National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Imperva SecureSphere v11.5

Report Number: CCEVS-VR-VID10653-2015
Dated: December 23, 2015
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

List of Tables

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160, and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160, and Virtual Machine Appliance: VM150 comprising a common software code base. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Imperva SecureSphere v11.5 Patch 5 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in December 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1.

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160, and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160 and Virtual Machine Appliance: VM150 comprising a common software code base is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Imperva SecureSphere v11.5 Patch 5 software running on two or more of the Imperva appliances listed below, including one or more Management Servers and one or more Gateways:

Hardware appliance:

- Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510
- MX Management Server Appliances: M110, M160

Virtual Machine Appliances:

- V1000, V2500, V4500 (for Gateway)
- VM150 (for MX)

And optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance:

- Appliances: M160

Virtual Machine Appliance: VM150

The network on which it resides is considered part of the operational environment.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	**Identifier**
Evaluated Product	Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160, and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160 and Virtual Machine Appliance: VM150. **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 choses the application to install.
Sponsor & Developer	Imperva Inc. 3400 Bridge Parkway, Suite 200 Redwood Shores, CA 94065 United States
CCTL	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	December 2015
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012

Item	Identifier
PP	Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1.
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160, and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160 and Virtual Machine Appliance: VM150 by any agency of the U.S. Government and no warranty of Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160 and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160 and Virtual Machine Appliance: VM150 is either expressed or implied.
Evaluation Personnel	Greg Beaver Cody Cummins Tony Apted
Validation Personnel	Paul Bicknell Jay Vora

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Imperva SecureSphere Security Target
ST Version	0.4
Publication Date	12 November 2015
Vendor	Imperva Inc.
ST Author	Leidos (formerly SAIC)
TOE Reference	Imperva SecureSphere v11.5 Patch 5 Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 and MX Management Server Appliances: M110, M160, and Virtual Machine Appliances: V1000, V2500, V4500 (for Gateway), VM150 (for MX) and optionally a SecureSphere Operations Manager (SOM) Management Server appliance or Virtual Machine Appliance: Appliances: M160 and Virtual Machine Appliance: VM150
TOE Hardware Models	Gateway Appliances: X1010, X10K, X2010, X2510, X4510, X6510, X8510 MX Management Server Appliances: M110, M160 SecureSphere Operations Manager (SOM) Management Appliance: M160
TOE Virtual Machine Models	V1000, V2500, V4500 (for Gateway) VM150 (for MX or SOM)
TOE Software Version	Imperva SecureSphere v11.5 Patch 5
Keywords	Intrusion Detection System, Intrusion Prevention System

2.1 Threats

The ST references the Protection Profile for Network Devices to identify the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain

unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- User data may be inadvertently sent to a destination not intended by the original sender.

2.2 Organizational Security Policies

The ST references the Protection Profile for Network Devices to identify following organizational security policy that the TOE and its operational environment are intended to fulfill:

- The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3 Architectural Information

The Target of Evaluation (TOE) is a combination of Imperva SecureSphere v11.5 Patch 5 appliances. More specifically, the TOE consists of

- One[1] MX Management Server appliance; and
- One or more Gateway appliances; and optionally:
- One SecureSphere Operations Manager (SOM) Management Server appliance.

SecureSphere v11.5 Patch 5 provides protection from attacks against database, file, Web, and Web Services assets, both within the organization (insider attacks) and from without. Installed on the network as a reverse Hypertext Transfer Protocol (HTTP) proxy, a transparent inline bridge or as an offline network monitor (sniffer), a SecureSphere v11.5 Patch 5 Gateway monitors application-level protocols for attacks, and reacts by blocking the attacks and/or reporting them to a centralized management server.

The TOE is deployed as one Gateway appliance controlled by a MX appliance that in turn is managed by a SecureSphere Operations Manager (SOM) Management Server. The Management Server (MX) and SOM are two different management applications using the same code base, SOM is a manager of MXs. Both MX and SOM are running over M-Appliances (M160), except for M110 which is an MX only appliance.

Administrators connect to the Management/SOM Servers using a standard Web browser (outside of the Target of Evaluation). The TOE authenticates Administrators using a local password based mechanism. Additionally, the TOE can be configured to use the services of a trusted LDAP server in the operational environment.

As noted above, all TOE appliance models run the same software and provide all claimed security functionality.

The TOE generates logs for security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator and can also be configured to send the logs to a designated external log server. The communication channel with the external syslog server is protected using TLS.

