Imperva SecureSphere 6

Security Target

Version 1.6

February 5, 2009

Prepared for:

Imperva Inc.
950 Tower Lane, Suite 1550
Foster City, CA 94404

Prepared by:

Metatron Security Services Ltd.
66 Yosef St.,
Modiin, Israel 71724

Document Version Control Log

Version	Date	Description
0.3	July 27, 2006	Submitted for initial review.
0.5	May 28, 2007	Resolved iVOR issues.
0.7	January 7, 2008	Updated version identification to SecureSphere 6.
1.0	August 7, 2008	Updated version identification to SecureSphere 6.0.6. Added references to FIPS validation.
1.2	October 10, 2008	Fixes in response to ASE ETR.
1.5	February 3, 2009	Post-FVOR fixes.
1.6	February 5, 2009	Non-proprietary version for public release.

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1. ST Identification

Title: Imperva SecureSphere 6 Security Target

ST Version: 1.6

ST Date: February 5, 2009

Author: Nir Naaman

TOE Identification: The Target of Evaluation (TOE) consists of one or more of the Imperva SecureSphere 6 appliances listed below:

SecureSphere 6 Appliance	**Role**
G4, G8	Gateway (with optional management)
G16	Gateway
MX	Management server
G4 FTL, G8 FTL, MX FTL	Fault-tolerant versions (dual hard drive)

The software build number for the TOE is 6.0.6.6274.

CC Version: Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, CCMB-2005-08-001

Evaluation Assurance Level (EAL):

EAL 2, augmented with ALC_FLR.1 (basic flaw remediation).

Keywords: IDS/IPS, Web application firewall, database security gateway, Web Services security, intrusion detection, dynamic profiling

1.2. ST Overview

The SecureSphere 6 product lines provide unified protection from attacks against database, Web, and Web Services assets, both within the organization (insider attacks) and from without. Installed on the network as a HTTP proxy, a transparent inline bridge or as an offline network monitor (sniffer), SecureSphere 6 monitors application-level protocols for attacks, and reacts by blocking the attacks and/or reporting them to a centralized management console.

Imperva's Dynamic Profiling technology automatically builds a model of legitimate application behavior that is used by the product to identify illegitimate traffic. In addition, attack signatures are preconfigured into the product and can be periodically updated from an external Application Defense Center.

The products' comprehensive database traffic auditing capability is augmented by a database security assessment capability that scans databases for known vulnerabilities and policy violations.

1.3. Conformance Claims

1.3.1. CC Conformance

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002, extended (Part 2 Extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003, conformant (Part 3 Conformant)

1.3.2. Assurance Package Conformance

The TOE is conformant with the following CC specifications:

- Evaluation Assurance Level (EAL) 2 augmented with ALC_FLR.1.

1.3.3. PP Conformance

The TOE is Protection Profile Conformant with the following Protection Profiles:

- Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006

1.4. Document Organization

Section 1 provides the introductory material for the security target.

Section 2 is the TOE description.

Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 6 describes the security functions and assurance measures provided by the TOE that address the security requirements. In addition, it identifies the method used to determine compliance with cryptographic standards[1].

Section 7 is the Protection Profile claims statement. The PP claims statement describes any tailoring or additions made on top of the claimed PPs.

Section 8 provides a rationale that traces through the levels of abstraction given in the ST (environment, requirements, objectives, and TSS) in order to demonstrate that the ST is a complete and cohesive set of requirements, providing an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the stated requirements. The rationale also demonstrates that the PP conformance claim is valid.

[1] Identification of Standards compliance determination per guidance given in [I-0427].

1.5. References

The following external documents and standards are referenced in this Security Target.

Identifier	Document
[CC]	Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 2.3, August 2005, CCMB-2005-08-001, 002 and 003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004
[FIPS 140-2]	NIST FIPS PUB 140–2, Security Requirements for Cryptographic Modules, December 3, 2002
[FIPS 180-2]	FIPS PUB 180-2 – Secure Hash Signature Standard (SHS), August 1, 2002
[FIPS 186-2]	FIPS PUB 186-2 – Digital Signature Standard (DSS), January 27, 2000
[FIPS 197]	NIST FIPS PUB 197 – Specification for the Advanced Encryption Standard (AES), November 26, 2001
[I-0388]	NIAP Interpretation I-0388: What Is The Difference Between "Sort" and "Order"?
[I-0422]	NIAP Interpretation I-0422: Clarification of "Audit Records"
[I-0427]	NIAP Interpretation I-0427: Identification of Standards
[IDSSPP]	Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006
[PD-0071]	NIAP Precedent Decision PD-0071: Identification of Operations on Security Functional Requirements
[PD-0087]	NIAP Precedent Decision PD-0087: STs Adding Requirements to Protection Profiles
[PD-0091]	NIAP Precedent Decision PD-0091: Dependencies of Requirements on the IT Environment
[PD-0097]	Compliance with IDS System PP Export Requirements
[PD-0118]	Assumptions in the IDS PP v1.4
[PKCS#1]	IETF RFC 3447 – Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003
[RFC 1305]	IETF RFC 1305 – Network Time Protocol (Version 3), March 1992
[RFC 2246]	IETF RFC 2246 – The TLS Protocol Version 1.0, January 1999
[X9.31]	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998

1.6. Conventions

The notation, formatting, and conventions used in this Security Target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

1.6.1. Security Environment Considerations and Objectives

The naming convention for security environment considerations and for objectives is as follows:

- Assumptions are denoted by the prefix “A.”, e.g. “A.ACCESS”.
- Organizational Security Policy statements are denoted by the prefix “P.”, e.g. “P.DETECT”.
- Threats are denoted by the prefix “T.”, e.g. “T.COMINT”.
- Objectives for the IT TOE are denoted by the prefix “O.”, e.g. “O.PROTCT”.

1.6.2. Security Functional Requirements

The CC permits four functional and assurance requirement component operations: assignment, iteration, refinement, and selection. These operations are defined in the Common Criteria, Part 1, paragraph 4.4.1 as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

1.6.2.1. Iteration

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component to cover each aspect is permitted. Iteration is used together with assignment, selection, and refinement in order to specify the different iterations. In this document, iterations are identified with a number inside parentheses ("(#)"). These follow the short family name and allow components to be used more than once with varying operations.

Security functional requirements for the IT environment are identified by an iteration identifier of the form "(Env)".

1.6.2.2. Assignment

Some components have elements that contain parameters that enable the ST author to specify a set of values for incorporation into the ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter. Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

1.6.2.3. Selection

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

1.6.2.4. Refinement

For all components, the ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details. In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

- A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the ST;
- In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement;
- The refined requirement does not extend the scope of the original requirement; and
- The refined requirement does not alter the list of dependencies of the original requirement.

1.6.3. Other Notations

1.6.3.1. Extended Requirements

Extended requirements are additional functional requirements defined in this ST that are not contained in Part 2 and/or additional assurance requirements not contained in Part 3. These requirements are used when security functionality is provided by the TOE that cannot be described by Part 2 or Part 3 requirements. A rationale for the usage of such extended requirements is given in Section 8.2.5. Extended requirements receive names similar to existing Part 2 and Part 3 components, with an additional suffix of (EXP) which is appended to the component’s short name.

1.6.3.2. *Footnotes*

Footnotes[2] are used to provide further clarification for a statement, without breaking the flow of the text.

1.6.3.3. *References*

References to other documents are given using a short name in square brackets, e.g. "[PD-0097]". The identification of the referenced document is provided in Section 1.5.

1.6.4. Highlighting Conventions

The conventions for SFRs described above in sections 1.6.2 and 1.6.3 are expressed in chapter 5 by using combinations of bolded, italicized, and underlined text as specified in Table 1-1 below.

These conventions are applied in respect to requirements derived from the IDS System PP (IDSSPP). Assignments, selections, and refinements that were already performed in the IDSSPP are not identified via a highlighting convention in this ST. This is consistent with the guidance given in [PD-0071].

Table 1-1- SFR Highlighting Conventions

Convention	Purpose	Operation
Boldface	Boldface text denotes completed component assignments. Example: *5.1.1.2 Audit review (FAU_SAR.1)* FAU_SAR.1.1 The TSF shall provide **authorised administrators with System Events permission** with the capability to read **all audit information** from the audit records.	(completed) Assignment
Underline	Underlined text denotes completed component selections (out of a set of selection options provided in the original CC requirement). Example: *5.1.5.6 Prevention of System data loss (IDS_STG(EXP).2)* IDS_STG(EXP).2.1 The System shall overwrite the oldest stored System data and send an alarm if the storage capacity has been reached.	(completed) Selection

[2] This is an example of a footnote.

Convention	Purpose	Operation
Boldface Underline	Underlined boldface text highlights component refinements. This includes refinement of an operation that was completed in the PP. Example: *5.1.1.6. Protected audit trail storage (FAU_STG.2)* FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.2.2 The TSF shall be able to detect **unauthorized** modifications to the **stored** audit records **in the audit trail**.	Refinement
Extended Requirement (EXP)	The suffix "(EXP)" denotes an extended requirement that was not taken from Part 2 or Part 3 of the CC, but was explicitly defined specifically to provide security functionality that is relevant to this ST. Examples: *5.1.8.3. Analyzer react (IDS_RCT(EXP).1)* IDS_RCT(EXP).1.1 The System shall send an alarm…	Extended Requirement

1.7. Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. Additional definitions are provided in [IDSSPP]. The following sections are a refined subset of those definitions, listed here to aid the user of this ST. The glossary is augmented with terms that are specific to the Imperva SecureSphere 6 product line.

1.7.1. Glossary

Access	Interaction between an entity and an object that results in the flow or modification of data.
Access Control	Security service that controls the use of resources[3] and the disclosure and modification of data.[4]
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.
Administrator	A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Attack	An intentional act attempting to violate the security policy of an IT system.
Audit	Related to audit requirements in [IDSSPP], and referring to the SecureSphere 6 system events log.
Authentication	Security measure that verifies a claimed identity.
Authentication data	Information used to verify a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Authorized user	An authenticated user who may, in accordance with the TSP, perform an operation.
Availability	Timely[5], reliable access to IT resources.
Bridge	A layer-two device that forwards frames received from one network segment to another segment, based on their MAC address.
Compromise	Violation of a security policy.

[3] Hardware and software.

[4] Stored or communicated.

[5] According to a defined metric.

Confidentiality A security policy pertaining to disclosure of data.

Correlated Attack Validation An Imperva technology that addresses attacks by basing ID decisions on multiple observations.

Database audit Database queries and responses collected and recorded by SecureSphere 6 gateways.

Dynamic Profiling An Imperva technology that creates and maintains a comprehensive model (profile) of an application's legitimate protocol structure and dynamics through the examination of live traffic.

Entity A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.

External IT entity An IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Identity A representation (e.g., a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity A security policy pertaining to the corruption of data and TSF mechanisms.

Intrusion Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection (ID) Pertaining to techniques which attempt to detect intrusion.

Named Object An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to request a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

Network Two or more machines interconnected for communications.

Object An entity that contains or receives information and upon which subjects perform operations.

Operational Environment

The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Packet A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.

Packet Sniffer A device or program that monitors the data traveling between computers on a network.

Router A layer-3 device that routes IP packets based on their destination address and predefined routing tables.

Security attributes TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.

Server Group A defined group of protected servers.

SPAN A special networking switch port that is used by the TOE to collect network traffic flowing through the switch, via port mirroring.

Subject An entity within the TSC that causes operations to be performed.

System A subset of the TOE security functionality referring to the ID monitoring, analysis, and reaction mechanisms as specified by the IDS SFRs.

System administrator An administrator that performs management functions related to System security functionality, attributes, and data.

Tap A device that provides a non-intrusive fault-tolerant method of viewing traffic on a network segment.

Threat Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorised operation with the TOE.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Universal User Tracking An Imperva technology that identifies and tracks the user identity across both Web application server and database queries.

Vulnerability A weakness that can be exploited to violate the TOE security policy.

1.7.2. Abbreviations

Abbreviation	Description
ADC	Application Defense Center
AES	Advanced Encryption Standard
CAV	Correlated Attack Validation
CC	Common Criteria
CM	Configuration Management
DASA	Database Active Security Assessment
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Intrusion Detection
IDS	Intrusion Detection System
IDSSPP	Intrusion Detection System System Protection Profile
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
PP	Protection Profile
RFC	Request for Comment
SFR	Security Functional Requirement
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security

Abbreviation	Description
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User Datagram Protocol
UUT	Universal User Tracking

2. TOE Description

2.1. Overview

The TOE Description consists of the following subsections:

- **Product Types –** describes the product types of the Target of Evaluation (TOE) in order to give the reader a general understanding of the intended usage of the product in its evaluated configuration.
- **Physical Scope and Boundaries of the TOE –** describes hardware and software components that constitute the TOE and their relationship with the product.
- **Logical Scope and Boundaries of the TOE –** describes the IT features offered by the TOE and any product features excluded from the evaluated configuration.
- **TOE Security Functionality** – summarizes the security features of the TOE that are claimed in this ST.

2.2. Product Type

Imperva SecureSphere 6 protects Web and database servers by analyzing network traffic flowing to and from protected servers, detecting requests that may be indicative of intrusion, and reacting by reporting the events and/or blocking the suspected traffic. In addition, SecureSphere 6 provides a Database Active Security Assessment (DASA) capability for scanning databases for vulnerabilities and policy violations.

In this ST, the TOE is categorized as an IDS/IPS product. SecureSphere 6 meets the requirements of the IDS System Protection Profile (IDSSPP). The IDSSPP defines an IDS System as a set of one or more Sensors and/or Scanners, and optionally one or more Analyzers. Sensors collect data about events as they occur on an IT System (e.g. a network), whereas Scanners collect static configuration information about an IT System. Analyzers receive data from identified Sensors and Scanners, process it to make intrusion and vulnerability determinations, respectively, and provide a response capability.

