Imperva SecureSphere 12.1 Security Target v1.1

jtsec (http://www.jtsec.es)

2018-09-26

Created by

Table of contents

1 ST Introduction

1.1 ST Reference

Title: Imperva SecureSphere 12.1 Security Target

Version: v1.1

Author: jtsec (http://www.jtsec.es)

Date of publication: 2018-09-26

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

1.2 TOE Reference

TOE Name: Imperva SecureSphere

TOE Developer: Imperva

TOE Version: v12.1.0.51_0.25311

- Gateway: v12.1.0.51_0.25311
- Management: v12.1.0.51_0.25311
- SOM: v12.1.0.51_0.25311
- Agents:
    - Linux: v12.0.0.1084
    - Windows: v12.0.0.1085

1.3 TOE Overview

1.3.1 TOE Type

Imperva SecureSphere 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 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. IDS System is defined 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, file servers or databases), 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.

1.3.2 TOE Usage & Major Security Features

The TOE 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 HTTP proxy, a transparent inline bridge or as an offline network monitor (sniffer), a SecureSphere 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.

In addition the TOE provides local monitoring of file servers and databases through the use of Agents, software installed in the monitored server that connects to the configured gateway through a secure connection.

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 12.1 software and provide all claimed security functionality, but may differ in throughput and storage capacity. SecureSphere 12.1 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 12.1 appliance hardware. The VMware Hypervisor and underlying hardware is considered to be outside of the boundaries of the Target of Evaluation.

The security functionality includes protection of communications between TOE components and trusted IT entities, identification and authentication of administrators, auditing of security-relevant events, ability to verify the source and integrity of updates to the TOE, and it specifies FIPS-validated cryptographic mechanisms.

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.

1.3.3 Non-TOE Hardware/Software/Firmware

1.3.3.1 Clients of SecureSphere Management Interfaces

SecureSphere 12.1 GUI is managed using a standard Web browser. SecureSphere supports the following browsers:

- Adobe Flash: Most recent stable version.
- Microsoft Internet Explorer: 10 and up
- Mozilla Firefox: Most recent stable version.
- Apple Safari: Most recent stable version.

The OpenAPI is also accessed using clients outside of the TOE.

1.3.3.2 VMware Hypervisor if Deploying a SecureSphere Virtual Appliance

SecureSphere 12.1 management and/or Gateway software can be installed on a Virtual Machine hosted by a VMware ESX/ESXi Hypervisor. The virtual (VM) appliances are delivered as an installation disk (or ISO image). They require that the minimum following hardware and software be installed on the host system:

- VMware ESXi 5.x with virtual hardware version 9.0 and newer
- Dual core or higher number of cores, Intel based server
- IvyBridge supported Microprocessor or newer generation of Intel based CPUs: 3rd Generation Intel Core processors, Intel Xeon processor E3-1200 v2 product family, Next Generation Intel Xeon processors, Intel Xeon processor E5 v2 and E7 v2 families or newer Intel Xeon processors.
- 250 GB Hard Drive
- Hypervisor-supported network interface card
- If ESXi is in cluster, the EVC level must be set to L5 (IvyBridge) or higher

The main reason for using IvyBridge CPUs for Common Criteria is because of the need to use RDRAND command, any IvyBridge CPU is compatible with this requirement and therefore all IvyBridge CPUs can be used as ESX servers.

Detailed minimum requirements for each Guest SecureSphere Virtual Appliance depends on the platform and include the following:

Specification	Gateways				Management Server
Model	V6500	V4500	V2500	V1000	VM150

CPU	8	4	2	2	2
Memory	16GB	8GB	4GB	4GB	4GB
Minimum Disk Space	250 GB	160 GB	160 GB	160 GB	160 GB

Table 1 SecureSphere Virtual Appliance Specifications

VM150 can be optionally configured with 4 CPUs.
VM150 can be optionally configured with up to 32 GB of memory
The number given here is for WAF appliances. File Security and Database Security products may require more space for audit files.

All of the VM Machines in the CCTL test configuration were tested on an Ivy Bridge supported Intel Core i5-3350P processor @ 3.10 GHz with VMware ESXi v5.1.0 with virtual hardware version 9.

1.3.3.3 IT Environment Components

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

Category	Supported Products	Supported Versions
Data Collection (Sniffing and Bridging) and Analysis	Any	IPv4, IPv6
Protected Web servers	Any	HTTP 1.1, HTTP 1.2
Protected database servers	DB2 LUW	7.2, 8, 9, 9.5, 9.7, 10.0, 10.5
	Informix	7.31, 9.x, 10.x, 11.0-11.5, 11.7, 12.1
	MS-SQL	7, 2000, 2005, 2008, 2008 R2, 2012, 2014
	MySQL	4.1-5.7
	Netezza	4.x, 5.0, 6.0, 7.0- 7.2
	Oracle	8i, 9i, 10g, 11g, 12c build 12.1.0.2.0 (Standard or Enterprise)

	Sybase ASE	11.9, 12.0, 12.5.x, 15.0-15.7, 16.0
	Sybase IQ	12.5, 12.6, 12.7, 15.0-15.4, 16.0
	Sybase Anywhere	11, 12, 16, 17
	Progress Openedge	10.1c, 10.2a, 10.2b, 11.3
	Teradata	2.6, 12, 13.0, 13.1, 14, 14.1, 15.0, 15.1
	PostgreSQL	8.4 - 9.4
	IMS for z/OS	11, 12, 13
	DB2 for z/OS	10, 11
	SAP HANA	v1 SPS 8, 9, 10, 11, 12
Protected file servers	Microsoft Windows Server	2003, 2008
	NAS (e.g. NetApp, EMC)	CIFS (SMB, SMB2, SMB2.1)
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

Table 2 Non-TOE Components Supported by the TOE

1.3.3.4 Hardware

When the product is provided as a hardware appliance, the TOE scope is limited to the software part of the product, and therefore the hardware is out of the scope of this evaluation.

Imperva SecureSphere v12.1 software can run on two or more of the Imperva appliances listed below, including one or more Management Servers and one or more Gateways.

Appliance	Role	FT	TP	HD	RAM	FF
X2510	Gateway (64 bit)	✓	0.5	500 Gb	16 Gb	2U
X4510	Gateway (64 bit)	✓	1	500 Gb	32 Gb	2U
X6510	Gateway (64 bit)	✓	2	3 x 2 Gb	64 Gb	2U
X8510	Gateway (64 bit)	✓	5	3 x 2 Gb	128 Gb	2U
X10K	Gateway (64 bit)	✓	10	3 x 2 Gb	128 Gb	2U
M160	Management Server	✓	N/A	2 x 500 Gb	32 Gb	2U

Table 3 *List of Supported TOE Appliances*

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.

Figure 1 *SecureSphere Gateway Appliance*

1.3.3.5 Software

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

- Active Modules: SecureSphere 12.1 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 12.1 provides an alternative high-performance Imperva proxy infrastructure that is included in the evaluated configuration.

- SSH (only used during installation): SecureSphere 12.1 appliances can support local console access and remote access to appliance operating system-level installation and configuration CLI over the SSH protocol. Once an appliance is correctly configured and operational, all management should be performed via the SecureSphere GUI.

1.4 TOE Description

1.4.1 Introduction

SecureSphere 12.1 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 ;
- Excluded functionality that is not available in the TOE 's evaluated configuration.
- 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.

1.4.2 TOE Logical Scope

1.4.2.1 SecureSphere on VMware Hypervisor

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 12.1 software assumes that the hypervisor provides complete separation for all Virtual Machine resources allocated for SecureSphere 12.1 components, as would be the case with a physical appliance.

The identified software is provided in the form of Virtual Appliance images that are run on a VMware ESX/ESXi Hypervisor:

- V1000, V2500, V4500, V6500 for Gateway
- VM150 for MX and SOM

Note: MX and SOM are two management applications using the same code base. MX, Gateway and SOM are all installed using the same image, during installation user chooses the application to install.

1.4.2.2 Summary of TOE Security Functionality

1.4.2.2.1 IDS Component

Imperva SecureSphere 12.1 is an IDS/IPS that monitors network traffic between clients and servers in real-time, analyses that traffic for suspected intrusions, and provides a reaction capability. Reaction options include recording and monitoring suspected traffic and ID events, blocking traffic, and generating alarms containing event notifications. Database auditing allows you to record selected user database queries for audit purposes. Web and file server queries and responses can also be selectively recorded. In addition, monitored databases can be actively scanned to identify potential vulnerabilities and agents may be installed in file and web servers to provide addtional insights.

1.4.2.2.2 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 or OpenAPI. Administrators log in to the Management Server and are authenticated using a password or X.509 certificates. The server provides a trusted path for the management session using the 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.

1.4.2.2.3 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.

1.4.2.2.4 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 while transfer of information between the gateways and the agents is encrypted. Audit data that is stored on an archive outside of the TOE is cryptographically protected from disclosure or tampering. ADC content and ThreatRadar updates' authenticity and integrity is verified by the TOE before updates are applied, ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. SecureSphere also protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE includes its own time clock to ensure that reliable time information is available (e.g., for log accountability) but requires an NTP Server in the operational environment in order to synchronize its clock with that of the external time server. The TOE uses **[HTTPS]** to protect communications between distributed TOE components and with the users.

1.4.2.2.5 Cryptographic Support

The TOE provides a FIPS mode of operation, which must be enabled in the evaluated configuration. The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions. The TOE uses the RSA Crypto-J version 6.1.2 and **[FIPS 140-2]** OpenSSL version 1.0.2h with FIPS canister version FIPS 2.0.12 (cert #2398) cryptomodules for all of the cryptographic functionality. The modules provide key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of higher level cryptographic protocols, including SSH, TLS and HTTP over TLS.

1.4.2.3 Imperva SecureSphere Products

SecureSphere 12.1 functionality is enabled by entering Imperva licenses for SecureSphere "products". The following Imperva products are included in the evaluated configuration.

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.

Table 4 SecureSphere Products

1.4.2.4 SecureSphere Deployment Scenarios

From a physical point of view, all SecureSphere 12.1 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 both modes system administrators shall ensure that the connection between GW and MX is over an OOB network and that there is IP connectivity between the GWs, the MX, and the optional SOM, and between the Agents and the GWs. Note that in order to connect the agents with the Gateway, you need to use a specific interface for this purpose different for the one used for the bridge or proxy.

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.

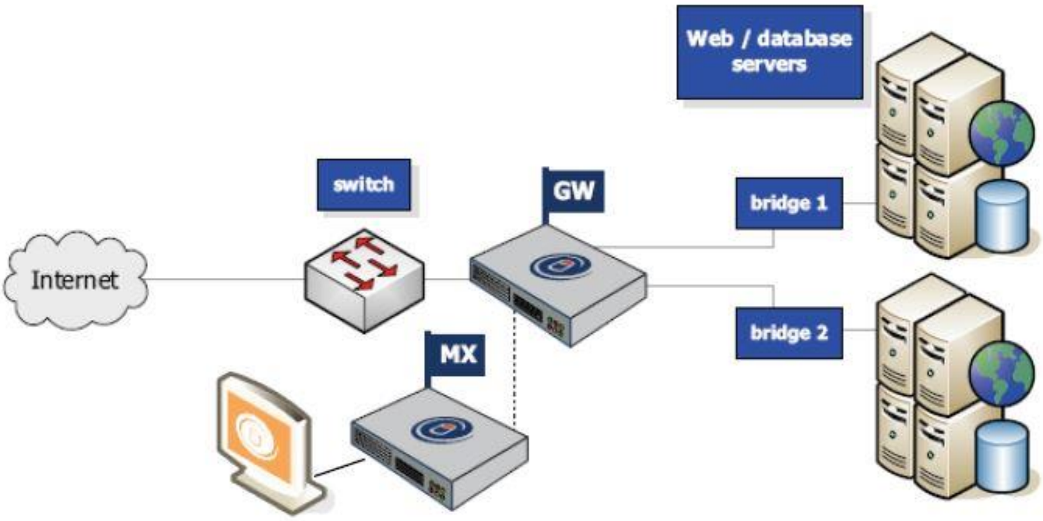


Figure 2 SecureSphere Inline Deployment

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 (mirror) port on the switch, or a dedicated TAP device. Traffic is copied to it instead of passing directly through it. TCP resets are transmitted over a "blocking" NIC.

