Imperva SecureSphere 9.0

Security Target

Version 0.8

September 19, 2012

Prepared for:

Imperva Inc.
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
United States

Prepared by:

Metatron Security Services Ltd.

Document Version Control Log

Version	Date	Author	Description
Version 0.1	April 15, 2011	Nir Naaman	Initial draft.
Version 0.2	April 29, 2011	Nir Naaman	Updated ST in relation to ASE ETR comments.
Version 0.21	May 1, 2011	Nir Naaman	Additional pre-iVOR updates.
Version 0.3	June 6, 2011	Nir Naaman	Post-iVOR updates: clarified security claims for different appliance models included in TOE.
Version 0.31	July 26, 2011	Nir Naaman	Additional post-iVOR updates: defined single configuration for the TOE, with no statements of optional security-relevant functionality.
Version 0.4	December 6, 2011	Nir Naaman	Updated to SecureSphere 9.0 including Virtual Appliances in the TOE. Described new SecureSphere 9.0 administrator roles and authorisations model. Added support for Kerberos authentication for administrators.
Version 0.5	February 23, 2012	Nir Naaman	Changed TOE identification to 9.0.0.1_0. Key generation algorithm is FIPS 186-2 instead of X9.31 (see RNG Cert. #389).
Version 0.6	July 5, 2012	Nir Naaman	Changed TOE identification to 9.0.0.3_0.
Version 0.7	August 30, 2012	Nir Naaman	Moved list of non-TOE components supported by the TOE to Appendix A
Version 0.8	September 19, 2012	Nir Naaman	Changed TOE identification to 9.0.0.5_0.

Table of Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Reference

Title: Imperva SecureSphere 9.0 Security Target

ST Version: 0.8

ST Date: September 19, 2012

Author: Nir Naaman

CC Version: Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009

Evaluation Assurance Level:

EAL 2, augmented with ALC_FLR.2 (flaw reporting procedures).

Protection Profile conformance:

U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007

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

1.2. TOE Reference

TOE Identification: Imperva SecureSphere 9.0 (version 9.0.0.5_0) software running on two or more of the Imperva appliances listed below, including one or more Management Servers and one or more Gateways:

Table 1-1 - SecureSphere Appliances

Appliance	Role	FT[1]	TP[1]	HD[1]	RAM	FF[1]
X1000	Gateway (32 bit)	×	0.1	500 Gb	2 Gb	1U
X2000	Gateway (64 bit)	×	½	500 Gb	4 Gb	1U
X2500	Gateway (64 bit)	✓	½	2 x 500 Gb	4 Gb	2U
X4500	Gateway (64 bit)	✓	1	2 x 1 Tb	8 Gb	2U
X6500	Gateway (64 bit)	✓	2	2 x 1 Tb	8 Gb	2U
M100	Management Server	×	N/A	300 Gb	4 Gb	1U
M150	Management Server	✓	N/A	2 x 300 Gb	4 Gb	2U

[1] **FT** = Fault Tolerant: dual hot-swap hard drives, power supplies, and fans. **TP** = Throughput: measured throughput for mediated Web and Database traffic in Gbps. File security products can typically handle four times the identified throughput. **HD** = hard drive capacity in Terabyte. **FF** = Form Factor.

In addition, the identified software is provided in the form of Virtual Appliance images that are run on a VMware ESX/ESXi Hypervisor. The VMware Hypervisor and underlying hardware is considered to be outside of the boundaries of the TOE.

1.3. Document Organization

Section 1 provides the introductory material for the security target, including ST and TOE references, TOE Overview, and TOE Description.

Section 2 identifies the Common Criteria conformance claims in this security target

Section 3 describes the security problem solved by the TOE, in terms of the expected operational environment and the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through additional environmental controls identified in the TOE documentation.

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

Section 5 is intended to be used to define any extended requirements claimed in this security target that are not defined in the Common Criteria

Section 6 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 7 explains how the TOE meets the security requirements defined in section 6, and how it protects itself against bypass, interference and logical tampering.

Section 8 provides supplemental information that is intended to aid the reader, including highlighting conventions, terminology, and external references used in this security target document.

Appendix A summarizes the components in the Information Technology (IT) environment supported by the TOE including identification of supported versions.

1.4. TOE Overview

1.4.1. Usage and Major Security Features of the TOE

SecureSphere 9.0 provides protection from attacks against database, file, Web, and Web Services assets, both within the organization (insider attacks) and from without. Installed on the network as a reverse Hypertext Transfer Protocol (HTTP) proxy, a transparent inline bridge or as an offline network monitor (sniffer), a SecureSphere 9.0 Gateway monitors application-level protocols for attacks, and reacts by blocking the attacks and/or reporting them to a centralized management server.

The product is deployed as one or more Gateway appliances controlled by a MX (Management Server) appliance. In multi-tier management configurations, one or more MX Management Servers may in turn be managed by a SecureSphere Operations Manager (SOM) Management Server.

Administrators connect to the Management Server using a standard Web browser (outside of the Target of Evaluation). They are required to authenticate their identity before being allowed any further action.

The different appliance models all run the same SecureSphere 9.0 software and provide all claimed security functionality, but may differ in throughput and storage capacity. SecureSphere 9.0 software (including management and/or Gateway components) may alternatively be installed on a Virtual Machine (VM) hosted by a VMware ESX/ESXi Hypervisor. The Virtual Machine emulates the SecureSphere 9.0 appliance hardware. The VMware Hypervisor and underlying hardware is considered to be outside of the boundaries of the Target of Evaluation.

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 (ADC). The ADC also provides ADC Insights – these are pre-packaged security policy rules and reports for commonly used applications.

The product’s comprehensive application auditing capability is augmented by a discovery and assessment capability that scans databases and file servers for known vulnerabilities and policy violations, identifies sensitive data, and enables automatic aggregation and review of user rights across the organization. The product can also integrate information from external sources such as web vulnerability scanners.

1.4.2. TOE Type

Imperva SecureSphere 9.0 protects file, Web and database servers by analyzing network traffic flowing to and from protected servers and applications, detecting requests that may be indicative of intrusion, and reacting by reporting the events and/or blocking the suspected traffic. In addition, SecureSphere 9.0 provides a Database Discovery and Assessment (DAS) capability for scanning databases for vulnerabilities and policy violations.

In this Security Target, the Target of Evaluation is categorized as an IDS/IPS product. SecureSphere 9.0 meets the requirements of the IDS System Protection Profile (IDSSPP). The IDSSPP defines an Intrusion Detection System (IDS) 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.

1.4.3. Non-TOE Hardware/Software/Firmware Required by the TOE

1.4.3.1. Web Browser for the SecureSphere GUI Management Interface

SecureSphere 9.0 is managed using a standard Web browser that includes an Adobe Flash plug-in (version 9 or 10). SecureSphere supports the following browsers:

- Microsoft Internet Explorer versions 7, 8 and 9
- Firefox versions 3, 3.6 and 4
- Safari version 3.2

1.4.3.2. VMware Hypervisor if Deploying a SecureSphere Virtual Appliance

SecureSphere 9.0 management and/or Gateway software can be installed on a Virtual Machine hosted by a VMware ESX/ESXi Hypervisor. VMware ESX/ESXi versions 3.x and 4.x are supported. Minimum requirements for each Guest SecureSphere Virtual Appliance are:

- 2 CPUs
- 4 GB memory
- 80 GB disk space

1.4.3.3. Secure Wiping Tool for Persistent RSA Keys

SecureSphere 9.0 creates persistent RSA keys that are stored on the appliance’s hard disk. TOE evaluated configuration guidance provides the administrator with instructions for secure wiping of TOE appliances' disks using third-party tools in the IT environment.

1.5. TOE Description

1.5.1. Introduction

SecureSphere 9.0 provides a broad range of services, features and capabilities. This ST makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality. The evaluated configuration must be established in accordance with the evaluated configuration guidance.

This part of the ST describes the physical and logical scope and boundaries of the Target of Evaluation (TOE). This description effectively partitions product functionality into three classes:

- Claimed security functionality that is evaluated in the context of this ST;
- Other functionality that is in the TOE but is not evaluated in the context of this ST except for the determination that it cannot compromise any claimed security functionality;
- Excluded functionality that is not available in the TOE's evaluated configuration.

The TOE Description consists of the following subsections:

- **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 security features offered by the TOE.
- **Functionality Excluded from the TOE Evaluated Configuration** – describes the product features excluded from the evaluated configuration.
- **Non Security-Relevant Functionality Included in the TOE** – identifies product functionality that is included in the evaluated configuration but not claimed as security functionality.

1.5.2. Physical Scope and Boundaries of the TOE

1.5.2.1. TOE Hardware, Firmware, and Software

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

- One[2] MX Management Server appliance; and
- One or more Gateway appliances; and optionally:
- One SecureSphere Operations Manager (SOM) Management Server appliance.

Figure 1-1 - SecureSphere Gateway Appliance

All appliance hardware and software is included in the TOE, with the following exceptions:

- **HSM and SSL Accelerator Cards**: SecureSphere 9.0 Gateway appliances may be purchased with an internal Hardware Security Module (HSM) or Secure Sockets Layer (SSL) accelerator PCI card that offloads key storage and cryptographic operations used for network traffic deciphering from the appliance CPU. These functions are not claimed security functionality. The cards may be used in the evaluated configuration but are considered to be part of the IT environment of the TOE. Gateway appliances can also be configured to interface with network-connected HSMs in the IT environment for the same purposes.
- **Active Modules**: SecureSphere 9.0 includes an Active Module software engine that is used to distribute value-added insights and capabilities generated by ADC, including the features Track Value Changes and Change Tracking, and the legacy Web Vulnerability Scanner (from WhiteHat Sentinel). Active Modules are distributed as Java .jar files as part of the ADC Content Updates mechanism. These features are not used in the evaluated configuration.
- **Apache Reverse Proxy**: Imperva supports a reverse proxy implementation for HTTP traffic based on public domain Apache Web server software, which can be installed on SecureSphere gateways. Such an installation is not included in the evaluated configuration. SecureSphere 9.0 provides an alternative high-performance Imperva kernel-based proxy infrastructure that is included in the evaluated configuration.