The TOE is operated in FIPS mode and includes cryptographic modules from both RSA BSAFE Crypto-J 6.1.3 FIPS 140-2 validated cryptographic module and OpenSSL 2.0.1 FIPS-certified with certificate number 1747.

SecureSphere Deployment Scenarios include 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.

A sniffing gateway is a passive sniffing device. It connects to corporate hubs and switches and taps the traffic sent to and from protected servers, using a SPAN (Switch Port Analyzer) mirror port on the switch, or a dedicated TAP device. Traffic is copied to it instead of passing directly through it. Transmission Control Protocol (TCP) resets are transmitted over a “blocking” Network Interface Card (NIC). For an example of this type of deployment, see the TOE guidance documentation.

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 to four network segments. For examples of deployment types, see the TOE guidance documentation.

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

X1010 and X2010 appliance models have six network interface ports. Two of the ports are used for management: one to connect to the management server and the other is optional. The other four ports are part of two bridges that are used for inline inspection of up to two different protected network segments.

X2510, X4510, X6510, X8510 and X10K appliance models have 2 fixed network interface ports and 2 optional network cards, each card contains two to four network ports. The two fixed ports are used for management: one to connect to the management server and the other is optional. The other optional two cards (each with two to four ports) are part of one to four bridges that are used for inline inspection of up to four different protected network segments.

The MX Management Server Appliances: M110 and M160 each have an RJ45 Connector Serial Port, two USB ports, and two management ports. The appliance models differ only in size of memory and hard drive. While the physical form factor of each appliance differs, the underlying hardware shares a similar architecture.

A given Imperva configuration includes 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. Each Imperva appliance is a self-contained hardware appliance or VM designed to interact with its environment via network connections.

Figure 1 below depicts the TOE in its operational environment. SecureSphere v11.5 Patch 5 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, and the communication between the gateways and the Management Server is protected using HTTPS. SOM Management Servers (not shown) are in the TOE and would be connected to the Management Server and communications protected using HTTPS. The operational environment also requires LDAP, TOE Update, syslog, and NTP servers.

Descriptions of the interconnecting lines in the figure are as follows:

- The Blue Line to the monitor represents the TLS protected communications between the administrator workstation and the MX Management Server.
- The Red Lines represent the TLS protected communications between the TOE components and between instances of a TOE.
- The Orange Lines represent the Internet data filtered and processed by the TOE.