2.3. *Physical Scope and Boundaries of the TOE*

2.3.1. Definition

The Target of Evaluation (TOE) includes the following components:

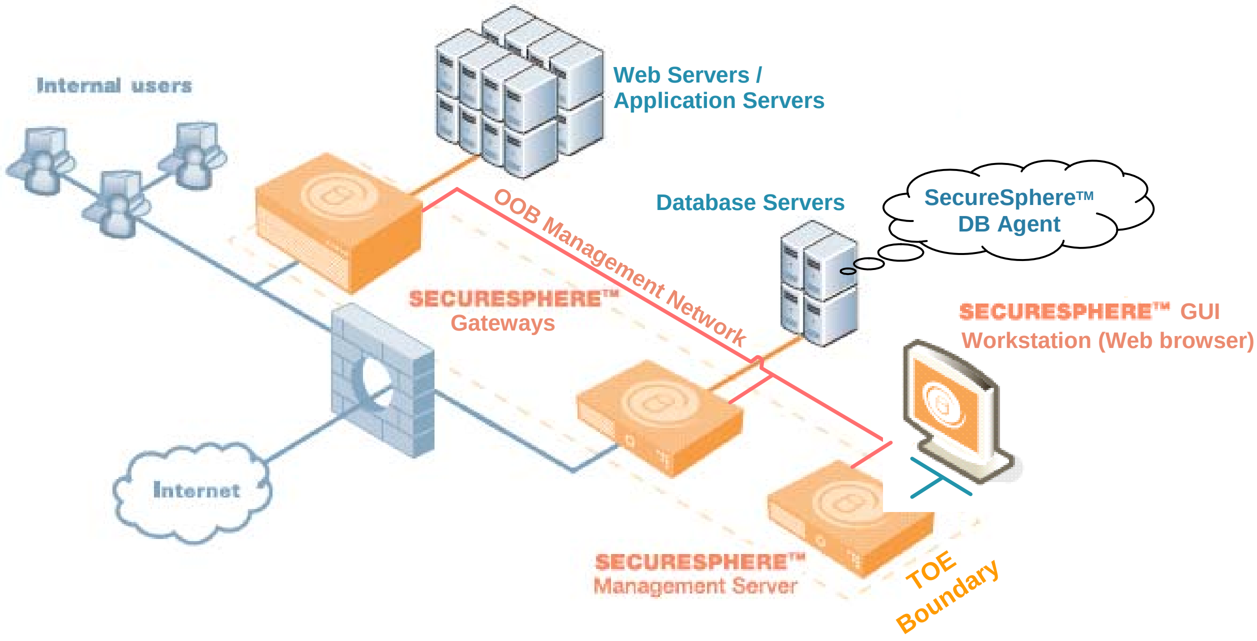
- One or more gateway appliances (G4, G8, or G16); and
- One or two Management Servers (MX).

All gateway and management appliance hardware and software is included in the TOE.

The G4 and G8 gateway modules include an option to run the management component on the gateway itself, thus avoiding the need to purchase an MX appliance. However, if you run the management server on the gateway itself, it will only be able to manage the gateway on which it is installed. To manage more than a single gateway the MX Management Server appliance must be used.

Figure 2-1 depicts the TOE protecting Web, Web Services and database assets. SecureSphere 6 gateways are installed in front of the protected resources. They are connected to the Management Server using dedicated out of band (OOB) management network interfaces, so that the communication between the gateways and the Management Server is not exposed to any internal or external users.

Figure 2-1- Physical Scope and Boundaries of the TOE



2.3.2. Hardware and Software Excluded from the TOE Boundary

The TOE boundary does **not** include the following components, supported by the evaluated configuration:

- **Administrator workstations** used for managing the TOE: a standard Web browser (Microsoft Internet Explorer 5.0 or later) is used to connect to a SecureSphere GUI Web-based management application running on the SecureSphere Management Server, via a dedicated management network interface. The administrator workstation and browser are considered to be outside the TOE. It is assumed that the environment will provide adequate access protection for administrator workstations and for the OOB management network.
- **Protected Servers**: the TOE provides protection for server-based applications that use Web, database, and IP protocols to communicate with client applications. The TOE can provide protection for protocols used by the following database products: Oracle 8.0/8i/9i/10g, Sybase 12.5.0/12.5.2, IBM DB2 for Unix, Linux, Windows and zOS, Microsoft SQL Server 7.0/2000/2005, and IBM Informix 9 and 10.
- **SecureSphere DB Agents**: Imperva markets optional add-on sensor software agents that run on the database server, and transmit all database access requests to the SecureSphere 6 gateway. This allows the gateway to analyze database events that cannot be identified from network traffic, e.g. by applications running on the database server host itself.

  Disabled by default, agent support may be enabled in the evaluated configuration if the customer purchases and installs DB agents on protected database servers.
- **Active Modules**: SecureSphere 6 includes an Active Module engine that is used to distribute value-added insights and capabilities generated by ADC, including such features as Track Value Changes, Auto Server Discovery, Sensitive Data Discovery, Change Tracking, and third party Scanner Integration. Active Modules are distributed as Java .jar files as part of the ADC Content Updates mechanism.

In addition, the following functionality is excluded from the evaluated configuration:

- **SSH**: SecureSphere 6 appliances can support remote access to appliance operating system-level installation and configuration interfaces over the SSH protocol. Once an appliance is correctly configured and operational, all management is performed via the SecureSphere GUI. Evaluated configuration guidance instructs the administrator to disable remote user access to SSH in the evaluated configuration.
- **Audit archiving over SCP**: this functionality is not supported in FIPS mode, as configured in accordance with evaluated configuration administrator guidance.
- **Apache Reverse Proxy**: Imperva supports a reverse proxy implementation for HTTP traffic based on the public domain Apache Web server, which can be installed on SecureSphere gateways. This has been superseded in SecureSphere 6 by a high-performance Imperva kernel-based proxy infrastructure.

2.3.3. SecureSphere Deployment Scenarios

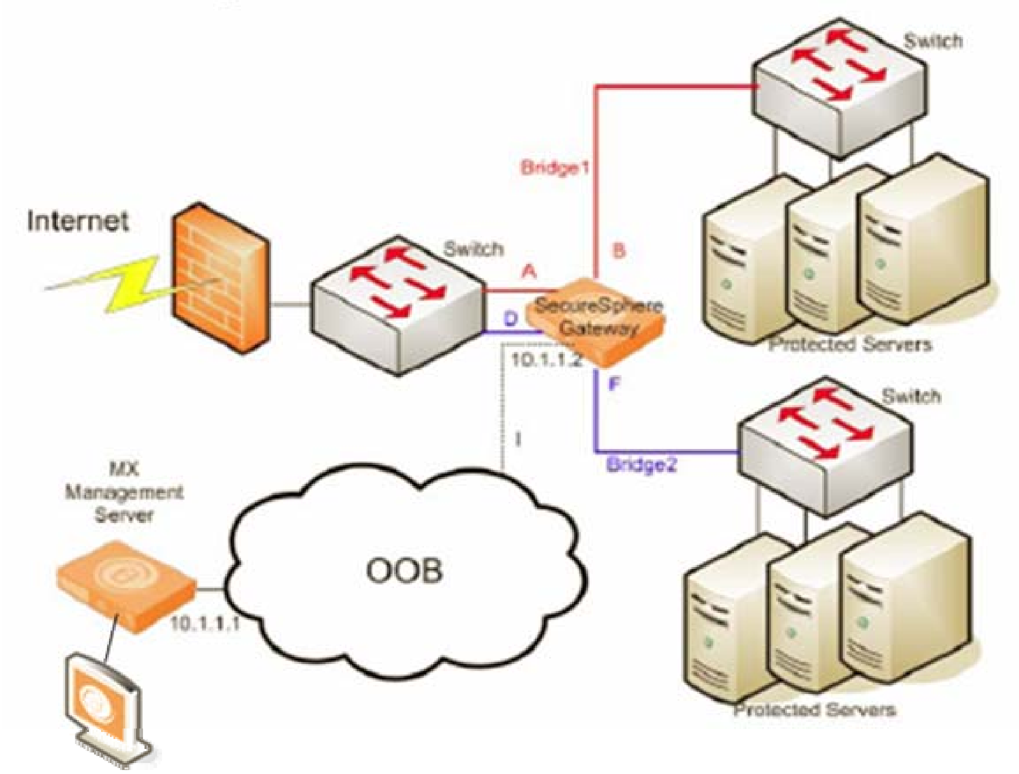
The SecureSphere 6 network architecture supports both non-inline (sniffing) and inline gateways. An inline gateway is more invasive but provides better blocking capabilities. A sniffing gateway is totally noninvasive but provides less foolproof blocking capabilities (i.e. TCP resets).

2.3.3.1. Inline Topology

To achieve inline blocking capabilities, SecureSphere 6 gateways can be deployed in inline mode. In this scenario, the gateway acts as a bridging device between the external network and the protected network segment. The gateway will block malicious traffic inline (i.e. drop packets).

A single inline gateway protects one or two network segments. It has six network interface cards. Two of the cards are used for management: one to connect to the management server and the other is optional. The other four cards are part of two bridges that are used for inline inspection of up to two different protected network segments. Each bridge includes one card for the external network and one for the protected network.

Figure 2-2- Example Inline Topology



2.3.3.2. Sniffing Topology

A sniffing gateway is a passive sniffing device. It connects to corporate hubs and switches and taps the traffic sent to and from protected servers. Traffic is copied to it instead of passing directly through it.

A single SecureSphere 6 gateway can monitor more than one network segment as it includes multiple network interface cards which can be used for sniffing different network segments. The only limitation is the total traffic volume that a gateway can handle. A single gateway can monitor different types of servers (e.g. Web servers, databases, Email servers). It is not necessary to separate these tasks or assign them to different gateways.

Figure 2-3- Example Sniffing Topology – SPAN/Mirror Port

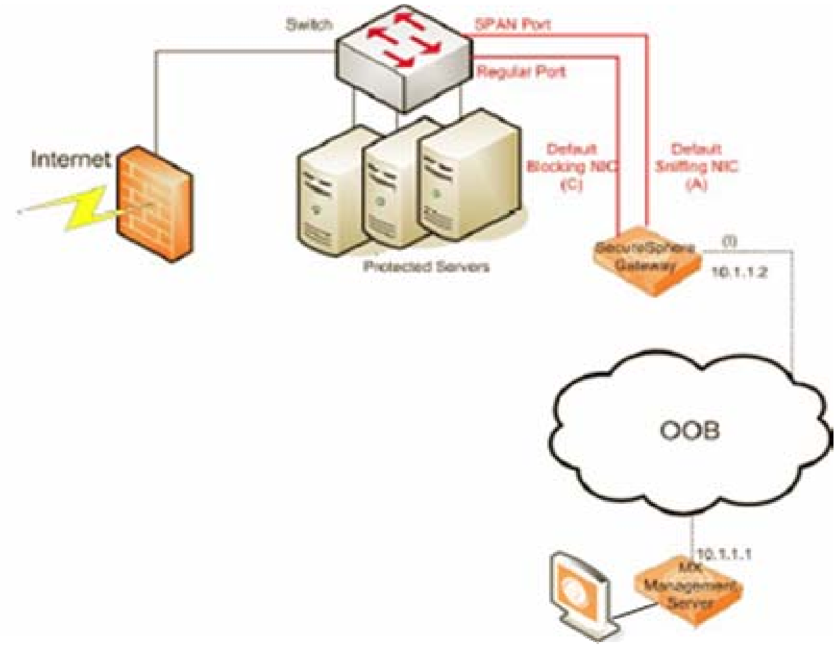
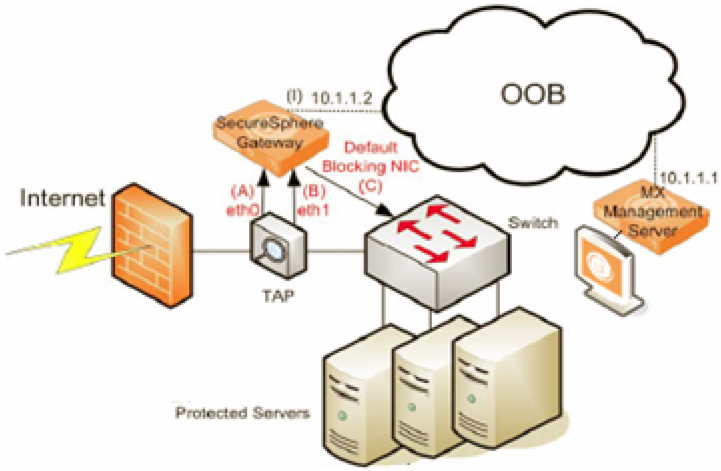


Figure 2-4- Example Sniffing Topology – TAP



2.3.3.3. Management Network

TOE guidance instructs the administrator to ensure that the SecureSphere 6 gateways connect to the SecureSphere Management Server through an out of band management network. In this configuration, all gateway-Management Server communication is carried encrypted over a dedicated and secure network that is completely separated from production traffic. In both sniffing and bridging configurations (except for non-transparent reverse proxy configurations), the gateways are further separated from the production network as all sniffing/bridging network interface cards have no IP address.

Separation between the production traffic and the OOB management network is achieved by allocating a separate (onboard) NIC for this purpose on SecureSphere 6 gateways. As depicted below in Figure 2-5 and Figure 2-6, the Management NIC is clearly separated from other appliance NICs (the second onboard NIC adjacent to the Management NIC is always inactive). The SecureSphere 6 gateway operating system does not bridge or route packets to or from the Management NIC.