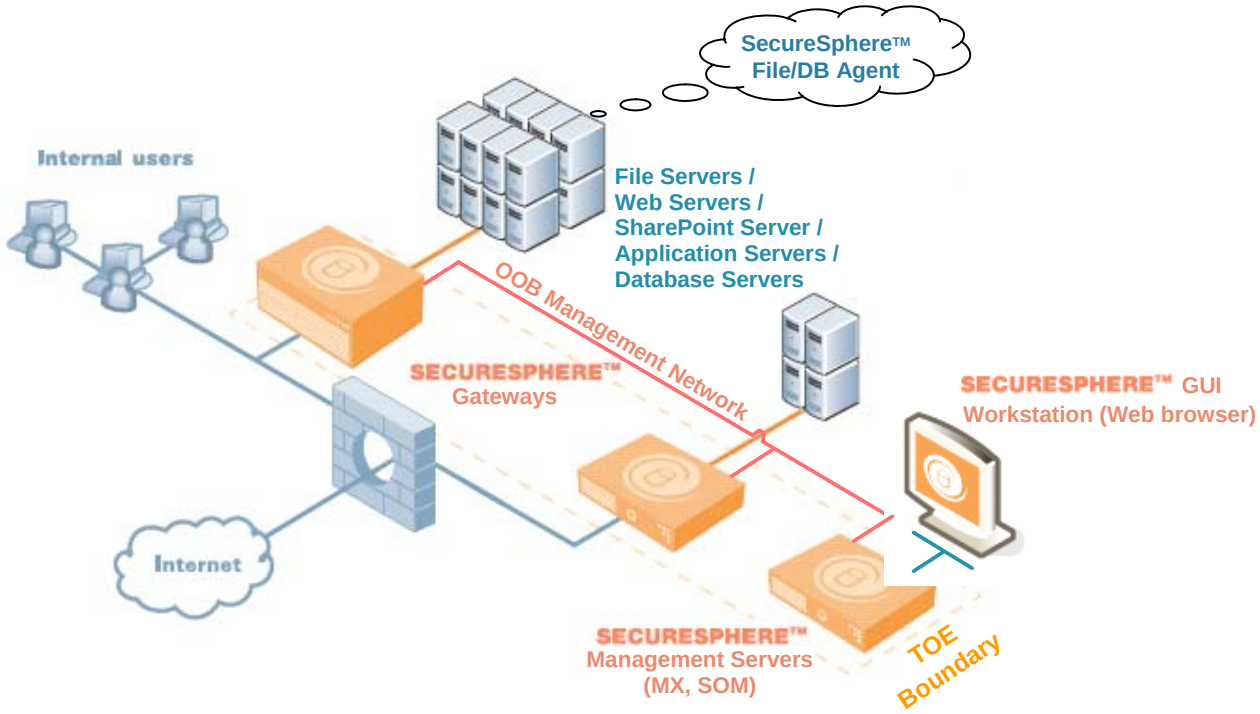
[2] Onebox mode (where both the SecureSphere management server and SecureSphere gateway are integrated in a single machine) is not included in the evaluated configuration.

- **SSH**: SecureSphere 9.0 appliances can support local console access and remote access to appliance operating system-level installation and configuration Command Line Interface (CLI) over the Secure Shell (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 restrict physical access to appliances and to disable remote user access to SSH in the evaluated configuration.

As a supported alternative to a physical appliance, each of the TOE components may be installed as software running on a Virtual Appliance hosted on a VMware hypervisor. The VMware ESX/ESXi server software and hardware are outside the boundaries of the TOE. The Imperva SecureSphere 9.0 software assumes[3] that the hypervisor provides complete separation for all Virtual Machine resources allocated for SecureSphere 9.0 components, as would be the case with a physical appliance.

Figure 1-2 below depicts the TOE protecting file, Web, Web Services and database assets[4]. SecureSphere 9.0 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 1-2- Physical Scope and Boundaries of the TOE

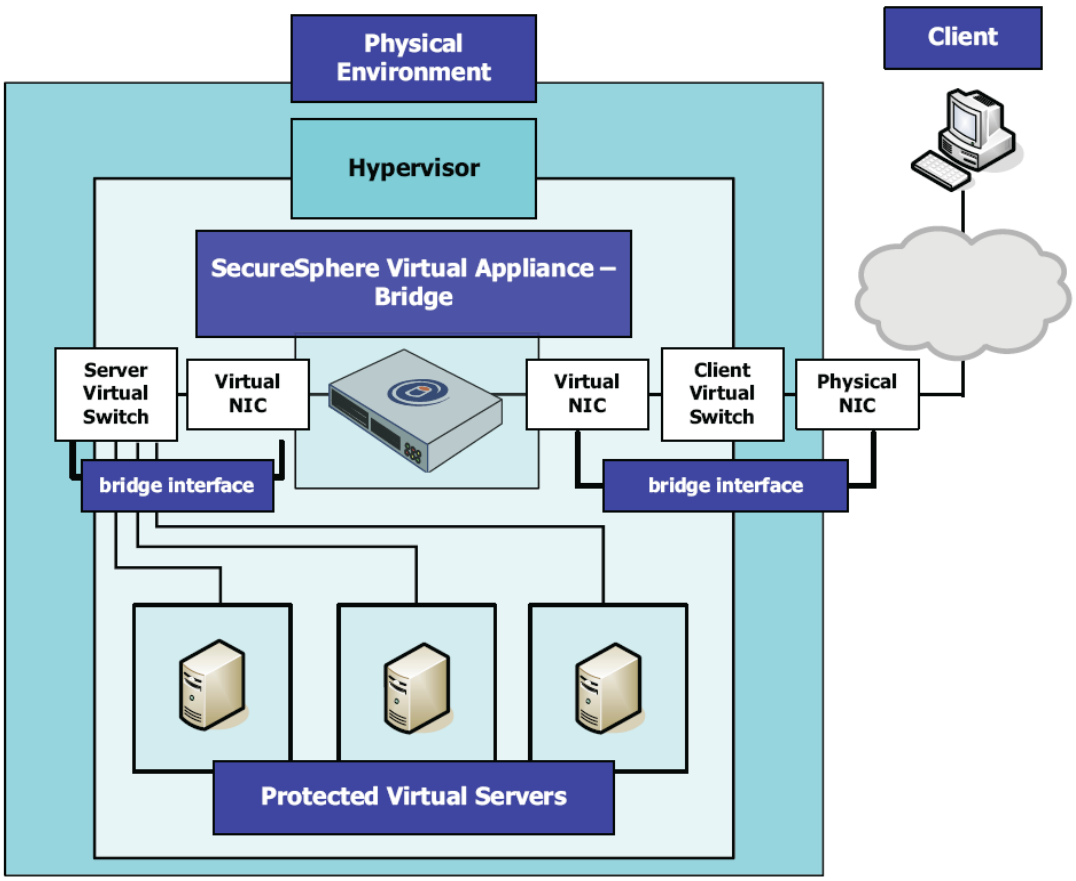


[3] Supported VMware ESX/ESXi servers versions 3.5, 4.0 Update 1, and 4.1 have all been certified to EAL4. See http://www.commoncriteriaportal.org/products for additional information on these evaluations.

[4] SharePoint assets are protected using an Imperva SharePoint application-specific configuration of file, Web, Web Services, and database protections.

Figure 1-3 below depicts a sample deployment where the Gateway is installed on a Virtual Appliance, protecting servers installed on other Virtual Machines hosted by the same VMware hypervisor. Note that the Management Server(s) may be installed on separate Virtual Machines on the same or other hypervisor, or on physical appliances. The boundary of the TOE in Figure 1-3 includes only the SecureSphere 9.0 software; the hypervisor, virtual switches, protected servers, and physical environment are all considered to be in the IT environment of the TOE.

Figure 1-3 – Sample Virtual Appliance Deployment



The browser (see also section 1.4.3 above), used to manage the TOE via the Secure-Sphere GUI Web interface, is also considered to be outside the boundary of the TOE. It is assumed that the environment will provide adequate access protection for administrator workstations and for the OOB management network.

The following Imperva software is considered to be outside of the TOE boundary:

- **SecureSphere DB and File Security Agents**: Imperva sensor software agents that run on the database or file server (outside the TOE), and transmit all access requests to the SecureSphere 9.0 gateway. This allows the gateway to analyze events that cannot be identified from network traffic, e.g. by applications running on the database or file server host itself.

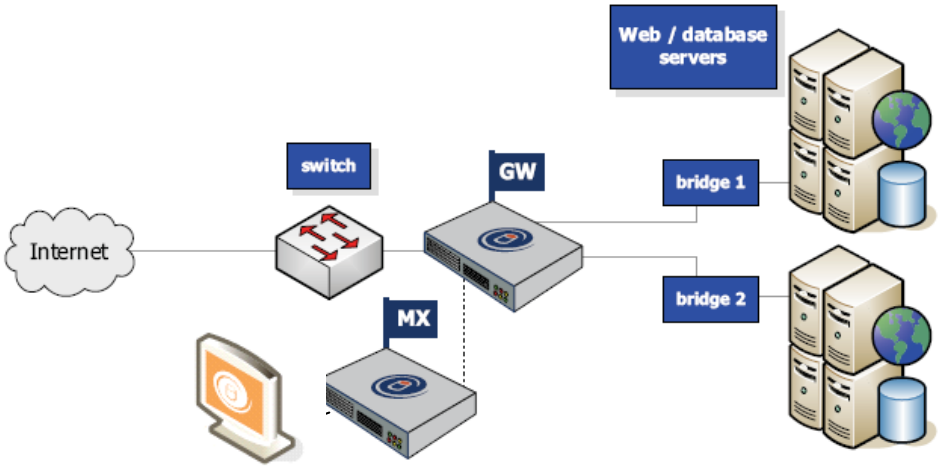
  Disabled by default, agent support may be enabled in the evaluated configuration.

1.5.2.2. SecureSphere Deployment Scenarios

All SecureSphere 9.0 appliance models support 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 effective blocking capabilities.

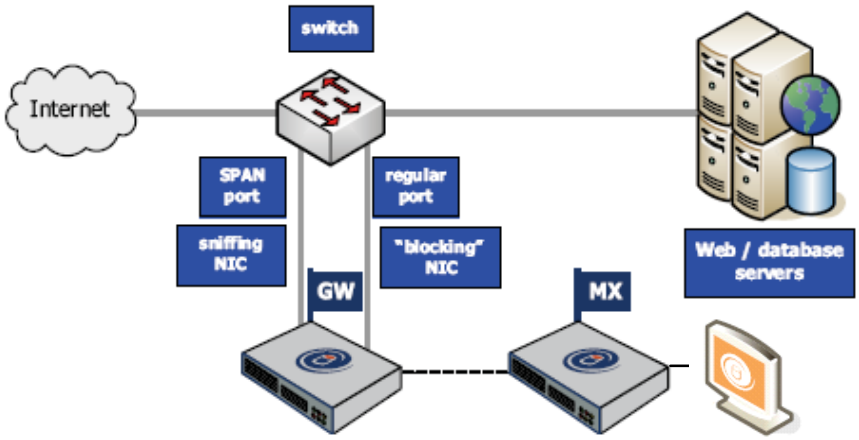
In the inline scenario, the gateway acts as a bridging device between the external network and the protected network segment. The gateway will block malicious traffic inline (i.e. drop packets). A single inline gateway protects one or two network segments. It has six network interface cards. Two of the 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 1-4- Example Inline 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, using a SPAN (Switch Port Analyzer) mirror port on the switch, or a dedicated TAP device. Traffic is copied to it instead of passing directly through it. Transmission Control Protocol (TCP) resets are transmitted over a “blocking” Network Interface Card (NIC).

