National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Imperva SecureSphere
Version 6

Report Number: CCEVS-VR-VID10238-2009

Dated: February 20, 2009
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 6757
Fort George G. Meade, MD 20755-6757

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

The Target of Evaluation (TOE) is the **Imperva SecureSphere 6** product. The TOE was evaluated by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in the United States, and completed in February 2009. The evaluation was for the Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1 (Basic Flaw Remediation). The evaluation was conducted in conformance with the Common Criteria (CC) for Information Technology Security Evaluation and the Common Evaluation Methodology (CEM) for Information Technology Security, version 2.3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

The Imperva SecureSphere 6 product lines are intrusion detection/prevention (IDS/IPS) products that include gateway and management server appliances. Imperva SecureSphere 6 protects Web and database servers from attacks originating both within the organization (insider attacks) and from without. The gateways appliances are installed in front of the protected resources and are connected to the management server using a dedicated management network. The Imperva SecureSphere 6 product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target. The TOE claims and meets conformance to the Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006 (IDSSPP).

The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. The *Imperva SecureSphere 6 Security Target***,** Version 1.6, dated February 5, 2009, identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Imperva SecureSphere 6 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

1 IDENTIFICATION

Evaluated Product:	**Imperva SecureSphere 6**
Sponsor & Developer:	Imperva Inc. 950 Tower Lane, Suite 1550 Foster City, CA 94404
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046

Completion Date: February 5, 2009

CC: Common Criteria for Information Technology Security Evaluation, Version 2.3

Interpretations: There were no applicable interpretations used for this evaluation.

CEM: Common Methodology for Information Technology Security Evaluation, Version 2.3

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

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

Imperva SecureSphere 6 includes the following gateway and Management Server appliances running the SecureSphere 6 software image: G4, G8, G16, MX, G4 FTL, G8 FTL and MX FTL.

Disclaimer The information contained in this Validation Report is not an endorsement of the Imperva SecureSphere 6 product by any agency of the U.S. Government and no warranty of the Imperva SecureSphere 6 product is either expressed or implied.

PP: The TOE is Protection Profile Conformant with the following Protection Profiles:
Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006

Evaluation Personnel
Eve Pierre
Terrie Diaz

Validation Body: National Information Assurance Partnership CCEVS

Threats to Security

The following are the threats that the evaluated product addresses:

Table 1Threats

Threat	TOE Threats
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

2 SECURITY POLICY

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

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

3.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 2 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

3.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 Physical Assumptions

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3 Clarification of Scope

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

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

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

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

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

- **Administrator workstations** used for managing the TOE: a standard Web browser (Microsoft Internet Explorer 5.0 or later) is used to connect to a SecureSphere GUI

Web-based management application running on the SecureSphere Management Server, via a dedicated management network interface. The administrator workstation and browser are considered to be outside the TOE.

- **Protected Servers**: the TOE provides protection for server-based applications that use Web, database, and IP protocols to communicate with client applications. The TOE can provide protection for protocols used by the following database products: Oracle 8.0/8i/9i/10g, Sybase 12.5.0/12.5.2, IBM DB2 for Unix, Linux, Windows and zOS, Microsoft SQL Server 7.0/2000/2005, and IBM Informix 9 and 10.
- **SecureSphere DB Agents**: Imperva markets optional add-on sensor software agents that run on the database server, and transmit all database access requests to the SecureSphere 6 gateway. This allows the gateway to analyze database events that cannot be identified from network traffic, e.g. by applications running on the database server host itself.

  Disabled by default, agent support may be enabled in the evaluated configuration if the customer purchases and installs DB agents on protected database servers.
- **Active Modules**: SecureSphere 6 includes an Active Module engine that is used to distribute value-added insights and capabilities generated by ADC, including such features as Track Value Changes, Auto Server Discovery, Sensitive Data Discovery, Change Tracking, and third party Scanner Integration. Active Modules are distributed as Java .jar files as part of the **Error! Reference source not found.** mechanism.

