in Table 19 in addition to the source system, date and time. The Scanner generates its own timestamps for scan events and does not rely on the IT Environment. During installation, if multiple Scanners are deployed, the time can be synchronized between the Scanners during configuration. However, since each Scanner manages its own time internally, a guarantee of time synchronization cannot be kept. Scan Events report systems, services and vulnerabilities found as well as vulnerabilities not found. Scan Events are sent to SiteProtector and stored in the IT Environment supplied DBMS. Upon receipt of the Scan Events, SiteProtector processes the Scan Events into an analysis view format and stores the Scan Events in the DBMS (IT Environment).

System data is stored on disk using the IT Environment supplied DBMS interface. If the TOE attempts to store system data and the DBMS is full, the DBMS will return a response indicating storage exhaustion. Upon receipt of a storage exhaustion response, the TOE will generate an alarm (SNMP trap) indicating the DBMS is full. If the DBMS enters this state, the TOE directs the DBMS to overwrite the system data based on age (oldest overwritten). In this state, a DBMS administrator (IT Environment) is required to correct the situation (back-up or delete old data).

system data reports must be generated by an administrator. Reports are stored on disk using the OS' file I/O functionality (IT Environment). If the system data reports exhaust the OS' storage space, the OS will ignore any new requests to store reports In this state, an OS administrator (IT Environment) is required to correct the situation (back-up or delete old data).

6.1.5 System Data Viewing Security Function

The TOE's System Data Viewing Security Function provides administrator support functionality that enables administrators to view system data (the results of discovery and assessment scans) in human readable format via the SiteProtector Console. The TOE offers two methods for viewing system data: Analysis Views and Reports. Both methods use Scan Events as input to display scan results. Analysis View data is automatically generated and displayed by SiteProtector upon receipt of Scan Events from the scanners. Conversely, Reports must be generated by administrators.

The Analysis View functionality provided by SiteProtector enables an administrator to view vulnerability Scan Events organized by the following predefined formats: asset, vulnerability detail, object, and vulnerability name. Analysis Views also permit administrators to view host discovery and service discovery Scan Events. The list and description of the Analysis Views is included in Table 20.

The Reporting Module supplies an alternative method from Analyst Views to view Scan Events, including the results of discovery scans; services discovered as the result of assessment scans; and vulnerabilities discovered as the result of assessment scans. The TOE supports multiple administrator selectable reports, enabling an administrator to view information formatted in different ways. The list and description of the reports is included in Table 20.

An authorized administrator must create system data reports (Management Security Function); system data reports are not automatically generated. When a system data report is generated, the TOE fetches the Scan Events from the DBMS; formats the Scan Events in human readable format; formats the complete report; and stores the system data reports on disk using the OS' file I/O functionality (supplied by the IT Environment). The reports related to scanning are identified by *Category/Template Name* (and identified as System Data –Reports in Table 3). Each report has a specific group permission associated with it. An administrator must be assigned the Full Access To All Functionality global permission or the group's Report/*Category/template name* group permission at the Modify level in order to create or delete a *Category/Template Name* Report. Once created, an administrator assigned the Full Access To All Functionality global permission or the group's Report/*Category/template name* group permission at the View or Modify level may view a list of all previously created reports and open each report. The IT Environment is responsible for managing system data reports and notifying the administrator if storage exhaustion is reached. If the system data reports exhaust the OS' storage space, the OS will ignore any new requests to store reports (system data) and generate an alarm (displayed on the console). In this state, an OS administrator (IT Environment) is required to correct the situation (back-up or delete old data).

When viewing scan events from multiple Scanners, the administrator should understand that time is not necessarily synchronized between the different Scanners because timestamps are generated internally for each Scanner.

6.1.6 Self Protection Security Function

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the permissions are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC.

TLS 1.0 (tested by the CCTL) is used to protect communication between the scanners and SiteProtector. The TLS implementation is included in the TOE boundary in the scanners and is part of the IT Environment with SiteProtector. The cipher suite used for the TLS session is TLS_RSA_WITH_3DES_EDE_CBC_SHA. The Scanners initiates the connection with SiteProtector. SiteProtector responds with its RSA certificate; the Sensors authenticate the server (SiteProtector) by comparing the SiteProtector-supplied certificate to the certificate saved in the Scanner during installation. The pre-master secret is generated with the Scanner'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 3DES (CAVP cert TBD) operating with 168 bit keys in CBC mode. SHA-1 (CAVP cert TBD) is used for message integrity checking. Session keys held in memory are zeroized when a session ends. RSA certificates are generated by the IT Environment during TOE installation.