Figure 1-5- Example Sniffing Topology – via SPAN (mirror) Port



1.5.2.3. Management Network

TOE guidance instructs the administrator to ensure that the SecureSphere 9.0 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 Internet Protocol (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 9.0 gateways. As depicted below in Figure 1-6 and Figure 1-7, the Management NIC is clearly separated from other appliance NICs. The SecureSphere 9.0 gateway operating system does not bridge or route packets between production NICs and Management NICs.

Figure 1-6 - Management NIC on 1U Appliances

Figure 1-7 - Management NIC on 2U Appliances

Management NIC separation is also maintained on a SecureSphere 9.0 Virtual Appliance. The virtual management NIC is selected during initial configuration of the appliance.

1.5.2.4. TOE Guidance

The following Imperva guidance documentation is considered part of the TOE:

Figure 1-8 – TOE Guidance

Title	**Date**
SecureSphere Administration Guide Version 9.0	November 2011
SecureSphere Web Application Security User Guide Version 9.0 (v2.0)	January 2012
SecureSphere Database Security User Guide Version 9.0	November 2011
SecureSphere File Security User Guide Version 9.0	November 2011
SecureSphere SharePoint Security User Guide Version 9.0	November 2011
SecureSphere Virtual Appliance VMware ESX Configuration Guide Version 9.0	November 2011
SecureSphere Operations Manager User Guide Version 1.0	November 2011
Imperva SecureSphere 9.0 Common Criteria Evaluated Configuration Guide	July 2012

1.5.3. Logical Scope of the TOE

1.5.3.1. Summary of TOE Security Functionality

IDS Component

Imperva SecureSphere 9.0 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 Intrusion Detection (ID) events, blocking traffic, and generating alarms containing event notifications. Database auditing allows you to record selected user database queries for audit purposes. Web and file server queries and responses can also be selectively recorded. In addition, monitored databases can be actively scanned to identify potential vulnerabilities.

Security Management, Identification and Authentication and Trusted Path

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 or Kerberos authenticator. The server provides a trusted path for the management session using the Transport Layer Security (TLS) protocol. 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.

Security Audit

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.

Protection of the TSF

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 is cryptographically protected from disclosure or tampering. ADC content and ThreatRadar update authenticity and integrity is verified by the TOE before updates are applied.

Cryptographic Support

The TOE uses the RSA BSAFE Crypto-J 4.0 FIPS 140-2 validated cryptographic module for the implementation of the administrator trusted path, audit data protection, and cryptographic verification of ADC and ThreatRadar updates.

1.5.3.2. Imperva SecureSphere Products

SecureSphere 9.0 functionality is enabled by entering Imperva licenses for SecureSphere "products". The following Imperva products are included in the evaluated configuration:

Table 1-2 - SecureSphere Products

Category	Product Name	Acronym	Description
Database Security	Database Activity Monitoring	DAM	Auditing and visibility into database data usage.
	Database Firewall	DF	Activity monitoring and real-time protection for databases.
	Discovery and Assessment Server	DAS	Vulnerability assessment, configuration management, and data classification for databases.
	User Rights Management for Databases	URMD	Review and manage user access rights to sensitive databases.
	ADC Insights		Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security.
	Database Agent Listener		Supports Gateway communication with remote agent software installed on protected servers.
File Security	File Activity Monitoring	FAM	Auditing and visibility into file data usage.
	File Firewall	FF	Activity monitoring and real-time protection for critical file data.
	User Rights Management for Files	URMF	Review and manage user access rights to sensitive files.
	File Agent Listener		Supports Gateway communication with remote agent software installed on protected servers.
Web Application Security	Web Application Firewall	WAF	Automated protection against online threats.
	ThreatRadar		Reputation-based Web application security service.

1.5.3.3. 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) when configured as a reverse proxy for HTTP traffic.
  - **Enrichment** – the TOE queries user directories for user information and DNS servers for host name resolution in order to store collected data with its human-readable source identification.
  - **DB and File Security Agents** – the TOE supports event collection from SecureSphere agents that act as IDS sensors for database and file access events.
  - **Log Collectors** – the TOE connects over the network to protected databases and collect event records from native database logs.
  - **Discovery and Assessment** – the TOE performs remote file server and database scans for sensitive data discovery and user rights analysis. Database scans also support identification of known vulnerabilities and defined-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 (in sniffing topology) signals servers to reset TCP connections that are suspect of being associated with malicious traffic.
  - **Action Interfaces** – the TOE reacts to system and security events by sending alarms, audit data, reports, and assessments to third-party analysis and reporting tools in the IT environment, enabling (Security Information and Event Management) SIEM/SIM (Security Information Management) tool integration.
- **Security Management**
  - **Management** – authorized administrators manage the TOE and review audit trail and IDS System data via the SecureSphere GUI.
  - **Content Updates** – the TOE imports updated ADC content updates including IDS attack signatures, database security assessment patterns, compliance policies, and predefined reports. An Imperva ThreatRadar service provides categorized reputation-based IP blocking lists in near real-time.

- **Time Updates** – the TOE synchronizes its clock with that of an external time server, using the Network Time Protocol (NTP).

1.5.3.4. Network Traffic Data Collection

1.5.3.4.1. Overview

SecureSphere 9.0 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.

1.5.3.4.2. Sniffing

When configured in sniffing topology, SecureSphere 9.0 gateways are configured with one or more NICs in *sniffing mode*. Sniffing 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.

1.5.3.4.3. Bridging

When configured in inline topology, SecureSphere 9.0 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.

1.5.3.4.4. Reverse Proxy

When configured in inline topology, SecureSphere 9.0 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).

1.5.3.4.5. Fail-Safe Modes

SecureSphere 9.0 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.

1.5.3.5. DB and File Security Agents

SecureSphere 9.0 gateways provide support for SecureSphere agents, IDS sensors outside of the TOE that are installed on database or file servers. Agents extend the reach of the TOE to database and file events that would not be otherwise visible to the gateway. The agent monitors all database and file access request traffic, including both network traffic and local access on the database or file server, and transmits the traffic to a network

segment monitored by SecureSphere 9.0 gateways for IDS data collection and analysis. The gateway inspects this traffic just like regular database or file traffic collected by the gateway.

Imperva DB Agents are available for Windows, AIX, Linux, Solaris, AS/400, and z/OS operating systems. File Security Agents are available for Windows operating systems.

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

1.5.3.6. Log Collectors

SecureSphere 9.0 Gateways can be configured to collect native database logs over File Transfer Protocol (FTP) or Standard Query Language (SQL) network protocols. The log records are integrated with the database audit records collected by the Gateway from database access network activity.

1.5.3.7. Discovery and Assessment (DAS)

The SecureSphere 9.0 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.

Both databases and file servers can be scanned for analysis of sensitive data and for user rights assessment (URMD and URMF products, respectively).

1.5.3.8. Analysis and Reaction

1.5.3.8.1. Overview

SecureSphere 9.0 applies different layers of intrusion detection logic to analyzed network traffic, as depicted below in Figure 1-9. 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.

SecureSphere supports the following two blocking methods:

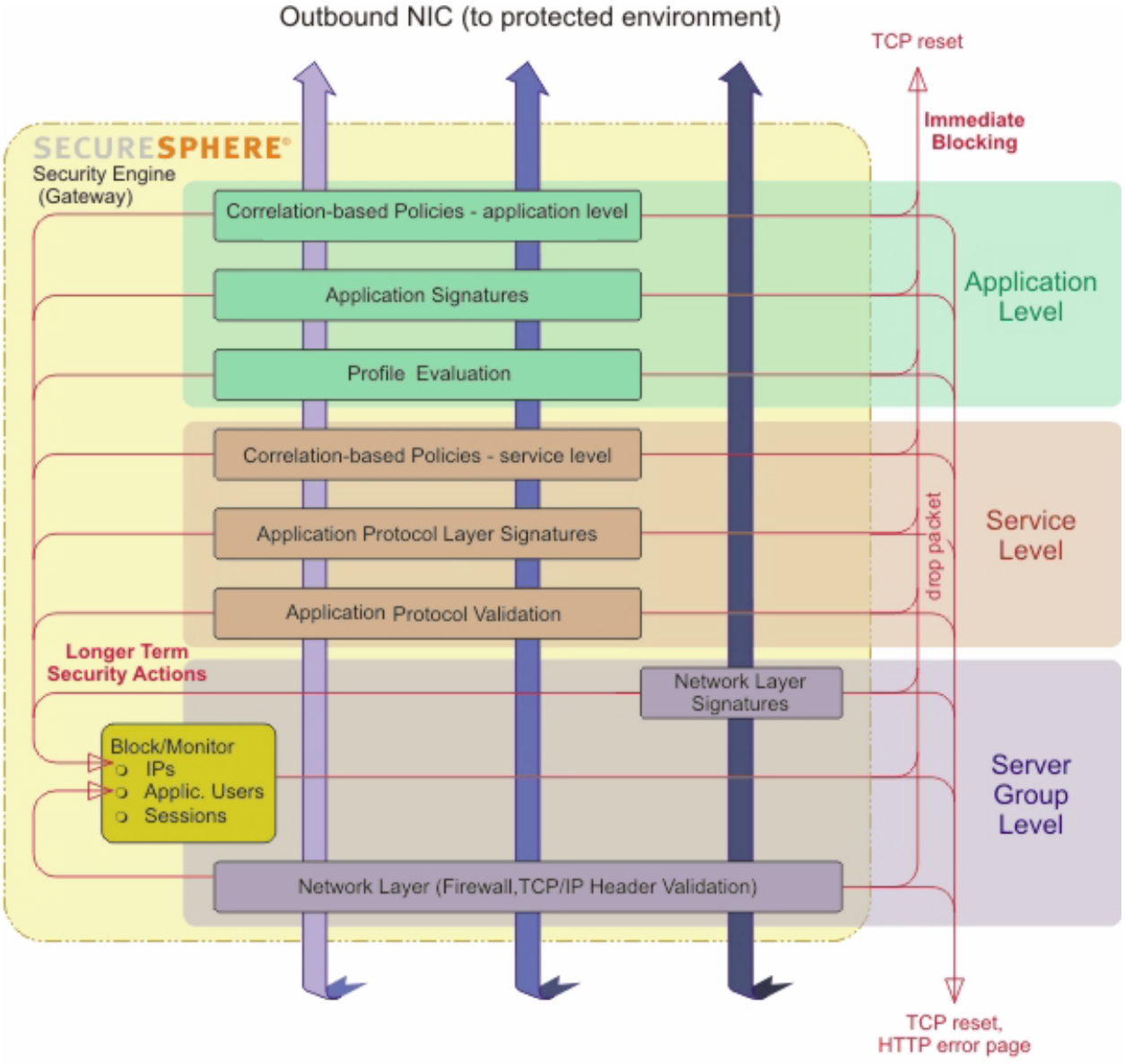
- TCP Reset (sniffing topology): SecureSphere can signal protected servers to disconnect malicious users using TCP reset, a special TCP packet that signals TCP peers to close the TCP session. SecureSphere spoofs a TCP reset packet and sends it to the protected server. It is assumed that a standards-conformant 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 9.0 blocks a Web connection it can be configured to display an error page to the blocked user.