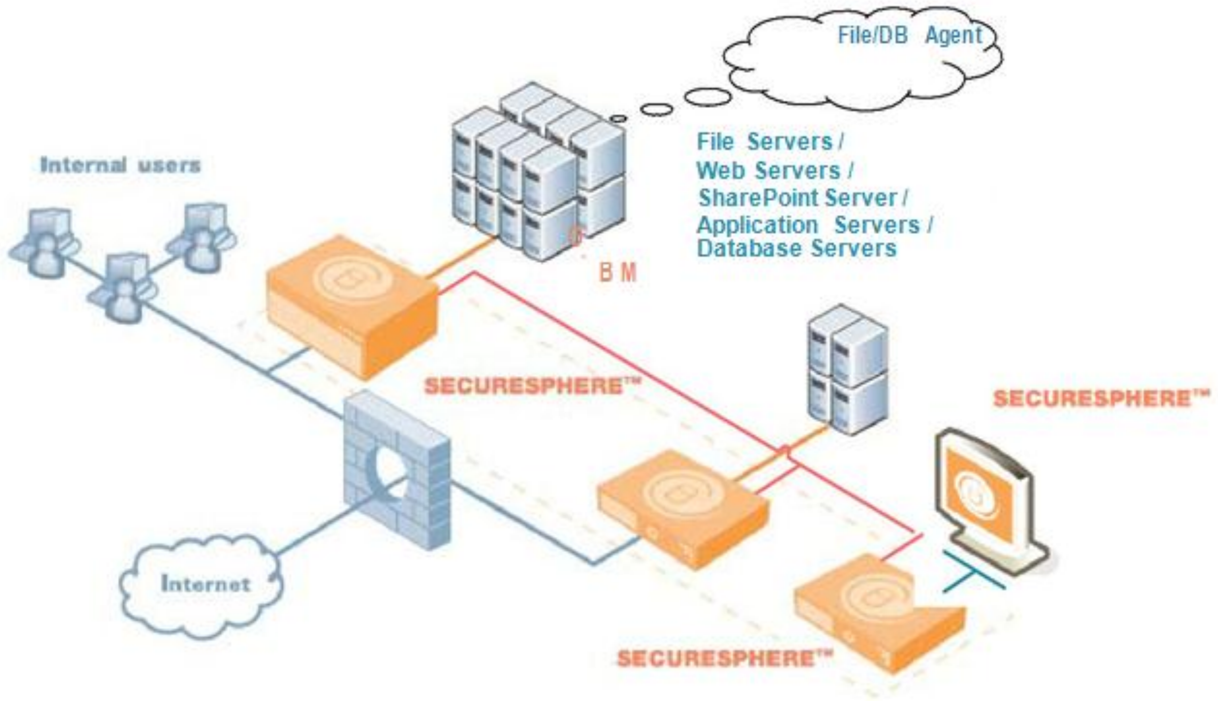

Figure 1 Physical Scope and Boundaries of the TOE

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 (http://en.wikipedia.org/wiki/List_of_Intel_Xeon_microprocessors#Ivy_Bridge-based_Xeons) 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.

The VM appliances also require the following minimums:

	VM150	**V1000**	**V2500**	**V4500**
CPU	2	2	2	4
Memory	4GB	4 GB	4 GB	8 GB
Disk Space	160GB	160 GB	160 GB	160 GB

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

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

- Hardware Security Module (HSM) and SSL Accelerator Cards: SecureSphere v11.5 Patch 5 Gateway appliances may be purchased with an internal HSM or SSL accelerator PCI card that offloads key storage and cryptographic operations used for network traffic deciphering from the appliance CPU. The cards are not included in the evaluated configuration.
- The TOE monitors network traffic between clients and servers in real-time, provides analyses of that traffic for suspected intrusions, and provides a reaction capability. 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. The Imperva Agent software is installed on the client machines to support these features and may be used in the evaluated configuration but the agents are considered to be outside the scope of the TOE and the functionality was not evaluated or tested.
- The VMware ESXi Hypervisor virtualization software and the hardware it is installed on.

4 Assumptions

The ST references the Protection Profile for Network Devices to identify following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. The TOE requires the following components in its operational environment:
    a. Browser: Microsoft Internet Explorer; Chrome, Firefox; or Apple Safari utilizing Adobe Flash in order for an MX Management Client to connect via web-based.
    b. NTP Server - to synchronize its clock with that of the external time server.
    c. Syslog server - to receive audit records when the TOE is configured to deliver them to an external log server.
    d. LDAP servers - the TOE can be configured to use external authentication servers.
    e. Management Workstation - the TOE supports remote access to the CLI over SSHv2. As such, an administrator requires an SSHv2 client to access the CLI remotely.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

5.1 Security Audit

The TOE is designed to be able to generate logs for security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator and can also be configured to send the logs to a designated external log server.

5.2 Cryptographic Support

The TOE is operated in FIPS mode and includes both NIST-validated RSA B-Safe and NIST-validated OpenSSL cryptographic modules. 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.

5.3 User Data Protection

The TOE is designed to ensure that it does not inadvertently reuse data found in network traffic.

5.4 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers a network accessible GUI (HTTP over TLS) and console available locally and remotely via SSH for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of a trusted LDAP server in the operational environment.

5.5 Security Management

The TOE provides remote access to a CLI using SSHv2 and a GUI to access the wide range of security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

The TOE also provides the ability to manage the TOE locally via direct serial console connection. The direct serial console is used mainly for initial configuration and then the TOE is designed to be managed and monitored using the Web GUI from a remote HTTPS/TLS client; or using the CLI from an SSHv2 client. The TOE provides the Administrator role which corresponds to the NDPP Security Administrator.

5.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It 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 synchronizes its clock with that of the external time server.

The TOE uses HTTPS to protect communications between distributed TOE components (FPT_ITT.1).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

5.7 TOE Access

The TOE can be configured to display an informative banner that will appear prior to an administrator being permitted to establish an interactive session. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated. Administrators can also terminate their own sessions by logging out.

5.8 Trusted Path/Channels

The TOE protects interactive communication with remote administrators using SSH or HTTP over TLS. TLS ensures both integrity and disclosure protection.