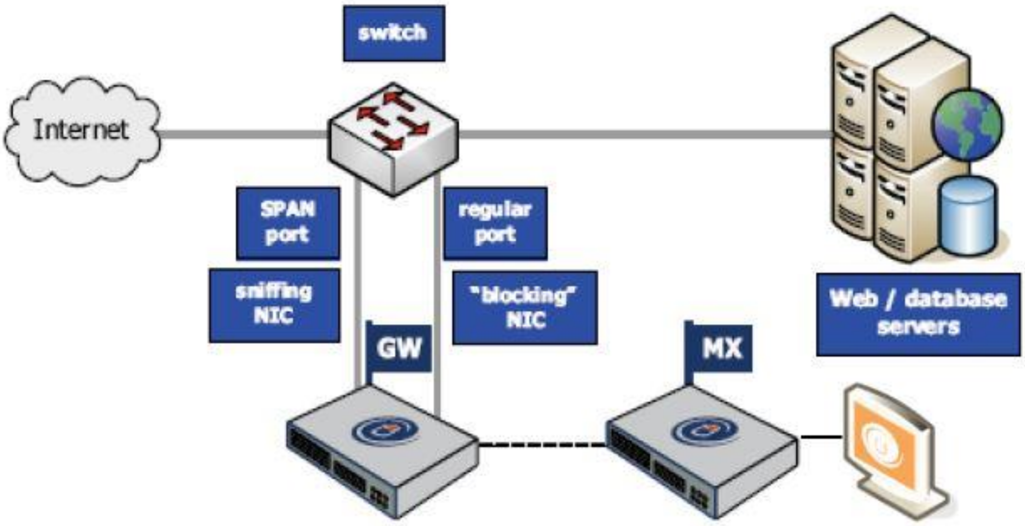


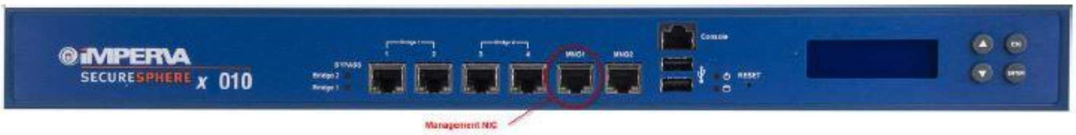
Figure 3 SecureSphere Sniffing Deployment

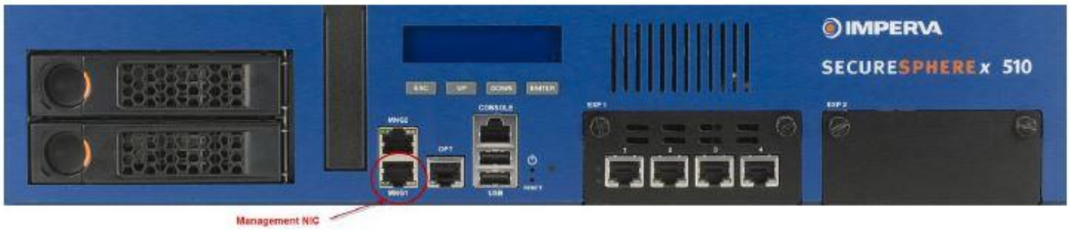
Onebox mode, where both the SecureSphere management server and SecureSphere gateway are integrated in a single machine is not included in the evaluated configuration.

1.4.2.5 Management Network

TOE guidance instructs the administrator to ensure that the SecureSphere 12.1 gateways connect to the SecureSphere Management Server through an out of band management network. In this configuration, all Gateway-Management Server communication is carried over a dedicated and secure network that is completely separated from production traffic.

Separation between the production traffic and the OOB management network is achieved by allocating a separate (onboard) NIC for this purpose on SecureSphere 12.1 gateways. As depicted below, the Management NIC is clearly separated from other appliance NICs. The SecureSphere 12.1 gateway operating system does not bridge or route packets between production NICs and Management NICs.





Management NIC separation is also maintained on a SecureSphere 12.1 Virtual Appliance. The virtual management NIC is selected during initial configuration of the appliance.

1.4.2.6 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. In this mode we can also use Transparent Reverse Proxy to improve packet inspection.
  - Proxying – the TOE (when in inline topology) transfers HTTP requests and responses 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.

    - SecureSphere DB and File Security Agents – Imperva sensor software agents that run on the monitored database or file server, and transmit all access requests to the SecureSphere 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.

- 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 SIEM / SIM tool integration.
- Security Management
    - Management – authorized administrators manage the TOE and review audit trail and IDS System data via the SecureSphere GUI or OpenAPI.
    - 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 NTP protocol. SecureSphere agents use the host machine clock where needed. The host machine is assumed to be an enterprise-class machine with an accurate clock (using NTP or any other method).

Figure below depicts the TOE protecting file, web, web services and database assets. SecureSphere 12.1 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.

The SecureSphere File/DB Agents running in File Servers and DB Servers, are connected to the gateway through a secure connection between these separated parts of the TOE boundary. This connection is different from the one used to scan the servers.

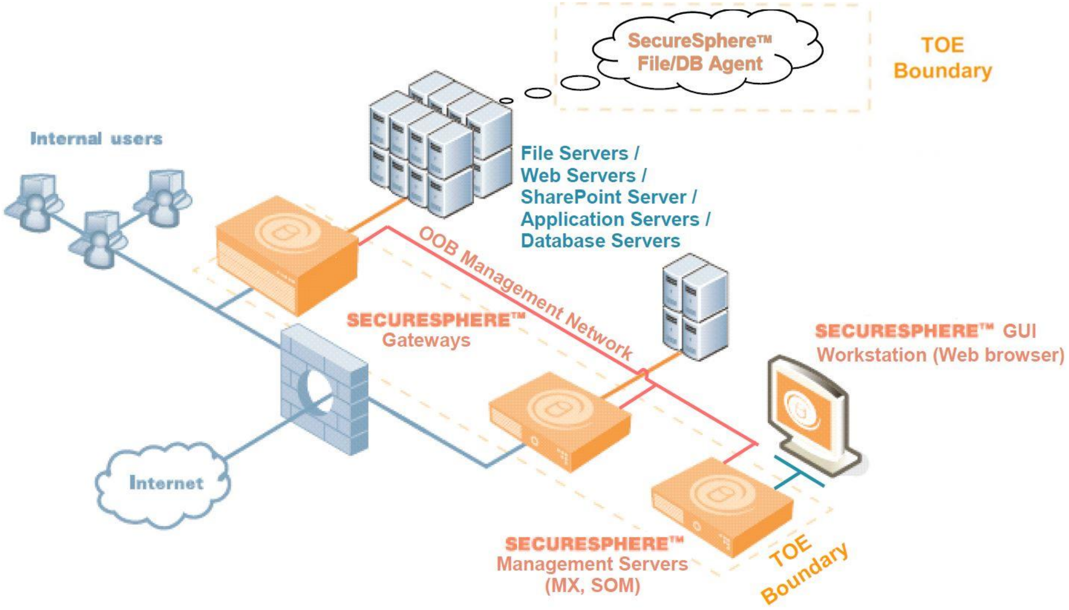


Figure 4 *Protecting File, Web, Webservices and Database Assets*

Figure 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 below includes only the SecureSphere 12.1 software (the virtual appliances and the agents that may be installed in the virtual servers); the hypervisor, virtual switches, protected servers, and physical environment are all considered to be part of the IT environment and outside the boundary of the TOE.

Please, note that the connection to the MX or SOM using the SecureSphere GUI may be performed through a potentially unsecure LAN network or using the OOB management network. Both possibilities are allowed. In the first scenario the cryptographic functionality will protect the channel, while in the second one another extra layer of security will be added through the use of the out of band network.

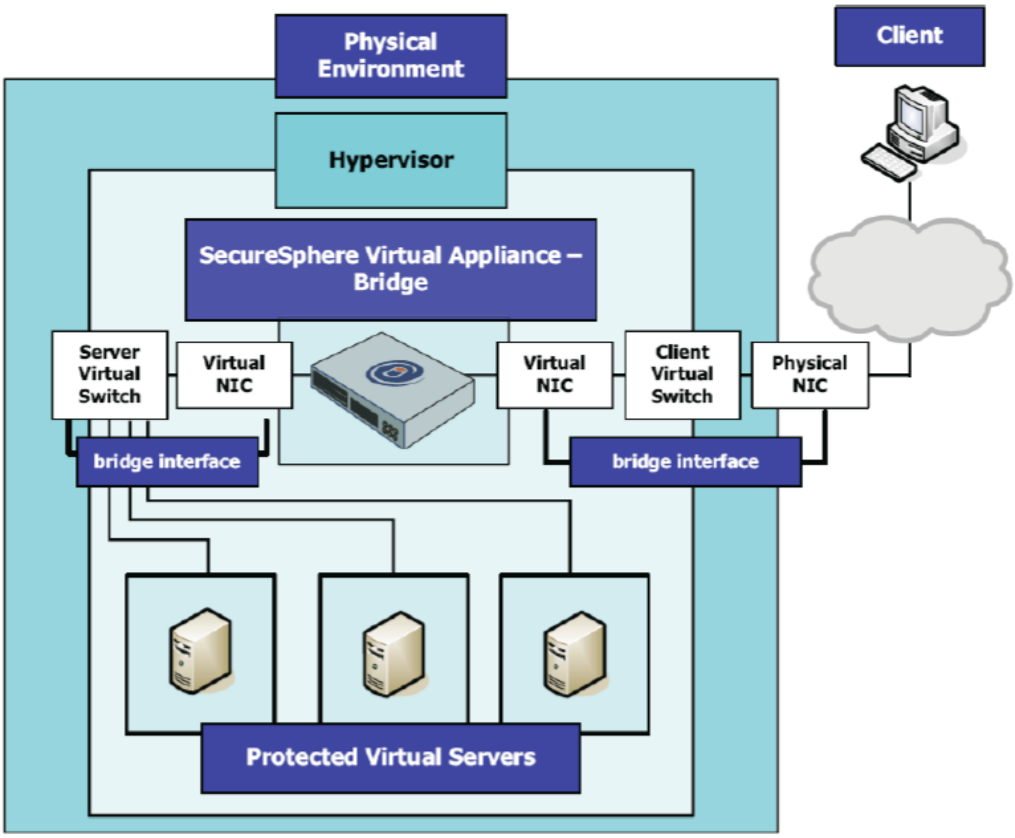


Figure 5 *Virtual Deployment*

The browser used to manage the TOE via the SecureSphere 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.

1.4.2.7 Network Traffic Data Collection Modes

SecureSphere 12.1 collects and records network traffic using either the sniffing or inline topologies described above. The traffic is analyzed using the TOE's IDS 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.

1.4.2.7.1 Sniffing

When configured in sniffing topology, SecureSphere 12.1 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.

1.4.2.7.2 Bridging

When configured in inline topology, SecureSphere 12.1 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, transmitted it on the paired segment. This mode is known as “Transparent Bridge”.

This traffic data collection mode, has an optional feature that utilizes the reverse proxy mechanism and is called Transparent Reverse Proxy (TRP) and can be found in the Administrative Guide under Reverse Proxy (even that it is actually a bridge).

1.4.2.7.3 Reverse Proxy

When configured in inline topology, SecureSphere 12.1 gateways can be configured in Reverse Proxy mode. Transparent Reverse Proxy Mode is similar to bridging; however, instead of processing each individual frame, TCP segments are accumulated and the proxy processes complete HTTP 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).

This data collection mode, can be used in bridge mode. In this case it is known a “Transparent Reverse Proxy in bridge mode.”

Reverse Proxy also supports “Kernel Reverse Proxy” (KRP), but it is not available in FIPS mode so it is not part of an evaluated configuration.

1.4.2.8 Fail-Safe Modes

SecureSphere 12.1 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. By default the TOE uses safe mode.

1.4.2.9 DB and File Security Agents

SecureSphere 12.1 gateways provide support for SecureSphere agents, IDS sensors 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 network traffic and local access on the database or file server, and transmits the traffic to a network segment monitored by SecureSphere 12.1 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.

1.4.2.10 Log Collectors

SecureSphere 12.1 Gateways can be configured to collect native database logs over FTP or SQL network protocols. The log records are integrated with the database audit records collected by the Gateway from database access network activity.

1.4.2.11 Discovery and Assessment (DAS)

The SecureSphere 12.1 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).

1.4.2.12 Analysis and Reaction

1.4.2.12.1 Overview

SecureSphere 12.1 applies different layers of intrusion detection logic to analyzed network traffic, as depicted below in Figure 6. 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 12.1 blocks a Web connection it can be configured to display an error page to the blocked user.