6.2 Assurance Measures

6.2.1 TOE Security Assurance Requirements

Table 26 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Configuration Items	IBM ISS performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE. The configuration items are uniquely identified and each release of the TOE has a unique reference.
ADO_DEL.1	Delivery process documentation	IBM ISS documents the delivery procedure for the TOE to include how components of the TOE are delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained.
ADO_IGS.1	Installation guidance	IBM ISS documents the installation,

Assurance Component	Documentation Satisfying Component	Rationale
		generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ADV_FSP.1	Functional specification	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by IBM ISS development evidence.
ADV_HLD.1	Descriptive High Level Design	The subsystems and the communication between the subsystems of the TOE are documented in IBM ISS development evidence.
ADV_RCR.1	Correspondence analysis	The correspondence is contained in the documents used for ADV_FSP.1 and ADV_HLD.1.
AGD_ADM.1	Administrator guidance	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_USR.1	User guidance	User guidance is provided for those roles defined in the TOE that do not have all the authorizations as the administrative role.
ATE_COV.1	Evidence of Coverage	IBM ISS demonstrates the external interfaces tested during functional testing using a coverage analysis.
ATE_FUN.1	Test plan, procedures, and results	IBM ISS functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	TOE	IBM ISS will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_SOF.1	Strength of function analysis	IBM ISS documents the strength of function associated with any permutational or probabilistic mechanisms satisfies the minimum strength of function claimed in the ST.
AVA_VLA.1	Vulnerability analysis	IBM ISS documents their vulnerability analysis search for obvious flaws and weaknesses in the TOE.

6.2.2 Rationale for TOE Assurance Requirements

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

The general level of assurance for the TOE is:

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

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

CHAPTER 7

7. Protection Profile Claims

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

7.1 Protection Profile Reference

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

7.2 Protection Profile Refinements

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

7.3 Protection Profile Additions

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

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions, threats and policies. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functionality.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each assumption, threat and policy is addressed by a security objective.

The following table identifies for each assumption, threat, and policy, the security objective(s) that address it.

Table 27 - Assumptions, Threats and Policies to Security Objectives Mapping

Assumptions, Threats and Policies	Security Objectives																		
	O.PROTECT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
A.ACCESS														X					
A.DYNMIC													X	X					
A.ASCOPE														X					
A.PROTCT											X								
A.LOCATE											X								
A.MANAGE													X						
A.NOEVIL										X	X	X							
A.NOTRUST											X	X							
T.COMINT	X				X	X			X							X			X
T.COMDIS	X				X	X			X							X			X
T.LOSSOF	X				X	X			X							X			X
T.NOHALT	X				X	X													X
T.PRIVIL	X				X	X										X			X

Assumptions, Threats and Policies	Security Objectives																		
	O.PROTECT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
T.IMPCON				X	X	X				X									X
T.INFLUX							X												
T.FACCNT								X											
T.SCNCFG		X																	
T.SCNMLC		X																	
T.SCNVUL		X																	
T.FALREC			X																
T.FALASC			X																
P.DETECT		X													X				
P.ANALYZ			X																
P.MANAGE	X			X	X	X				X		X	X			X			X
P.ACCESS	X				X	X										X	X		X
P.ACCACT						X		X											
P.INTGTY									X										
P.PROTCT	X						X				X					X			

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the assumption, threat and policy to security objectives mapping.

Table 28 - Assumption, Threat and Policy to Security Objectives Rationale

Assumption, Threat, and Policy	Security Objectives Rationale
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The O.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

Assumption, Threat, and Policy	Security Objectives Rationale
	The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will be managed appropriately.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The O.INTROP objective ensures the TOE has the necessary interactions with the IT Systems it monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The O.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
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. The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRUST	The TOE can only be accessed by authorized users. The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified without authorization. The O.PROTECT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified without authorization. The O.PROTECT objective addresses this threat by

Assumption, Threat, and Policy	Security Objectives Rationale
	providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified without authorization. The O.PROTECT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
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. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. . The O.PROTECT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH and OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE to handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in an IT System the TOE monitors.