Figure 1-9 – Intrusion Analysis and Reaction



1.5.3.8.2. 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).

1.5.3.8.3. File Firewall

The File Firewall (FF) controls access to files based on user categorization and file classification. Classification can be performed via the SecureSphere GUI or by manually importing Comma Separated Value (CSV)-format classification files generated by third-party Data Leak Prevention (DLP) products.

1.5.3.8.4. 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.

Blocked IPs can also be introduced via Imperva's ThreatRadar service, which provides categorized lists of potentially malicious IP addresses.

1.5.3.8.5. Traffic Monitoring and Recording

SecureSphere 9.0 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.

1.5.3.8.6. 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 Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet

Protocol (IP). Protocol-related violations such as bad checksum, bad IP addresses and bad options can be detected and blocked.

1.5.3.8.7. Protocol Violations

SecureSphere protocol compliance checks ensure that protocols meet Request for Comment (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.

1.5.3.8.8. Universal User Tracking (UUT)

SecureSphere 9.0 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), Secure-Sphere correlates the Web and database requests, providing a Web to Database User Tracking capability.

1.5.3.8.9. 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 Unified Resource Locators (URLs), HTTP methods, parameters, cookies, Simple Object Access Protocol (SOAP) actions, eXtensible Markup Language (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.

1.5.3.8.10. 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 Secure-Sphere'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.

1.5.3.9. 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 9.0:

- **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 Simple Network Management Protocol (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 and file 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 encrypts and/or signs the archived records to prevent unauthorized disclosure or modification of the records outside the TOE's scope of control.
- **Operating System Command**[5]: 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.

[5] 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.

- **Tasks**: review or actionable tasks may be created as a follow up action for the event, assigned to a specified SecureSphere GUI administrator.

1.5.3.10. Management

The TOE is managed from the MX Management Server. Administrators use a standard Web browser (outside of the TOE) to connect to a Web-based SecureSphere GUI interface that is used for all management activities once the TOE is operational. Configuration settings are downloaded from the Management Server to SecureSphere 9.0 gateways, and event information is uploaded from the gateways to the MX Management Server.

The TOE can optionally include a SOM Management Server. Administrators use the SecureSphere GUI to define policies that are applied to one or more MX servers that are registered with the SOM. The SOM queries the MX server for IDS System data for review by the SOM administrator. System Events can be configured to be automatically forwarded to the SOM for audit record review by the SOM administrator.

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

1.5.3.11. ADC Content Updates

SecureSphere 9.0 attack signatures are text strings that match known server vulnerabilities and attack patterns. SecureSphere 9.0 maintains a set of signatures based on the Snort database and Imperva's Application Defense Center (ADC). The ADC (part of the TOE environment) 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 database) 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.

Each ADC content update is digitally signed by the ADC, and its authenticity and integrity verified by the Management Server before it is applied. TOE administrators can use the ADC classifications and corresponding documentation to selectively enable signature matching for applicable signatures.

1.5.4. Functionality Excluded from the TOE Evaluated Configuration

All SecureSphere 9.0 functionality is included in the TOE Evaluated Configuration, with the following exceptions:

- Imperva SecureSphere 9.0 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 also be configured to be performed using an external user directory that supports the LDAP protocol, an external RADIUS server, or an external SQL database. These options are not included in the Evaluated configuration. In the evaluated configuration, administrators are always authenticated locally by the Management Server.

1.5.5. Non Security-Relevant Functionality Included in the TOE

This section discusses product functionality included in the evaluated configuration that is not being claimed in this ST as security functionality.

1.5.5.1. Compliance with Standards and Regulations

SecureSphere 9.0 helps organizations address many compliance regulations such as PCI, SOX, and HIPAA by satisfying technical requirements stated in those regulations. This is not being evaluated in the context of this ST. In addition to CC evaluation, Imperva relies on different third-party evaluation schemes such as NSS, ICSA, and others to attest to the effectiveness of its products.

1.5.5.2. Interoperability with Third-Party Products

SecureSphere 9.0 provides protections for a large number of third-party applications, such as SAP, Oracle, PeopleSoft, and others. Interoperability with proprietary third-party applications is not being evaluated in the context of this ST.

1.5.5.3. Non Security-Relevant Cryptographic Mechanisms

This ST makes a claim of compliance with the [IDSSPP]. The [IDSSPP] levies no cryptographic security requirements on the TOE; IDS is not considered a cryptographic function. Nevertheless, the SecureSphere 9.0 product does provide cryptographic mechanisms, implemented using different cryptographic libraries.

The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. The CC allows the definition of cryptographic security requirements by reference to a cryptographic standard (see also section 6.3.4).

The approach taken in this ST is to define cryptographic mechanisms as security functionality where they are directly supportive of a [IDSSPP] security requirement and where their correctness of implementation can be attested to by third-party assurances,

i.e. through reference to a NIST FIPS 140-2 certificate for the underlying cryptographic library.

The following cryptographic mechanisms included in the SecureSphere 9.0 product are not considered to be security-relevant in the context of this ST:

- **Network traffic decryption** – some of the network protocols collected and analyzed by the Gateway include encryption of protocol data. SecureSphere 9.0 Gateways can be configured to decrypt this data in order to be able to record and analyze the mediated network traffic. Such decryption can be achieved in the Gateway kernel (using cryptographic library functions), or using a HSM that is either installed as an add-on card in the Gateway appliance (see section 1.5.2.1) or is a network-connected HSM device.

  Traffic decryption is considered to be an objective for the IT environment (OE.INTROP), and is therefore not claimed as a security function in this ST. Imperva recommends the use of FIPS 140 validated HSMs for this purpose.

- **Communication between the MX Management Server and Gateway** – management communications between the MX and Gateway are encrypted. This encryption is not claimed as a security function. The protection of the communication is achieved through the physical separation of management communications from mediated traffic, as explained in section 1.5.2.3.

- **Encryption of audit data stored on Gateways** – the Gateway can be configured to encrypt stored IDS System data. Note that since the decryption key is stored on the gateway, this provides only partial protection. The data is protected because the Gateway prevents unauthorized access to the data, regardless of whether it is stored in encrypted or plaintext form.

- **Web cookie signing** – Web applications sometimes embed 'cookie' objects in responses sent to Web clients in order to maintain session state; the client is expected to return the cookie in subsequent communications. SecureSphere 9.0 can be configured to apply a cryptographic mechanism that detects cookie tampering or cookie injection attacks. This protection is not claimed as a security requirement.

- **Parsing and verification of Kerberos authenticators** – Kerberos is a cryptographic authentication protocol used in many environments, e.g. in a Microsoft Windows domain. SecureSphere 9.0 can be configured with appropriate keys that allow it to parse Kerberos protocol elements in order to extract user identification from mediated network traffic. In addition, administrator authentication to the SecureSphere 9.0 management servers can be configured to use Kerberos authenticators. Kerberos is not used by the TOE to cryptographically protect user data. Note that Kerberos uses non FIPS-Approved cryptographic algorithms.

2. Conformance Claims

2.1. CC Conformance

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, CCMB-2009-07-002, extended (CC Part 2 extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, conformant (CC Part 3 Conformant)

2.2. Assurance Package Conformance

The TOE is package-name augmented with the following assurance package:

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

2.3. PP Conformance

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

- U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007

2.4. Conformance Rationale

2.4.1. Introduction

This section is intended to demonstrate that the statements of the security problem definition, security objectives, and security requirements in this ST are consistent with the PP for which conformance is being claimed: [IDSSPP].

The claimed protection profile is a CCv3.1 PP that requires demonstrable PP conformance.

2.4.2. Consistency of the Security Problem Definition

The security problem definition in this ST is equivalent to the security problem definition of the claimed PP. This is established by reproducing all of the assumptions, threats, and OSPs defined in the claimed PP in this ST.

2.4.3. Security Objectives Conformance

The statement of security objectives in this ST is equivalent to the security objectives defined in [IDSSPP]. This is established by reproducing all of the security objectives for

the TOE and for the environment defined in the claimed PP in this ST, with the following exceptions:

- O.EXPORT - Omitted as per the guidance given by [PD-0097].
- OE.AUDIT_PROTECTION and OE.AUDIT_SORT were restarted in this ST as TOE security objects,

2.4.4. Security Functional Requirements Conformance

This section demonstrates that the SFRs in the ST are equivalent or more restrictive than the SFRs in the PP. This means that all TOEs that would meet the SFRs in the ST would also meet the SFRs in the PP.

The TOE demonstrably meets and exceeds all security requirements of the claimed [IDSSPP], except for the FIA_AFL.1, FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 requirements that are inapplicable to the TOE.

All security requirements from the claimed PP have been restated in this ST, except for the SFRs listed above as exceptions. For some requirements, a hierarchical component was selected in place of one or more of the PPs' requirements; 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 PPs. Permitted operations performed on PP security functional requirements are identified in Table 6-1.

This ST claims additional SFRs that are not drawn from the claimed PP. Table 6-1 identifies these requirements. Section 6.3.1 provides rationale for the consistency of these SFRs with the claimed PP. The auditable events defined for the claimed basic level of audit have been added to Table 6-2 - Auditable Events.

The following subsections provide conformance rationale for individual SFRs that were omitted as exceptions or refined in respect to the claimed PP, clarifying the relationship of an SFR to the claimed PP.

2.4.4.1. FAU_STG.2

The [IDSSPP] FAU_STG.2 was refined to conform with CCv3.1 syntax. This is also consistent with [I-0422].

In FAU_STG.2.2, the selection is given as 'prevent' from the Firewall PPs as it is stronger than 'detect' given in [IDSSPP].

2.4.4.2. FIA_AFL.1

The [IDSSPP] FIA_AFL.1 Authentication failure handling requirement relates to external IT products that might authenticate to the TOE.

This SFR has been omitted as per the guidance given in [PD-0097], which states that this requirement was incorrectly included in the system PP.

2.4.4.3. FIA_UID.1 and FIA_UAU.1

This ST claims FIA_UID.2 and FIA_UAU.2, which are hierarchical to the corresponding [IDSSPP] FIA_UID.1 and FIA_UAU.1 SFRs.

2.4.4.4. FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1

These SFRs have been omitted as per the guidance given in [PD-0097], which states that these requirements were incorrectly included in the system PP.

2.4.4.5. Applicable NIAP Precedent Decisions

The following precedent decisions have been used as guidance for interpreting demonstrable conformance with the claimed PP, in relation to claimed SFRs:

Table 2-1- 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
[PD-0151]	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FMT_SMF.1, FPT_ITT.1, FPT_STM.1, FTP_TRP.1	Additional features not required by the claimed PP may be added as long as the ST does not violate the "demonstrable conformance" definition.