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

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

4 ARCHITECTURAL INFORMATION

Figure 1 shows the physical scope and boundaries of the TOE. Imperva SecureSphere 6 product lines are IDS/IPS products that include gateway and Management Server (MX) appliances. SecureSphere 6 protects Web and database servers from attacks originating both within the organization (insider attacks) and from without. The gateways appliances are installed in front of the protected resources and 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.

A SecureSphere 6 gateway can be deployed on the network as a HTTP proxy, a transparent inline bridge or an offline network monitor (sniffer). SecureSphere 6 monitors application-level protocols for attacks, and reacts by blocking the attacks and/or reporting them to a centralized management console. SecureSphere 6 automatically builds a model of legitimate application behavior and uses it to identify illegitimate traffic. In addition to a comprehensive database traffic auditing capability, SecureSphere 6 provides a Database Active Security Assessment (DASA) capability for scanning databases for vulnerabilities and policy violations.

A single gateway in inline mode protects one or two network segments. It has six network interface cards: two of the cards are used for management; the other 4 cards are part of the 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. In inline mode the gateway will block malicious traffic inline (i.e. drop packets).

A single gateway in sniffing mode protects more then one network segment as it includes multiple network interface cards. A single sniffing gateway can monitor different types of servers (i.e. Web servers, databases, Email Servers) and it is not necessary to separate these tasks or assign them to different gateways. In sniffing mode, the gateway is a passive device that connects to corporate hubs and switches and taps the traffic sent to and from protected servers.

The TOE uses the following FIPS 140-2 validated cryptographic modules for the implementation of cryptographic functionality: RSA BSAFE Crypto-J 4.0, OpenSSL version FIPS 1.1

SecureSphere 6 gateways are installed in front of the protected resources. They are connected to the Management Server using dedicated out of band (OOB) management network interfaces, so that the communication between the gateways and the Management Server is not exposed to any internal or external users.

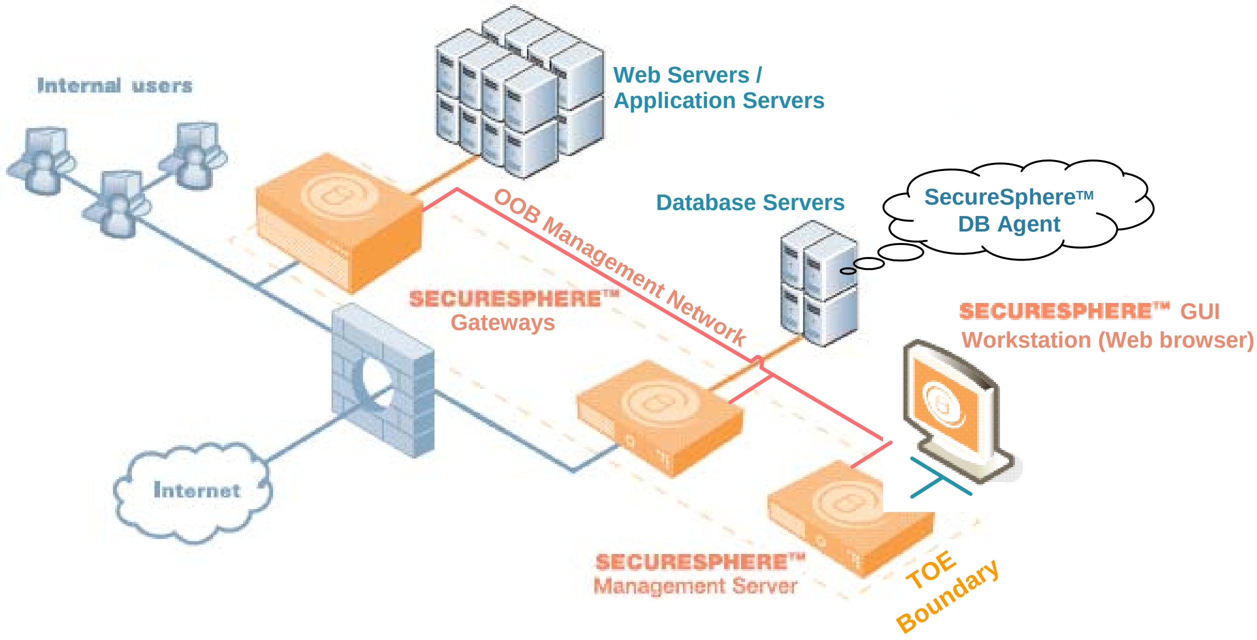

Figure 2 Physical Scope and Boundaries of the TOE

5 DOCUMENTATION

The following end-user Imperva documents were used in the evaluation.