Assumption, Threat, and Policy	Security Objectives Rationale
	The O.IDSCAN objective counters this threat by requiring the TOE to collect and store asset information that might be indicative of a configuration setting change.
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. The O.IDSCAN objective counters this threat by requiring the TOE to collect and store vulnerability information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring the TOE to collect and store vulnerability that might be indicative of a vulnerability.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on the network data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities from a data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of the network data received from all data sources. The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities from multiple data sources.
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. The O.IDSCAN objective addresses this policy by requiring collection of Scanner data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.ANALYZ	Analytical processes and information to derive conclusions about vulnerabilities must be applied to incoming Scanner network data and appropriate notification provided. The O.IDANLZ objective requires analytical processes be applied to data by Scanners.
P.MANAGE	The TOE shall only be managed by authorized users. The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTECT objective addresses this policy by providing TOE self-protection. . The OE.PROTECT objective supports the TOE protection from the IT Environment.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized

Assumption, Threat, and Policy	Security Objectives Rationale
	purposes. The O.IDAUTH and OE.IDAUTH objectives provide for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the system data trail. The O.PROTECTand OE.PROTECT objective addresses this policy by providing TOE self-protection.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.IDAUTH objective provides for identification of administrative users, enabling their actions to be audited. The O.AUDITS objective provides for audit records of the actions of administrative users to be created.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE to handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications. The O.PROTECT and OE.PROTECT objectives support the TOE from unauthorized access.

8.2 Rationale for Security Functional Requirements (SFRs)

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 29 - TOE SFRs to Security Objectives Mapping

TOE SFRs	TOE Security Objectives								
	O.PROTECT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_GEN.1								X	
FAU_SAR.1				X	X				
FAU_SAR.2				X	X				
FAU_SEL.1				X				X	

TOE SFRs	TOE Security Objectives								
	O.PROTECT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_STG.4							X		
FCS_CKM.1	X								
FCS_CKM.4(1)	X								
FCS_COP.1(1)	X								
FIA_ATD.1(1)					X	X			
FMT_MOF.1	X			X	X				
FMT_MTD.1	X			X	X	X			X
FMT_SMF.1				X					
FMT_SMR.1				X	X	X			
FPT_ITT.1(1)	X								
FPT_RVM_SFT.1	X								
FPT_SEP_SFT.1	X								
FPT_STM.1(1)		X							
IDS_ANL.1		X	X						
IDS_RDR.1				X	X				
IDS_STG.2							X		

The following table provides the detail of TOE security objective(s).

Table 30 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized administrators of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE with appropriate permissions may query system data and audit data, and authorized administrators of the TOE with appropriate permissions may query and modify all other TOE data [FMT_MTD.1]. The TOE protects itself from bypass [FPT_RVM_SFT.1] and interference [FPT_SEP_SFT.1] from subjects within the TSC. The TOE also protects information sent from Scanners to SiteProtector, which would be another attack vector for interference or tampering [FPT_ITT.1(1)]. This protection is provided by cryptographic functionality [FCS_CKM.1(1), FCS_CKM.4(1), FCS_COP.1(1)].

Security Objective	SFR and Rationale
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. A System containing a Scanner is required to collect and store static configuration information of an IT System [IDS_ANL.1]. Timestamps are provided by the Scanner that performs the scan [FPT_STM.1(1)].
O.IDANLZ	The TOE must accept data from Scanners and then apply analytical processes and information to derive conclusions about vulnerabilities. Scanners are required to perform vulnerability analysis and generate conclusions [IDS_ANL.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability for authorized administrators to view system data and audit data [IDS_RDR.1, FAU_SAR.1, FAU_SAR.2]. The TOE enables a authorized administrators to enable and disable audit records [FAU_SEL.1]. The TOE must be able to recognize administrators that exist for the TOE [FMT_SMR.1]. The TOE provides a set of management functions that allow effective management of the TOE [FMT_SMF.1]. This set includes functions that effect security behaviour [FMT_MOF.1] and functions that enable an administrator to view/modify TSF data are identified [FMT_MTD.1].
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.1, FAU_SAR.2]. The TOE is required to restrict the review of system data to those granted with explicit read-access [IDS_RDR.1]. Security attributes and group ownership is used to enforce the access policy [FIA_ATD.1(1)]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized system administrators of the TOE may query and modify TOE data [FMT_MTD.1]. The TOE must be able to recognize the user role and permissions that exists for the TOE [FMT_SMR.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE works with the IT Environment to identify and authenticate administrators. Once authenticated, only users who have been properly configured may log into the TOE [FMT_SMR.1, FMT_ATD.1]. Administrators' privileges are individually configured [FMT_MTD.1].
O.OFLOWS	The TOE must appropriately handle potential audit data and system data storage overflows. The TOE must prevent the loss of audit data and system data in the event its trail is full [FAU_STG.4 and IDS_STG.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1].