2.4.5. Security Assurance Requirements Conformance

The assurance requirements in this ST are identical to the assurance requirements stated in the [IDSSPP].

3. Security Problem Definition

3.1. 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):

3.1.1. 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.

3.1.2. 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.

3.2. 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):

3.2.1. 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[6].

3.2.2. 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.

3.2.3. 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.

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

3.3. Organizational Security Policies

The following OSPs are defined in [IDSSPP]. [IDSSPP] does not identify which organization and which organizational security policy any of these OSPs are drawn from.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

4.1. Security Objectives for the TOE

This section describes the TOE security objectives (identical[7] 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.

O.AUDIT_PROTECTION

The TOE must provide the capability to protect audit information.

O.AUDIT_SORT

The TOE must provide the capability to sort the audit information

[7] [IDSSPP] security objectives omitted from this ST: O.EXPORT was omitted per the guidance given in [PD-0097]. O.AUDIT_PROTECTION and O.AUDIT_SORT were restated as TOE security objectives in this ST.

4.2. Security Objectives for the Operational Environment

4.2.1. 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.

4.2.2. Security Objectives for the Environment Upholding Assumptions

The assumptions made in this ST about the TOE's operational environment must be upheld by corresponding security objectives for the environment.

The following security objectives are intended to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they are intended to be satisfied largely through application of procedural or administrative measures.

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

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

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

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

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

4.3. Security Objectives Rationale

4.3.1. IT Security Objectives Rationale

The security problem description and security objectives in this ST are equivalent to the corresponding elements stated in the [IDSSPP], as established in sections 2.4.2 and 2.4.3 above. See section 6.1 of [IDSSPP] for the IT security objectives rationale.

The [IDSSPP] traces OE.AUDIT_PROTECTION and OE.AUDIT_SORT to P.ACCESS and P.ACCACT, respectively. In this ST, these objectives are restated as security objectives for the TOE. O.AUDIT_PROTECTION supports P.ACCESS by providing protection for audit data. O.AUDIT_SORT supports P.ACCACT by allowing the administrator to sort audit data providing for user accountability.

4.3.2. Non-IT Security Objectives Rationale

See section 6.2 of [IDSSPP].

5. Extended Components Definition

This security target contains the following extended security requirements defined in [IDSSPP]: IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, IDS_STG.2.

Extended security functional requirements are not drawn from [CC] Part 2 components. The [IDSSPP] provides the following explanation for why these requirements cannot be clearly expressed using existing components, and in particular why the FAU class could not be refined to achieve the same result. Note that FAU deals with events that are internal to the TOE, whereas IDS deals with events occurring in the IT environment.

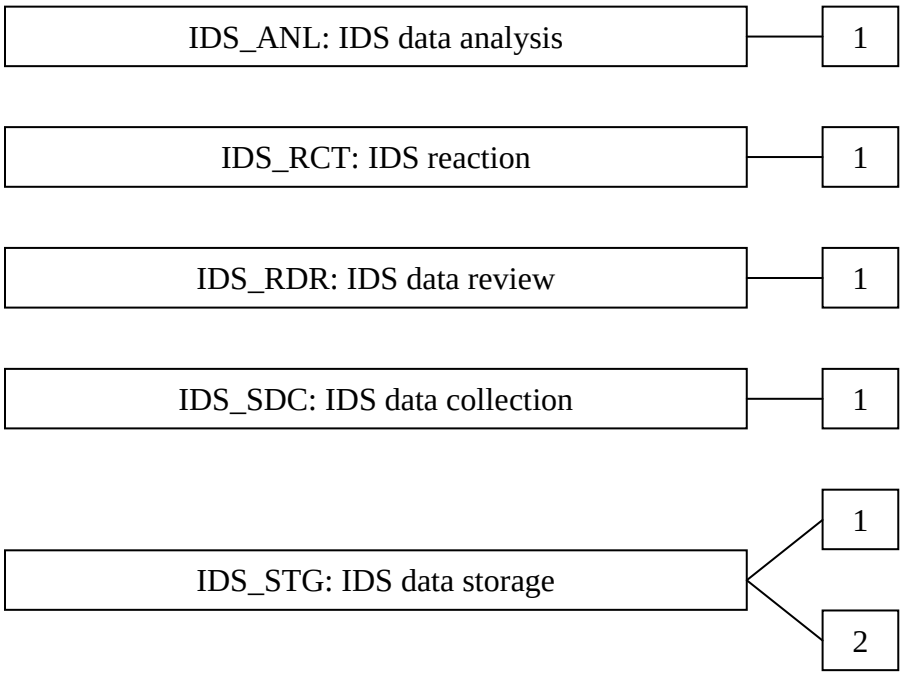
> "*A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data.*"

The Extended Components Definition presented here defines an extended component for each extended security requirement, using the existing CC components, families, classes, and methodology as a model for presentation.

5.1. Class IDS: Intrusion Detection

This class is used to satisfy security objectives that pertain to intrusion detection and prevention (IDS/IPS) systems. These include data collection and analysis, automatic reaction capabilities, review, and protection of IDS System data.

Figure 5-1 - IDS: Intrusion detection class decomposition



5.1.1. IDS data analysis (IDS_ANL)

Family Behaviour

This family defines requirements for automated means that analyse IDS System data looking for possible or real security violations.

The actions to be taken based on the detection can be specified using the IDS reaction (IDS_RCT) family as desired.

Component levelling

IDS_ANL: IDS data analysis	1

In IDS_ANL.1 Analyser analysis, statistical, signature, or integrity based analysis is required.

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the parameters of the analytical functions.

Audit: IDS_ANL.1

The following actions should be auditable if IDS_ANL IDS data analysis is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

5.1.1.1. IDS_ANL.1 Analyser analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

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

a) [selection: *statistical*, *signature*, *integrity*]; and

b) [assignment: *any other analytical functions*].

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

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: *any other security relevant information about the result*].

5.1.2. IDS reaction (IDS_RCT)

Family Behaviour

This family defines the response to be taken in case when an intrusion is detected.

Component levelling

IDS_RCT: IDS reaction	1

At IDS_RCT.1 IDS reaction, the TSF shall send an alarm and take action when an intrusion is detected.

Management: IDS_RCT.1

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit: IDS_RCT.1

The following actions should be auditable if IDS_RCT IDS reaction is included in the PP/ST:

a) Minimal: Actions taken due to detected intrusions.

5.1.2.1. IDS_RCT.1 Analyser react

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser analysis

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

5.1.3. IDS data review (IDS_RDR)

Family Behaviour

This family defines the requirements for tools that should be available to authorised users to assist in the review of IDS System data.

Component levelling

IDS_RDR: IDS data review	1

IDS_RDR.1 IDS data review, provides the capability to read information from the System data and requires that there are no other users except those that have been identified as authorised users that can read the information.

Management: IDS_RDR.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data.

Audit: IDS_RDR.1

The following actions should be auditable if IDS_RDR IDS data review is included in the PP/ST:

a) Basic: Reading of information from the System data.

b) Basic: Unsuccessful attempts to read information from the System data.

5.1.3.1. IDS_RDR.1 Restricted data review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

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

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

5.1.4. IDS data collection (IDS_SDC)

Family Behaviour

This family defines requirements for recording information from the targeted IT System resource(s).

Component levelling

IDS_SDC: IDS data collection	1

IDS_SDC.1 IDS data collection, defines the information to be collected from the targeted IT System resource(s), and specifies the data that shall be recorded in each record.

Management: IDS_SDC.1

There are no management activities foreseen.

Audit: IDS_SDC.1

There are no auditable events foreseen.

5.1.4.1. IDS_SDC.1 System data collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration*

changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities]; and

b) [assignment: *other specifically defined events*].

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

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

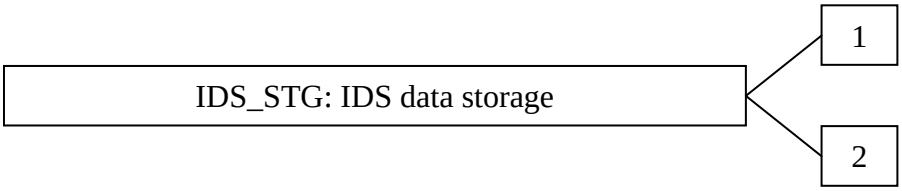
b) [assignment: *other additional information*].

5.1.5. IDS data storage (IDS_STG)

Family Behaviour

This family defines requirements for protecting IDS System data after it is recorded and stored by the TOE.

Component levelling



At IDS_STG.1 Guarantees of System data availability, specifies the guarantees that the TSF maintains over the system data given the occurrence of an undesired condition.

IDS_STG.2 Prevention of System data loss, specifies actions in case of exceeded storage capacity.

Management: IDS_STG.1

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

a) maintenance (deletion, modification, addition) of the actions to be taken in case of storage failure.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

5.1.5.1. IDS_STG.1 Guarantees of System data availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

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

IDS_STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].

5.1.5.2. IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_STG.1 Guarantees of system data availability

IDS_STG.2.1 The System shall [selection: '*ignore System data*', '*prevent System data, except those taken by the authorised user with special rights*', '*overwrite the oldest stored System data* '] and [assignment: *other actions to be taken in case of storage failure*] if the storage capacity has been reached.

6. IT Security Requirements

6.1. Security Functional Requirements

The functional security requirements (SFRs) for this ST are taken from [IDSSPP][8]. These SFRs are identified in the 'PP' column of Table 6-1 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).

Subjects, objects, and operations are as defined in the [IDSSPP].

The CC defined operations of assignment, selection, and refinement were applied in relation to the requirements specified in [IDSSPP] as described in column 4 of Table 6-1 below. 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.

Table 6-1 –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_CKM.4	Cryptographic key destruction		Assignment
FCS_COP.1	Cryptographic operation		Refinement, assignment
FIA_ATD.1	User attribute definition	✓	Assignment, refinement
FIA_UAU.2	User authentication before any action	✓	Hierarchical

[8] 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_UID.2	User identification before any action	✓	Hierarchical
FMT_MOF.1	Management of security functions behaviour	✓	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_STM.1	Reliable time stamps	✓	None
FTP_TRP.1	Trusted path		Selection, assignment
IDS_SDC.1	System Data Collection	✓	Refinement, selection, assignment
IDS_ANL.1	Analyser analysis	✓	Selection, assignment
IDS_RCT.1	Analyser react	✓	Assignment
IDS_RDR.1	Restricted Data Review	✓	Assignment
IDS_STG.1	Guarantee of System Data Availability	✓	Assignment, selection
IDS_STG.2	Prevention of System data loss	✓	Selection

6.1.1. Security Audit (FAU)

6.1.1.1. 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 level of audit; and

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

Table 6-2 - Auditable Events

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	
FCS_CKM.1, FCS_CKM.2, FCS_CKM.4	Success and failure of the activity	The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
FCS_COP.1	Success and failure, and the type of cryptographic operation	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FIA_UAU.2	Any use of the authentication mechanism.	User identity, location
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	
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

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 6-2 - Auditable Events.