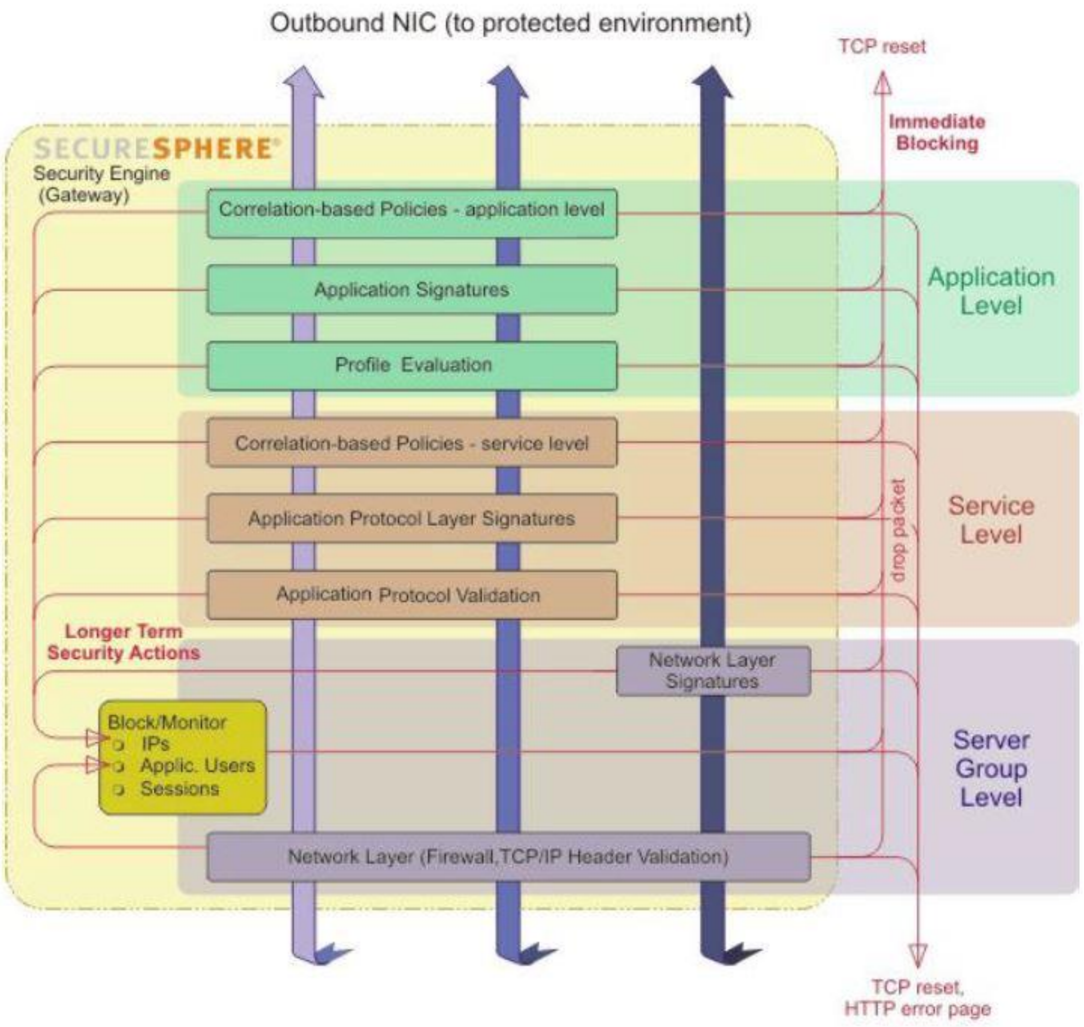

Outbound NIC (to protected environment)
TCP reset
Immediate Blocking
SECURESPHERE
Security Engine (Gateway)
Correlation-based Policies - application level
Application Signatures
Profile Evaluation
Application Level
Correlation-based Policies - service level
Application Protocol Layer Signatures
Application Protocol Validation
Service Level
drop packet
Longer Term Security Actions
Network Layer Signatures
Block/Monitor
IPs
Applic. Users
Sessions
Server Group Level
Network Layer (Firewall,TCP/IP Header Validation)
TCP reset, HTTP error page

Figure 6 SecureSphere Layered Intrusion Detection

1.4.2.12.2 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).

1.4.2.12.3 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 CSV-format classification files generated by third-party DLP products.

1.4.2.12.4 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 ThreatRadar service, which provides categorized lists of potentially malicious IP addresses.

1.4.2.12.5 Traffic Monitoring and Recording

SecureSphere 12.1 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.

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

1.4.2.12.7 Protocol Violations

SecureSphere protocol compliance checks ensure that protocols meet RFC and expected usage requirements. By ensuring that the protocol meets guidelines, protocol compliance prevents attacks on both known and unknown vulnerabilities in commercial Web server implementations. Imperva has conducted comprehensive research and collected a group of protocol violations that usually indicate attack attempts. You can enable or disable each of these violations for each group of protected servers.

1.4.2.12.8 Universal User Tracking (UUT)

SecureSphere 12.1 gateways analyze both Web and database protocols to identify the user identity, using both direct user tracking where the user identity is included in the request and application user tracking which maps requests to a user session context, with user identity acquired by the gateway during session establishment (user authentication).

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

1.4.2.12.9 Profile Violations

SecureSphere Web and database profiles represent a comprehensive model of all "allowed" interactions between users and the two key elements of the enterprise network: Web servers and database servers. The Web Profile includes legitimate URLs, HTTP methods, parameters, cookies, SOAP actions, XML structures and more. The Database Profile includes all legitimate SQL queries per database user, valid IP addresses per database user, and more. The profiles are built automatically through a learning process and adapt to changes in the application environment over time by observing live traffic and applying SecureSphere 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.

1.4.2.12.10 Correlated Attack Validation (CAV)

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

For example, a signature violation such as the "union" string may indicate a SQL injection attack. On the other hand, the word "union" may be part of a legitimate URL.

Therefore, rather than risk blocking a legitimate user, CAV will classify that user as "suspicious" and begin tracking his/her actions to validate true intent. When SecureSphere 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.

1.4.2.13 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 12.1:

- Email: This interface allows sending an email over SMTP to a specific group of email addresses hosted on mail servers in the IT environment.

- SNMP Traps: An interface that sends SNMP traps to a SNMP manager host in the IT environment.

- Syslog: This interface allows sending a Syslog message to a Syslog server in the IT environment.

- Audit Archiving: database 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 Commands: an interface to the SecureSphere Management Server operating system. This interface allows execution of an operating system command or a specific file on the Management Server.

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

1.4.2.14 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 or OpenAPI interface that are used for all management activities once the TOE is operational. Configuration settings are downloaded from the Management Server to SecureSphere 12.1 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 OpenAPI or 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.

1.4.2.15 SecureSphere Gateway Clocks

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

1.4.2.16 ADC Content Updates

SecureSphere 12.1 attack signatures are text strings that match known server vulnerabilities and attack patterns. SecureSphere 12.1 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.

1.4.2.17 Non-TOE Security Features

1.4.2.17.1 Functionality Excluded from the TOE Evaluated Configuration

All SecureSphere 12.1 functionality is included in the TOE Evaluated Configuration, with the following exceptions:

Imperva SecureSphere 12.1 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 using password or X.509 certificates..

1.4.2.17.2 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

Compliance with Standards and Regulations

SecureSphere 12.1 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.

Interoperability with Third-Party Products

SecureSphere 12.1 provides protection 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.

Non Security-Relevant Cryptographic Mechanisms

This ST levies no cryptographic security requirements on the TOE; IDS is not considered a cryptographic function. Nevertheless, the SecureSphere 12.1 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.

The approach taken in this ST is to define cryptographic mechanisms as security functionality 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.

1.4.3 TOE Physical Scope

1.4.3.1 TOE Hardware, Firmware, and Software

The Target of Evaluation (TOE) is pure a software TOE and includes the following components.

Please note that as seen in table below, the MX Management Server, the Gateway appliances and the Operations Manager (SOM) Management Server are all delivered using the same files. During the installation process the user shall select the appliance to install. This also applies to the patch file used to upgrade to the evaluated version.

Name	Type	Version	Distribution format	Notes
MX Management Server	software	v12.1.0.51_0.25311	Physical: Zip file containing (usb-disk-12.0.0.40_0.23977-x86_64.img) Virtual: Zip file containing (SecureSphere-12.0.0.40_0.23977_x86_64.ovf and SecureSphere-OVF-disk1.vmdk) Patch file: SecureSphereV12.1.0-x86_64-Patch51_0.x	
Gateway appliances	software	v12.1.0.51_0.25311	Physical: Zip file containing (usb-disk-12.0.0.40_0.23977-x86_64.img) Virtual: Zip file containing (SecureSphere-12.0.0.40_0.23977_x86_64.ovf and SecureSphere-OVF-	

			disk1.vmdk) Patch file: SecureSphereV12.1.0-x86_64-Patch51_0.x	
SecureSphere Operations Manager (SOM) Management Server	software	v12.1.0.51_0.25311	Physical: Zip file containing (usb-disk-12.0.0.40_0.23977-x86_64.img) Virtual: Zip file containing (SecureSphere-12.0.0.40_0.23977_x86_64.ovf and SecureSphere-OVF-disk1.vmdk) Patch file: SecureSphereV12.1.0-x86_64-Patch51_0.x	
Agent for Linux	software	v12.0.0.1084	Imperva-ragent-RHEL-v6-kSMP-pi386-b12.0.0.1084.tar.gz	Installed on server machine
Agent for Windows	software	v12.0.0.1085	Imperva-ragent-Windows-b12.0.0.1085.zip	Installed on server machine
Imperva SecureSphere Admin Guide Version 12.1	guidance	v5	Imperva-SecureSphere-v12.1-Administration-Guide-v5.pdf	
Imperva SecureSphere Web Security User Guide Version 12.1	guidance	v5	Imperva-SecureSphere-v12.1-Web-Security-User-Guide-v5.pdf	
Imperva SecureSphere Database Security User Guide Version 12.1	guidance	v3	Imperva-SecureSphere-v12.1-Database-Security-User-Guide-v3.pdf	

Imperva SecureSphere File Security User Guide Version 12.1	guidance	v2	Imperva-SecureSphere-v12.1-File-Security-User-Guide-v2.pdf	
Imperva SecureSphere Security for SharePoint User Guide Version 12.1	guidance	v2	Imperva-SecureSphere-v12.1-Security-for-Sharepoint-User-Guide-v2.pdf	
Imperva SecureSphere VMware ESX Configuration Guide v12.1	guidance	v6	Imperva-SecureSphere-v12.1-VMware-ESX-Configuration-Guide-v6.pdf	
Imperva SecureSphere Operations Manager (SOM) User Guide Version 12.1	guidance	v3	Imperva-SecureSphere-v12.1-Operations-Manager-SOM-User-Guide-v3.pdf	
Imperva SecureSphere Agent Release Notes v12.1	guidance	v4	Imperva-SecureSphere-v12.1-Agent-Release-Notes-v4.pdf	
Imperva SecureSphere API Configuration Guide User Guide v12.1	guidance	v3	Imperva-SecureSphere-v12.1-API-Configuration-Guide-v3.pdf	
Imperva SecureSphere Directory Services Monitoring User Guide	guidance	v2	Imperva-SecureSphere-v12.1-Directory-Services-Monitoring-User-Guide-v2.pdf	

v12.1				
Imperva SecureSphere 12.1 Evaluated Configuration Guideance	guidance	v1.1	Imperva SecureSphere - ECG v1.1.pdf	

Table 5 *List of TOE components*

All the TOE components are distributed from the Imperva website using secure methods (FTPS/HTTPS).

After downloading software, calculate a hash for each of the downloaded files, and verify that it matches the corresponding hash given in the following table using standard tools (e.g. sha256sum).

Image Type	File	SHA256 Hash
Windows Agent	Imperva-ragent-Windows-b12.0.0.1085.zip	d0b9b06c39127ec3c48aff74d105466058f965be40c7a2b02b0bdde347b8f748
Linux Agent	Imperva-ragent-RHEL-v6-kSMP-pi386-b12.0.0.1084.tar.gz	030d5a7a57c5d1cf7af8f95f7c8ef24849f462574703a8ff609086c103a32da6
Appliance Images	usb-disk-12.0.0.40_0.23977-x86_64.img	2e6e4f587247105bc2caf41ef16b631164316769eb98b9760f7cdc12a9708843
Virtual Appliances – OVF File	SecureSphere-12.0.0.40_0.23977_x86_64.ovf	246781c93917f164e6301b09b80acd862b14ef0c1b945a0f56de0baa799538ae
Virtual Appliances – VMDK file	SecureSphere-OVF-disk1.vmdk	a5b6e31837fe4823c3ab33701596f48b31583842d28e23d2b346db61d881858b
Patch File	SecureSphereV12.1.0-x86_64-Patch51_0.x	8d87b8ddb700b0075a8254fba0e3e7c86f7be2bb1cbc010728f5db4ee9260bc1

2 Conformance Claims

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R4.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R4P2] extended.
- Conformance with [CC31R4P3].

