Reference: 2017-1-INF-2579-v1
Target: Público
Date: 22.11.2018

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-1**
TOE	**Imperva SecureSphere v12.1.0.51_0.25311**
Applicant	**030460133Z - Imperva, Inc.**
References	
	[EXT-4394] ETR vM0

Certification report of the product Imperva SecureSphere v12.1.0.51_0.25311, as requested in [EXT-3241] dated 02/01/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-4394] received on 25/10/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Imperva SecureSphere v12.1.0.51_0.25311.

Imperva SecureSphere protects file, Web and database servers by analysing 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.

Imperva SecureSphere 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.

Developer/manufacturer: Imperva, Inc.

Sponsor: Imperva, Inc.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 EAL3.

Evaluation end date: 25/10/2018.

All the assurance components required by the evaluation level EAL3 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Imperva SecureSphere v12.1.0.51_0.25311, a positive resolution is proposed.

TOE SUMMARY

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.

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.

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.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 according to Common Criteria v3.1 R4.

Class	**Family/Component**
ASE: Security Target Evaluation	ASE_CCL.1 , ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ASE_TSS.1
ADV: Development	ADV_ARC.1, ADV_FSP.3 and ADV_TDS.2
AGD: Guidance documents	AGD_OPE.1 and AGD_PRE.1
ALC: Life cycle support	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1 and ALC_LCD.1
ATE: Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1 and ATE_IND.2
AVA: Vulnerability assessment	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	**Component**
FAU (Security Audit)	FAU_GEN.1 (Data Generation) FAU_SAR.1 (Review)

	FAU_SAR.2 (Review) FAU_SAR.3 (Review) FAU_STG.2 (Storage) FAU_STG.4 (Storage) FAU_STG.5 (Storage)
Cryptographic Support (FCS)	FCS_CKM.1 (Key Management) FCS_CKM.5 (Key Management) FCS_COP.1 (Operation) FCS_HTT.1 (HTTPS) FCS_RBG.1 (Random Bit Generation) FCS_SSH.1 (SSH Protocol) FCS_TLS.1 (TLS)
Identification and Authentication (FIA)	FIA_ATD.1 (User Attribute Definition) FIA_UAU.2 (User Authentication) FIA_UID.2 (User Identification)
Security Management (FMT)	FMT_MOF.1 (Management of Functions in TSF) FMT_MTD.1 (Management of TSF Data) FMT_SMF.1 (Specification of Management Functions) FMT_SMR.1 (Security Management Roles)
Protection of the TSF (FPT)	FPT_ITT.1 (Internal TOE TSF data transfer) FPT_STM.1 (Time Stamps)
Trusted Path/Channel (FTP)	FTP_TRP.1 (Trusted Path)
Intrusion Detection (IDS)	IDS_ANL.1 (IDS data analysis) IDS_RCT.1 (IDS reaction) IDS_RDR.1 (IDS data review) IDS_SDC.1 (IDS data collection)

	IDS_STG.1 (IDS data storage) IDS_STG.2 (IDS data storage)

IDENTIFICATION

Product: Imperva SecureSphere v12.1.0.51_0.25311

Security Target: Imperva SecureSphere 12.1 Security Target v1.1

Protection Profile: None

Evaluation Level: Common Criteria v3.1 R4 EAL3.

SECURITY POLICIES

The use of the product Imperva SecureSphere v12.1.0.51_0.25311 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the [ST], chapter 3.2 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.3 (Assumptions), are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.1 (Threats to Security), do not suppose a risk for the product Imperva SecureSphere v12.1.0.51_0.25311, although the agents implementing attacks have the attack potential according to the Basic attack potential of EAL3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security objectives for the operational environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

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.
  - 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.
  - 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.
- 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.

- 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.
  - Time Updates – the TOE synchronizes its clock with that of an external time server, using the NTP protocol.

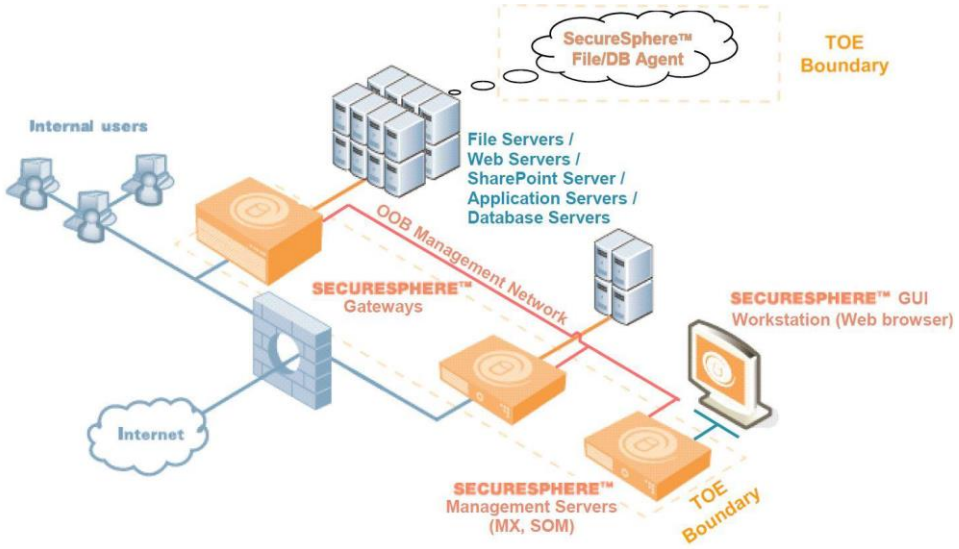

Figure 1. TOE Logical Interactions with its Operational Environment.