Security Objective	SFR and Rationale
O.INTEGR	The TOE must ensure the integrity of all TSF data. Only authorized administrators of the TOE with appropriate permissions may query or modify TSF data [FMT_MTD.1].

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each IT Environment security objective, the SFR(s) that address it.

Table 31 - IT Environment SFRs to Security Objectives Mapping

IT Environment SFRs	IT Environment Security Objectives				
	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.SD_PROTECTION	OE.IDAUTH
FAU_STG.1			X		
FCS_CKM.4(2)		X			
FCS_COP.4(2)		X			
FIA_ATD.1(2)					X
FIA_UAU.1					X
FIA_UID.1					X
FPT_ITT.1(2)		X			
FPT_RVM_OS.1		X			
FPT_SEP_OS.1		X			
FPT_STM.1(2)	X				
IDS_STG.1				X	

The following table provides the detail of TOE security objective(s).

Table 32 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
OE.TIME	The IT Environment will provide reliable timestamps to the TOE. Timestamps used by SiteProtector for audit data generation are provided by the IT Environment [FPT_STM.1(2)].
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering. The IT Environment must ensure that functions are invoked and succeed on the SiteProtector Host before each function may proceed [FPT_RVM_OS.1]. The TSF must be protected from interference that would prevent the TSF from performing its functions on the SiteProtector Host [FPT_SEP_OS.1]. The IT Environment also protects information sent from the SiteProtector to a Scanner, which would be another attack vector for interference or tampering [FPT_ITT.1(2)]. This protection is provided by cryptographic functionality [FCS_CKM.4(2), FCS_COP.1(2)].
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information. The IT Environment is required to protect the audit data from deletion [FAU_STG.1].
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data. The IT Environment is required to protect the system data from deletion [IDS_STG.1].
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to the TOE allowing access to TOE functions and data. The IT Environment is required to successfully identify and authenticate administrators prior to the TSF being invoked [FIA_UAU.1, FIA_UID.1]. The IT Environment is able to associate a password with specific userids in order to perform authentication [FIA_ATD.1(2)].

8.3 Rationale for TOE Summary Specification

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 33 - SFRs to TOE Security Functions Mapping

	Security Functions

	Audit Data Generation and Viewing	Management	Scanning	Self Protection	System Data Generation	System Data Viewing
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SEL.1	X					
FAU_STG.4	X					
FCS_CKM.1				X		
FCS_CKM.4(1)				X		
FCS_COP.1(1)				X		
FIA_ATD.1(1)	X	X				X
FMT_MOF.1		X				
FMT_MTD.1		X				
FMT_SMF.1		X				
FMT_SMR.1	X	X				X
FPT_ITT.1(1)				X		
FPT_RVM_SFT.1				X		
FPT_SEP_SFT.1				X		
FPT_STM.1(1)					X	
IDS_ANL.1			X		X	
IDS_RDR.1						X
IDS_STG.2					X	