The methodology to be used for the evaluation is described in the “Common Evaluation Methodology” of the Common Criteria standard of September 2012, version 3.1 revision 4 with an evaluation assurance level of EAL3.

This Security Target does not claim conformance with any protection profile.

3 Security Problem Definition

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE
- The organizational security policies that the TOE has to adhere to
- The TOE usage assumptions in the suggested operational environment.

Although there is no declared conformance with any protection profile, the SPD and the extended requirements in this ST are heavily based in those from these PPs:

- [NDPP11] to describe the FIPS compliant cryptography implemented in the TOE
- [IDSPP17] to describe the IDS capabilities of the TOE

3.1 Threats to Security

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

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: An unauthorized user may attempt to access TOE data or security functions by undetected attacks.

T.SCNCFG: An IT administrator may configure security settings incorrectly in the IT system that the TOE monitors preventing the TOE from fully monitoring the IT system.

T.SCNVUL: Vulnerabilities may exist in the IT System that the TOE monitors, thus preventing the TOE from fully monitoring the IT system.

T.FALACT: The TOE administrator may configure the TOE incorrectly, thus causing the TOE to fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC: A malicious user may try to exploit vulnerabilities or run inappropriate actions in the IT system that the TOE monitors, in a way that the TOE may fail to recognize based on IDS data received from each data source.

T.FALASC: A malicious user may try to exploit vulnerabilities or run inappropriate actions in the IT system that the TOE monitors, in a way that the TOE may fail to recognize based on association of IDS data received from all data sources.

T.MISUSE: Malicious or unauthorized users may access the IT system that the TOE monitors overriding the TOE security mechanisms.

T.INADVE: Unauthorized users may inadvertently access the IT System the TOE monitors overriding the TOE security mechanisms.

3.2 Organizational Security Policies

The organizational Security policies are defined as follows.

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.

3.3 Assumptions

The assumptions when using the TOE are the following:

A.ACCESS: The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC: The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE: The TOE is appropriately scalable to the IT System the TOE monitors.

A.PROTCT: The TOE software and the hardware where it is installed will be protected from unauthorized physical modification, including administrator workstations and the OOB network.

A.LOCATE: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

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

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

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

A.TIME: The NTP server configured in the TOE for synchronization must be accurate and reliable so when the TOE acts as a server itself, it will provide good timestamps. The part of the TOE that runs in monitored file and database servers (agents) also depends on the host clock, so it is assumed to provide a good time source.

4 Security Objectives

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These consist of:

- the security objectives for the operational environment.
- the security objectives for the TOE

4.1 Security objectives for the TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in enforcing the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

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

O.IDSCAN: The Scanner must collect configuration information that might be indicative of the potential for a future 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 access 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.

O.TIME: The TOE must provide a reliable time source.

4.2 Security objectives for the operational environment

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

OE.TIME: The IT Environment (external NTP server and hardware clock sources) will provide reliable timestamps to the TOE.

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

OE.PHYCAL: Those responsible for the TOE must ensure that the software of the TOE and the hardware where it runs is protected from any physical attack, including administrator workstations and OOB network.

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

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs and the security objectives for the operational environment uphold all assumptions.

	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	O.TIME	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP
T.COMINT	X						X	X			X			X	X					
T.COMDIS	X						X	X												
T.LOSSOF	X						X	X			X									
T.NOHALT		X	X	X			X	X								X	X	X	X	
T.PRIVIL	X						X	X								X	X	X	X	
T.IMPCON						X	X	X								X	X	X	X	
T.INFLUX									X											
T.FACCNT										X										
T.SCNCFG		X																		
T.SCNVUL		X																		

	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	O.TIME	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP
T.FALACT					X															
T.FALREC				X																
T.FALASC				X																
T.MISUSE			X							X										
T.INADVE			X							X										
P.DETECT		X	X							X				X	X					
P.ANALYZ				X																
P.MANAGE	X					X	X	X								X		X	X	
P.ACCESS	X						X	X				X								
P.ACCACT								X		X			X	X	X					

	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	O.TIME	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP
P.INTGTY											X									
P. PROTCT									X								X			
A.ACCESS																				X
A.DYNMIC																			X	X
A.ASCOPE																				X
A.PROTCT																	X			
A.LOCATE																	X			
A.MANAGE																			X	
A.NOEVIL																X	X	X		
A.NOTRST																	X	X		

	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	O.TIME	OE.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP
A.TIME															**X**				**X**	

Table 6 Security Objectives vs Security Problem Definition

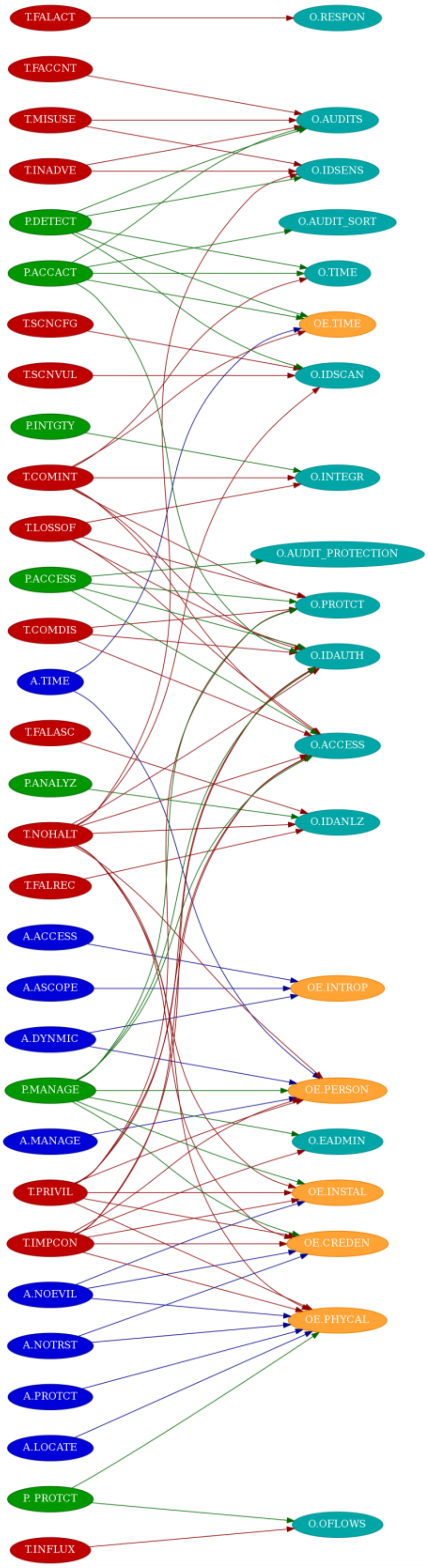


Figure 7 Mapping of Security Problem Definition to Security Objectives

4.3.1 Threats

T.COMINT: The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE data. The **O.INTEGR** objective ensures no TOE data will be modified. The **O.PROTCT** objective addresses this threat by providing TOE self-protection. **OE.TIME** and **O.TIME** together supports this OSP providing an accurate time and date.

T.COMDIS: The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE data. The **O.PROTCT** objective addresses this threat by providing TOE self-protection from unauthorized modifications and access to its functions and data.

T.LOSSOF: The **O.IDAUTH** objective provides for authentication of users prior to any TOE data access. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE data. The **O.INTEGR** objective ensures no TOE data will be deleted. The **O.PROTCT** objective addresses this threat by providing TOE self-protection.

T.NOHALT: The **OE.PERSON** (administrators carefully selected and trained), **OE.CREDEN** (all access credentials protected), **OE.PHYCAL** (protected access) and **OE.INSTAL** (the TOE is delivered, installed, managed and operated according to IT security) security objectives for the operational environment together provides mitigation to this threat with responsible administrators and forbidden physical access to the TOE. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE functions. The **O.IDSCAN**, **O.IDSENS**, and **O.IDANLZ** objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL: The **OE.PERSON** (administrators carefully selected and trained), **OE.CREDEN** (all access credentials protected), **OE.PHYCAL** (protected access) and **OE.INSTAL** (the TOE is delivered, installed, managed and operated according to IT security) security objectives for the operational environment together provides mitigation to this threat with responsible administrators and forbidden physical access to the TOE. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE functions. The **O.PROTCT** objective addresses this threat by providing TOE self-protection.

T.IMPCON: The **OE.PERSON** (administrators carefully selected and trained), **OE.CREDEN** (all access credentials protected), **OE.PHYCAL** (protected access) and **OE.INSTAL** (the TOE is delivered, installed, managed and operated according to IT security) security objectives for the operational environment together provides mitigation to this threat with responsible administrators and forbidden physical access to the TOE. The **O.EADMIN** objective ensures the TOE has all the necessary administrator functions to manage the product. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE functions.

T.INFLUX: The **O.OFLOWS** objective counters this threat by requiring the TOE handle data storage overflows.

T.FACCNT: The **O.AUDITS** objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

T.SCNCFG: The **O.IDSCAN** objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

T.SCNVUL: The **O.IDSCAN** objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

T.FALACT: The **O.RESPON** objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC: The **O.IDANLZ** objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC: The **O.IDANLZ** objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

T.MISUSE: The **O.AUDITS** and **O.IDSENS** objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.INADVE: The **O.AUDITS** and **O.IDSENS** objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.COMINT	O.IDAUTH O.ACCESS O.INTEGR O.PROTCT O.TIME OE.TIME
T.COMDIS	O.IDAUTH O.ACCESS O.PROTCT
T.LOSSOF	O.IDAUTH O.ACCESS O.INTEGR O.PROTCT

Threats	Security Objectives
T.NOHALT	O.IDAUTH O.ACCESS O.IDSCAN O.IDSENS O.IDANLZ OE.PERSON OE.CREDEN OE.PHYCAL OE.INSTAL
T.PRIVIL	O.IDAUTH O.ACCESS O.PROTCT OE.PERSON OE.CREDEN OE.PHYCAL OE.INSTAL
T.IMPCON	O.EADMIN O.IDAUTH O.ACCESS OE.PERSON OE.CREDEN OE.PHYCAL OE.INSTAL
T.INFLUX	O.OFLOWS
T.FACCNT	O.AUDITS
T.SCNCFG	O.IDSCAN
T.SCNVUL	O.IDSCAN
T.FALACT	O.RESPON

Threats	Security Objectives
T.FALREC	O.IDANLZ
T.FALASC	O.IDANLZ
T.MISUSE	O.AUDITS O.IDSENS
T.INADVE	O.AUDITS O.IDSENS

Table 7 Threats vs Security Objectives

4.3.2 Organizational Security Policies

P.DETECT: The **O.AUDITS**, **O.IDSENS**, and **O.IDSCAN** objectives address this policy by requiring collection of audit, Sensor, and Scanner data. **OE.TIME** supports this OSP providing an accurate time and date to the part of the TOE where the NTP server is installed while **O.TIME** ensures that this NTP server provides an accurate time and date to other parts of the TOE acting as clients.

P.ANALYZ: The **O.IDANLZ** objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.MANAGE: The **OE.PERSON** objective ensures competent administrators will manage the TOE and the **O.EADMIN** objective ensures there is a set of functions for administrators to use. The **OE.INSTAL** objective supports the **OE.PERSON** objective by ensuring administrator follow all provided documentation and maintain the security policy. The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE functions. The **OE.CREDEN** objective requires administrators to protect all authentication data. The **O.PROTCT** objective addresses this policy by providing TOE self-protection.

P.ACCESS: The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses. The **O.ACCESS** objective builds upon the **O.IDAUTH** objective by only permitting authorized users to access TOE functions. The **O.PROTCT** objective addresses this policy by providing TOE self-protection. **O.AUDIT_PROTECTION** supports this objective by providing protection for audit data.

P.ACCACT: The **O.AUDITS** objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The **O.IDAUTH** objective supports this objective by ensuring each user is uniquely identified and authenticated. **O.AUDIT_SORT** supports this objective by allowing the administrator to sort audit data providing for user accountability.

OE.TIME and **O.TIME** together supports this OSP providing an accurate time and date.

P.INTGTY: The **O.INTEGR** objective ensures the protection of data from modification.

P. PROTCT: The **O.OFLOWS** objective counters this policy by requiring the TOE handle disruptions. The **OE.PHYCAL** objective protects the TOE from unauthorized physical modifications.