1. Imperva SecureSphere Version 6.0.6 Reference Guide July 26, 2008
2. Imperva SecureSphere Version 6.0.6 Administrator July 29, 2008 Manual
3. Imperva SecureSphere Version 6.0.6 User Guide July 29, 2008
4. Imperva SecureSphere Version 6.0.6 Release Notes July 31, 2008
5. G4 AH Appliance Quick Start Guide G4-AH QSG version 6.2, 6/3/2008
6. G4-G8 CL Appliance Quick Start Guide G4-G8-CL QSG version 6.2, 6/3/2008
7. G4-G8 FTL Appliance Quick Start Guide G4-G8-FTL QSG version 6.2, 6/3/2008
8. G16 FTL Appliance Quick Start Guide G16-FTL QSG version 6.2, 6/3/2008
9. MX AH Appliance Quick Start Guide MX-AH QSG version 6.2, 6/3/2008
10. MX Appliance Quick Start Guide MX-CL QSG version 6.2, 6/3/2008
11. MX FTL Appliance Quick Start Guide MX-FTL QSG version 6.2, 6/3/2008
12. SecureSphere 6 Common Criteria Evaluated Configuration Guidance, Version 0.7, October 7, 2008

6 IT PRODUCT TESTING

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a subset of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST. The tests were conducted using:

- One G4 appliance running both the gateway and management server software (one box configuration)
- One G4 and one G8 appliances running the SecureSphere 6 Gateway software
- One Management Server (MX) appliance running the SecureSphere 6 management server software.
- Two database servers (MSSQL, and Oracle)

The developer test suite was examined and found to provide adequate coverage of the security functions; where the vendor test suite provided insufficient coverage, the evaluation team devised additional test cases to adequately test the security functions.

A subset of the developer tests were run and the results were found to be consistent with the results generated by the developer.

No vulnerabilities in the TOE were found during a search of vulnerability databases.

7 EVALUATED CONFIGURATION

The evaluated configuration is one or more of the G4, G8, G16 gateway appliances, and one or more Management Server (MX) appliances. Figures 2 and 3 show the two deployment scenarios that were tested during the evaluation.