PHYSICAL ARCHITECTURE

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 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.

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.

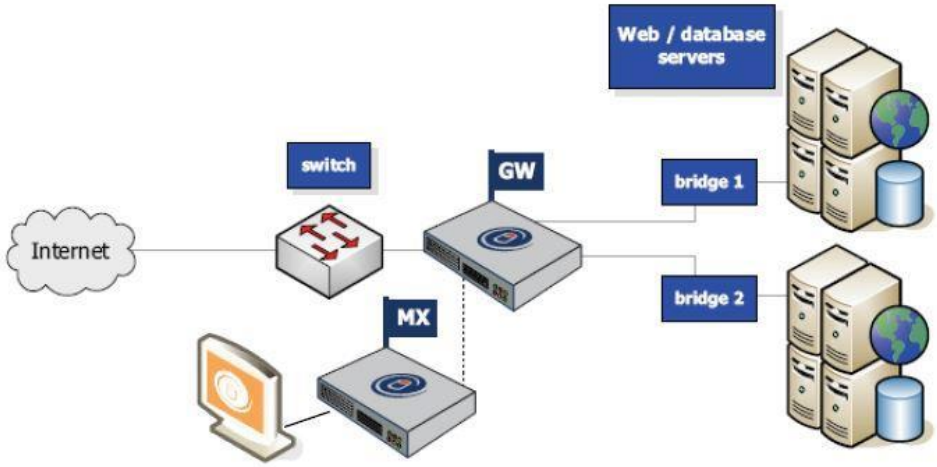

Figure 2. SecureSphere Inline Deployment.

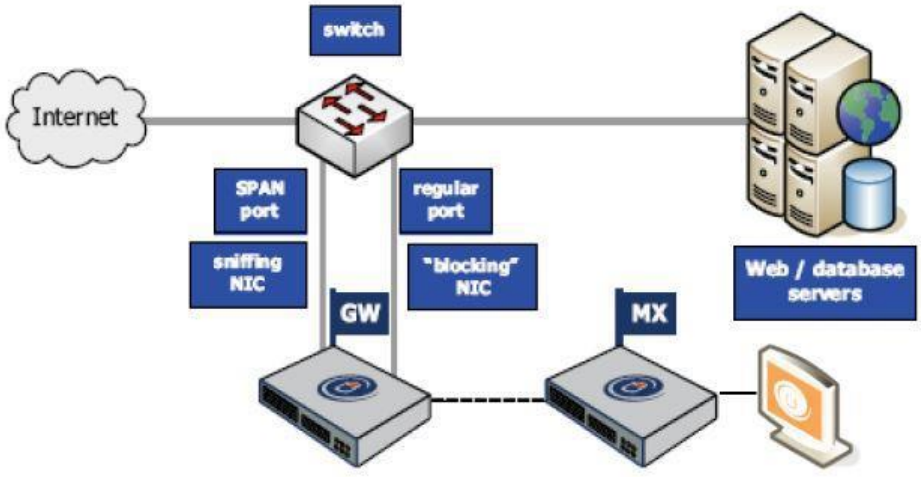

Figure 3. SecureSphere Inline Deployment.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

Imperva SecureSphere Admin Guide Version 12.1 - v5

Imperva SecureSphere Web Security User Guide Version 12.1 - v5

Imperva SecureSphere Database Security User Guide Version 12.1 - v3

Imperva SecureSphere File Security User Guide Version 12.1 - v2

Imperva SecureSphere Security for SharePoint User Guide Version 12.1 - v2

Imperva SecureSphere VMware ESX Configuration Guide 12.1 - v6

Imperva SecureSphere Operations Manager (SOM) User Guide Version 12.1 - v3

Imperva SecureSphere Agent Release Notes 12.1 - v4

Imperva SecureSphere API Configuration Guide User Guide 12.1 - v3

Imperva SecureSphere Directory Services Monitoring User Guide - v2

Imperva SecureSphere 12.1 Evaluated Configuration Guidance - v1.1

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator has devised and executed a test plan where a subset of test which covers the main number of test from the vendor has been repeated. Also the evaluator has devised and executed an independent testing plan to complement the evaluator's tests and give more assurance to the functionality coverage.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Imperva SecureSphere v12.1.0.51_0.25311 it is necessary the disposition of the following software components:

MX Management Server	v12.1.0.51_0.25311
Gateway appliances	v12.1.0.51_0.25311
SecureSphere Operations Manager (SOM) Management Server	v12.1.0.51_0.25311
Agent for Linux	v12.0.0.1084
Agent for Windows	v12.0.0.1085

Regarding the hardware components, the only requirement is that they shall support the software elements previously detailed.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

Appliance	Role	FT	TP	HD	RAM	FF
X2510	Gateway (64 bit) **[GW]**	✓	0.5	500 Gb	16 Gb	2U
M160	Management Server **[MX]**	✓	N/A	2 x 500 Gb	32 Gb	2U

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.

EVALUATION RESULTS

The product Imperva SecureSphere v12.1.0.51_0.25311 has been evaluated against the Security Target Imperva SecureSphere 12.1 Security Target v1.1.

All the assurance components required by the evaluation level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The laboratory gives the following security recommendation for the TOE in operational state:
The Out-Of-Band network plays an important role in the secure functioning of the TOE, as such the laboratory recommends high degree of security in place to protect the network.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

[ST] Imperva SecureSphere 12.1 Security Target v1.1, Date 2018-09-26

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Imperva SecureSphere 12.1 Security Target v1.1 (2018-09-26).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.