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.DETECT	O.AUDITS O.IDSENS O.IDSCAN O.TIME OE.TIME
P.ANALYZ	O.IDANLZ
P.MANAGE	O.EADMIN O.IDAUTH O.ACCESS O.PROTCT OE.PERSON OE.INSTAL OE.CREDEN
P.ACCESS	O.IDAUTH O.ACCESS O.PROTCT O.AUDIT_PROTECTION
P.ACCACT	O.AUDITS O.IDAUTH O.AUDIT_SORT O.TIME OE.TIME
P.INTGTY	O.INTEGR
P. PROTCT	O.OFLOWS OE.PHYCAL

Table 8 OSPs vs Security Objectives

4.3.3 Assumptions

A.ACCESS: The OE.INTROP objective ensures the TOE has the needed access.

A.DYNMIC: The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.

A.ASCOPE: The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT: The OE.PHYCAL provides for the physical protection of the TOE software and the hardware where it runs, including administration workstations and OOB network.

A.LOCATE: The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE: The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE

A.NOEVIL: The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST: The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.TIME: This assumption is directly covered by OE.TIME. OE.PERSON

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.ACCESS	OE.INTROP
A.DYNMIC	OE.INTROP OE.PERSON
A.ASCOPE	OE.INTROP
A.PROTCT	OE.PHYCAL
A.LOCATE	OE.PHYCAL
A.MANAGE	OE.PERSON

Assumptions	Security Objectives
A.NOEVIL	OE.INSTAL OE.PHYCAL OE.CREDEN
A.NOTRST	OE.PHYCAL OE.CREDEN
A.TIME	OE.TIME OE.PERSON

Table 9 Assumptions vs Security Objectives for the Operational Environment

5 Extended Components Definition

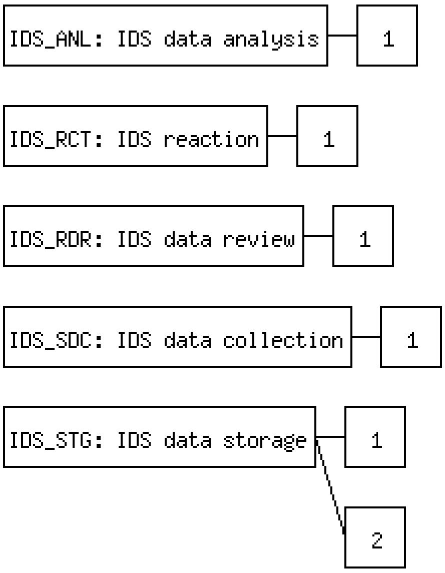
5.1 Class IDS: Intrusion Detection

Introduction

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.

Informative notes

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


IDS_ANL: IDS data analysis
1
IDS_RCT: IDS reaction
1
IDS_RDR: IDS data review
1
IDS_SDC: IDS data collection
1
IDS_STG: IDS data storage
1
2

5.1.1 IDS data analysis (IDS_ANL)

Family behavior

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

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 FAU_GEN is included in the PP/ST:
a) Minimal: Enabling and disabling of any of the analysis mechanisms.

IDS_ANL.1: Analyser analysis

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

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]***

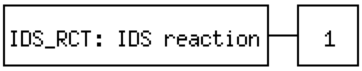
IDS_ANL.1.2: ***The System shall record within each analytical result at least the following information: a) Date and time of the result, type of result, identification of data source; and b) [assignment: any other security relevant information about the result] .***

5.1.2 IDS reaction (IDS_RCT)

Family behavior

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

Component levelling



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 FAU_GEN is included in the PP/ST:
a) Minimal: Actions taken due to detected intrusions.

IDS_RCT.1: Analyser react

Hierarchical to:

No other components.

Dependencies:

IDS_ANL.1

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 behavior

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 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 FAU_GEN 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.

IDS_RDR.1: Restricted data review

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

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 behavior

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

Component levelling

IDS_SDC: IDS data collection
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.

IDS_SDC.1: System data collection

Hierarchical to:

No other components.

Dependencies:

FPT_STM.1

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

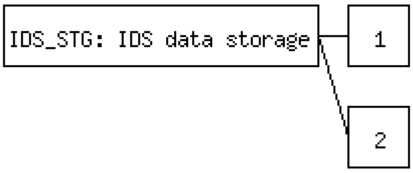
IDS_SDC.1.2: ***At a minimum, the System shall collect and record the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) [assignment: other additional information]***

5.1.5 IDS data storage (IDS_STG)

Family behavior

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

Component levelling



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

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.

IDS_STG.1: Guarantees of System data availability

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

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]***

IDS_STG.2: Prevention of System data loss

Hierarchical to:

No other components.

Dependencies:

IDS_STG.1

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.***

5.2 Class FCS: Cryptographic support

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

The FCS class is composed of two families: FCS_CKM and FCS_COP. The FCS_CKM family addresses the management aspects of cryptographic keys, while the FCS_COP family is concerned with the operational use of those cryptographic keys.

This class is extended to satisfy security objectives that pertain to secure handling, transport and disposal of sensitive IDS target systems data. These include protection of data related to the systems that the IDS protects or audits and ensuring that the data is available to the appropriate personal.

5.2.1 Random Bit Generation (FCS_RBG)

Family behavior

The requirements of this family ensure that the TSF will generate random numbers in accordance with an approved cryptographic standard.

Component levelling

FCS_RBG: Random Bit Generation
1

This SFR requires the TOE to perform random bit generation in accordance with a defined standard.

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:
a) Basic: Failure of the randomization process.

FCS_RBG.1: Random Bit Generation

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FCS_RBG.1.1: ***The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using Hash_DRBG (any), NIST Special Publication 800-90 using HMAC_DRBG (any), NIST Special Publication 800-90 using CTR_DRBG (AES), FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection, choose one of: a software-based noise source, a TSF-hardware-based noise source,]***

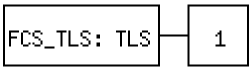
FCS_RBG.1.2: ***The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate***

5.2.2 TLS (FCS_TLS)

Family behavior

The requirements of this family ensure that the TSF will implement the TLS protocol in accordance with an approved cryptographic standard.

Component levelling



This SFR requires the TOE to implement TLS in accordance with a defined standard.

Management: FCS_TLS.1

There are no management activities foreseen.

Audit: FCS_TLS.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:
a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

FCS_TLS.1: TLS

Hierarchical to:

No other components.

Dependencies:

FCS_COP.1

FCS_TLS.1.1: ***The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA Optional Ciphersuites: [selection: None, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,***

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,]

5.2.3 HTTPS (FCS_HTT)

Family behavior

The requirements of this family ensure that the TSF will implement the HTTPS protocol in accordance with an approved cryptographic standard.

Component levelling

FCS_HTT: HTTPS
1

This SFR requires the TOE to implement HTTPS in accordance with a defined standard.

Management: FCS_HTT.1

There are no management activities foreseen.

Audit: FCS_HTT.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:
a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

FCS_HTT.1: HTTPS

Hierarchical to:

No other components.

Dependencies:

FCS_TLS.1

FCS_HTT.1.1: ***The TSF shall implement the HTTPS protocol that complies with RFC 2818.***

FCS_HTT.1.2: ***The TSF shall implement HTTPS using TLS as specified in FCS_TLS.1.***

5.2.4 SSH Protocol (FCS_SSH)

Family behavior

This family identifies the behavior of the TOE when the SSH protocol is implemented. The TOE must implement one or more of the identified protocols and ciphersuites.

The FCS_SSH family contains one component with 6 elements.

Component levelling

This SFR requires the TOE to implement the SSH protocol.

Management: FCS_SSH.1

There are no management activities foreseen.

Audit: FCS_SSH.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:
Basic:
a) Failure to establish an SSH Session
b) Establishment/Termination of an SSH session

FCS_SSH.1: SSH Protocol

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FCS_SSH.1.1: ***The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [selection: 5656, 6668, no other RFCs]***

FCS_SSH.1.2: ***The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based, none]***

FCS_SSH.1.3: ***The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.***

FCS_SSH.1.4: ***The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: aes128-cbc, aes256-cbc, [selection: aes256-ctr, aes192-ctr, aes128-ctr, blowfish-ctr, aes192-cbc, blowfish-cbc, 3des-ctr, 3des-cbc, AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms]***

FCS_SSH.1.5: ***The TSF shall ensure that the SSH transport implementation uses [selection: SSH_RSA, ecdsa-sha2-nistp256] and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, ecdsa-sha2-nistp384, SSH_DSS, no other public key algorithms]***

FCS_SSH.1.6: ***The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1-96, hmac-sha1, hmac-md5-96, hmac-md5, hmac-sha2-256, hmac-sha2-512]***

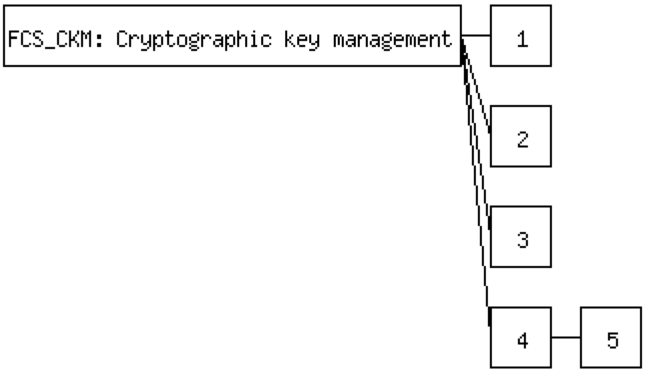
FCS_SSH.1.7: ***The TSF shall ensure that diffie-hellman-group14-sha1 and [selection: diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, no other methods] are the only allowed key exchange methods used for the SSH protocol.***

5.2.5 Cryptographic key management (FCS_CKM)

Family behavior

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

Component levelling



This SFR requires the TOE to zeroize CSPs.

Management: FCS_CKM.5

There are no management activities foreseen.

Audit: FCS_CKM.5

The following actions should be auditable if FAU_GEN is included in the PP/ST:
a) Basic: Failure of the key zeroization process.

FCS_CKM.5: Cryptographic Key Zeroization

Hierarchical to:

FCS_CKM.4

Dependencies:

FCS_CKM.1

FCS_CKM.5.1: ***The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.***

5.3 Class FAU: Security audit

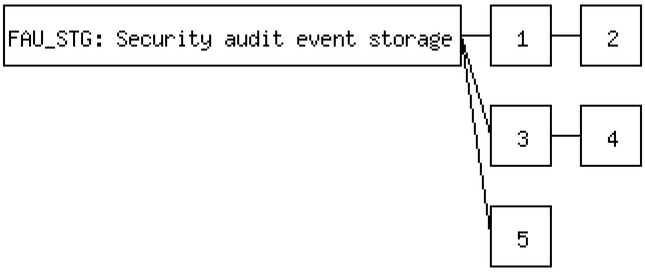
Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities (i.e. activities controlled by the TSF). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.

5.3.1 Security audit event storage (FAU_STG)

Family behavior

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

Component levelling



This requirement allows defining mechanisms that allow exporting or purging of audit data in manual or scheduled ways.

Management: FAU_STG.5

There are no management activities foreseen.

Audit: FAU_STG.5

There are no auditable events foreseen.

FAU_STG.5: Audit export and purge

Hierarchical to:

No other components.

Dependencies:

FAU_GEN.1

FAU_STG.5.1: ***The TSF shall enable [selection: manual, scheduled] [selection: archiving, purging] of audit data.***

6 Security Requirements

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word "assignment" is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Selections. They appear between square brackets. The word "selection" is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Iterations. It includes "/" and an "identifier" following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.
- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 Security Functional Requirements

6.1.1 FAU: Security audit

6.1.1.1 FAU_GEN.1: Audit data generation

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

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

b) All auditable events for the ***[selection: not specified]*** level of audit; and

c) ***[assignment: - All configuration changes. This includes all actions (CUD = Create, Update, Delete) on all entities (policies, users, roles, authentication schema, authorization schema, permissions, access or communication keys, certificates, lists of signatures, lists of IP addresses).***
- Export of information from SecureSphere (configuration export, data sent to cloud for analysis, audit archive).
- Purge of information.
- All actions related to patch and version changes – availability of a new version, installation on a machine, failure to install.
- SecureSphere deployment changes.
- Failover events, MXs registration and removal from SOM, adding or removing agents and gateways, gateway move within group/cluster or out of it, agent move in or out of cluster.

- All actions related to users and permissions – including the above (CUD) – and also accessing these screens.
- Access to the audit screens.

- Failure to upload configuration and access violations.
- Expiry of licenses and certificates.
- All actions of network configuration – IP addresses, interfaces, default route, etc.] .

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[assignment: none]*** .