6.1.1.2. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **all users** 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.

6.1.1.3. 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.

6.1.1.4. 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.

6.1.1.5. 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[9].

6.1.1.6. 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**[10] **unauthorised** modifications to the **stored** audit records **in the audit trail**[11].

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.

---

[9] 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.

[10] 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.

[11] The FAU_STG.2.2 element has been updated to conform with the CCv3.1 syntax. This is consistent with NIAP interpretation [I-0422].

6.1.1.7. 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.

6.1.2. Cryptographic support (FCS)

6.1.2.1. 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 **FIPS 186-2 (SHA-1)** and specified cryptographic key sizes **1024 bits for RSA keys, 128 bits for AES keys** that meet the following: **FIPS 140-2 level 1**.

6.1.2.2. 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]**.

6.1.2.3. Cryptographic key destruction (FCS_CKM.4)

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

6.1.2.4. Cryptographic operation (FCS_COP.1)[12]

FCS_COP.1.1 The TSF shall perform **the cryptographic operations listed in Table 6-3** 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 6-3:**

Table 6-3 - 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 +**	**1024 bits**	**DER-encoded PKCS #1 using**

[12] FCS_COP.1 assignments 'cryptographic algorithm' and 'cryptographic key sizes' are both completed as '**listed in Table 6-3**'; the component has been refined to omit these assignments for clarity.

Operation	Alg.	Key Size	Standard
	SHA-1		**SHA-1**
ADC content updates verification	**RSA + SHA-1**	**1024 bits**	**DER-encoded PKCS #1 using SHA-1**

6.1.3. Identification and authentication (FIA)

6.1.3.1. 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[13].

6.1.3.2. 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.

6.1.3.3. 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.

6.1.4. Security Management (FMT)

6.1.4.1. 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.

6.1.4.2. 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 **users with the authorisations as specified in Table 6-4 below.**

[13] 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.

6.1.4.3. 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 6-4.**

Table 6-4- 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**
FMT_MTD.1	**Query audit data**	**All users**
	Query and add System data	**Authorised administrator with View permission on applicable objects**
	Query (export) and modify (create, delete, import) audit archive protection keys	**Authorised administrator with Settings permission**
	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 SecureSphere role**	**Authorised System administrator**

6.1.4.4. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following roles[14]**:** authorised administrator, authorised System administrators, and **authorised administrators with one or more of the following authorisations identified in Table 6-4: Settings permission, View permission on applicable objects**.

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

[14] SecureSphere 9.0 provides a role based authorisations model that supports assignments of users to one or more roles, and granting of access permissions to objects or special permissions for roles and for specific users. The authorized System administrator role defined in FMT_SMR.1 corresponds to the predefined SecureSphere 9.0 Administrator role, which is granted all permissions, and is the only role that is allowed to access the SecureSphere GUI Admin workspace in order to manage users, roles, and authorisations. The authorized administrator role defined in FMT_SMR.1 corresponds to other roles that are defined without Edit permissions to applicable objects in relation to FMT_MOF.1; if a role is assigned Edit permissions, then it is considered an authorized System administrator role in that context. In addition, all users defined in the SOM are considered authorized System administrators, and have authorisations to all management functions identified in Table 6-4.

6.1.5. Protection of the TSF (FPT)

6.1.5.1. 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.

6.1.5.2. Reliable time stamps (FPT_STM.1)

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

6.1.6. Trusted path/channels (FTP)

6.1.6.1. 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.

6.1.7. IDS Component Requirements (IDS)

6.1.7.1. System Data Collection (IDS_SDC.1)

IDS_SDC.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, access control configuration, detected known vulnerabilities[15].

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

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

b) The additional information specified in the Details column of Table 6-5 – System Events.

Table 6-5 - System Events

Component	Event	Details
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address

[15] IDS_SDC.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 6-5 has been tailored to omit all PP event descriptions not selected for IDS_SDC.1.1 a).

Component	Event	Details
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	Access control configuration	Location, access settings
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

6.1.7.2. Analyser analysis (IDS_ANL.1)

IDS_ANL.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 6-6**.

Table 6-6 - IDS Analysis Functions

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

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

a) Date and time of the result, type of result, identification of data source and

b) **Destination Server Group**.

6.1.7.3. Analyser react (IDS_RCT.1)

IDS_RCT.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.

6.1.7.4. Restricted Data Review (IDS_RDR.1)

IDS_RDR.1.1 The System shall provide **users** with the capability to read **Alerts, audit records, discovery and assessment results, collected application profiles, System configuration and Gateway Status as constrained by the users' authorisations** from the System data.

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

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

6.1.7.5. Guarantee of System Data Availability (IDS_STG.1)

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

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

IDS_STG.1.3 The System shall ensure that **250,000 Alert records and up to 80 Gb of audit files per gateway of** System data will be maintained when the following conditions occur: System data storage exhaustion.

6.1.7.6. Prevention of System data loss (IDS_STG.2)

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

6.2. 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.2.

No operations are applied to the assurance components.

Table 6-7- TOE Security Assurance Requirements

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing

Assurance Class	Assurance Components	
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.3. Security Requirements Rationale

6.3.1. Security Functional Requirements Rationale

See section 6.3 of [IDSSPP] for the rationale for all PP-derived SFRs. The following is rationale for the SFRs added to this ST in addition to [IDSSPP] SFRs:

- FMT_SMF.1 was introduced to satisfy CCv 3.1 dependencies for FMT_MOF.1 and FMT_MTD.1, as identified in Table 6-9. It can therefore be seen to support the security objectives O.PROTCT, O.ACCESS and O.IDAUTH in which these three requirements are grounded. FMT_SMF.1 also directly supports O.EADMIN, in that it includes a set of functions that allow effective management of TOE functions and data.
- 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.1, it can be seen to map to O.ACCESS as well. In addition, FPT_ITT.1 can be seen to uphold O.PROTCT, because it prevents unauthorized modifications and access for TSF data transmitted between the separate parts of the TOE.
- FTP_TRP.1 can be seen to uphold O.PROTCT, by providing a trusted path for remote users initiating communication for administrator sessions, protecting SecureSphere GUI data and functions from unauthorized access over the network.
- The cryptographic SFRs: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1 were added to the ST in support of FTP_TRP.1, implemented in the TOE using cryptographic mechanisms. They are therefore also mapped to O.PROTCT. FCS_COP.1 further supports O.PROTCT, because it provides cryptographic verification for ADC content updates loaded into the TOE. FCS_CKM.1 and FCS_COP.1 also support FPT_ITT.1 and IDS_RDR.1 in relation to cryptographic protection of archived audit data, thereby further supporting O.ACCESS and O.INTEGR.

Table 6-8 summarizes the rationale. It maps security functional requirements to security objectives described in section 4.1. The table clearly demonstrates that each objective is met by at least one SFR and that each SFR meets at least one objective.

Table 6-8 - Tracing of SFRs to security objectives for the TOE

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.AUDIT_PROTECTION	O.AUDIT_SORT
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_CKM.4	✓												
FCS_COP.1	✓						✓				✓		
FIA_ATD.1								✓					
FIA_UAU.2							✓	✓					
FIA_UID.2							✓	✓					
FMT_MOF.1	✓						✓	✓					
FMT_MTD.1	✓						✓	✓			✓		
FMT_SMF.1	✓						✓	✓					
FMT_SMR.1								✓					
FPT_ITT.1	✓						✓				✓		
FPT_STM.1										✓			
FTP_TRP.1	✓												
IDS_SDC.1		✓	✓										
IDS_ANL.1				✓									
IDS_RCT.1					✓								

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.AUDIT_PROTECTION	O.AUDIT_SORT
IDS_RDR.1						✓	✓	✓					
IDS_STG.1	✓						✓	✓	✓		✓		
IDS_STG.2									✓				

6.3.2. 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.2.

Section 6.4 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.2 (Flaw reporting procedures) 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, and providing guidance to TOE users for how to submit security flaw reports to the developer. This is consistent with the [IDSSPP] which also includes this requirement.

6.3.3. Dependency Rationale

Table 6-9 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 6-9- Security Requirements Dependency Mapping

SFR	CC dependency	ST dependency	Justification (where needed)
FAU_GEN.1	FPT_STM.1	FPT_STM.1	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	

SFR	CC dependency	ST dependency	Justification (where needed)
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FMT_GEN.1, FMT_MTD.1	
FAU_STG.2	FAU_GEN.1	FAU_GEN.1	
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	FCS_COP.1, FCS_CKM.4	Note: the TOE destroys all ephemeral cryptographic keys in accordance with FCS_CKM.4. In addition, the TOE stores persistent RSA keys for trusted path and audit archiving. The dependency on FCS_CKM.4 for persistent keys is intended to be met by the IT environment. TOE evaluated configuration guidance provides the administrator with instructions for secure wiping of TOE appliances' disks using third-party tools in the IT environment. It is assumed (A.NOEVIL and OE.INSTAL) that authorized administrators will follow and abide by these instructions.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	See justification above for FCS_CKM.1 and FCS_CKM.2.
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	
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_SMF.1	None		

SFR	CC dependency	ST dependency	Justification (where needed)
FMT_SMR.1	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_ITT.1	None		
FPT_STM.1	None		
FTP_TRP.1	None		
IDS_SDC.1	None		
IDS_ANL.1	None		
IDS_RCT.1	None		
IDS_RDR.1	None		
IDS_STG.1	None		
IDS_STG.2	None		
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	**ADV_FSP.2**, ADV_TDS.1	Consistent with EAL2
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1	
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2	
AGD_OPE.1	ADV_FSP.1	**ADV_FSP.2**	Consistent with EAL2
AGD_PRE.1	None		
ALC_CMC.2	ALC_CMS.1	**ALC_CMS.2**	Consistent with EAL2
ALC_CMS.2	None		
ALC_DEL.1	None		
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, **ASE_REQ.2**	Consistent with EAL2
ASE_ECD.1	None		
ASE_INT.1	None		
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	
ASE_SPD.1	None		
ASE_TSS.1	ASE_INT.1, ASE_REQ.1,	ASE_INT.1, **ASE_REQ.2,**	Consistent with EAL2

SFR	CC dependency	ST dependency	Justification (where needed)
	ADV_FSP.1	**ADV_FSP.2**	
ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1	
ATE_FUN.1	ATE_COV.1	ATE_COV.1	
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	

6.3.4. 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 6.1.2 therefore reference external standards that the implementation must meet when providing the required capabilities.