Figure 2-5 - Management NIC on G4/G8 Appliances

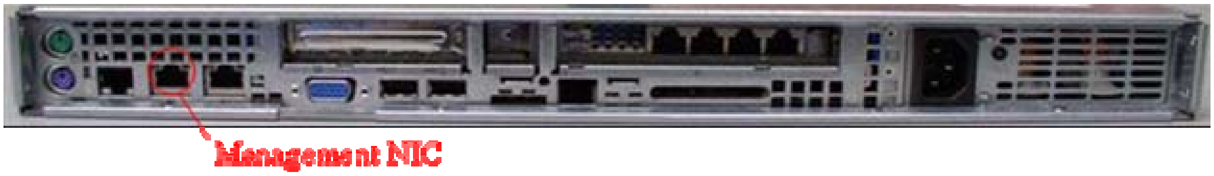
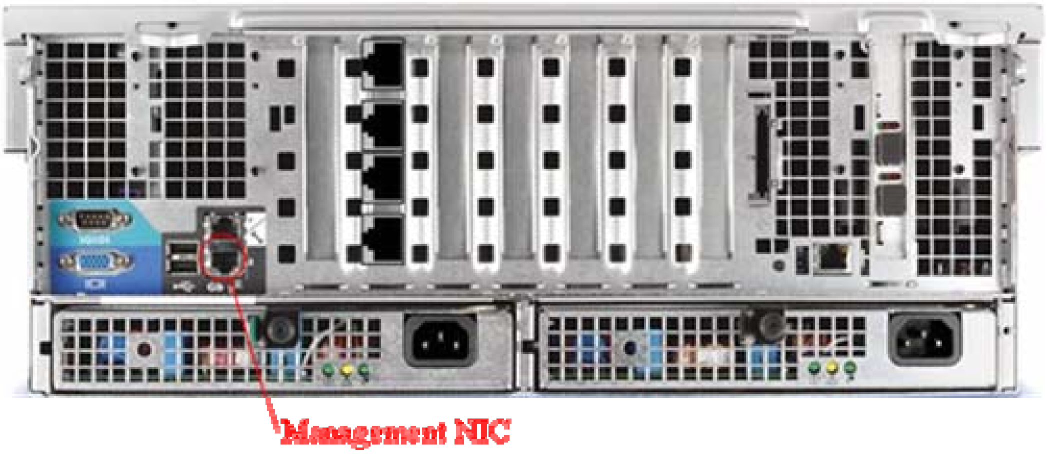


Figure 2-6 - Management NIC on G16 Appliance



2.3.4. TOE Guidance

The following Imperva guidance is considered part of the TOE:

Figure 2-7 – TOE Guidance

Title	**Part Number / Date**
SecureSphere Version 6.0.6 Reference Guide	July 26, 2008
SecureSphere Version 6.0.6 Administrator Manual	July 29, 2008
SecureSphere Version 6.0.6 User Guide	July 29, 2008
SecureSphere Version 6.0.6 Release Notes	July 31, 2008
G4 AH Appliance Quick Start Guide	G4-AH QSG version 6.2, 6/3/2008
G4-G8 CL Appliance Quick Start Guide	G4-G8-CL QSG version 6.2, 6/3/2008
G4-G8 FTL Appliance Quick Start Guide	G4-G8-FTL QSG version 6.2, 6/3/2008
G16 FTL Appliance Quick Start Guide	G16-FTL QSG version 6.2, 6/3/2008
MX AH Appliance Quick Start Guide	MX-AH QSG version 6.2, 6/3/2008
MX Appliance Quick Start Guide	MX-CL QSG version 6.2, 6/3/2008
MX FTL Appliance Quick Start Guide	MX-FTL QSG version 6.2, 6/3/2008
SecureSphere 6 Common Criteria Evaluated Configuration Guidance	Version 0.7, October 7, 2008

2.4. Logical Scope and Boundaries of the TOE

2.4.1. TOE Logical Interactions with its Operational Environment

The TOE supports the following logical interactions with its environment:

- **Data Collection**
    - **Sniffing** – The TOE (when in sniffing topology) collects network frames and analyses them to identify suspicious traffic.
    - **Bridging** – The TOE (when in inline topology) forwards frames between bridged segments.
    - **Proxying –** The TOE (when in inline topology) can be configured as a reverse proxy for HTTP traffic.
    - **DB Agents** – The TOE supports event collection from SecureSphere DB Agents that act as IDS sensors for database events.
    - **Database Active Security Assessment –** the TOE can be configured to perform remote database scans for vulnerabilities and policy violations.
- **Analysis and Reaction**
    - **Blocking –** The TOE (when in inline topology) blocks frames that are suspect of being associated with malicious traffic.
    - **Resetting –** The TOE (when in sniffing topology) signals servers to reset TCP connections that are suspect of being associated with malicious traffic.
    - **Action Interfaces –** The TOE can be configured to react to system and security events by sending alarms, audit data, reports, and assessments to trusted external IT entities.
- **Security Management**
    - **Management –** Authorized administrators manage the TOE and review audit trail and IDS System data via the SecureSphere GUI.
    - **Content Updates –** the TOE can import updated ADC content including IDS attack signatures, database security assessment patterns, compliance policies, and predefined reports.
    - **Time Updates –** the TOE can optionally be configured to synchronize its clock with that of an external time server, using the NTP protocol.

2.4.2. Network Traffic Data Collection

2.4.2.1. Overview

SecureSphere 6 collects and records network traffic using either the sniffing or inline topologies described above. The traffic is analyzed using the TOE's ID functionality. In addition to its data collection role, the TOE may play an active role in ensuring network connectivity (inline topology). This section describes these different configurations.

2.4.2.2. Sniffing

When configured in sniffing topology, SecureSphere 6 gateways are configured with one or more NICs in *promiscuous mode*. Promiscuous mode allows the gateway to read all frames transmitted on the monitored network segment. Frames picked up from the network are then passed to the gateway's analysis and reaction logic.

2.4.2.3. Bridging

When configured in inline topology, SecureSphere 6 gateways can be configured to bridge pairs of NICs. When bridging, frames are picked up from one network segment, and if the destination MAC address belongs to the paired segment, and the frame is not blocked by the analysis and reaction logic, transmits it on the paired segment.

2.4.2.4. Reverse Proxy

When configured in inline topology, SecureSphere 6 gateways can be configured in Reverse Proxy mode. Transparent Reverse Proxy Mode is similar to bridging; however, instead of processing each individual frame, IP fragments are accumulated and the proxy processes complete messages. In non-Transparent mode, the gateway is assigned an IP address, and HTTP clients proxy traffic through the gateway. Reverse Proxy configurations are used to provide support for HTTP translation rules (e.g. URL rewriting).

2.4.2.5. Fail-Safe Modes

SecureSphere 6 G4/G8/G16 gateway appliances in inline topology can be configured to either block all traffic in the event of a software, hardware, or power failure, or to allow all traffic to pass transparently through the gateway.

2.4.3. DB Agents

SecureSphere 6 gateways provide support for SecureSphere DB Agents, IDS sensors running on database servers. DB Agents extend the reach of the TOE to database events that would not be otherwise visible to the gateway. The DB Agent monitors all database access request traffic, including both network traffic and local access on the database server, and transmits the traffic to a network segment monitored by SecureSphere 6 gateways for IDS data collection and analysis. The gateway inspects this traffic just like regular database traffic collected by the gateway.

Imperva DB Agents are available for Windows, AIX, Linux, and Solaris operating systems. Supported databases include: Oracle, Sybase, DB2 and Microsoft SQL Server.

Note that blocking and resetting capabilities are not available for DB Agent traffic.

2.4.4. Database Active Security Assessment (DASA)

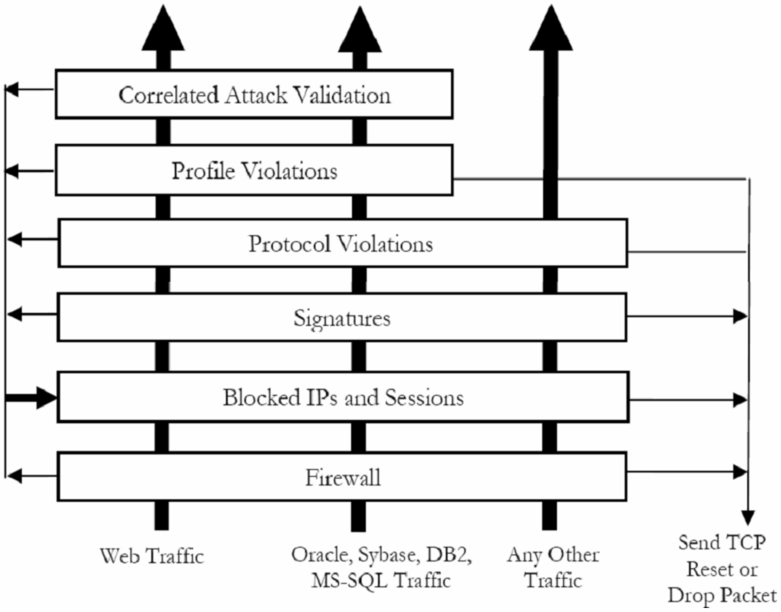
The SecureSphere 6 Management Server can be configured as a database client in order to perform database queries that scan the database for known vulnerabilities and for compliance with a suite of security policies, predefined by the Imperva ADC, and distributed together with the ADC content updates.

2.4.5. Analysis and Reaction

2.4.5.1. Overview

SecureSphere 6 applies five layers of intrusion detection logic to analyzed network traffic, as depicted below in Figure 2-8. Some of these layers are applicable to all network traffic; some are relevant only for Web traffic and/or database access protocols. In addition, Imperva's Correlated Attack Validation (CAV) technology examines sequences of events and identifies suspicious traffic based on a correlation of multiple analysis layers. Identified malicious traffic is blocked.

Figure 2-8 – Intrusion Analysis and Reaction



SecureSphere supports the following two blocking methods:

- TCP Reset (sniffing topology): SecureSphere can signal protected servers to disconnect malicious users using TCP reset, a special TCP packet that signals

TCP peers to close the TCP session. SecureSphere spoofs a TCP reset packet and sends it to the protected server. It is assumed that a standards-conformant server would immediately drop the attacker's session on receipt of the TCP reset packet.

Note: TCP reset is considered inferior to inline blocking (see below) because it does not actively block the malicious traffic from reaching the server; blocking depends on the server's correct and timely session termination behavior.

- Inline Blocking: the gateway drops the packet, so that it doesn't reach its intended destination, and sends a TCP reset to the server.

  Note: When SecureSphere 6 blocks a Web connection it can be configured to display an error page to the blocked user.

2.4.5.2. Network Firewall

When deployed in an inline topology, the administrator can define a firewall policy that can be described either as a white list (i.e. nothing is allowed except for specific rules) or as a black list (i.e. everything is allowed except for specific rules).

Rules are a combination of service (e.g. FTP, SMTP) and a source or destination IP address group. It is possible to define a different policy for each protected server group and for each traffic direction (inbound or outbound).

2.4.5.3. Blocked IPs and Sessions

The Blocked IPs and Sessions engine consults a dynamic list of IP addresses and Session Identifiers that have been identified by the other ID layers as blocked traffic. Blocking can be configured by source IP address, or by Web session identifier. Session identifiers are stored either within session cookies or in the HTTP parameters. Blocking entries persist for a specified period of time.

2.4.5.4. Traffic Monitoring and Recording

SecureSphere 6 gateways can be configured to react to suspected intrusions events by recording all traffic from the identified source for a period of time. The recorded events can be reviewed by an administrator.

2.4.5.5. Signature-based Intrusion Prevention

SecureSphere provides Snort™-based signature detection to protect applications from worms (and other attacks) that target known vulnerabilities in commercial infrastructure software (Apache, IIS, Oracle, etc.). The Snort database is enhanced by Imperva's Application Defense Center (ADC) with new signatures and content such as affected systems, risk, accuracy, frequency, and background information. The attack signature database can be updated automatically over the Web, or manually by the administrator.

To easily use the signature database, SecureSphere includes the concept of Signature Dictionaries. A dictionary is a collection of signatures generated by applying a filter on the SecureSphere signature database. For example, you could easily define a filter of all high-risk, highly accurate, IIS 6 signatures.

SecureSphere comes with a predefined set of dictionaries, defined by the Imperva ADC. It is possible to select whether or not to use each dictionary with each one of the protected server groups. When a certain dictionary is selected for a specific server group, SecureSphere will detect the signatures in the dictionary if they appear in a communication to the protected server group.

SecureSphere's Intrusion Prevention System also includes protocol compliance checks for TCP, UDP and IP. Protocol-related violations such as bad checksum, bad IP addresses and bad options can be detected and blocked.

2.4.5.6. Protocol Violations

SecureSphere protocol compliance checks ensure that protocols meet RFC and expected usage requirements. By ensuring that the protocol meets guidelines, protocol compliance prevents attacks on both known and unknown vulnerabilities in commercial Web server implementations.

Imperva has conducted comprehensive research and collected a group of protocol violations that usually indicate attack attempts. You can enable or disable each of these violations for each group of protected servers.

2.4.5.7. Universal User Tracking (UUT)

SecureSphere 6 gateways analyze both Web and database protocols to identify the user identity, using both direct user tracking where the user identity is included in the request and application user tracking which maps requests to a user session context, with user identity acquired by the gateway during session establishment (user authentication).

A common pattern in Web/database deployments involves users accessing an application server using Web protocols, invoking application server logic that triggers database queries on the user's behalf. In order to associate the correct user identity with database queries (instead of the application server's identity, as seen by the database), SecureSphere correlates the Web and database requests, providing a Web to Database User Tracking capability.

2.4.5.8. Profile Violations

SecureSphere's Web and database profiles represent a comprehensive model of all "allowed" interactions between users and the two key elements of the enterprise network: Web servers and database servers. The Web Profile includes legitimate URLs, HTTP methods, parameters, cookies, SOAP actions, XML structures and more. The Database Profile includes all legitimate SQL queries per database user, valid IP addresses per database user, and more. The profiles are built automatically through a learning process and adapt to changes in the application environment over time by observing live traffic and applying SecureSphere's Persistent Learning technologies. The profiles, therefore, require no manual configuration or tuning.

By comparing these profiles of "allowed behavior" to actual traffic, SecureSphere is able to identify and block potentially malicious behavior that does not necessarily match known attack signatures. Since SecureSphere profiles both Web and database behaviors, SecureSphere is able to detect Web-based attacks from the Internet as well as direct attacks on SQL database assets that originate from within the corporate network.