6.1.1.2 FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide ***[assignment: users with appropriate permissions]*** with the capability to read ***[assignment: 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 FAU_SAR.2: Restricted audit review

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

6.1.1.4 FAU_SAR.3: Selectable audit review

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

6.1.1.5 FAU_STG.2: Guarantees of audit data availability

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

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

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

6.1.1.6 FAU_STG.4: Prevention of audit data loss

FAU_STG.4.1 The TSF shall ***[selection: ``overwrite the oldest stored audit records'']*** and ***[assignment: send an alarm]*** if the audit trail is full.

Application Note

The “overwrite the oldest audit records” action indicates that the oldest audit records (as defined in the Purge Definitions by size option) are marked to be removed (while adding new records) once the purge/archive method, automatically (according Scheduling Definitions configuration) or manually, is executed, these old records will be removed.

6.1.1.7 FAU_STG.5: Audit export and purge

FAU_STG.5.1 The TSF shall enable ***[selection: manual, scheduled] [selection: archiving, purging]*** of audit data.

6.1.2 FCS: Cryptographic support

6.1.2.1 FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***[assignment: NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes]*** and specified cryptographic key sizes ***[assignment: equivalent to, or greater than, a symmetric key strength of 112 bits.]*** that meet the following: ***[assignment: NIST SP 800-56B]*** .

6.1.2.2 FCS_CKM.5: Cryptographic Key Zeroization

FCS_CKM.5.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

6.1.2.3 FCS_COP.1: Cryptographic operation

FCS_COP.1.1 The TSF shall perform ***[assignment: the cryptographic operations listed in Application Note]*** in accordance with a specified cryptographic algorithm ***[assignment: the cryptographic algorithms listed in Application Note]*** and cryptographic key sizes ***[assignment: the cryptographic key sizes listed in Application Note]*** that meet the following: ***[assignment: the standards listed in Application Note]*** .

Application Note

Operation	Alg.	Key Size	Standard
encryption and decryption	AES-CBC	128 and 256 bits	FIPS PUB 197 in CBC mode and [NIST SP 800-38A].
cryptographic signature services	RSA Digital Signature Algorithm (rDSA)	2048 bits or greater	RSA Digital Signature Algorithm FIPS PUB 186-2 or FIPS

			PUB 186-3, “Digital Signature Standard”
cryptographic hashing services	SHA-1, SHA-256, SHA-512	160, 256 and 512 bits	FIPS Pub 180-3, 'Secure Hash Standard.'
keyed-hash message authentication	HMAC-SHA-1	160 bits	FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

Table 10 *Cryptographic Operations*

6.1.2.4 FCS_RBG.1: Random Bit Generation

FCS_RBG.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with ***[selection: NIST Special Publication 800-90 using CTR_DRBG (AES)]*** seeded by an entropy source that accumulates entropy from ***[selection: a software-based noise source]***

FCS_RBG.1.2 The deterministic RBG shall be seeded with a minimum of ***[selection: 256 bits]*** of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate

6.1.2.5 FCS_TLS.1: TLS

FCS_TLS.1.1 The TSF shall implement one or more of the following protocols ***[selection: TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA Optional Ciphersuites: ***[selection: None]***

6.1.2.6 FCS_HTT.1: HTTPS

FCS_HTT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS.1.

6.1.2.7 FCS_SSH.1: SSH Protocol

FCS_SSH.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and ***[selection: 5656]***

FCS_SSH.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, ***[selection: password-based]***

FCS_SSH.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than ***[assignment: 256K]*** bytes in an SSH transport connection are dropped.

FCS_SSH.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: aes128-cbc, aes256-cbc, ***[selection: aes256-ctr, aes192-ctr, aes128-ctr, blowfish-ctr, aes192-cbc, blowfish-cbc, 3des-ctr, 3des-cbc]***

FCS_SSH.1.5 The TSF shall ensure that the SSH transport implementation uses ***[selection: SSH_RSA]*** and ***[selection: SSH_DSS]***

FCS_SSH.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is ***[selection: hmac-sha1-96, hmac-sha1, hmac-md5-96, hmac-md5]***

FCS_SSH.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and ***[selection: diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1]*** are the only allowed key exchange methods used for the SSH protocol.

6.1.3 FIA: Identification and authentication

6.1.3.1 FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: ***[assignment: a) User identity;***
b) Authentication data; and
c) Authorisations] .

6.1.3.2 FIA_UAU.2: User authentication before any action

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 FIA_UID.2: User identification before any action

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 FMT: Security management

6.1.4.1 FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***[selection: modify the behaviour of]*** the functions ***[assignment: of System data collection, analysis and reaction]*** to ***[assignment: authorised System administrators]*** .

6.1.4.2 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to ***[selection: query, modify, [assignment: add]]*** the ***[assignment: System data, audit data and other TOE data]*** to ***[assignment: users with the authorisations as specified in FMT_SMF.1 Application Note]*** .

6.1.4.3 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: as specified in Application Note]*** .

Application Note

Component	Management Function	Required Authorisations	Management Functionality
FMT_MOF.1	Modify the behaviour of the functions of System data collection, analysis and reaction	Authorised System administrator	Authorised System administrators use the SecureSphere GUI interface to modify Server Group definitions, define Action Interfaces and Action Policies, configure Security Rules for each Server Group, enable collection, analysis and reaction capabilities, and manage Profiles and Signatures.
FMT_MTD.1	Query audit data	Authorized administrator with appropriate permissions	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.
	Query and add System data	Authorised administrator with View permission on applicable objects	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.
	Query (export) and modify (create, delete, import) audit archive protection keys	Authorised administrator with Settings permission	Authorised administrators with Settings permission can use the OpenAPI or 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.
	Query and modify all other (non-System and audit) TOE data	Authorised administrator	Authorised administrators can use the OpenAPI or SecureSphere GUI interface for reviewing and modifying all other TOE data (e.g. jobs or tasks).
FMT_SMR.1	Modify the group of users that are part of a SecureSphere role	Authorised System administrator	SecureSphere GUI allows authorised administrators belonging to the Administrators group with access to the Users and Roles screen, providing the ability to add, edit, and delete user accounts, and reset their passwords.

Table 11 Specification of Management Functions

6.1.4.4 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment: authorised System administrators (main System administrator user assigned when first logging to the web), and authorised administrators with one or more of the authorisations identified in FMT_SMF.1]*** .

Application Note

SecureSphere 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 Administrator role, which is granted all permissions, and is the only out of the box role that is allowed to access the screens in the SecureSphere GUI Admin workspace equivalent in order to manage users, roles, and authorisations. In addition, users defined locally in the SOM are considered authorized System administrators, and have authorisations to all management functions identified in FMT_SMF.1 application note table.

The authorized administrator role defined in FMT_SMR.1 corresponds to other roles that are defined without Create/Edit permissions to applicable objects in relation to FMT_MOF.1; if a role is assigned Create permissions, then it is considered an authorized System administrator role in that context.

Therefore, from the CC point of view, there are just two roles managed by the product, the System administrators who can access all the functionality, and the administrators, who based on assigned permissions can access more or less functionality. Every other role described in the product documentation will fall under one of these two categories.

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

6.1.5 FPT: Protection of the TSF

6.1.5.1 FPT_ITT.1: Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from ***[selection: disclosure, modification]*** when it is transmitted between separate parts of the TOE.

6.1.5.2 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note

This SFR is implemented by the TOE using an NTP server in the management server which provides reliable timestamps to its clients.

6.1.6 FTP: Trusted path/channels

6.1.6.1 FTP_TRP.1: Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***[selection: 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 ***[selection: modification, disclosure]*** .

FTP_TRP.1.2 The TSF shall permit ***[selection: remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[selection: [assignment: administrator sessions]]*** .

6.1.7 IDS: Intrusion Detection

6.1.7.1 IDS_ANL.1: Analyser analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received: a) ***[selection: signature, integrity]*** ; and b) ***[assignment: the analysis functions specified in Application Note]***

Application Note

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

Table 12 IDS Analysis 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: Destination Server Group and username (if applicable)]*** .

6.1.7.2 IDS_RCT.1: Analyser react

IDS_RCT.1.1 The System shall send an alarm to ***[assignment: configurable alarm destinations listed in application note]*** and take ***[assignment: action to block and/or monitor applicable network traffic]*** when an intrusion is detected.

Application Note

- Sending a syslog message to a syslog server
- Sending a message to the audit log
- Running a shell command on the intrusion data
- Create an SNMP trap to an SNMP destination
- Create a review task inside SecureSphere for the intrusion

6.1.7.3 IDS_RDR.1: Restricted data review

IDS_RDR.1.1 The System shall provide ***[assignment: users with authorization]*** with the capability to read ***[assignment: Alerts, audit records, discovery and assessment results, collected application profiles, System configuration and Gateway Status]*** 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.

6.1.7.4 IDS_SDC.1: System data collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): ***[selection: identification and authentication events, data accesses, service requests, network traffic, data introduction, access control configuration, detected known vulnerabilities]*** ; and b) ***[assignment: none]***

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: The additional information specified in the Details column of Application Note]***

Application Note

Event	Details
Identification and authentication events	User identity, location, source address, destination address
Data accesses	Object IDs, requested access, source address, destination address
Service requests	Specific service, source address, destination

	address
Network traffic	Protocol, source address, destination address
Access control configuration	Location, access settings
Detected known vulnerabilities	Identification of the known vulnerability

Table 13 *System Events*

6.1.7.5 IDS_STG.1: Guarantees of System data availability

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: 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: ***[selection: System data storage exhaustion]***

6.1.7.6 IDS_STG.2: Prevention of System data loss

IDS_STG.2.1 The System shall ***[selection: 'overwrite the oldest stored System data']*** and ***[assignment: send an alarm, backup and purge the older 250000]*** if the storage capacity has been reached.

Application Note

The TOE keeps two tables of 250000 records each, so when it exhausts – it has 500000 records – it backs up the older 250000 and purge them.

6.2 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL3**

The following table shows the assurance requirements by reference the individual components in [CC31R4P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition

Assurance Class	Assurance Components
	ASE_INT.1: ST introduction ASE_TSS.1: TOE summary specification ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_SPD.1: Security problem definition
ALC: Life-cycle support	ALC_CMC.3: Authorisation controls ALC_CMS.3: Implementation representation CM coverage ALC_DEL.1: Delivery procedures ALC_DVS.1: Identification of security measures ALC_LCD.1: Developer defined life-cycle model
ADV: Development	ADV_ARC.1: Security architecture description ADV_FSP.3: Functional specification with complete summary ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_COV.2: Analysis of coverage ATE_DPT.1: Testing: basic design ATE_FUN.1: Functional testing ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 14 Security Assurance Requirements

6.3 Security Requirements Rationale

6.3.1 Necessity and sufficiency analysis

SFR / TOE Security Objective	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	O.TIME
FAU_GEN.1										X				

SFR / TOE Security Objective	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	O.TIME
FAU_SAR.1						X								
FAU_SAR.2							X	X						
FAU_SAR.3													X	
FAU_STG.2	X						X	X	X		X	X		
FAU_STG.4									X	X				
FCS_CKM.1	X						X				X			
FCS_COP.1	X						X				X			
FIA_ATD.1								X						
FIA_UAU.2							X	X						
FIA_UID.2							X	X						
FMT_MOF.1	X						X	X						
FMT_MTD.1	X						X	X			X			
FMT_SMF.1	X					X	X	X						
FMT_SMR.1								X						
FPT_ITT.1	X										X			
FTP_TRP.1	X													
IDS_SDC.1		X	X											
IDS_ANL.1				X										
IDS_RCT.1					X									

SFR / TOE Security Objective	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	O.TIME
IDS_STG.1	X						X	X	X		X			
IDS_STG.2									X					
FPT_STM.1														X
FCS_TLS.1	X						X				X			
FCS_SSH.1		X												
FCS_HTT.1							X				X			
FCS_CKM.5	X						X				X			
FCS_RBG.1	X						X				X			
FAU_STG.5									X	X				
IDS_RDR.1						X	X	X						