The TOE uses TLS to ensure that any authentication operations, and exported audit records, are sent only to the configured Syslog or authentication servers so they are not subject to inappropriate disclosure or modification. TLS is also used to ensure TOE updates are transmitted securely.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

- Imperva SecureSphere v11.5 Admin Guide, Version 11.5, August 2015
- Imperva SecureSphere Operations Manager (SOM) User Guide, Version 11.5, August 2015
- Imperva SecureSphere Configuring Common Criteria Compliance User Guide, Version 11.5, December 2015
- Imperva SecureSphere Upgrade Guide, Version 11.5, August 2015

Supporting TOE Guidance Documentation

- Imperva SecureSphere Security Target, Version 0.4, 12 November, 2015

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Evaluation Team Test Report Imperva SecureSphere Common Criteria Test Report and Procedures, Version 0.5, December 11, 2015

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1.

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Leidos facility in Columbia, Maryland from August 26 – September 4, 2015.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1 are fulfilled.

8 Tested Configuration

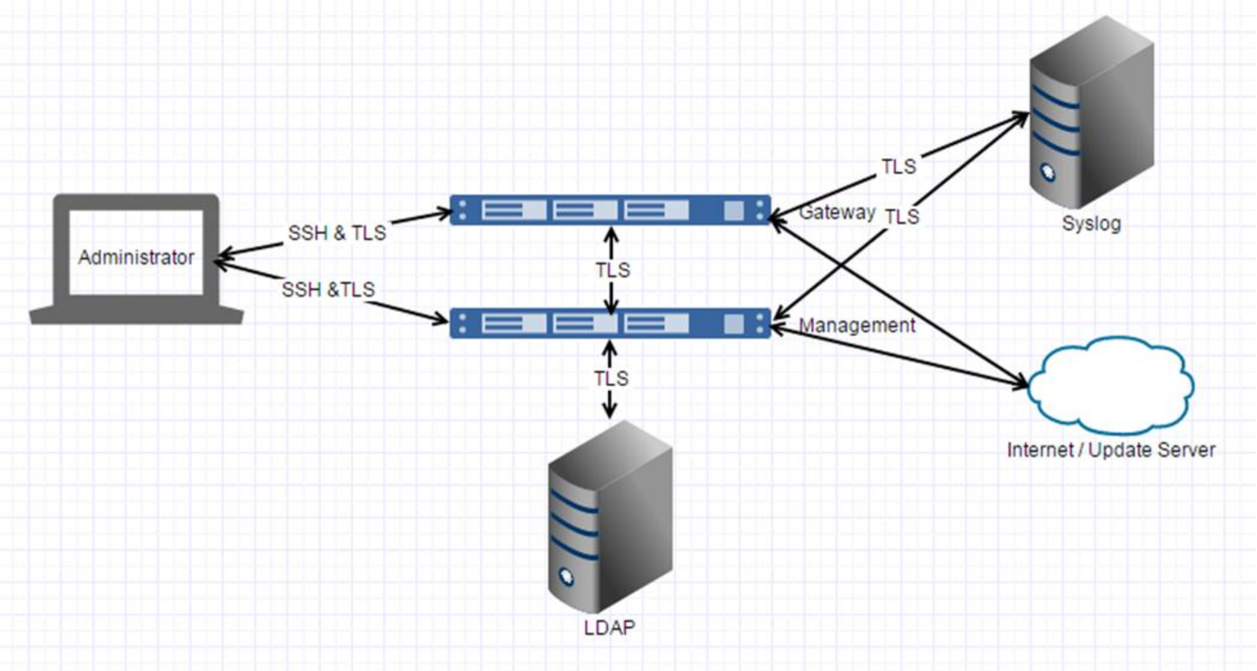

Figure 1 Evaluation Team Evaluated Test Configuration (Hardware)

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

- Hardware/Software
  - One management Server Appliance: M160
  - Three Gateway Appliances: x2010, x4510, x6510

    Note: All three Gateway Appliances were tested and part of the evaluated test configuration. Figure 1 only identifies a single gateway appliance to simply the drawing.