Table 34 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	Audit Data Generation and Viewing Security Function - The TOE generates audit records reporting the security relevant management actions including modification of TSF Data and modification of TOE system behavior. Included in each audit record is date and time, type of event, identity of the system that generated the record, and outcome of event.
FAU_SAR.1	Audit Data Generation and Viewing Security Function – The TOE enables authorized administrators to view all audit records generated as the result of a management command including modification to TSF data and modification of TSF behavior. Only authorized users who have successfully authenticated to the SiteProtector OS (IT Environment supplied Windows OS) and who have permission to view audit records may view audit records. Permissions are configured on a user or user group bases. All audit record viewing is done via the SiteProtector Console which supplies a GUI interface for human users.
FAU_SAR.2	Audit Data Generation and Viewing Security Function - Only authorized users who have successfully authenticated to the SiteProtector OS (IT Environment supplied Windows OS) and who have been configured to view audit records may view audit records. Audit data is not available to users who have not met the above criteria.
FAU_SEL.1	Audit Data Generation and Viewing Security Function – The audit events generated by the TOE as the result of management activity may be disabled according to event type. Event types include logging into and out of the SiteProtector Console; adding and removing groups, assets; modifications to global and group permissions; and creating and viewing audit and system data.
FAU_STG.4	Audit Data Generation and Viewing Security Function – SiteProtector communicates with the DBMS to store audit records. When the DBMS becomes full, the DBMS responds to a store command sent from the TOE indicating the DBMS is full. The TOE in turn will generate an alarm (an SNMP trap). If this state occurs, the TOE instructs the DBMS to overwrite old audit records with new data.
FCS_CKM.1	Self Protection Security Function – The TOE's Sensors protects TSF data from disclosure and modifications when it is transmitted between separate parts of the TOE by using TLS. The TOE's Scanners generate a session key for the TLS session.
FCS_CKM.4(1)	Self Protection Security Function – The TOE's Scanners protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by using TLS. When a session ends, the key is zeroized.
FCS_COP.1(1)	Self Protection Security Function – The TOE's Scanners protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by using TLS. The encryption algorithm is 3DES (EDE CBC), RSA is used for key agreement, and message integrity uses SHA-1.

SFR	SF and Rationale
FIA_ATD.1(1)	Management Security Function – SiteProtector interacts with the OS to determine if a user has properly identified and authenticated through the SiteProtector logon screen. The TSF maintains an internal representation of a user profile after the user has successfully logged on through the SiteProtector logon screen. The user profile includes SiteProtector user group membership; group membership; global permissions; group permissions; and group ownership. The TSF uses this user profile to determine what management functions a user has or does not have access to. Audit Data Generation and Viewing Security Function – SiteProtector interacts with the OS to determine if a user has properly identified and authenticated through the SiteProtector logon screen. The TSF maintains an internal representation of a user profile after the user has successfully logged on through the SiteProtector logon screen. The user profile includes SiteProtector user group membership; group membership; global permissions; group permissions; and group ownership. The TSF uses this user profile to determine if the user has or does not have access to audit data. System Data Viewing Security Function – SiteProtector interacts with the OS to determine if a user has properly identified and authenticated through the SiteProtector logon screen. The TSF maintains an internal representation of a user profile after the user has successfully logged on through the SiteProtector logon screen. The user profile includes SiteProtector user group membership; group membership; global permissions; group permissions; and group ownership. The TSF uses this user profile to determine what system data (records) a user has or does not have access to.
FMT_MOF.1	Management Security Function – The TOE support multiple functions that enable an administrator to modify scans including modifying scan parameters and modifying scan jobs (disable, pause, rerun). The permissions of the administrator determine the level of ability to modify the behaviour of the scanning function.
FMT_MTD.1	Management Security Function – The TOE enables authorized administrators to view and modify TSF data. The permissions of the user determine the level of access to the TSF data.
FMT_SMF.1	Management Security Function – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	Management Security Function – The TOE provides a single administrator role. Granularity of permissions is provided via per-user or per-user-group permissions. The permissions assigned administrators and group ownership determine what operations an administrator can perform. Audit Data Generation and Viewing Security Function – The permissions assigned administrators determine if the administrator is authorized to view audit data. System Data Viewing Security Function - The permissions assigned administrators determine if the administrator is authorized to view system data.
FPT_ITT.1(1)	Self Protection Security Function – The TOE protects itself by protecting communication from the Scanners to the SiteProtector from disclosure and modification by using TLS to encrypt all traffic sent from the Scanners.