2.4.5.9. Correlated Attack Validation (CAV)

To identify complex attack patterns and reconnaissance activity, SecureSphere's Correlated Attack Validation (CAV) engine tracks low-level violations over time across the different SecureSphere protection layers to identify specific attack patterns.

For example, a signature violation such as the "union" string may indicate a SQL injection attack. On the other hand, the word "union" may be part of a legitimate URL. Therefore, rather than risk blocking a legitimate user, CAV will classify that user as "suspicious" and begin tracking his/her actions to validate true intent. When SecureSphere's Web and Database Profiles subsequently identify "Unknown Parameter and "Unauthorized SQL Query" violations from that user, it becomes clear that the user in question should be blocked. By looking at a sequence of events, as opposed to a single event, CAV can accurately separate actual attacks from harmless low-level violations, without manual configuration or tuning.

2.4.6. Action Interfaces

An Action Set defines a set of actions and operations that can be executed when an identified event occurs (e.g. sending an alarm), or on a defined schedule (e.g. audit archiving). The administrator can define different Action Sets and use them for different events.

In addition to the blocking, resetting and monitoring actions described above, event notifications can be sent to defined action interfaces. The following types of interfaces are available for SecureSphere 6:

- **Email:** This interface allows sending an email over SMTP to a specific group of email addresses hosted on mail servers in the IT environment.
- **SNMP Traps**: An interface that sends SNMP traps to a SNMP manager host in the IT environment.
- **Syslog**: This interface allows sending a Syslog message to a Syslog server in the IT environment.
- **Audit Archiving**: database audit records can be archived to an external IT entity, in order to free up storage on the Management Server. The audit records can still be displayed from the TOE, by issuing queries to the archive. The TOE can be configured to encrypt and/or sign the archived records to prevent unauthorized disclosure or modification of the records outside the TOE's scope of control.

- **Operating System Command**[6]: an interface to the SecureSphere Management Server operating system. This interface allows execution of an operating system command or a specific file on the Management Server.
- **Tasks**: review or actionable tasks may be created as a follow up action for the event, assigned to a specified SecureSphere GUI administrator.

2.4.7. Management

The TOE is managed from the Management Server. Configuration settings are downloaded from the Management Server to SecureSphere 6 gateways, and event information is uploaded from the gateways to the Management Server.

IDS System configuration is managed via the SecureSphere GUI interface.

The TOE uses the NTP protocol to synchronize gateway clocks with that of the Management Server, providing reliable timestamps for audit and System data.

2.4.8. ADC Content Updates

SecureSphere 6 attack signatures are text strings that match known server vulnerabilities and attack patterns. SecureSphere 6 maintains a list of over 5000 signatures based on the Snort database and Imperva’s Application Defense Center (ADC). The ADC tests each new Snort signature and makes sure it’s valid. It then classifies the signature according to different attributes such as the severity of the attack described by the signature, the accuracy of the signature (sensitivity to false positive scenarios), the systems that are affected by this attack (e.g. IIS Web server, Apache Web Server, Oracle 9i) and more. In addition to classifying the signature, ADC also documents it. Once the signature is verified, classified and documented, it is added to the Imperva Signature Database on the Imperva Web site from which it can be downloaded either automatically (if your SecureSphere Management Server has connectivity to the Internet) or manually by the authorized administrator.

ADC content updates can also include updated database security assessment patterns, compliance policies and predefined reports, as well as Active Module updates.

Each ADC content update is digitally signed by the ADC, and its authenticity and integrity verified by the Management Server before it is applied.

[6] Operating System (OS) commands can be defined as an Action, providing a highly flexible extension to the built-in Action mechanisms. Because it is not possible to reasonably enumerate all possible commands and provide assurance that they cannot adversely affect any SFRs in this ST, this mechanism was excluded from the evaluated configuration. TOE evaluated configuration guidance instructs the administrator not to define OS command Actions.

2.4.9. Functionality Excluded from the TOE Evaluated Configuration

All SecureSphere 6 functionality is included in the TOE Evaluated Configuration, with the following exceptions:

- SecureSphere 6 gateways can be installed in Routing Mode, where packets are forwarded by the gateway in accordance with their presumed IP address and gateway routing tables. This mode also supports Network Address Translation (NAT). Routing Mode is disabled in the evaluated configuration.
- Imperva SecureSphere 6 gateways and management servers can be installed in high-availability (HA) modes, in which multiple gateways are deployed for a single information flow path, or multiple management servers are used in a failover configuration. HA is disabled in the evaluated configuration.
- Administrator authentication can be configured to be performed using an external user directory that supports the LDAP protocol. In the evaluated configuration, administrators are authenticated locally by the Management Server.

2.5. TOE Security Functionality

Imperva SecureSphere 6 is an IDS/IPS that monitors network traffic between clients and servers in real-time, analyses that traffic for suspected intrusions, and provides a reaction capability. Reaction options include recording and monitoring suspected traffic and ID events, blocking traffic, and generating alarms containing event notifications. Database auditing allows you to record selected user database queries for audit purposes. Web queries and responses can also be selectively recorded. In addition, monitored databases can be actively scanned to identify potential vulnerabilities.

Administrators manage System configuration settings using the SecureSphere GUI, a Web-based interface provided by the Management Server. Administrators log in to the Management Server authenticated using a password. The server provides a trusted path for the management session over TLS. A role based scheme is used to define administrator authorizations. Only designated authorized System administrators may modify the behavior of IDS System data collection, analysis and reaction capabilities. Other authorized administrators may only query System and audit data and modify other TOE data.

The TOE records TOE events related to ADC content updates, administrator logins, changes to configuration, activation of settings, building profiles, automatic profile updates, server start/stop, etc. in an audit trail. Administrators are provided with reporting tools to review audit trail and System data. The TOE provides protection against modification and unauthorized deletion of audit records and System data, as well as storage exhaustion.

The TOE protects itself and its data from tampering. Transfer of information between the gateways and the Management Server is physically separated from other information flows by the use of the dedicated OOB management network interface. Audit data that is stored on an archive outside of the TOE can be cryptographically protected from disclosure or tampering. ADC content update authenticity and integrity is verified by the TOE before updates are applied.

The TOE uses the following FIPS 140-2 validated cryptographic modules for the implementation of cryptographic functionality: RSA BSAFE Crypto-J 4.0, OpenSSL version FIPS 1.1.2.

3. TOE Security Environment

3.1. Assumptions

The following conditions are assumed to exist in the operational environment (identical to the set of assumptions made in [IDSSPP], provided here for the benefit of the reader of the ST):

3.1.1. Intended Usage Assumptions

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[7].

3.1.2. Physical Assumptions

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.

3.1.3. Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

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

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

[7] A.ASCOPE is an assumption that is upheld by the O.INTROP objective for the environment. Per the guidance given in [PD-0118], this assumption is given in the wording used in [IDSSPP].

3.2. Threats

This section describes the threats that are addressed either by the TOE or the environment (identical to the set of threats described in [IDSSPP], provided here for the benefit of the reader of the ST):

3.2.1. 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.

3.2.2. IT System Threats

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

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

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3. Organizational Security Policies

[IDSSPP] defines a set of organizational security policies that are applicable to the PP. These are not repeated here as they are not needed to establish the rationale for the set of TOE SFRs – all [IDSSPP] security objectives mitigate at least one defined threat.

4. Security Objectives

4.1. Information Technology (IT) Security Objectives

This section describes the TOE security objectives (identical[8] to the set of TOE security objectives described in [IDSSPP], provided here for the benefit of the reader of the ST):

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

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

[8] [IDSSPP] security objectives omitted from this ST: O.EXPORT was omitted per the guidance given in [PD-0097].

4.2. Security Objectives for the Environment

4.2.1. Non-IT Security Objectives for the Environment

The assumptions made in [IDSSPP] about the TOE's operational environment must be upheld by corresponding non-IT security objectives for the environment. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

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

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

O.INTROP The TOE is interoperable with the IT System it monitors.

4.2.2. IT Security Objectives for the Environment

The following security objective for the IT Environment is allowed in [IDSSPP] to support external time keeping. It is applicable for configurations that use the NTP protocol for synchronizing the TOE's clock with that of an external time server.

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

5. IT Security Requirements

5.1. TOE Security Functional Requirements

The bulk of the functional security requirements (SFRs) for this ST are taken from [IDSSPP][9]. These SFRs are identified in the 'PP' column of Table 5-1 below. Additional SFRs were added in this ST for the TOE's trusted path functionality and for protection of audit archive data (together with supporting cryptographic and management SFRs), as described in Section 7.3.

The CC defined operations of iteration, assignment, selection, and refinement were applied in relation to the requirements specified in [IDSSPP] as described in column 4 of Table 5-1. Where a requirement component that is hierarchical to that specified in the PP was selected, 'hierarchical' is identified in column 4. For components that were not drawn from the PP, assignment, selection and refinement operations are described in relation to the corresponding [CC] Part 2 requirement.

The TOE satisfies a minimum strength of function 'SOF-basic'. The only applicable (i.e., probabilistic or permutational) security functional requirement is FIA_UAU.2.

Table 5-1 –Security functional requirement components

Functional Component		PP	CC Operations Applied
FAU_GEN.1	Audit data generation	✓	None
FAU_SAR.1	Audit review	✓	Assignment
FAU_SAR.2	Restricted audit review	✓	None
FAU_SAR.3	Selectable audit review	✓	None
FAU_SEL.1	Selective audit	✓	Assignment, refinement
FAU_STG.2	Guarantees of audit data availability	✓	Refinement, assignment, selection
FAU_STG.4	Prevention of audit data loss	✓	Selection
FCS_CKM.1	Cryptographic key generation		Refinement, assignment
FCS_CKM.2	Cryptographic key distribution		Assignment
FCS_COP.1	Cryptographic operation		Refinement, assignment
FIA_ATD.1	User attribute definition	✓	Assignment, refinement

[9] The FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 SFRs defined in [IDSSPP] were omitted per the guidance given in [PD-0097].

Functional Component		PP	CC Operations Applied
FIA_UAU.2	User authentication before any action	✓	Hierarchical
FIA_UID.2	User identification before any action	✓	Hierarchical
FMT_MOF.1	Management of security functions behaviour	✓	None
FMT_MSA.1	Management of security attributes		Refinement, selection, assignment
FMT_MSA.2	Secure security attributes		None
FMT_MTD.1	Management of TSF data	✓	Assignment
FMT_SMF.1	Specification of management functions	✓	Assignment
FMT_SMR.1	Security roles	✓	Assignment
FPT_ITT.1	Basic internal TSF data transfer protection		Selection
FPT_RVM.1	Non-bypassability of the TSP	✓	None
FPT_SEP.1	TSF domain separation	✓	None
FPT_STM.1	Reliable time stamps	✓	None
FTP_TRP.1	Trusted path		Selection, assignment
IDS_SDC(EXP).1	System Data Collection	✓	Selection, assignment
IDS_ANL(EXP).1	Analyser analysis	✓	Selection, assignment
IDS_RCT(EXP).1	Analyser react	✓	Assignment
IDS_RDR(EXP).1	Restricted Data Review	✓	Assignment
IDS_STG(EXP).1	Guarantee of System Data Availability	✓	Assignment, selection
IDS_STG(EXP).2	Prevention of System data loss	✓	Selection

5.1.1. Security Audit (FAU)

5.1.1.1. Audit data generation (FAU_GEN.1)

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[10] level of audit; and

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

Table 5-2 - Auditable Events

Functional Component	Auditable Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System Data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1	Any use of the authentication mechanism.	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MSA.1	All modifications of the values of audit archive protection keys.	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role.	User identity
FTP_TRP.1	All attempted uses of the trusted path functions.	User identity

[10] The **basic** level of audit is defined in [IDSSPP] as the auditable events included in Table 5-2 - Auditable Events.

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, outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the additional information specified in the Details column of Table 5-2 - Auditable Events.

5.1.1.2. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authorised administrators with System Events permission** with the capability to read **all audit information** 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. Restricted audit review (FAU_SAR.2)

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. Selectable audit review (FAU_SAR.3)

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

5.1.1.5. Selective audit (FAU_SEL.1)

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[11].

5.1.1.6. Protected audit trail storage (FAU_STG.2)

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

FAU_STG.2.2 The TSF shall be able to **prevent**[12] **unauthorised** modifications to the **stored** audit records **in the audit trail**[13].

FAU_STG.2.3 The TSF shall ensure that **an administrator-configurable number of** audit records will be maintained when the following conditions occur: audit storage exhaustion.

[11] FAU_SEL.1.1 subsection b) assignment ‘list of additional attributes that audit selectivity is based upon’ is completed as ‘None’; the component has been refined to omit subsection b) for clarity.

[12] The FAU_STG.2.2 selection 'prevent' was used in place of 'detect' as used in [IDSSPP]. Prevention is stronger than detection and is therefore consistent with the intent of the PP.

[13] The FAU_STG.2.2 element has been updated to conform with the CCv2.3 syntax. This is consistent with [I-0422].

5.1.1.7. Prevention of audit data loss (FAU_STG.4)

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

5.1.2. Cryptographic support (FCS)

5.1.2.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys **for trusted path and for audit data archiving protection** in accordance with a specified cryptographic key generation algorithm **ANSI X9.31 (TDES-2Key)** and specified cryptographic key sizes **1024 bits for RSA keys, 128 bits for AES keys** that meet the following: **FIPS 140-2 level 1**.

5.1.2.2. Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **TLSv1.0** that meets the following: **[RFC 2246]**.