Table 6-10 summarizes the standards compliance claims made in Section 6.1.2 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 6-10- Cryptographic Standards and Method of Determining Compliance

Standard claimed	SFRs	Method of determining compliance
FIPS 140-2 Level 1	FCS_CKM.1, FCS_CKM.4, FCS_COP.1	FIPS 140-2 Cert. #1048
Key generation per NIST PUB FIPS 186-2	FCS_CKM.1	RNG Cert. #389
AES 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. TOE Summary Specification

7.1. SFR Mapping

Table 7-1 provides a description of the general technical mechanisms that the TOE uses to satisfy each SFR defined in section 6. The table includes the description of security functionality given in each SFR by reference, and provides a high-level view of their implementation in the TOE, referencing section 1.5.2 and 1.5.3 for descriptions of the physical and logical components of the TOE, respectively.

Note: Refer to Table 8-2 for the list of supported IT environment components.

Table 7-1 - TOE Summary Specification SFR Mapping

Component	Description of mechanism
7.1.1. Security Audit (FAU)	
FAU_GEN.1	The MX Management Server described in section 1.5.2 hosts an internal database that is used for storing audit records (System Events), IDS System data (Alerts), application Profiles, user attributes and configuration information. 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 on the MX Management Server: • 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). SecureSphere 9.0 generates the required audit records as shown in Table 7-2 below, derived from Table 6-2, and provides more details on how the TOE meets each auditable event requirement in FAU_GEN.1. As explained above, each system log record includes the following information: date and time of the event, type of event, subject identity, Severity, and object IDs (primary URI) where applicable. Location is identified by the administrator's IP address. The outcome (success or failure) of the related event is implied from the event Type. The SOM administrator can pre-select System Event types that will be automatically forwarded from the MX server to the SOM for storage and audit review by the SOM administrator. System Events are also generated by the SOM (e.g. for SOM administrator logins and SOM user account management) and are stored locally on the SOM server.

Component	Description of mechanism

Table 7-2- TSS Mapping for FAU_GEN.1

Component	Auditable Event	Mapping
FAU_GEN.1	Start-up and shutdown of audit functions	Audit functions start up when the Management Server starts up, and cannot be shut down. The requirement for logging of start-up and shutdown events is therefore not applicable to the TOE.
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 audit records	All SecureSphere GUI users can read audit records (System Events). All SecureSphere GUI logins are logged.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Unsuccessful SecureSphere GUI logins are logged.
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.
FCS_CKM.1, FCS_CKM.2, FCS_CKM.4	Success and failure of the activity	Successful and unsuccessful SecureSphere GUI logins are logged, including user identity where applicable.
FCS_COP.1	Success and failure, and the type of cryptographic operation	Successful and unsuccessful SecureSphere GUI logins are logged, including user identity where applicable. Audit archiving events are logged. Successful and unsuccessful ADC content updates are logged. In all cases, the cryptographic mode of operation is constant and is therefore not explicitly logged.
FIA_UAU.2	Any use of the authentication mechanism.	Successful and unsuccessful SecureSphere GUI logins are logged.
FIA_UID.2	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_SMF.1	Use of the management functions.	All configuration changes and user administration operations are logged.

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>
<table>
<tr><td>FMT_SMR.1</td><td>Modifications to the group of users that are part of a role.</td><td>All user administration operations are logged.</td></tr>
<tr><td>FTP_TRP.1</td><td>All attempted uses of the trusted path functions.</td><td>Successful and unsuccessful SecureSphere GUI logins are logged.</td></tr>
</table>
</td></tr>
<tr><td>FAU_SAR.1, FAU_SAR.2</td><td>The SecureSphere GUI described in section 1.5.3.10 allows users to read audit information from the audit records using a Web-based interface. Users without access authorisations to SecureSphere GUI cannot view audit records.</td></tr>
<tr><td>FAU_SAR.3</td><td>SecureSphere GUI 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.</td></tr>
<tr><td>FAU_SEL.1</td><td>The System Events Log supports audit pre-selection during the installation and preparation of the TOE, via editing of configuration files.</td></tr>
<tr><td>FAU_STG.2 , FAU_STG.4</td><td>System Events log records are stored in a MX Management Server database table, and may also be forwarded for storage on a corresponding SOM database. The TOE does not provide any interface for modifying audit records. Audit records can only be archived and purged by an authorized System administrator via the SecureSphere GUI management interface.

By default, the Management Server retains up to 100,000 System Event records, and purges the oldest records when this configurable threshold is exceeded. An authorized System administrator with appropriate permissions can modify this threshold, or specify a time period for which System Event records must be retained. System Event records can also be archived to external storage before being purged on a defined schedule. An alarm can be configured to be sent to an Action Interface if the audit trail is full.

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.</td></tr>
<tr><td colspan="2">7.1.2. Cryptographic support (FCS)</td></tr>
<tr><td>FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1</td><td>All claimed cryptographic operations are implemented using the FIPS 140-2 validated RSA BSAFE Crypto-J 4.0 cryptographic library. Ephemeral keys are zeroized by the cryptographic module.

SecureSphere GUI is a browser-based interface to the Management Server that allows authorised administrators to access TOE management functions. It is implemented by a Web server component on the Management Server. TOE evaluated configuration guidance instructs the administrator to configure the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite for the SecureSphere GUI interface.

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,</td></tr>
</table>

Component	Description of mechanism
	and stored together with the data. • Keys are generated as described for FCS_CKM.1 by the SecureSphere application on the Management Server. • The database audit archive keys are stored on the Management Server, and can be managed by an authorised administrator. ADC content updates loaded either manually or automatically into the TOE are verified by the SecureSphere application on the Management Server before the update is applied: the updates are signed by the ADC using 1024 bit RSA over a SHA-1 hash prior to application to prevent tampering.
7.1.3. User identification and authentication (FIA)	
FIA_ATD.1	The SecureSphere application on the Management Server maintains the following required security attributes in the Management Server database (described above for FAU_GEN.1) for each authorised administrator user, as follows: • User identity - User name • Authentication data – Authentication method (SecureSphere or External), Password (if method is SecureSphere) • Authorisations – Role assignments, user-specific permissions.
FIA_UAU.2, FIA_UID.2	The Web Server component on the Management Server requires identification and authentication for all SecureSphere GUI requests. If the browser offers Kerberos-based authentication, the received Kerberos ticket and authenticator are verified against the configured list of trusted Service Principals. Otherwise, the Web Server requires HTTP Basic Authentication from the user, and sends the user's password to the SecureSphere application on the Management server for validation against the authentication data stored in the database.
7.1.4. Security Management (FMT)	
FMT_MOF.1, FMT_MTD.1, FMT_SMR.1	As explained above for FIA_ATD.1, each authorised administrator may be associated with role(s) and user-specific permissions in the SecureSphere GUI database. Roles are associated with permissions. Users associated with the role 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. They are associated with the user's session, and affect which objects are displayed and which operations may be performed. The predefined Administrator role is granted all permissions, and is the only role that is allowed to access the SecureSphere GUI Admin workspace in order to manage MX server users, roles, and authorisations. Permissions are defined on managed objects (Applications, Policies, Gateways, Sites, Servers, and Global Objects), as View, Edit, or Create. Edit permission implies View permission. Create permission implies Edit permission. An authorised administrator is defined in this ST (see FMT_SMR.1) to be an authorised System administrator for a subset of System data if assigned Edit permissions to the corresponding System objects. In particular, the predefined Web/DB/File/SharePoint Security Admin roles provide authorized System administrator permissions to the corresponding functional subsets of System data. Special permissions allow users to activate settings and navigate to certain pages, e.g. the Alerts permissions allow access to the Alerts viewer or for viewing Alerts reports. In this example, users assigned with this special permission will only see report data regarding alerts generated on Server Groups for which they have View permission. In particular, the Settings permission is required for

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>access to database audit archiving configuration and key management interfaces.

All administrator accounts defined in the SOM database allow access to all SOM functions, including SOM administrator account management.</td></tr>
<tr><td>FMT_SMF.1</td><td>The SecureSphere GUI is used by authorised administrators to manage all IDS/IPS System and audit capabilities as described in Table 7-3:

Table 7-3- Management Functions
<table>
<tr><th>Component</th><th>Management Function</th><th>Management Functionality</th></tr>
<tr><td>FMT_MOF.1</td><td>Modify the behaviour of the functions of System data collection, analysis and reaction</td><td>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.</td></tr>
<tr><td rowspan="4">FMT_MTD.1</td><td>Query audit data</td><td>Audit records are stored as System Events and may be reviewed using the SecureSphere GUI in an online tabular format or as System Events reports.</td></tr>
<tr><td>Query and add System data</td><td>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 assessments.</td></tr>
<tr><td>Query (export) and modify (create, delete, import) audit archive protection keys</td><td>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.</td></tr>
<tr><td>Query and modify all other (non-System and audit) TOE data</td><td>Authorised administrators can use the SecureSphere GUI interface for reviewing and modifying all other TOE data (e.g. Tasks).</td></tr>
<tr><td>FMT_SMR.1</td><td>Modify the group of users that are part of a role</td><td>SecureSphere GUI allows authorised administrators belonging to the Administrators group with access to the Admin tab, providing the ability to add, edit, and delete user accounts, and reset their passwords.</td></tr>
</table></td></tr>
</table>

Component	Description of mechanism
7.1.5. Protection of the TSF (FPT)	
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 explained in section 1.5.2.3. Neither the Management Server nor the SecureSphere gateways route or bridge network traffic between the Management NIC 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. Section 1.5.2.2 describes supported SecureSphere deployment configurations. In both sniffing and bridging configurations (except for non-transparent reverse proxy configurations), SecureSphere 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.
	FPT_ITT.1 requires protection of TSF data when it is transmitted between separate parts of the TOE, i.e. while it is in transit outside of the TOE. In the case of audit archiving (see section 1.5.3.9), 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, as described for FCS_COP.1. 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.
FPT_STM.1	The SecureSphere 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 Management Server's clock can be synchronized with an external NTP server.
7.1.6. Trusted path/channels (FTP)	
FTP_TRP.1	The TOE provides a trusted path for authorised administrator sessions to the SecureSphere GUI. 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 or Kerberos authenticator for authenticating the administrator. This is required for all administrator sessions.
7.1.7. Intrusion Detection (IDS)	
IDS_ANL.1	The System performs the analysis functions described in Section 1.5.3.8 on IDS System data collected as described for IDS_SDC.1 below. Events that are matched by any of the ID analysis engines are recorded as an Alert. 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. 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.