Table 15 SFRs / TOE Security Objectives coverage

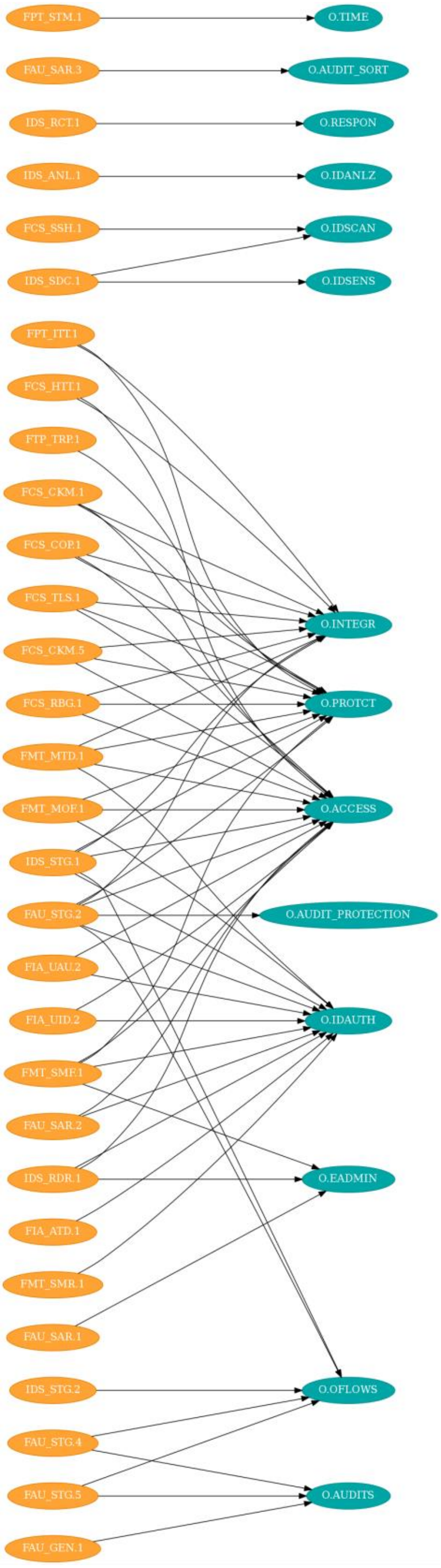


Figure 8 Mapping of SFRs to TOE Security Objectives

6.3.2 Security Requirement Sufficiency

O.PROTCT: The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**, **FMT_SMF.1**]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [**FMT_MTD.1**]. The TOE provides a trusted path for remote users initiating communication for administrator sessions, protecting OpenAPI and SecureSphere GUI data and functions from unauthorized access over the network [**FTP_TRP.1**]. It also prevents unauthorized modifications and access for TSF data transmitted between the separate parts of the TOE [**FPT_ITT.1**] (that is, the MX and the agent). This requires some cryptographic capabilities [**FCS_CKM.1**, **FCS_TLS.1**, **FCS_CKM.5**, **FCS_COP.1**, **FCS_RBG.1**]. The TOE provides cryptographic verification for ADC content updates loaded [**FCS_COP.1**]

O.IDSCAN: A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [**IDS_SDC.1**].

SSH connections to monitored system allows discovery and assessment of misconfiguration and vulnerable versions. [**FCS_SSH.1**]

O.IDSENS: A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [**IDS_SDC.1**].

O.IDANLZ: The Analyzer is required to perform intrusion analysis and generate conclusions [**IDS_ANL.1**].

O.RESPON: The TOE is required to respond accordingly in the event an intrusion is detected [**IDS_RCT.1**].

O.EADMIN: The TOE must provide the ability to review and manage the audit trail of the System [**FAU_SAR.1**]. The System must provide the ability for authorized administrators to view all System data collected and produced [**IDS_RDR.1**]. The TOE includes a set of functions that allow effective management of TOE functions and data [**FMT_SMF.1**].

O.ACCESS: Users authorized to access the TOE are defined using an identification and authentication process [**FIA_UID.2**, **FIA_UAU.2**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**, **FMT_SMF.1**]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the may query and modify all other data [**FMT_MTD.1**].

The connection to the user interface cannot be modified or intercepted because secure access mechanisms are implemented [**FCS_HTT.1**, **FCS_TLS.1**, **FCS_CKM.5**, **FCS_RBG.1**].

The TOE is required to restrict the review of audit data to those granted with explicit read-access [**FAU_SAR.2**]. The System is required to restrict the review of System data to those granted with explicit read-access [**IDS_RDR.1**], archived audit data is encrypted [**FCS_CKM.1**, **FCS_COP.1**]. The

TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion [**IDS_STG.1**].

O.IDAUTH: The TOE is required to restrict the review of audit data to those granted with explicit read-access [**FAU_SAR.2**]. The System is required to restrict the review of System data to those granted with explicit read-access [**IDS_RDR.1**]. The TOE is required to protect the stored audit records from unauthorized deletion [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [**FIA_ATD.1**]. Users authorized to access the TOE are defined using an identification and authentication process [**FIA_UID.2**, **FIA_UAU.2**]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [**FMT_MOF.1**, **FMT_SMF.1**]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [**FMT_MTD.1**]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [**FMT_SMR.1**].

O.OFLOWS: The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The TOE must prevent the loss of audit data in the event its audit trail is full [**FAU_STG.4**, **FAU_STG.5**]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [**IDS_STG.1**]. The System must prevent the loss of audit data in the event its audit trail is full [**IDS_STG.2**].

O.AUDITS: Security-relevant events must be defined and auditable for the TOE [**FAU_GEN.1**]. The TOE must prevent the loss of collected data in the event the its audit trail is full [**FAU_STG.4**, **FAU_STG.5**].

O.INTEGR: The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**]. The System is required to protect the System data from any modification and unauthorized deletion [**IDS_STG.1**]. Only authorized administrators of the System may query or add audit and System data [**FMT_MTD.1**]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between separated parts of the TOE [**FPT_ITT.1**, **FCS_COP.1**, **FCS_TLS.1**, **FCS_CKM.5**, **FCS_CKM.1**] (that is, the MX and the agent) or when accessed by the users [**FCS_COP.1**, **FCS_TLS.1**, **FCS_HTT.1**, **FCS_RBG.1**].

O.AUDIT_PROTECTION: The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [**FAU_STG.2**].

O.AUDIT_SORT: The TOE must provide the ability to review and manage the audit trail of the System to include sorting the audit data [**FAU_SAR.3**].

O.TIME: The NTP server in the management server provides a reliable time source [**FPT_STM.1**].

6.3.3 SFR Dependency Rationale

6.3.3.1 Table of SFR dependencies

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	None
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	None
FAU_STG.2	FAU_GEN.1	FAU_GEN.1	None
FAU_STG.4	FAU_STG.1	FAU_STG.2 (h.a. FAU_STG.1)	None
FCS_CKM.1	FCS_CKM.4, [FCS_CKM.2 or FCS_COP.1]	FCS_CKM.5 (h.a. FCS_CKM.4), FCS_COP.1	None
FCS_COP.1	FCS_CKM.4, [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.5 (h.a. FCS_CKM.4), FCS_CKM.1	None
FIA_ATD.1	None	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FIA_UID.2	None	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FPT_ITT.1	None	None	None
FTP_TRP.1	None	None	None
IDS_SDC.1	FPT_STM.1	FPT_STM.1	None
IDS_ANL.1	IDS_SDC.1	IDS_SDC.1	None
IDS_RCT.1	IDS_ANL.1	IDS_ANL.1	None
IDS_STG.1	IDS_SDC.1	IDS_SDC.1	None
IDS_STG.2	IDS_STG.1	IDS_STG.1	None
FPT_STM.1	None	None	None
FCS_TLS.1	FCS_COP.1	FCS_COP.1	None
FCS_SSH.1	None	None	None
FCS_HTT.1	FCS_TLS.1	FCS_TLS.1	None

SFR	Required	Fulfilled	Missing
FCS_CKM.5	FCS_CKM.1	FCS_CKM.1	None
FCS_RBG.1	None	None	None
FAU_STG.5	FAU_GEN.1	FAU_GEN.1	None
IDS_RDR.1	IDS_SDC.1	IDS_SDC.1	None

Table 16 SFR Dependencies

6.3.4 SAR Rationale

The level of assurance chosen for this ST is commensurate to the assurance levels required for this kind of product and market demands.

6.3.5 SAR Dependency Rationale

6.3.5.1 Table of SAR dependencies

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2 (hierarchically above ASE_REQ.1)	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (hierarchically above ASE_REQ.1), ADV_FSP.3 (hierarchically above ADV_FSP.1)	None
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	ALC_CMS.3 (hierarchically above ALC_CMS.1), ALC_DVS.1, ALC_LCD.1	None
ALC_CMS.3	None	None	None
ADV_FSP.3	ADV_TDS.1	ADV_TDS.2 (hierarchically above ADV_TDS.1)	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.3 (hierarchically above ADV_FSP.1)	None

SAR	Required	Fulfilled	Missing
AGD_PRE.1	None	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.3 (hierarchically above ADV_FSP.2), AGD_OPE.1, AGD_PRE.1, ATE_COV.2 (hierarchically above ATE_COV.1), ATE_FUN.1	None
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.3 (hierarchically above ADV_FSP.2), ADV_TDS.2 (hierarchically above ADV_TDS.1), AGD_OPE.1, AGD_PRE.1	None
ASE_SPD.1	None	None	None
ALC_DEL.1	None	None	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.3 (hierarchically above ADV_FSP.1), ADV_TDS.2 (hierarchically above ADV_TDS.1)	None
ADV_TDS.2	ADV_FSP.3	ADV_FSP.3	None
ALC_DVS.1	None	None	None
ALC_LCD.1	None	None	None
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.3 (hierarchically above ADV_FSP.2), ATE_FUN.1	None
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.2 (hierarchically above ATE_COV.1)	None

Table 17 SAR dependencies

7 TOE Summary Specification

7.1 Security Audit (FAU)

FAU_GEN.1	The MX Management Server described in section 1.4.4.1.2 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, OpenAPI and 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). 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.
FAU_SAR.1 **FAU_SAR.2**	The SecureSphere GUI allows users to read audit information from the audit records using a Web-based interface. Users without access authorisations to OpenAPI or SecureSphere GUI cannot view audit records.
FAU_SAR.3	SecureSphere GUI allow 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.
FAU_STG.2 **FAU_STG.4** **FAU_STG.5**	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.

7.2 Cryptographic support (FCS)

FCS_CKM.1

FCS_CKM.5

FCS_COP.1

FCS_HTT.1

FCS_RBG.1

FCS_SSH.1

FCS_TLS.1

The TOE provides a FIPS mode, which must be enabled in the evaluated configuration. The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions. The TOE uses the RSA Crypto-J version 6.1.2 and FIPS 140-2 OpenSSL version 1.0.2h with FIPS canister version FIPS 2.0.12 (cert #2398) cryptomodules for all of the cryptographic functionality. The following functions have been certified in accordance with the identified standards.

Function	Algorithm	Options	Cert #
Random Number Generation; Symmetric key generation	[SP 800--90] DRBG Prediction resistance supported for all variations	Hash DRBG HMAC DRBG, no reseed CTR DRBG (AES), no derivation function	607 723 845 1027 1182 1256 1414 1451
Encryption, Decryption and CMAC	[SP 800--67]	3-Key TDES TECB, TCBC, TCFB, TOFB; CMAC generate and verify	1780 1853 1942 2086 2190 2263 2366 2399
	[FIPS 197] AES [SP 800--38B] CMAC [SP 800--38C] CCM [SP 800--38D] GCM [SP 800--38E] XTS	128/ 192/256 ECB, CBC, OFB, CFB 1, CFB 8, CFB 128, CTR, XTS; CCM; GCM; CMAC generate and verify	3090 3264 3451 3751 3990 4141 4391 4469
Message Digests	[FIPS 180--3]	SHA-1, SHA-2 (224, 256, 384, 512)	2553 2702 2847 3121 3294

			3411 3620 3681
Keyed Hash	[FIPS 198] HMAC	SHA-1, SHA-2 (224, 256, 384, 512)	1937 2063 2197 2452 2605 2714 2918 2966
Digital Signature and Asymmetric Key Generation	[FIPS 186--2] RSA	GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS, SigVer9.31, SigVerPKCS1.5, SigVerPSS (2048/3072/4096 with all SHA-2 sizes)	1581 1664 1766 1928 2048 2258 2374 2444
	[FIPS 186--4] DSA	PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver (1024/2048/3072 with all SHA-2 sizes)	896 933 970 1040 1085 1124 1170 1195
	[FIPS 186--2] ECDSA	PKG: CURVES(P-224 P-384 P-521 K-233 K283 K-409 K-571 B-233 B-283 B-409 B-571) PKV: CURVES(P-192 P-224 P-256 P-384 P521 K-163 K-233 K-283 K-409 K-571 B-163 B233 B-283 B-409 B-571)	558 620 698 801 886 952 1050 1091
	[FIPS 186--4] ECDSA	PKG: CURVES(P-224 P-256 P-384 P-521 K224 K-256 K-384 K-521 B-224 B-256 B-384 B521 ExtraRandomBits TestingCandidates) PKV: CURVES(ALL-P ALL-K ALL-B) SigGen: CURVES(	558 620 698 801 886