5.1.2.3. Cryptographic operation (FCS_COP.1)[14]

FCS_COP.1.1 The TSF shall perform **the cryptographic operations listed in Table 5-3** in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet the following: **FIPS 140-2 level 1 and the standards identified in Table 5-3:**

Table 5-3 - Cryptographic Operations

Operation	Alg.	Key Size	Standard
Trusted path encryption/decryption	AES	128 bits	FIPS PUB 197 in CBC mode
Trusted path server authentication	RSA	1024 bits	PKCS #1
Secure hash computation for trusted path	SHA-1	N/A	FIPS PUB 180-2
Encryption of audit archive data	AES	128 bits	FIPS PUB 197 in ECB mode
Key wrapping for audit archive data	RSA	1024 bits	PKCS #1
Signature of audit archive data	RSA + SHA-1	1024 bits	DER-encoded PKCS #1 using SHA-1
ADC content updates verification	RSA + SHA-1	1024 bits	DER-encoded PKCS #1 using SHA-1

[14] FCS_COP.1 assignments 'cryptographic algorithm' and 'cryptographic key sizes' are both completed as '**listed in Table 5-3**'; the component has been refined to omit these assignments for clarity.

5.1.3. Identification and authentication (FIA)

5.1.3.1. User authentication before any action (FIA_UAU.2)

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

5.1.3.2. User attribute definition (FIA_ATD.1)

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

a) User identity;

b) Authentication data; and

c) Authorisations[15].

5.1.3.3. User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4. Security Management (FMT)

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

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions of System data collection, analysis and reaction to authorised System administrators.

5.1.4.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall restrict[16] the ability to <u>change_default</u>, <u>create</u>, <u>delete</u>, **import and export** the security attributes **audit archive protection keys** to **authorised administrators with Settings permissions**.

5.1.4.3. Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

[15] FIA_ATD.1.1 subsection d) assignment ‘any other security attributes’ is completed as ‘None’; the component has been refined to omit subsection d) for clarity.

[16] FMT_MSA.1 was refined to complete the assignment ‘enforce the [assignment: access control SFP, information flow control SFP]’ as ‘**no SFP**’; FMT_MSA.1 is included in this ST in support of FPT_ITT.1, rather than any explicitly defined SFP.

5.1.4.4. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to query and add System and audit data, and shall restrict the ability to query and modify all other TOE data to **authorised administrators with the authorisations as specified in Table 5-4 below.**

5.1.4.5. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **as specified in Table 5-4.**

Table 5-4- Specification of Management Functions

Component	Management Function	Required Authorisations
FMT_MOF.1	**Modify the behaviour of the functions of System data collection, analysis and reaction**	**Authorised System administrator[17] (authorised administrator with Edit permission on applicable objects)**
FMT_MSA.1	**Change default, create, delete, import and export audit archive protection keys**	**Authorised administrator with Settings permission**
FMT_MTD.1	**Query audit data**	**Authorised Audit Viewer[18] (authorised administrator with System Events permissions)**
	Query and add System data	**Authorised administrator with View permission on applicable objects**
	Query and modify all other (non-System and audit) TOE data	**Authorised administrator**
FMT_SMR.1	**Modify the group of users that are part of a role**	**Authorised administrator with administrator permission**

5.1.4.6. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following roles**:** authorised administrator, authorised System administrators[17], and **authorised Audit Viewer[18], and authorised adminis-**

[17] In this ST, the authorised System administrator role is a superset of the authorised administrator role that is assigned Edit permissions on applicable objects, in relation to FMT_MOF.1.

[18] The authorised Audit Viewer role is a superset of the authorised administrator role that is assigned System Events permissions. The other authorised roles should not be assigned these permissions. Evaluated configuration guidance instructs administrators to assume this role exclusively for the purpose of querying audit data, i.e. it is not to be used for other management functions.

trators with one or more of the following authorisations identified in Table 5-4: Settings permission, View permission on applicable objects, administrator permission.

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. Basic internal TSF data transfer protection (FPT_ITT.1)

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

5.1.5.2. Non-bypassability of the TSP (FPT_RVM.1)

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

5.1.5.3. TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

5.1.5.4. Reliable time stamps (FPT_STM.1)

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

5.1.6. Trusted path/channels (FTP)

5.1.6.1. Trusted path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for administrator sessions.

5.1.7. IDS Component Requirements (IDS)

5.1.7.1. System Data Collection (IDS_SDC(EXP).1)

IDS_SDC(EXP).1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) identification and authentication events, data accesses, service requests, network traffic, detected known vulnerabilities[19].

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

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

b) The additional information specified in the Details column of Table 5-5 – System Events.

Table 5-5 - System Events

Component	Event	Details
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address
IDS_SDC.1	Data accesses	Object IDS, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

5.1.7.2. Analyser analysis (IDS_ANL(EXP).1)

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

a) signature; and

b) **the analysis functions specified in Table 5-6**.

Table 5-6 - IDS Analysis Functions

Analysis Function	Applies to network traffic type
Matching traffic with predefined Firewall Policy	**All (only in inline topology)**
Protocol violations	**All**
Profile violations	**Web and database traffic**
Correlated Attack Validation	**Web and database traffic**
Database Active Security Assessment	**None – applies to active database scans**

IDS_ANL(EXP).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

[19] IDS_SDC(EXP).1.1 subsection b) assignment 'other specifically defined events' is completed as 'None'; the component has been refined to omit subsection b) for clarity. In addition, Table 5-5 has been tailored to omit all PP event descriptions not selected for IDS_SDC(EXP).1.1 a).

b) **Destination Server Group**.

5.1.7.3. Analyser react (IDS_RCT(EXP).1)

IDS_RCT(EXP).1.1 The System shall send an alarm to **defined Action Interfaces** and take **action to block and/or monitor applicable network traffic** when an intrusion is detected.

5.1.7.4. Restricted Data Review (IDS_RDR(EXP).1)

IDS_RDR(EXP).1.1 The System shall provide **authorised administrators** with the capability to read **Alerts, database audit records, database active security assessment results, collected application profiles, System configuration and Gateway Status as constrained by the administrator's permissions** from the System data.

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

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

5.1.7.5. Guarantee of System Data Availability (IDS_STG(EXP).1)

IDS_STG(EXP).1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_STG(EXP).1.2 The System shall protect the stored System data from modification.

IDS_STG(EXP).1.3 The System shall ensure that **200,000 Alert records and up to 199 Gb of database audit files per gateway of** System data will be maintained when the following conditions occur: <u>System data storage exhaustion</u>.

5.1.7.6. Prevention of System data loss (IDS_STG(EXP).2)

IDS_STG(EXP).2.1 The System shall <u>overwrite the oldest stored System data</u> and send an alarm if the storage capacity has been reached.

5.2. *TOE Security Assurance Requirements*

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 2 components defined in Part 3 of the Common Criteria ([CC]), augmented with the [CC] Part 3 component ALC_FLR.1.

Note: [IDSSPP] requires EAL2.

No operations are applied to the assurance components. Where assurance requirements have been updated in CCv2.3 (ACM_CAP.2, ADO_IGS.1, and AVA_VLA.1), the assurance requirements in this ST conform to those updated requirements, by reference.

Table 5-7- TOE Security Assurance Requirements

Assurance Class	**Assurance Components**	
Configuration Management (ACM)	ACM_CAP.2	Configuration items
Delivery and Operation (ADO)	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Lifecycle support (ALC)	ALC_FLR.1	Basic flaw remediation
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment (AVA)	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.3. Security Functional Requirements for the IT Environment

FCS_CKM.4(Env) is a security functional requirement for the IT environment, intended to constrain the IT measures that should be used by the administrator, in order to ensure secure destruction of cryptographic keys in the context of the O.CREDEN security objective for the (non-IT) environment.

FPT_STM.1(Env) is allocated to the IT environment to support configurations where the TOE's clock is synchronized with that of a trusted external IT entity.

5.3.1. Cryptographic support (FCS)

5.3.1.1. Cryptographic key destruction (FCS_CKM.4(Env))

FCS_CKM.4.1(Env) The **IT Environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **full disk overwriting** that meets the following: **no standard**[20].

5.3.1.2. Reliable time stamps (FPT_STM.1(Env))

FPT_STM.1.1(Env) The **IT Environment** shall be able to provide reliable time stamps for the **TSF**.

[20] FCS_CKM.4(Env) does not mandate any specific disk overwrite solution, as long as the entire disk is overwritten.

6. TOE Summary Specification

This section describes the security functions of the TOE and the assurance measures taken to ensure correct implementation, and maps them to the security requirements.

6.1. TOE Security Functions

This section presents the IT security functions (SFs) and a mapping of security functions to security functional requirements. The TOE performs the following security functions:

- Data Collection
- ID Analysis
- Actions
- Security Management
- Audit
- TSF Protection

6.1.1. Data Collection

6.1.1.1. Network Traffic Collection

In both sniffing and inline topologies, the TOE collects all IP network traffic flowing between external and internal networks. Collected IP packets are recognized as UDP datagrams, TCP sessions, or other IP protocols, and forwarded to the TOE's analysis and reaction logic.

In addition to collecting network traffic, the TOE provides application-level monitoring for two protocol types: database access protocols (supported databases include Oracle, Sybase, DB2, Microsoft SQL Server, and Informix), and service requests for Web resources (over the HTTP and HTTPS protocols).

6.1.1.2. Universal User Tracking

The TOE can be configured to identify HTML form-based Web identification and authentication events, and associate the user's identity with the session. Because Web access often involves multiple HTTP sessions to the Web server for a single user session, the TOE can be configured to track Web session identifiers passed as HTTP parameters or in HTTP cookies, allowing it to trace users' activity more accurately across HTTP sessions.

Database access requests are parsed by the TOE. User identification and authentication events are identified, and the user's identity associated with queries passed on the corresponding database session.

The TOE correlates user Web requests and corresponding database requests that are invoked by an application server on the user's behalf, providing a Web to Database User Tracking capability.

6.1.1.3. Recording Alerts in the SecureSphere Database

Alerts are generated by the TOE's analysis logic. They can either be an indication of suspicious activity, or a result of an administrator request to monitor specified events.

Alerts are sent by the SecureSphere 6 gateway that generates the Alert to the Management Server, and stored in the SecureSphere database in a table that can hold up to 200,000 Alert records. When the table fills up, the Management Server switches to a second table of the same capacity, erasing its previous contents and overwriting them with new Alert records. The Management Server switches back to the first table when the second table fills up. This process guarantees that at the least the most recent 200,000 Alert records will be retained at any given point in time. Evaluated configuration guidance provides instructions on configuration of an alarm to be sent to a syslog server in the IT environment after a table switch is performed.

An authorised administrator may schedule automatically generated recurring reports that are sent from the Management Server in CSV or PDF format to an administrator-specified email address, containing all or a subset of the stored Alerts records.

Alert attributes include the following relevant fields:

- **Alert Severity** one of: Informative or Low, Medium, or High Severity.
- **Time** date and time when the Alert was generated.
- **Type** one of: Firewall, Signature, HTTP Worm, Protocol Violation, Profile Violation, Correlation.
- **Aggregated** Alert record is an aggregation of multiple network-level events.
- **Source IP** The source IP address that generated the alert.
- **Server Group** The name of the destination Server Group.
- **Action Policy** Followed Action policy name.
- **Description** Alert identification
- **Immediate Action** Blocked if the corresponding connection was blocked.
- **User identity** The identity of the user associated with the event (if available).

In addition, the Alert Type-specific information is recorded. Among other attributes, this includes:

Table 6-1- Recorded Alert Type-Specific Details

Event	Details
Firewall Events (network traffic)	Source and Destination Ports, Protocol (TCP/UDP/ICMP), Service name (if recognized)
Signature Events	All packet contents, HTTP or database query
Protocol violation	Specific service request
Profile Violations	
Worms	
Correlation Rules	

6.1.1.4. Database Auditing

Database auditing records database queries for audit purposes. For each database server group you can define an unlimited number of audit rules. The administrator defines rules for audited queries. Rules are defined as a function of user names, source IP addresses, source applications, audited database tables and operations, and time of day. When a rule is enabled, gateways save all matching queries into files on the gateway.

For each database query, at least the following information is recorded:

- Date and time;
- Source and destination IP addresses;
- Source application;
- User name;
- Query; and
- Success or failure.

Database audit files are stored in files on the gateway, and can be queried using the SecureSphere GUI. Each gateway allocates 199 Gb of disk space for database audit storage. The gateway will automatically delete the oldest files when database audit file storage is exhausted (as defined by an administrator-configurable min-free-disk-space threshold) and overwrites the storage space with new data. An alarm is sent as a System Event when this occurs.

6.1.1.5. Database Audit Archiving

An authorised administrator can configure the TOE to automatically archive and/or purge the database audit files on a defined schedule. Archiving sends the database audit files in CSV format to be stored on a server outside the TOE. Archived database audit data can still be queried from the TOE.

In order to protect the archived database audit data from unauthorised read access or modification, the TOE encrypts and signs the files as follows:

- A SHA-1 hash of the data is computed, signed with an administrator-specified 1024 bit RSA signing key, and stored together with the data as a DER-encoded PKCS#1 block.
- The data is encrypted using a randomly generated 128 bit AES key in ECB mode.
- The AES key is encrypted using an administrator-specified 1024 bit RSA encryption key, and stored together with the data.
- Keys are generated as described for FCS_CKM.1.
- The database audit archive keys are stored on the Management Server, and can be managed by an authorised administrator.

6.1.1.6. Database Active Security Assessment

The TOE can invoke active assessment tests on databases using remote SQL queries and SSH connections to their host operating systems[21]. The active assessment engine can receive test updates via the ADC content updates mechanism. Assessment tests can be invoked manually by an authorised administrator, or automatically on a defined schedule, and generate reports that can be viewed by the administrator.

Reports available include database users and permissions, known database and operating system vulnerabilities, compliance analysis (e.g. SOX, PCI, HIPAA), and general database information. For each report, at least the following information is recorded:

- Date and time;
- Assessment test identification;
- Success, failure, or error status; and
- Detected known vulnerabilities.

6.1.1.7. System Data Protection

Recorded System data is reviewed by authorised administrators via the SecureSphere GUI management interface (see Security Management SF below). Authorised administrators can selectively delete System data, but have no interface for modifying stored data.

[21] SSH-based active security assessment tests are unavailable in the TOE evaluated configuration.

The TOE does not provide any interface for unauthorised users to access System data.