Component	Description of mechanism
	• 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. • 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, Alert Type-specific information is recorded. Among other attributes, this may include source and destination ports, protocol (TCP/UDP/ICMP), service name (if recognized), packet contents, and HTTP, database, or file access query.
IDS_RCT.1	For each Security Rule, the Action Policy defined by the authorised System administrator can invoke two types of actions: • Immediate Actions- actions taken as an immediate response to an attack. SecureSphere 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. • Followed Actions- follow-up actions taken by the System. An Action Set defines a set of actions and operations that are executed by SecureSphere 9.0 as a result of an ID analysis. Configurable actions include: o **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. o **Blocking Attacking Session**-Blocking subsequent HTTP requests with the same session identifier as was recorded for the event, for a specified period of time. o **Block User**-Block subsequent requests associated with the same user as was identified for the event, for a specified period of time. o **Dispatch Alert**-Send alarm to specified Action Interfaces (see section 1.5.3.9) including relevant Alert details. o **Start Monitoring**-Record all requests/responses from the IP or session recorded for the event, for a specified period of time.
IDS_RDR.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 FMT_SMR.1. Audit data archived outside the TOE is cryptographically protected as described for FCS_COP.1, preventing unauthorized access to the data.
IDS_SDC.1	In both sniffing and inline topologies, the Gateway collects all IP network traffic flowing between external and internal networks, as described in section 1.5.3.4. Collected IP packets are recognized as UDP datagrams, TCP sessions, or other IP protocols, and forwarded to the TOE's analysis and reaction logic. As described above for IDS_ANL.1, Alerts may be generated by the analysis logic; these may be an indication of suspicious activity, or a result of an administrator request to monitor specified events. In addition to collecting network traffic, the TOE provides application-level monitoring for three protocol types: service requests for Web resources (over the HTTP and HTTPS protocols), database access protocols, and file access protocols (CIFS). The TOE can 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

Component	Description of mechanism
	sessions to the Web server for a single user session, the TOE can 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. Database access request event records may also be received from DB agents (see section 1.5.3.5) and from database log collectors (see section 1.5.3.6). File access events may be received from file agents. User identification can be enriched by querying a user directory or database in the IT environment, and the user's information recorded with applicable event records. Host names are resolved via Domain Name Server (DNS) queries. The Gateway records database queries and file access queries. For each server group you can define an unlimited number of audit rules. The administrator defines an audit policy that specifies match criteria and the server groups to which the audit policy is applied. When an audit policy is applied, Gateways save all matching queries into audit files on the Gateway. For each 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. As described in section 1.5.3.7, the TOE invokes discovery and assessment tests on databases using remote SQL queries and SSH connections to their host operating systems. 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. In addition, both databases and file servers can be scanned for analysis of sensitive data and for user rights assessment (URMD and URMF products, respectively). The Management Server includes a report generator application that is controlled via the SecureSphere GUI. 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

Component	Description of mechanism

Table 7-4- Recorded Information Mapping to IDS_SDC.1

Event	Requirement	Recording Alerts	Auditing	Database Assessment	User Rights Management
All	date and time of the event	Time	date and time	date and time	date and time
	type of event	type, alert severity, aggregated, description	query	test identification	grantee type
	subject identity	source IP, user identity	user name	N/A	grantee
	outcome	action policy, immediate action	success or failure	success, failure, or error status	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		destina-tion IP address		
Service requests	specific service	service name			
	source address	source IP			
	destination address	server group			
Network traffic	protocol	protocol, service name			
	source address	source IP, source port			
	destination address	server group, destination port			
Access control configu-ration	location				db/schema or folder and object identity
	access settings				permissions or privilege

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td></td><td></td><td>types</td></tr>
<tr><td>Detected known vulner-abilities</td><td>identification of the known vulnerability</td><td></td><td></td><td>detected known vulnerabilities</td><td></td></tr>
</table>
</td></tr>
<tr><td>IDS_STG.1, IDS_STG.2</td><td>Audit files are stored in files on the gateway, and can be queried using the SecureSphere GUI. Each gateway allocates up to 40% of the audit directory partition's disk space for audit storage (this is 80Gb on the appliance model with the minimum disk space). The gateway will automatically delete the oldest files when 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.

Alerts are sent by the Gateway that generates the Alert to the Management Server, and stored in the SecureSphere database in a table that can hold up to 250,000 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 250,000 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.

Recorded System data is reviewed by authorised administrators via the SecureSphere GUI. Authorised administrators can selectively delete System data, but have no interface for modifying stored data. The TOE does not provide any interface for unauthorised users to access System data. The TOE extends protection to archived database audit files by signing the files, allowing the TOE to detect any unauthorised modification of these files while outside the TOE. The TOE cannot prevent unauthorised deletion of data stored outside the TOE. System data storage capacity is described for IDS_SDC.1.

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. Audit files can be archived outside the TOE as described in section 1.5.3.9, either manually by the administrator or on an administrator-defined schedule.</td></tr>
</table>

7.2. Protection against Interference and Logical Tampering

7.2.1. Domain Separation

Neither the Management Server nor the SecureSphere 9.0 gateways route or bridge network traffic between the Management NIC (described above in Section 1.5.2.3) 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 9.0 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.

7.2.2. 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 administrator session is protected from modification and disclosure using the TLS protocol. The System Events Log records all administrative operations performed on the TOE.

7.2.3. Time Synchronization

The SecureSphere 9.0 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 9.0 Management Server’s clock can be synchronized with an external NTP server.

7.2.4. Content Update Verification

ADC content updates loaded either manually or automatically into the TOE and online ThreatRadar updates 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.

7.3. Protection against Bypass

7.3.1. Inline Configuration

TOE Gateways can be installed in an inline configuration, so that traffic blocked by the Gateway cannot reach its destination.

7.3.2. Defragmentation

IP packet fragments are reassembled by the TOE's reverse proxy prior to being processed by ID analysis engines, preventing fragmentation-based bypass attacks.

8. Supplemental Information

8.1. References

The following external documents may be 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]	NIAP Precedent Decision PD-0097: Compliance with IDS System PP Export Requirements
[PD-0118]	NIAP Precedent Decision PD-0118: Assumptions in the IDS PP v1.4
[PD-0151]	NIAP Precedent Decision PD-0151: Acceptable Demonstrable Assurance for the IDS System PP v1.7 (BR)
[FTP]	IETF RFC 0959 – File Transfer Protocol (FTP), October 1985
[SNMP Traps]	IETF RFC 1215 – A Convention for Defining Traps for use with the SNMP, March 1991
[NFSv3]	IETF RFC 1813 – NFS Version 3 Protocol Specification, June 1995
[TLSv1.0]	IETF RFC 2246 – The TLS Protocol Version 1.0, January 1999
[HTTP]	IETF RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1, June 1999
[HTTPS]	IETF RFC 2818 – HTTP over TLS, May 2000

[SMTP] IETF RFC 2821 – Simple Mail Transfer Protocol, April 2001

[SSHv2] IETF RFC 4251 – The Secure Shell (SSH) Protocol Architecture, January 2006

[Syslog] IETF RFC 3164 – The BSD syslog Protocol, August 2001

[PKCS#1] IETF RFC 3447 – Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003

[FIPS 186-2] NIST, Digital Signature Standard (DSS), FIPS PUB 186-2 (+Change Notice) January 27, 2000

8.2. 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.

8.2.1. 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”.

8.2.2. 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.

8.2.2.1. 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.

8.2.2.2. 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.

8.2.2.3. 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.

8.2.2.4. 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.

8.2.3. Other Notations

8.2.3.1. Footnotes

Footnotes[16] are used to provide further clarification for a statement, without breaking the flow of the text.

8.2.3.2. 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 8.2.3.2.

[16] This is an example of a footnote.

8.2.4. Highlighting Conventions

The conventions for SFRs described above in sections 8.2.2 and 8.2.3 are expressed in chapter 5 by using combinations of bolded, italicized, and underlined text as specified in Table 8-1 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 8-1- 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
<u>Underline</u>	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.2)* IDS_STG.2.1 The System shall <u>overwrite the oldest stored System data</u> and send an alarm if the storage capacity has been reached.	(completed) Selection
<u>Boldface Underline</u>	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 **<u>unauthorized</u>** modifications to the **<u>stored</u>** audit records **<u>in the audit trail</u>**.	Refinement

8.3. 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 9.0 product line.

8.3.1. 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[17] and the disclosure and modification of data.[18]
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.
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 9.0 system events log.
Audit Viewer	An administrator role established in accordance with evaluated configuration guidance that is used exclusively for the purpose of querying audit data.
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 SFRs, perform an operation.
Availability	Timely[19], 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.

[17] Hardware and software.

[18] Stored or communicated.

[19] According to a defined metric.

Compromise Violation of a security policy.

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 9.0 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.

Kerberos An authentication protocol based on cryptographically-generated single-use authenticators.

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 SFRs.
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 role that is assigned Edit permissions on management objects restricted by the TSF.
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 SFRs and perform an unauthorised operation with the TOE.
Target of Evaluation Security Functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
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.

8.3.2. Abbreviations

Abbreviation	Description
ADC	Application Defense Center
AES	Advanced Encryption Standard
CAV	Correlated Attack Validation
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CSV	Comma Separated Value
DAS	Discovery and Assessment
DLP	Data Leak Prevention
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability
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
MX	Management Server
NAS	Network Attached Storage
NIC	Network Interface Card
NTP	Network Time Protocol
OOB	Out Of Band
PP	Protection Profile
RFC	Request for Comment
SFR	Security Functional Requirement
SFP	Security Function Policy

Abbreviation	Description
SIEM	Security Information and Event Management
SIM	Security Information Management
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOM	SecureSphere Operations Manager
SPAN	Switch Port Analyzer
SQL	Standard Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UDP	User Datagram Protocol
URL	Uniform Resource Locator
URMD	User Rights Management for Databases
URMF	User Rights Management for File Servers
UUT	Universal User Tracking
XML	eXtensible Markup Language

Appendix A - IT Environment Components

The following table summarizes the components in the IT environment supported by the TOE including identification of supported versions.

Table 8-2 - Non-TOE Components Supported by the TOE

Category	Supported Products	Supported Versions
Data Collection (Sniffing and Bridging) and Analysis	Any	IPv4
Protected Web servers	Any	HTTP 1.1
Protected database servers	DB2	7.2, 8, 9, 9.5, 9.7, 10
	Informix	7.31, 9.x, 10.x, 11.x
	MS-SQL	7, 2000, 2005, 2008, 2008 R2
	MySQL	4.1, 5.x
	Netezza	4.x, 5.0, 6.0
	Oracle	8, 9, 10, 11
	Sybase ASE	11.9, 12.0, 12.5.x, 15.x
	Sybase IQ	12.5, 12.6, 12.7
	Progress Openedge	10.1c, 10.2a, 10.2b
	Teradata	2.6, 12
Protected file servers	Microsoft Windows Server	2003, 2008
	NAS (e.g. NetApp, EMC)	CIFS v1, v2
Directories (for querying user information)	Microsoft Active Directory	Windows 2000 and higher
	LDAP directories	Any
Host name resolution	Any	DNS
Time updates	Any	NTPv3
Alarm destinations	Any	SMTP, Syslog, SNMPv3, SOAP
Audit archiving	Any	NFSv3, FTP, SCP
Supported network HSMs	nCipher netHSM	
	SafeNet LunaSA	
Supported DB/file agents	SecureSphere file agent	6, 7, 8.5, 9.0
	SecureSphere DB agent	6, 7, 8.5, 9.0