SFR	SF and Rationale
FPT_RVM_SFT.1	Self Protection Security Function – The TOE protects itself from bypass within the TSC by providing well-defined interfaces and ensuring that the security policies are enforced for security-relevant interfaces.
FPT_SEP_SFT.1	Self Protection Security Function – The TOE protects itself from interference within the TSC by providing well-defined interfaces and ensuring that permissions for each administrator are properly associated with each session.
FPT_STM.1(1)	System Data Generation Security Function – The Scanners provide a timestamp to record the time of scan results that are stored in the DBMS (IT Environment supplied).
IDS_ANL.1	Scanning Security Function – The TOE analyzes the results of the scanning performed to determine the results of scans. System Data Generation Security Function – Scan events, generated by the Scanners reporting the results of analyzing network data, are stored in the DBMS.
IDS_RDR.1	System Data Viewing Security Function – The TOE provides the ability for authorized administrators to view scan events and view reports reporting the scan events. The scan events and reports describe the vulnerabilities, services, and systems detected via the scans. Data access is limited to administrators who have been assigned the specific View permission.
IDS_STG.2	System Data Generation Security Function – If the storage space for system data stored in the DBMS is exhausted, the oldest data is saved, an alarm will be generated, and the most recent data is ignored.

8.4 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE SFRs include the appropriate hierarchy and dependencies.

8.4.1 TOE Security Functional Component Hierarchies and Dependencies

The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 35 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by the IT Environment's FPT_STM.1(2).
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_SEL.1	No other components	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1 is satisfied, FMT_MTD.1 is satisfied

SFR	Hierarchical To	Dependency	Rationale
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by the IT Environment's FAU_STG.1
FCS_CKM.1	No other components	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP is satisfied by FCS_COP.1(1). FCS_CKM.4 is satisfied by FCS_CKM.4(1). Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FCS_CKM.4(1)	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Key agreement (FCS_COP.1(1)) is used rather than key generation. Therefore, FCS_CKM.1 is not required. Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FCS_COP.1(1)	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Key agreement (FCS_COP.1(1)) is used rather than key generation. Therefore, FCS_CKM.1 is not required. FCS_CKM.4 is satisfied by FCS_CKM.4(1). Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FIA_ATD.1(1)	No Other Components	None	N/A
FMT_MTD.1	No Other Components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No Other Components	None	N/A
FMT_SMR.1	No Other Components	FIA_UID.1	Satisfied by the IT Environment's FIA_UID.1.
FPT_ITT.1(1)	No other components.	None	N/A
FPT_RVM_SFT.1	No Other Components	None	N/A
FPT_SEP_SFT.1	No Other Components	None	N/A
FPT_STM.1(1)	No other components.	None	N/A
IDS_ANL.1	No Other Components	FPT_STM.1	Satisfied by FPT_STM.1(1).

SFR	Hierarchical To	Dependency	Rationale
IDS_RDR.1	No Other Components	None	N/A
IDS_STG.2	No Other Components	None	N/A

8.4.2 IT Environment Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified IT Environment SFRs include the appropriate hierarchy and dependencies.

The following table lists the IT Environment SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 36 - IT Environment SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_STG.1	No other components	FAU_GEN.1	FAU_GEN.1 is satisfied by the TOE.
FCS_CKM.4(2)	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Key agreement (FCS_COP.1(1)) is used rather than key generation. Therefore, FCS_CKM.1 is not required. Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FCS_COP.1(2)	No other components	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FMT_MSA.2	Key agreement (FCS_COP.1(1)) is used rather than key generation. Therefore. FCS_CKM.1 is not required. Attributes are automatically generated, not entered. Therefore, FMT_MSA.2 is not applicable.
FIA_ATD.1(2)	No Other Components	None	N/A
FIA_UAU.1	No Other Components	FIA_UID.1	Satisfied
FIA_UID.1	No Other Components	None	N/A
FPT_ITT.1(2)	No other components.	None	N/A
FPT_RVM_OS.1	No Other Components	None	N/A

SFR	Hierarchical To	Dependency	Rationale
FPT_SEP_OS.1	No Other Components	None	N/A
FPT_STM.1(2)	No other components.	None	N/A
IDS_STG.1	No Other Components	None	N/A

8.5 PP Claims Rationale

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

8.6 Strength of Function Rationale

SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, SOF-basic was chosen.

No permutational or probabilistic mechanisms are included in the TOE.