6.1.1.8. SFR Mapping

The following SFRs are satisfied by the Data Collection SF:

- **IDS_SDC(EXP).1 –** the System is able to collect the identified types of information from network traffic, as described for the Network Traffic Collection and the Database Active Security Assessment capabilities. The information recorded is detailed in the sections describing the Recording Alerts in the SecureSphere Database, Database Auditing and Database Active Security Assessment capabilities. User identity is derived as described for the Universal User Tracking capability. Data collection can be mapped to the information required in IDS_SDC(EXP).1.2 as follows:

Table 6-2- Recorded Information Mapping to IDS_SDC(EXP).1

Event	Requirement	Recording Alerts	Database Auditing	Database Assessment
All	date and time of the event	Time	date and time	date and time
	type of event	type, alert severity, aggregated, description	query	Test identification
	subject identity	source IP, user identity	user name	N/A
	outcome	action policy, immediate action	success or failure	Success, failure, or error status
I&A events	user identity	user identity		
	location	source IP		
	source address	source IP		
	destination address	server group		
Data accesses	object IDs		query	
	requested access		query	
	source address		source IP address	
	destination address		destination IP address	
Service requests	specific service	service name		
	source address	source IP		
	destination address	server group		
Network traffic	protocol	protocol, service name		

Event	Requirement	Recording Alerts	Database Auditing	Database Assessment
	source address	source IP, source port		
	destination address	server group, destination port		
Detected known vulnerabilities	Identification of the known vulnerability			Detected known vulnerabilities

- **IDS_STG(EXP).1 –**System data stored in the TOE is protected from unauthorised deletion and modification as described for the System Data Protection capability. The TOE extends protection to archived database audit files by signing the files, allowing the TOE to detect any unauthorised modification of the files while outside the TOE. The TOE cannot prevent unauthorised deletion of data stored outside the TOE. System data storage capacity is described for the Recording Alerts in the SecureSphere Database and Database Auditing capabilities.
- **IDS_STG(EXP).2 –** As described for both the Recording Alerts in the SecureSphere Database and Database Auditing capabilities, the oldest stored System data is delete when storage is exceeded to make space for the storage of new information. Alarms are generated in both cases, to a syslog server in the IT environment for the former, and as a System Event for the latter capability. The administrator can schedule generation of Alerts reports that are sent to an administrator-defined email address, as well as archive database audit files outside the TOE (as described for the Database Audit Archiving capability).
- **FCS_CKM.1, FCS_COP.1, FMT_MSA.2, FPT_ITT.1[22], IDS_RDR(EXP).1 –** The Database Audit Archiving capability signs and encrypts archived database audit data. This protects the data from disclosure (read access) and modification while it is outside the TOE. Key generation is as described for FCS_CKM.1. Only secure values are accepted for security attributes (i.e., cryptographic security parameters) by way of conformance to the identified cryptographic standards.
- **IDS_ANL(EXP).1 –** The Database Active Security Assessment capability includes both collection and analysis functions.

[22] FPT_ITT.1 requires protection of TSF data (database audit in this case) when it is transmitted between separate parts of the TOE, i.e. while it is in transit outside of the TOE. Here, the Management Server is sending the TSF data outside the TOE through untrusted media (the audit archive server) for later retrieval by same Management Server. The audit archive server does not have to be trusted to protect the data while it is outside the TOE – it is prevented from disclosing or modifying the data by the cryptographic protection applied to the data by the TOE. The FPT_ITT term “separate parts of the TOE” is interpreted in this context to mean that there is a gap (of potential insecurity) that is traversed by the data.

6.1.2. ID Analysis

6.1.2.1. Overview

Events that are matched by any of the ID analysis engines are recorded as an Alert and forwarded to the Actions SF for further processing.

The information recorded for each analytical result is described above for the Recording Alerts in the SecureSphere Database capability of the Data Collection SF.

6.1.2.2. Signature

Signature rules are activated when a signature is detected. Signature rules are defined for each dictionary defined in the system.

6.1.2.3. Firewall Policy

A Firewall Policy can be configured for protected Server Groups when in inline topology. A separate policy is applied to the inbound (to Server Group) and outbound (from Server Group) direction. A Firewall Policy is defined as a set of service/IP address combinations, specified by providing either a white list (restrictive) or a black list (permissive). In addition, the Firewall Policy can be configured to match all IP fragments as not allowed.

6.1.2.4. Protocol Violations

SecureSphere 6 verifies protocol compliance for IP, TCP, UDP, HTTP, and database access protocols. Authorised System administrators can select protocol violations that are identified by the TOE as indicative of an intrusion.

6.1.2.5. Profile Violations

This capability is only available for Web, Oracle, Sybase, DB2 Microsoft SQL Server and Informix Groups. For these types of server groups SecureSphere builds a Dynamic Profile and compares incoming and outgoing HTTP and SQL requests against the learned profile. Any deviation from the profile generates a Profile Violation.

Authorised System administrators can view and modify Dynamic Profiles. In addition, an authorised System administrator can configure Custom Policy Rules that match specific attributes of HTTP requests or SQL queries.

6.1.2.6. Correlated Attack Validation

SecureSphere 6 includes a correlation engine that correlates different types of security events over time. Each predefined correlation rule correlates different types of events and variables to detect different types of attacks. Each individual event might not be sufficient to positively identify an intrusion attempt; when the event is detected, a suspicion rating is assigned to the pertinent traffic, but the traffic is not immediately blocked. The CAV engine will identify a potential intrusion only when multiple events match a correlation rule and exceed the rule's decision threshold. Correlation rules allow accurate detection and low false positive rate as they rely on a sequence of security events and not a single event.

The authorised System administrator can selectively enable and disable correlation rules.

6.1.2.7. SFR Mapping

The following SFRs are satisfied by the ID Analysis SF:

- **IDS_ANL(EXP).1** – the System performs the analysis functions described in the preceding subsections on collected data. The information recorded in an Alert for each analytical result includes at least the following information: data and time of the result, type of result (Alert Type), identification of data source (IP address) and the destination Server Group.

6.1.3. Actions

6.1.3.1. Overview

Security Rules applied when an Alert is generated are defined per Server Group. There are six categories of Security Rules, defined by the type of ID analysis layer that generated the Alert: Network Firewall Rules, Signature Rules, Protocol Violation Rules, Web Worm Defender Rules, Profile Violation Rules, and Correlation Rules.

For each rule, the Action Policy defined by the authorised System administrator can invoke two types of actions:

- **Immediate Actions** Optional actions taken as an immediate response to an attack (see below, Blocking).
- **Followed Actions** Optional follow-up actions taken by the System (see below, Action Sets).

6.1.3.2. Blocking

SecureSphere 6 can be configured to immediately react to a specific identified intrusion type by blocking the network packet that generated the security event (by dropping it when in inline topology) or by sending a TCP reset to the attacked server (when in sniffing topology) to cause it to disconnect the corresponding session.

6.1.3.3. Action Sets

An Action Set defines a set of actions and operations that are executed by the SecureSphere 6 as a result of an ID analysis. Configurable actions include:

- **Blocking Attacking IP** Blocking subsequent IP packets with a presumed source address equal to that recorded for the event, for a specified period of time.
- **Blocking Attacking Session** Blocking subsequent HTTP requests with the same session identifier as was recorded for the event, for a specified period of time.
- **Block User** Block subsequent requests associated with the same user as was identified for the event, for a specified period of time.
- **Dispatch Alert** Send alarm to specified Action Interfaces including relevant Alert details.
- **Start Monitoring** Record all requests/responses from the IP or session recorded for the event, for a specified period of time.

6.1.3.4. Action Interfaces

SecureSphere 6 supports the following action interfaces, to which the Management Server sends an alarm when a given Alert is generated:

- **Syslog** The Alert is sent to an external syslog host using the Syslog protocol.
- **Email** The Alert is sent to an external SMTP server using the SMTP protocol.
- **SNMP** The Alert is sent to an external SNMP management host as an SNMP trap.
- **Task** The Alert is attached to a Review Task assigned to a specified administrator in the SecureSphere GUI.

6.1.3.5. SFR Mapping

The following SFRs are satisfied by the Actions SF:

- **IDS_RCT(EXP).1 –** When an intrusion is detected by the ID Analysis SF, alarms are sent via the Action Interfaces capability. Actions that can be taken to block and/or monitor applicable network traffic are described for the Blocking and Action Sets capabilities.

6.1.4. Security Management

6.1.4.1. Management Functions

The SecureSphere GUI is used by authorised administrators to manage all IDS/IPS System and audit capabilities as described in Table 6-3:

Table 6-3- Management Functions

Component	Management Function	Management Functionality
FMT_MOF.1	Modify the behaviour of the functions of System data collection, analysis and reaction	Authorised System administrators use the SecureSphere GUI interface to modify Server Group definitions, define Action Interfaces and Action Policies, configure Security Rules for each Server Group, enable collection, analysis and reaction capabilities, and manage Profiles and Signatures.
FMT_MSA.1	Change default, create, delete, import and export audit archive protection keys	Authorised administrators with Settings permission can use the SecureSphere GUI interface to create, delete, import and export and to set the default RSA keys used for signing and encrypting archived database audit data.
FMT_MTD.1	Query audit data	Authorised administrators with System Events permission can use the SecureSphere GUI interface to review the audit trail.
	Query and add System data	Authorised administrators can use the SecureSphere GUI interface to review System data for which they have View permission, to update Profiles and Signatures and to invoke database assessments.
	Query and modify all other (non-System and audit) TOE data	Authorised administrators can use the SecureSphere GUI interface for reviewing and modifying all other TOE data (e.g. Tasks).
FMT_SMR.1	Modify the group of users that are part of a role	SecureSphere GUI provides authorised administrators with administrator permission with the ability to add, edit, and delete user accounts, and reset their passwords.

6.1.4.2. SecureSphere GUI

SecureSphere GUI is a browser-based interface to the Management Server that allows authorised administrators to access TOE management functions. The TLSv1.0 protocol is used to provide a trusted path using a 1024 bit RSA key for Management Server authentication, 128 bit AES for session encryption, and SHA-1 for hash calculation, as described in FCS_CKM.2 and FCS_COP.1. Key generation is as described in FCS_CKM.1.

The SecureSphere GUI requires the administrator to enter a valid user name and password before allowing any other actions on behalf of the user. Table 6-4 lists SecureSphere GUI password constraints enforced by the TOE. TOE guidance instructs administrators to avoid overriding these controls.

Table 6-4 - SecureSphere GUI Password Constraints

Parameter	**Default Value**
Minimum password length	5 characters
A password must include lower case letters	True
A password must include capital letters	False
A password must include numbers	True
A password must include non alpha-numeric characters	False
Password validity period (in days)	90

Once successfully logged in, the SecureSphere GUI provides the user with administration and monitoring functions, restricted in accordance with the user's authorisations as described below for the Administrator Access Control capability.

6.1.4.3. Administrator Access Control

Each authorised administrator is associated with the following security attributes in the SecureSphere GUI application:

- User name
- Password
- Authorisations:
  - Group membership(s)
  - User-specific permissions

User groups are associated with permissions. Users associated with the group inherit these permissions in addition to any user-specific permissions they have been allocated.

Permissions are evaluated for each user when the user logs in, and affect which objects are displayed and which operations may be performed.

Permissions are defined on managed objects (Applications, Policies, Gateways, Sites, Servers, and Global Objects), as either View or Edit. An authorised administrator is defined in this ST to be an authorised System administrator for a subset of System data if assigned Edit permissions to the corresponding System objects.

Special permissions allow users to active settings and navigate to certain pages, e.g. the Alerts permissions allow access to the Alerts viewer or for viewing Alerts reports. Users assigned with this special permission will only see report data regarding alerts generated on Server Groups for which they have View permission. The System Events permissions[23] provide access to audit data. The Settings permission provides access to database audit archiving configuration and key management interfaces.

Users with administrator permissions can allocate or remove permissions for other users, or specify default permissions for newly created objects.

6.1.4.4. Audit Review

SecureSphere GUI allows authorised administrators with System Events permissions to view the System Events Log. The administrator can sort the System Log by event Type, User name, and by date and time.

6.1.4.5. SFR Mapping

The following SFRs are satisfied by the Security Management SF:

- **FAU_SAR.1, FAU_SAR.2 –** The Audit Review capability allows authorised administrators with System Events permissions to read audit information from the audit records using the SecureSphere GUI web-based interface. Administrators without applicable permissions cannot view audit records.
- **FAU_SAR.3 –** The Audit Review capability allows authorised administrators to perform sorting of audit data based on date and time, subject identity (user name), and event Type. The success or failure of the related event is implied from the event Type.

[23] There are three special permissions that can provide access to System Events: the System Events Navigation permission allows access to the System Events Log, the System Events Reports permission allows access to System Events reports, and the Dashboard Navigation permission allows the administrator to view the most recent audit records in the System Events log.

- **FIA_ATD.1** –The Administrator Access Control capability maintains the required security attributes for each authorised administrator user, as follows:

Table 6-5- Authorised administrator Attribute Mapping to FIA_ATD.1

FIA_ATD.1 Attribute	Authorised administrator Attribute
User identity	User name
Authentication data	Password
Authorisations	Group memberships, user-specific permissions

- **FIA_UID.2** and **FIA_UAU.2** – The SecureSphere GUI requires the user to identify and authenticate before allowing any other actions on behalf of the user.
- **FMT_SMR.1 –** The Administrator Access Control capability differentiates between the authorised administrator and authorised System administrator roles in relation to the administrator's assigned Edit permissions.
- **FMT_MOF.1, FMT_MSA.1, FMT_MTD.1 –** Restriction of management functions to roles is described for the Administrator Access Control capability.
- **FMT_SMF.1** – The Management Functions capability maps the management functions listed in this SFR to corresponding TOE management functions.
- **IDS_RDR(EXP).1 –** The SecureSphere GUI capability provides authorised administrators with the capability to read System data using a Web-based interface. Authorised administrator permissions are described for the Administrator Access Control capability.
- **FCS_CKM.1, FCS_CKM.2, FCS_COP.1, FMT_MSA.2, FTP_TRP.1 –** The TOE provides a trusted path for authorised administrator sessions as described for the SecureSphere GUI capability. The Management Server allows remote users to initiate communication via the trusted path by establishing TLSv1.0 sessions, using RSA for Management Server authentication and a password for authenticating the administrator. This is required for all administrator sessions. Only secure values are accepted for security attributes (i.e., cryptographic security parameters) by way of conformance to the identified cryptographic standards.