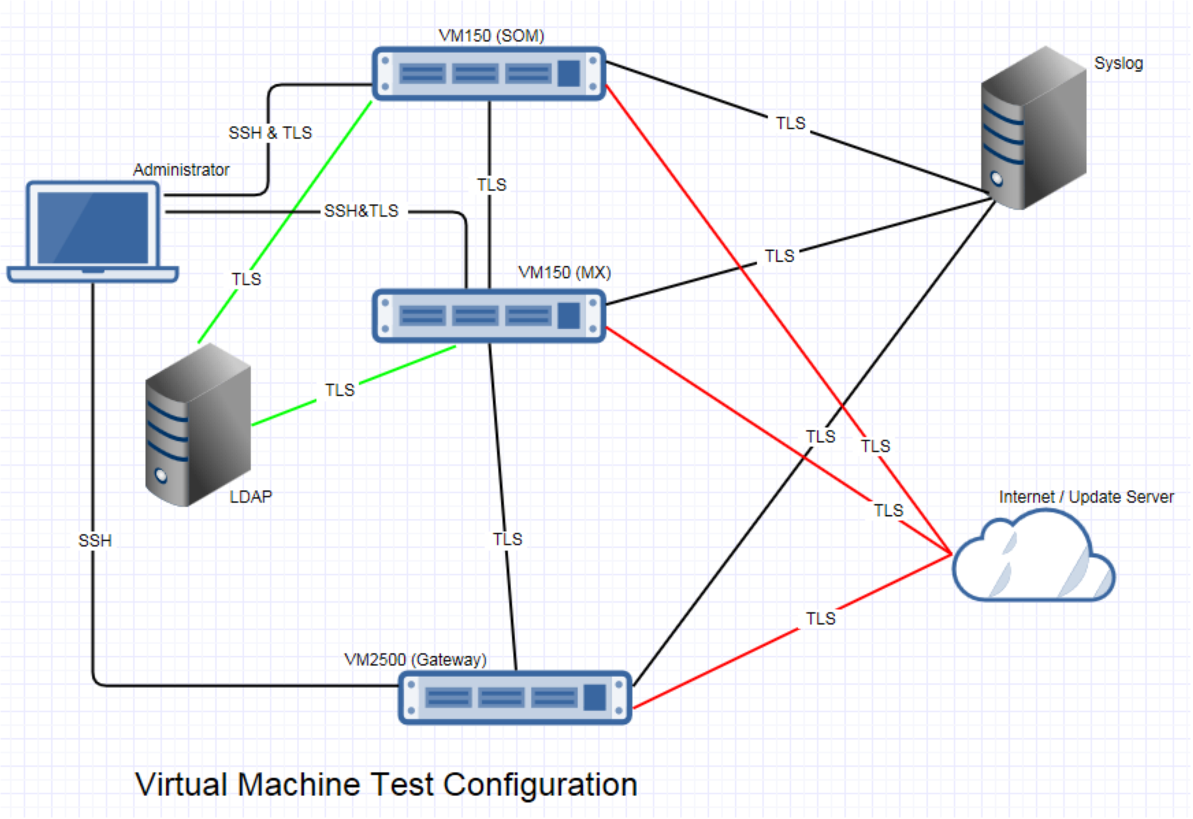

Figure 2 Evaluation Team Evaluated Test Configuration (Virtual Machine)

As documented in the diagram above, the following virtual machine components were included in the evaluated configuration during testing:

- Virtual Machine
  - One SecureSphere Operations Manager (SOM): VM150
  - One management virtual machine: VM150
  - One gateway virtual machine: VM2500

All of the VM Machines in the CCTL test configuration were installed on an Ivy Bridge supported Intel Core i5-3350P processor @ 3.10 GHz VMware ESXi v5.1.0 w/ hardware v9 platform.

The evaluated version of the TOE was installed and configured according to the Imperva SecureSphere Configuring Common Criteria Compliance User Guide, Version 11.5, November 2015 as well as the supporting guidance documentation identified in Section 6.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements as amended by Errata #3 dated 3 November 2014, and includes the additional optional SFRs: FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, and FPT_ITT.1, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

The validators have no further comments about the evaluation results.

11 Annexes

Not applicable.

12 Security Target

Imperva SecureSphere Security Target, Version 0.4, 12 November 2015

13 Abbreviations and Acronyms

Abbreviation	Description
ADC	Application Defense Center
AES	Advanced Encryption Standard
AWS	Amazon Web Services
CAV	Correlated Attack Validation
CC	Common Criteria
CLI	Command Line Interface
GUI	Graphical User Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Intrusion Detection
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
MX	Management Server
NIC	Network Interface Card
NTP	Network Time Protocol
OOB	Out Of Band
PP	Protection Profile
RFC	Request for Comment
SFR	Security Functional Requirement
SFP	Security Function Policy
SIEM	Security Information and Event Management
SOM	SecureSphere Operations Manager
SPAN	Switch Port Analyzer
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation

TSF	TOE Security Function(s)

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Imperva SecureSphere Security Target, Version 0.4, 12 November 2015

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Imperva SecureSphere v11.5 Part 2 (Leidos Proprietary), Version 1.0, November 13, 2015