		P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) P-521: (SHA-224, 256, 384, 512) K-233: (SHA-224, 256, 384, 512) K-283: (SHA-224, 256, 384, 512) K-409: (SHA-224, 256, 384, 512) K-571: (SHA-224, 256, 384, 512) B-233: (SHA-224, 256, 384, 512) B-283: (SHA-224, 256, 384, 512) B-409: (SHA224, 256, 384, 512) B-571: (SHA-224, 256, 384, 512)) SigVer: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P256: (SHA-1, 224, 256, 384, 512) P-384: (SHA1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: (SHA-1, 224, 256, 384, 512 B-163: (SHA-1, 224, 256, 384, 512) B233: (SHA-1, 224, 256, 384, 512) B-283: (SHA1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512))	952 1050 1091
ECC CDH (KAS)	[SP 800--56A] (§5.7.1.2)	All NIST defined B, K and P curves except sizes 163 and 192	372 472 534 699 814 947 1094 1181

Table 18 FIPS Approved Cryptographic Functions supported by OpenSSL

Functions	Standards	Certificates (openSSL)

Asymmetric key generation		
Domain parameter generation (key size 2048 bits)	NIST Special Publication 800-56B	RSA (Certs. #960, #1086, #1145, #1205, #1237, #1273, #1477, #1535 and #1581);
Encryption/Decryption		
AES CBC (128 and 256 bits)	FIPS PUB 197 NIST SP 800-38A	AES #2249 AES (Certs. #1884, #2116, #2234, #2342, #2394, #2484, #2824, #2929 and #3090)
Cryptographic signature services		
RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2 FIPS PUB 186-3	RSA #1154 RSA (Certs. #960, #1086, #1145, #1205, #1237, #1273, #1477, #1535 and #1581);
Cryptographic hashing		
SHA-1 (digest sizes 160 bits) SHA-256 (digest sizes 256 bits) SHA-512 (digest sizes 512 bits)	FIPS PUB 180-3	SHS #1938 SHS (Certs. #1655, #1840, #1923, #2019, #2056, #2102, #2368, #2465 and #2553)
Keyed-hash message authentication		

HMAC-SHA-1 (key size 160 bits and digest size 160 bits)	FIPS PUB 198-1 FIPS PUB 180-3	HMAC #1378 HMAC (Certs. #1126, #1288, #1363, #1451, #1485, #1526, #1768, #1856 and #1937)
Random bit generation		
CTR-DRBG(AES) with one independent software-based noise source of 256 bits of non-determinism	NIST Special Publication 800-90A	DRBG # 273 DRBG (Certs. #157, #229, #264, #292, #316, #342, #485, #540 and #607)

Table 19 Cryptographic Functions

The TOE implements a random number generator for RSA key establishment schemes; and for finite-based key establishment (conformant to NIST SP 800-56B).

The Gateway appliances (including virtual appliances) implement a software-based deterministic random bit generator that complies with NIST SP 800-90, using CTR_DRBG (AES) seeded with 256 bits of entropy. On the X10K, X2510, and X8510 appliances, the entropy source is the RDRAND instruction provided by Intel Ivy Bridge-based processors, which is assumed to provide 0.5 bits of entropy per bit sample. The same entropy source is also used on virtual gateway appliances, which require an Ivy Bridge-based processor on the hosting hardware. On X1010, X2010, X4510, and X6510 appliances, the entropy source is an Infineon SLB96xx Trusted Platform Module (TPM) processor, which is assumed to provide 1 bit of entropy per bit sample (i.e., full entropy).

The Management Server appliances (including the virtual Management Server appliance) implement a software-based deterministic random bit generator that complies with NIST SP 800-90, using HMAC_DRBG seeded with 256 bits of entropy. On M110 and M160 appliances, the entropy source is an Infineon SLB96xx Trusted Platform Module (TPM) processor, which is assumed to provide 1 bit of entropy per bit sample (i.e., full entropy).

The TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. The TOE uses the RSA Crypto-J and FIPS 140-2 OpenSSL cryptomodule functions for the zeroization of all ephemeral sensitive data. The TOE itself zeroizes the following secret and private keys when they are no longer required by the TOE.

#	Key/ CSP	Generation/	Description	Storage	Zeroization

	Name	Algorithm			
CSP1	RSA private keys	RSA(2048 bits)	Identity certificates for the security appliance itself and also used in TLS negotiations	Key Store on Disk RAM (plain text)	Overwriting file with a string of the original length of the sensitive data into the same location in the file; then delete.
CSP2	CA Certificates	RSA(2048 bits)	Trusted CAs	Trust Store on Disk RAM (plain text)	Overwriting file with a string of the original length of the sensitive data into the same location in the file; then delete.
CSP3	Domain and DB Credentials, Proxy Credentials	Secret (plain text)	Usernames and passwords for protected machines and their databases	Database (RSA-2048) RAM (plain text) Gateway Disk (RSA-2048) Transit (TLS with secrets generated by RSA-2048 private keys)	Overwrite with a fixed string of zeroes; then delete.
CSP5	SIEM Credentials	Secret	Used for sending syslog	See CSP3	See CSP3

			messages		
CSP6	External Machines Certificates	Various, can be shared secrets of any kind	Public Keys of machines for integration authentication	See CSP3	See CSP3
CSP7	Machine	Secret	admin login	Linux Hash saved on disk	Overwriting file with a string of the original length of the sensitive data into the same location in the file; then delete.
CSP8	Database Credentials	RSA(2048)	SecureSphere Database Access	Disk (RSA-2048) RAM (plain text)	Overwriting file with a string of the original length of the sensitive data into the same location in the file; then delete.

Table 20 *Key/CSP Zeroization Summary*

Administrator passwords for locally defined users are stored as SHA-512 hash in a database located on the MX Management Server.

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.

The TOE uses RSA B-SAFE and OpenSSL FIPS Object Module algorithms: AES (CBC) 128, 256 bit ciphers, in conjunction with HMAC-SHA-1 and RSA signature verification with 2048 bit key sizes. The implementations are in accordance with FIPS PUB 186-3, “Digital Signature Standard”, FIPS Pub 180-3, 'Secure Hash Standard', and FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code'.

	The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1. The TOEs SSH implementation complies with RFCs 4251, 4252, 4253, and 4254, 5656; supports RSA public key algorithm; and supports diffie-hellman-group14-sha1 key exchange method. Both public-key and password based authentication can be configured. The TOE manages a packet counter for each SSH session such that packets larger than the 256K bytes packet limit are dropped. The TOE's HTTPS protocol complies with RFC 2818 and is implemented using TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuite: TLS_RSA_WITH_AES_128_CBC_SHA. 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 and OpenAPI 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.

7.3 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), Hashed Password (if method is SecureSphere) Authorisations – Role assignments, user-specific permissions
FIA_UAU.2	The Web Server component on the Management

FIA_UID.2	Server requires identification and authentication for all SecureSphere GUI and OpenAPI requests. 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. Users may also be identified and authenticated using an X.509 certificate, such as by CAC.

7.4 Security Management (FMT)

FMT_MOF.1 **FMT_SMR.1** **FMT_MTD.1**	As explained above for **FIA_ATD.1**, each authorised administrator may be associated with role(s) and user-specific permissions in the OpenAPI and 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 out-of-the-box 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 access to database audit archiving configuration and key management interfaces.
FMT_SMF.1	The SecureSphere GUI is used by authorised administrators to manage all IDS/IPS System and audit capabilities as described in the SFR application note.

7.5 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 the ST introduction. 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. ST introduction 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, 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. This SFR is also implemented as part of the communication between GW and agents, where a SSL tunnel is configured in order to protect the information from modification and disclosure when traveling through an untrusted network. The cryptographic functionalitiy is provided by the **FCS_COP.1** requirement.
FPT_STM.1	The SecureSphere Management Server and gateways use the system 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. An external NTP server providing a reliable time source is required.

7.6 Trusted path/channels (FTP)

FTP_TRP.1	The TOE provides a trusted path for authorised administrator sessions to the OpenAPI and SecureSphere GUI. The Management Server allows remote users to initiate communication via the trusted path by establishing TLSv1.2 sessions, using RSA for Management Server authentication and a password for authenticating the administrator. This is required for all administrator sessions. Users may also be identified and authenticated using an X.509 certificate, such as by CAC.

7.7 Intrusion Detection (IDS)

IDS_ANL.1

The System performs the analysis functions described in ST Introduction 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.

Alert attributes include the following relevant fields:

- Alert Severity one of: Informative or Low, Medium, or High Severity.
- Time date and time when the Alert was generated.
- Type one of: Firewall, Signature, HTTP Worm, Protocol Violation, Profile Violation, Correlation.
- Aggregated Alert record is an aggregation of multiple network-level events.
- Source IP the source IP address that generated the alert.
- Server Group the name of the destination Server Group.
- 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 12.1 as a result of an ID analysis. Configurable actions include:
    - ○ **Blocking Attacking IP:** Blocking subsequent IP packets with a presumed source address equal to that recorded for the event, for a specified period

	of time. ○ **Blocking Attacking Session:** Blocking subsequent HTTP requests with the same session identifier as was recorded for the event, for a specified period of time. ○ **Block User:** Block subsequent requests associated with the same user as was identified for the event, for a specified period of time. ○ **Dispatch Alert:** Send alarm to specified Action Interfaces (see section 6.1.7.2) including relevant Alert details. ○ **Start Monitoring:** Record all requests/responses from the IP or session recorded for the event, for a specified period of time.
IDS_RDR.1	The OpenAPI and SecureSphere GUI provide authorised administrators with the capability to read System data using a Web-based interface or REST client. 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. 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 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 ST introduction) and from database log collectors (see ST introduction). 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

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	**[NDPP11]** 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 and A events	user identity	user identity			

	location	source IP			
	source address	source IP			
	destination address	server group			
Data accesses	object IDs		query		
	requested access		query		
	source address		source IP address		
	destination address		destination IP address		
Service requests	specific service	service name			
	source address	source IP			
	destination address	server group			
Network traffic	protocol	protocol, service name			
	source address	source IP, source port			
	destination address	server group, destination port			
Access control	location				db/schema or folder and object

configuration					identity
	access settings				permissions or privilege
Detected known vulnerabilities	identification of the known vulnerability			detected known vulnerabilities	

Table 21 Recorded Information Mapping to IDS_SDC.1

IDS_STG.1 **IDS_STG.2**	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 overwrite 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. 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 ST introduction, either manually by the administrator or on an administrator-defined schedule

8 Acronyms

The following table shows the acronyms used in this Security Target

Acronym	Meaning
ST	Security Target
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
IT	Information Technology
OSP	Organizational Security Policy
EAL	Evaluation Assurance Level
DAS	Discovery and Assessment
ADC	Application Defense Center
AES	Advanced Encryption Standard
CAV	Correlated Attack Validation
CLI	Command Line Interface
CM	Configuration Management
CSV	Comma Separated Value
DLP	Data Leak Prevention
GUI	Graphical User Interface
HA	High Availability
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Intrusion Detection
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
NAS	Network Attached Storage
NIC	Network Interface Card
NTP	Network Time Protocol
RFC	Request for Comment
SFP	Security Function Policy

Acronym	Meaning
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
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URMD	User Rights Management for Databases
URMF	User Rights Management for File Servers
UUT	Universal User Tracking
XML	eXtensible Markup Language
TSC	TSF Scope of Control
TSS	TOE Summary Specification

Table 22 Abbreviations

9 Glossary of Terms

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance
Bridge	A layer-two device that forwards frames received from one network segment to another segment, based on their MAC address.
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 12.1 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
Kerberos	An authentication protocol based on cryptographically-generated single-use authenticators.
Intrusion Detection (ID)	Pertaining to techniques which attempt to detect intrusion
Network	Two or more machines interconnected for communications
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.
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.
Universal User Tracking	An Imperva technology that identifies and tracks the user identity across both Web application server and database queries.

Table 23 Glossary of terms

10 Document References

The following table shows the documents referenced in this Security Target

Reference	Document
CC31R4P1	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 1: Introduction and general model
CC31R4P2	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 2: Security functional components
CC31R4P3	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, Part 3: Security assurance components
CEM31R4	Common Criteria Evaluation methodology, Version 3.1, Revision 4
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
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_CN	NIST, Digital Signature Standard (DSS), FIPS PUB 186-2 (+Change Notice) January 27, 2000
NDPP11	Protection Profile for Network Devices, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #3 dated 3 November 2014 and TD0032
IDSPP17	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007

Table 24 List of document references