6.1.5. Audit

6.1.5.1. System Events Log

The System Events Log includes activities related to ADC content updates, changes to configuration, activation of settings, building profiles, automatic profile updates, rebuilding database indexes, server start/stop, SecureSphere GUI logins/logouts, user administration operations.

For each event, the following attributes are recorded in the SecureSphere database:

- **Event Time** Date and time of the event.

- **Sub System** The subsystem that generated the log entry, e.g. User subsystem.
- **Severity** Type or severity, e.g. Warning, Notify, etc.
- **Message** A description of the event. For administrator login events, this includes the user's IP address.
- **User** The username that generated this event. If the event was generated by the SecureSphere system, the username is 'System'.
- **Primary URI** Managed object (where applicable).

Auditable events can be included or excluded based on event type during the installation and generation of the TOE.

6.1.5.2. Audit Protection

The System Events Log is reviewed by Authorised administrators via the SecureSphere GUI management interface (see Security Management SF above). Authorised administrators have no interface for modifying or deleting stored records.

System log records are stored in a Management Server database table. Evaluated configuration guidance provides instructions on configuration of an alarm to be sent to a syslog server in the IT environment when the number of records in the table exceeds a *max_system_events* threshold that can be configured during initial installation and configuration of the TOE. When this occurs, the oldest records in the table are deleted to make space for new records, down to a *min_system_events* threshold.

The authorised administrator may schedule automatically generated recurring reports that are sent from the Management Server in CSV or PDF format to an administrator-specified email address, containing all or a subset of the stored audit records.

6.1.5.3. SFR Mapping

The following SFRs are satisfied by the Audit SF:

- **FAU_GEN.1 –** SecureSphere 6 generates the required audit records, as shown in the following table derived from Table 5-2 - Auditable Events:

Table 6-6- Audit SF Mapping to FAU_GEN.1

Functional Component	**Auditable Event**	**Mapping**
FAU_GEN.1	Start-up and shutdown of audit functions	Log events are generated when a gateway goes up or goes down.
FAU_GEN.1	Access to System	SecureSphere GUI logins and logouts are logged.
FAU_GEN.1	Access to the TOE and System Data	SecureSphere GUI logins are logged.
FAU_SAR.1	Reading of information from the	Logins of the authorised Audit Viewer

Functional Component	Auditable Event	Mapping
	audit records	into SecureSphere GUI are logged. In accordance with evaluated configuration guidance, this role is used exclusively for querying the System Events log.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Unsuccessful SecureSphere GUI logins are logged, including authorised Audit Viewer login failures.
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	Modifications to the audit configuration can only be performed during initial installation and configuration, by editing a logging configuration file.
FIA_UAU.1	Any use of the authentication mechanism.	Successful and unsuccessful SecureSphere GUI logins are logged.
FIA_UID.1	All use of the user identification mechanism	Successful and unsuccessful SecureSphere GUI logins are logged.
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	All configuration changes are logged.
FMT_MTD.1	All modifications to the values of TSF data	All configuration changes are logged.
FMT_SMR.1	Modifications to the group of users that are part of a role.	All user administration operations are logged.
FTP_TRP.1	All attempted uses of the trusted path functions.	Successful and unsuccessful SecureSphere GUI logins are logged.

Each system log record includes the following information: date and time of the event, type of event, subject identity, outcome (Severity), and object IDs (primary URI) where applicable. Location is identified by the administrator's IP address.

- **FAU_SEL.1 –** the System Events Log capability supports audit pre-selection during the installation and generation of the TOE.
- **FAU_STG.2**, **FAU_STG.4 –** stored audit records are protected as described for the Audit Protection capability: the TOE does not provide any interface for modifying or deleting audit records; an administrator-configured batch job deletes old records when the number of audit records exceeds a threshold defined during initial installation and configuration, and sends an alarm to a syslog server in the IT environment; the authorised administrator can schedule reports that send audit records to an administrator-defined email address.

6.1.6. TSF Protection

6.1.6.1. Domain Separation

Neither the Management Server nor the SecureSphere 6 gateways route or bridge network traffic between the Management NIC (described above in Section 2.3.3.3) and the production NICs. This separation provides a separate network domain for the Out of Band (OOB) management network, protecting all gateway-Management Server communication from any access by authorised or unauthorised users.

In both sniffing and bridging configurations (except for non-transparent reverse proxy configurations), SecureSphere 6 gateways do not have an assigned IP address on all sniffing/bridging network interface cards (NICs), so that the gateways cannot be directly attacked over the network.

6.1.6.2. Reference Mediation

The TOE does not provide any unauthenticated management interfaces. All administrators are identified and authenticated before they can perform any other operations on the TOE. The System Events Log records all administrative operations performed on the TOE.

6.1.6.3. Time Synchronization

The SecureSphere 6 Management Server and gateways include a real time clock that provides reliable timestamps for recorded System data. The Management Server synchronizes the gateways' clocks with its own using the NTP protocol over the OOB management network.

The SecureSphere 6 Management Server’s clock can optionally be synchronized with an external NTP server.

6.1.6.4. ADC Content Update Verification

ADC content updates loaded either manually or automatically into the TOE are verified by the Management Server before the update is applied: the updates are signed by the ADC using 1024 bit RSA over a SHA-1 hash as described in FCS_COP.1, prior to distribution.

6.1.6.5. SFR Mapping

The following SFRs are satisfied by the TSF Protection SF:

- **FPT_RVM.1** – This SFR is directly met by the Reference Mediation capability.
- **FPT_SEP.1** – This SFR is directly met by the Domain Separation capability.
- **FPT_STM.1** – This SFR is directly met by the Time Synchronization capability.

- **FPT_ITT.1 –** The internal TOE transfer of TSF data is protected by the allocation of a physically separate NIC on both Management Server and gateways for gateway-Management Server communication, as described for the Domain Separation capability.
- **FCS_COP.1 –** ADC content updates are verified using 1024 bit RSA over SHA-1 prior to application to prevent tampering.

6.2. TOE Security Assurance Measures

This section describes the assurance measures provided for the TOE, and maps them to the security assurance requirements (SARs) in section 5.2.

The SARs in the ST are exclusively based on CC EALs and other [CC] Part 3 assurance components (namely ALC_FLR.1). The assurance measures are presented in the form of a reference to the documents that show that the assurance requirements are met. These documents are uniquely identified in the configuration list included in the Configuration Management documentation.

6.2.1. Process Assurance Documentation

6.2.1.1. Delivery Procedures

Delivery procedures describe the measures taken to ensure that the security of the configuration items of the TOE is maintained when distributing the TOE to a user's site.

6.2.1.2. Configuration Management

The Configuration Management (CM) documentation provides a unique reference for the TOE and includes a configuration list of all configuration items (CIs) that comprise the TOE, as well as a description of the method used to uniquely identify these CIs in the CM system.

6.2.1.3. Flaw Remediation

Flaw tracking and remediation procedures and guidance addressed to TOE developers describe the procedures used to track all reported security flaws and to find corrective actions for each of these flaws, as well as the distribution of reports and corrections to TOE users.

6.2.2. Development Documentation

6.2.2.1. Functional Specification

The Functional Specification identifies all of the TOE's security functions and external interfaces, and provides a description of all external TOE security function interfaces.

Correspondence with the TOE Summary Specification is demonstrated, as well as to the set of SFRs defined in this Security Target.

6.2.2.2. High-level Design

The High-level Design document provides a description of the TOE in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide.

Underlying hardware, firmware, and software are identified, as well as subsystem interfaces.

Correspondence with the Functional Specification is demonstrated, as well as to the set of SFRs defined in this Security Target.

6.2.3. The TOE

Instances of the TOE including administration guidance documentation (identified in section 2.3.4) are provided to the evaluators for evaluation of guidance and for independent testing.

Note that the TOE is not visible to non-administrative users; therefore, AGD_USR.1 is trivially satisfied.

6.2.4. Test Plan and Procedures

The Test Documentation document describes the testing of the TOE at the level of its functional specification. It consists of test plans, test procedure descriptions, expected test results and actual test results. Test plans identify the security functions tested and describe the goal of the tests to be performed. Test procedures descriptions identify the tests to be performed and describe the scenarios for testing each security function. The match between actual test results and expected test results demonstrates that each tested security function behaved as specified.

6.2.5. Vulnerability Analysis

The Vulnerability Analysis builds on the other evaluation evidence to show that the developer has searched for vulnerabilities in the TOE and provides reasoning about why they cannot be exploited in the intended environment for the TOE. The analysis references public sources of vulnerability information to justify that the TOE is resistant to obvious penetration attacks.

6.2.6. SAR Mapping

Table 6-7 maps evaluation evidence to SARs, showing that all of the assurance requirements of the TOE are met by appropriate assurance measures.

Table 6-7- Mapping of Evaluation Evidence to Assurance Requirements

Document	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1	ALC_FLR.1
Configuration Management	✓													
Delivery Procedures		✓	✓											
Flaw Remediation														✓
Functional Specification				✓		✓								
High-level Design					✓	✓								
Security Target[24]												✓		
Test Documentation									✓	✓				
The TOE			✓				✓	✓			✓			
Vulnerability Assessment													✓	

[24] This Security Target identifies all permutational or probabilistic security mechanisms and demonstrates that all of the relevant mechanisms fulfill the minimum strength of function claim, 'SOF-Basic'. See Section 8.3.3 in particular.

6.3. *Identification of Standards*

The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. The SFRs in the Cryptographic Support (FCS) class stated in Section 5.1.2 therefore reference external standards that the implementation must meet when providing the required capabilities.

Table 6-8 summarizes the standards compliance claims made in Section 5.1.2 and states for each the method used to determine compliance (aside from development assurances). The method may be an applicable NIST certificate number or a vendor assertion.

Table 6-8- Cryptographic Standards and Method of Determining Compliance

Standard claimed	**Cryptographic SFRs**	**Method of determining compliance**
FIPS 140-2 Level 1	FCS_CKM.1, FCS_COP.1	FIPS 140-2 Cert. #1048
AES in CBC mode per FIPS PUB 197	FCS_COP.1	AES Cert. #669
RSA per PKCS#1	FCS_COP.1	RSA Cert. #311
SHA-1 per NIST PUB FIPS 180-2	FCS_COP.1	SHS Cert. #702
TLSv1.0 per RFC 2246	FCS_CKM.2	Vendor assertion

7. PP Claims

7.1. PP Reference

The TOE meets all security objectives and requirements of [IDSSPP].

7.2. PP Tailoring

The security objectives for the TOE include all [IDSSPP] security objectives, with the qualifications specified in section 4.1. The security objectives for the environment are also taken from [IDSSPP].

All security requirements from [IDSSPP] have been restated in this ST, except for the SFRs listed in section 5.1 as exceptions, omitted per the guidance given in [PD-0097]. For the FIA_UID.1 and FIA_UAU.1 requirements, a hierarchical component was selected in their place; by definition a TOE meeting the hierarchical requirement would meet the original requirement as well.

Similarly, requirements have been qualified, within the bounds set by the PP. Permitted operations performed on PP security functional requirements are identified in Table 5-1. In some cases, application notes and footnotes were added in the statement of security functional requirements to clarify the relationship of an SFR to the PP. Footnotes have also been used to identify requirements that have been tailored to conform with CCv2.3 syntax.

No operations are applied to assurance components.

The following additional interpretations to the PP requirements have been implemented in this ST:

- The ST uses the authorised administrator role defined in the PP. It should be noted that the definition of this role in the ST is different from the authorised administrator role defined in the PP. Aside from its definition in FMT_SMR.1, the only PP SFR that refers to the ‘authorised administrator’ is FIA_AFL.1, which in accordance with [PD-0097] has not been included in the ST.
- Table 5-2 lists auditable events defined in the PP in the context of FAU_GEN.1. For the auditable events related to FAU_SAR.2, the TOE does not generate audit events for unsuccessful attempts to read information from the audit trail, because only the authorised Audit Viewer role gets the menu option to review the audit trail. The TOE offers no way for the other user roles to access the audit trail. FAU_SEL.1 is considered to be upheld because no modifications to the audit configuration can occur while the audit collection functions are operating.

7.3. PP Additions

All SFRs derived from [IDSSPP] as well as SFRs added in this ST are identified in Table 5-1. Rationale for the added SFRs is as follows:

- **FPT_ITT.1** was added following the guidance given in [PD-0097]. This requirement was mapped to the TOE's Domain Separation SF capability for protecting gateway to Management Server communications, and to archived audit data protection (as described for the Database Audit Archiving SF capability). **FMT_MSA.1** was added to restrict management of the latter capability to authorised administrators with Settings permissions.
- **FTP_TRP.1** was added to provide trusted path functionality for administrator sessions.
- **FCS_CKM.1**, **FCS_CKM.2**, and **FCS_COP.1** were added in support of both FPT_ITT.1 and FTP_TRP.1.
- **FMT_MSA.2**, and **FMT_SMF.1** were added to satisfy CCv2.3 dependencies.

The assurance level has been augmented in relation to that required by [IDSSPP] by the addition of the **ALC_FLR.1** requirement, as described in section 8.2.4.

8. TOE Rationale

8.1. Security Objectives Rationale

8.1.1. IT Security Objectives Rationale

See section 7.1 of [IDSSPP].

In accordance with the guidance given in the [IDSSPP] Errata Sheets, OE.TIME is mapped to P.ACCACT and P.DETECT policies which require audit and system data to be generated and include a timestamp.

8.1.2. Non-IT Security Objectives Rationale

See section 7.2 of [IDSSPP].

8.2. Security Requirements Rationale

8.2.1. Security Functional Requirements Rationale

See section 7.3 of [IDSSPP] for the rationale for all PP-derived SFRs. The following is rationale for the SFRs added to the PP additions listed in Section 7.3. Table 8-1 summarizes the rationale:

- FPT_ITT.1 was added following the guidance given in [PD-0097], replacing the [IDSSPP]-defined inter-TOE SFRs, which are mapped in the PP to O.INTEGR, with the following rationale: “the System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product”. As FPT_ITT.1 also supports IDS_RDR(EXP).1, it can be seen to map to O.ACCESS as well.
- FTP_TRP.1 can be seen to uphold O.INTEGR and O.ACCESS with the same rationale as for FPT_ITT.1.
- The cryptographic SFRs: FCS_CKM.1, FCS_CKM.2, FCS_COP.1 as well as FMT_MSA.2 were added to the ST in support of FPT_ITT.1 and FTP_TRP.1. They are therefore also mapped to O.INTEGR and O.ACCESS. FCS_COP.1 also supports O.PROTCT, because it provides cryptographic verification for ADC content updates loaded into the TOE.
- FMT_MSA.1 upholds O.PROTCT, O.ACCESS, and O.IDAUTH, with the same rationale given in [IDSSPP] for FMT_MOF.1 and FMT_MTD.1.
- FMT_SMF.1 was introduced to satisfy CCv2.3 dependencies for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1, as identified in Table 8-3. It can therefore be seen to support the security objectives O.PROTCT, O.ACCESS and O.IDAUTH in which these two requirements are grounded.

Table 8-1 - SFR Rationale Summary

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_GEN.1										✓	
FAU_SAR.1						✓					
FAU_SAR.2							✓	✓			
FAU_SAR.3						✓					
FAU_SEL.1						✓				✓	
FAU_STG.2	✓						✓	✓	✓		✓

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_STG.4									✓	✓	
FCS_CKM.1							✓				✓
FCS_CKM.2							✓				✓
FCS_COP.1	✓						✓				✓
FIA_ATD.1								✓			
FIA_UAU.2							✓	✓			
FIA_UID.2							✓	✓			
FMT_MOF.1	✓						✓	✓			
FMT_MSA.1	✓						✓	✓			
FMT_MSA.2							✓				✓
FMT_MTD.1	✓						✓	✓			✓
FMT_SMF.1	✓						✓	✓			
FMT_SMR.1								✓			
FPT_ITT.1							✓				✓
FPT_RVM.1	✓					✓		✓		✓	✓
FPT_SEP.1	✓					✓		✓		✓	✓
FPT_STM.1										✓	
FTP_TRP.1							✓				✓
IDS_SDC(EXP).1		✓	✓								
IDS_ANL(EXP).1				✓							
IDS_RCT(EXP).1					✓						
IDS_RDR(EXP).1						✓	✓	✓			
IDS_STG(EXP).1	✓						✓	✓	✓		✓
IDS_STG(EXP).2									✓		

8.2.2. Strength of Function (SOF) Rationale

The TOE Strength of Function is claimed to be SOF-basic or higher. See section 7.6 of [IDSSPP].

8.2.3. SFRs for the IT Environment Rationale

This ST draws all security objectives for the TOE and for the IT environment from [IDSSPP]. FPT_STM.1(Env) is allocated to the IT environment as allowed by the [IDSSPP] Errata Sheets (in addition to the FPT_STM.1 TOE SFR). This ST adds FCS_CKM.4(Env) as a security objective for the IT environment.

- **FPT_STM.1(Env) –** this requirement for the IT environment is mapped to OE.TIME. It requires that the IT environment provide reliable timestamps to the TOE. This applies when external NTP time synchronization is configured.
- **FCS_CKM.4(Env)** - Security objective for the non-IT environment O.CREDEN requires that all access credentials be protected in a manner which is consistent with IT security. The TOE maintains cryptographic keys, stored on appliance hard disks. These keys are used as access credentials. For example, unauthorized disclosure of the encryption keys used to protect audit archive data may allow an attacker to access System data stored outside the TOE. This ST therefore traces the FCS_CKM.4(Env) security functional requirement for the IT environment to O.CREDEN. This SFR requires that the IT environment allow the administrator to perform a full disk overwrite to ensure cryptographic key destruction.

8.2.4. Security Assurance Requirements Rationale

The level of assurance chosen for this ST is that of Evaluation Assurance Level (EAL) 2, as defined in [CC] Part 3, augmented with the [CC] Part 3 component ALC_FLR.1.

Section 7.4 of [IDSSPP] provides a rationale that EAL 2 is appropriate to meet the TOE's security assurance objectives.

In addition, the assurance requirements have been augmented with ALC_FLR.1 (Basic flaw remediation) to provide assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE.

8.2.5. Extended Requirements Rationale

This ST includes the following explicitly stated functional requirements, all taken from [IDSSPP]. See section 7.5 of [IDSSPP] for justification for these requirements.

Table 8-2- Explicitly Stated Security Functional Requirements

Extended Component	
IDS_SDC(EXP).1	System Data Collection
IDS_ANL(EXP).1	Analyser analysis
IDS_RCT(EXP).1	Analyser react
IDS_RDR(EXP).1	Restricted Data Review
IDS_STG(EXP).1	Guarantee of System Data Availability
IDS_STG(EXP).2	Prevention of System data loss

8.2.6. Dependency Rationale

Table 8-3 depicts the satisfaction of all security requirement dependencies. For each security requirement included in the ST, the CC dependencies are identified in the column "CC dependency", and the satisfied dependencies are identified in the "ST dependency" column. Iterated components (if any) are identified to help determine exactly which specific iteration is dependent on which SFR or SAR.

Dependencies that are satisfied by hierarchically higher or alternative components are given in **boldface**, and explained in the "Dependency description" column.

Table 8-3- Security Requirements Dependency Mapping

SFR	CC dependency	ST dependency	Dependency description
FAU_GEN.1	FPT_STM.1	FPT_STM.1, FPT_STM.1 (Env)	Audit dependency on secure time.
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	Audit review dependency on audit generation.
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FMT_GEN.1, FMT_MTD.1	Selective audit dependency on audit generation and on management of audit data.
FAU_STG.2	FAU_GEN.1	FAU_GEN.1	Protected audit trail storage dependency on audit generation.
FAU_STG.4	FAU_STG.1	**FAU_STG.2**	FAU_STG.2 is hierarchical to FAU_STG.1 so it can be used to satisfy the dependency.
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4 (Env), FMT_MSA.2	Dependency on FCS_CKM.4 is met by the corresponding IT environment SFR. This is consistent with the guidance provided in [PD-0091].
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4 (Env), FMT_MSA.2	Dependency on FCS_CKM.4 is met by the corresponding IT environment SFR. This is consistent with the guidance provided in [PD-0091].

SFR	CC dependency	ST dependency	Dependency description
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4 (Env), FMT_MSA.2	Dependency on FCS_CKM.4 is met by the corresponding IT environment SFR. This is consistent with the guidance provided in [PD-0091].
FIA_ATD.1	None		
FIA_UAU.2	FIA_UID.1	**FID_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UID.2	None		
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	Management restrictions dependency on management functions and administrator roles
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	Dependency on access control or information flow control SFP omitted in this ST as FMT_MSA.1 is included in support of FPT_ITT.1.
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	None	FMT_MSA.2 included in this ST as a dependency of the FCS class SFRs, and does not relate to any defined SFP or security attribute management requirements. ADV_SPM.1 was omitted as it not consistent with the EAL 2 assurance claims.
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	Management restrictions dependency on management functions and administrator roles
FMT_SMF.1	None		
FMT_SMR.1	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_ITT.1	None		
FPT_RVM.1	None		
FPT_SEP.1	None		
FPT_STM.1	None		
FTP_TRP.1	None		
IDS_SDC(EXP).1	None		
IDS_ANL(EXP).1	None		

SFR	CC dependency	ST dependency	Dependency description
IDS_RCT(EXP).1	None		
IDS_RDR(EXP).1	None		
IDS_STG(EXP).1	None		
IDS_STG(EXP).2	None		
ACM_CAP.2	None		
ADO_DEL.1	None		
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1	Consistent with EAL 2
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1	Consistent with EAL 2
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	ADV_FSP.1, ADV_RCR.1	Consistent with EAL 2
ADV_RCR.1	None defined explicitly	ADV_FSP.1, ADV_HLD.1	Correspondence demonstration dependency on the functional specification and high-level design
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1	Consistent with EAL 2
AGD_USR.1	ADV_FSP.1	ADV_FSP.1	Consistent with EAL 2
ALC_FLR.1	None		
ATE_COV.1	ADV_FSP.1, ATE_FUN.1	ADV_FSP.1, ATE_FUN.1	Consistent with EAL 2
ATE_FUN.1	None		
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	Consistent with EAL 2
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	ADV_FSP.1, ADV_HLD.1	Consistent with EAL 2
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	Consistent with EAL 2

8.2.7. Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole.

No operations have been performed on SARs. A base evaluation assurance level of EAL 2 was selected as described in section 8.2.4 to ensure the internal consistency and mutual support of the SARs in this ST. Section 8.2.4 also provides justification for any augmentations above EAL 2.

The dependency analysis in section 8.2.6 demonstrates that mutual support interactions defined in [CC] Part 2 and Part 3 have been correctly resolved: by definition, if requirement A has a dependency on requirement B, B supports A.

Because this ST claims compliance to a validated PP, justification has been provided in [IDSSPP] for the internal consistency and mutual support of its claimed requirements. This holds for FPT_ITT.1 as well, in accordance with [PD-0097]. FTP_TRP.1 was added to support O.ACCESS and O.INTEGR with similar rationale. The FCS class SFRs and FMT_MSA.2 were added in support of FPT_ITT.1 and FTP_TRP.1.

FMT_SMF.1 has been added to this Security Target to satisfy FMT class dependencies. For consistency's sake, it has been constructed to include the management functions described in FMT_MOF.1 and FMT_MTD.1.

FMT_MSA.1 was added to restrict administration of database audit archiving security attributes.

FPT_STM.1(Env) was added in accordance with the [IDSSPP] Errata Sheets, in addition to FPT_STM.1, to support external time synchronization using the NTP protocol. If external NTP is configured, the TOE relies on the IT environment for secure time stamps. If it is not, secure time stamps are generated by the TOE as required by FPT_STM.1.

8.3. TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security functional requirements (SFRs) and security assurance requirements (SARs).

The security requirements are mutually supportive and consistent, as shown above in section 8.2.7.

8.3.1. TOE Security Functions Rationale

The collection of security functions work together to provide all of the security functional requirements as indicated in Table 8-4. All points where this could cause conflict were examined and this was not the case. It is also evident from an inspection of the tables that the security functions described in the TSS are all necessary to address the required security functionality of the TSF.

Table 8-4- TOE Summary Specification Rationale Mapping

	Data Collection	**ID Analysis**	**Actions**	**Security Management**	**Audit**	**TSF Protection**
FAU_GEN.1					✓	
FAU_SAR.1				✓		
FAU_SAR.2				✓		
FAU_SAR.3				✓		
FAU_SEL.1					✓	
FAU_STG.2					✓	
FAU_STG.4					✓	
FCS_CKM.1	✓			✓		
FCS_CKM.2				✓		
FCS_COP.1	✓			✓		✓
FIA_ATD.1				✓		
FIA_UAU.2				✓		
FIA_UID.2				✓		
FMT_MOF.1				✓		
FMT_MSA.1				✓		
FMT_MSA.2	✓			✓		
FMT_MTD.1				✓		

	Data Collection	ID Analysis	Actions	Security Management	Audit	TSF Protection
FMT_SMF.1				✓		
FMT_SMR.1				✓		
FPT_ITT.1	✓					✓
FPT_RVM.1						✓
FPT_SEP.1						✓
FPT_STM.1						✓
FTP_TRP.1				✓		
IDS_SDC(EXP).1	✓					
IDS_ANL(EXP).1	✓	✓				
IDS_RCT(EXP).1			✓			
IDS_RDR(EXP).1	✓			✓		
IDS_STG(EXP).1	✓					
IDS_STG(EXP).2	✓					

8.3.2. Assurance Measures Rationale

The assurance measures that correspond to the security assurance requirements are demonstrated in Section 6, and are further explained in the referred documentation. Table 6-7 in particular shows that all SARs are met by appropriate documentation or physical evidence.

8.3.3. Strength of Function Rationale

The only security function for which a strength of function claim is appropriate is Security Management, tracing to FIA_UAU.2. A password-based mechanism is used for authentication to the *SecureSphere GUI* administration interface. Passwords are considered a probabilistic or permutational function and therefore require a strength of function analysis.

The SOF-basic strength of function claimed for the I&A capability meets the SOF-basic strength of function requirement for FIA_UAU.2.

The constraints enforced by the TOE on password selection are described in Section 6.1.4.2. Furthermore, TOE guidance instructs the administrator to avoid selecting easily-guessable passwords. Assuming the worst case scenarios, the minimum password space for each capability can be computed as follows:

5 character password, composed of both letters and digits:

26 letters

+10 digits

36 possible characters

36^5 = 60,466,176 combinations.

The TOE applies a one-second delay after each password entry (successful or unsuccessful). On average, an attacker would have to enter 30,233,088 passwords, over 350 days, before entering the correct password.

In accordance with the approach outlined in annex A.8 of the CEM, the password function is resistant to attackers with an attack potential lower than 17, and can be rated SOF-basic.

In addition, note that SecureSphere GUI passwords expire after an administrator-defined validity period (default 90 days).

8.4. PP Claims Rationale

This section is intended to explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

Chapter 7 describes the method used to tailor PP security objectives and requirements for this ST.

The following precedent decisions have been used as guidance for interpreting [IDSSPP]:

Table 8-5- References to Guidance on the Interpretation of Claimed PPs

Reference	Affected SFRs and objectives	Description
[PD-0097]	O.EXPORT, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FIA_AFL.1	Incorrectly included in the System PP – must be removed from the PP
	FPT_ITT.1	Should be added for distributed TOE.