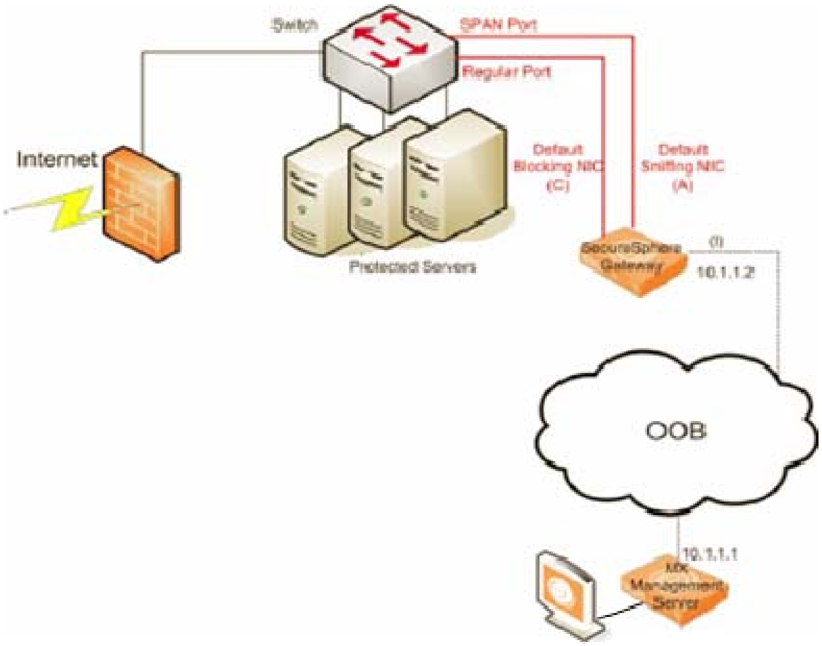

Figure 3 Example Sniffing Topology

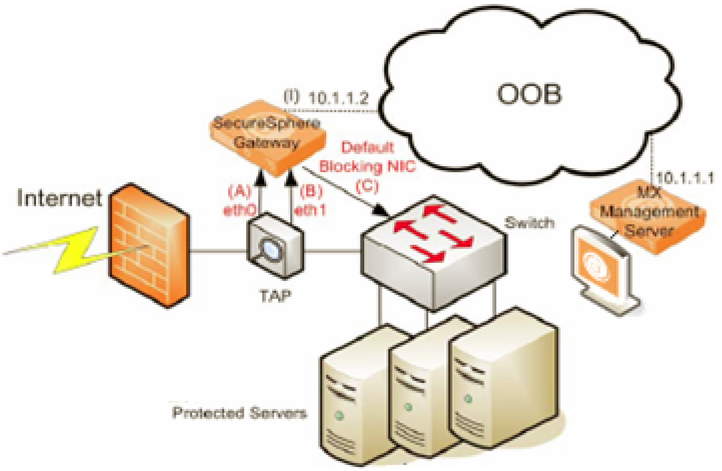

Figure 4 Example Sniffing Topology

8 RESULTS OF THE EVALUATION

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM. A Pass, Fail, or Inconclusive verdict was assigned to each work unit of assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The results of the evaluation of the assurance requirements are generally described in Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1. Details are provided in the proprietary ETR (Part 2)."

A verdict for an assurance component was determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined that the Imperva SecureSphere 6 TOE is compliant with the IDSSPP and that all claims in the ST are met. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report For the Imperva SecureSphere 6 Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> Section 6.1, ST Evaluation: Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Imperva SecureSphere 6 Security Target, version 1.6, February 5, 2009, is a CC compliant ST.
>
> Section 6.2, TOE Evaluation: The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured and operated according to the guidance documentation, the Imperva SecureSphere 6 TOE satisfies the claims made in the Imperva SecureSphere 6 Security Target.

Additionally, the evaluation team's performance of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST. The evaluation team uncovered no major security flaws for which the product had to be corrected.

9 VALIDATOR COMMENTS

The TOE does not claim cryptographic protection of data transmission between distributed parts of the TOE. The vendor recommends that all management traffic be transmitted over an Out of Band (OOB) network that provides physical or technical separation of management traffic from production traffic. If deployment is not consistent with vendor recommendations, (for example, the MX and gateway appliances are not co-located on a network separate from the production network) the customer should consider using cryptographic or other security mechanisms to secure communications traffic between the appliances.

10 SECURITY TARGET

The security target for this product's evaluation is *Imperva SecureSphere 6 Security Target***,** Version 1.6, February 5, 2009

11 GLOSSARY

Access Interaction between an entity and an object that results in the flow or modification of data.

Administrator A user who has been specifically granted the authority to manage the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

Attack An intentional act attempting to violate the security policy of an IT system.

Bridge A layer-two device that forwards frames received from one network segment to another segment, based on their MAC address.

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

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

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

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.

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

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

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

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

12 ACRONYMS

ADC	Application Defense Center
CC	Common Criteria
CM	Configuration Management
DASA	Database Active Security Assessment
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IDSSPP	Intrusion Detection System System Protection Profile
IPS	Intrusion Prevention System
IT	Information Technology
NIC	Network Interface Card
PP	Protection Profile
SFR	Security Functional Requirement
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 BIBLIOGRAPHY

URLs

- NIAP Common Criteria Evaluation and Validation Scheme (http://www.niap-ccevs.org/cc-scheme/)
- SAIC CCTL (http://www.saic.com/infosec/common-criteria/)
- Imperva Inc. (http://www.imperva.com)

NIAP CCEVS Documents:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005
- *Common Evaluation Methodology for Information Technology Security, version 2.3*, August 2005.
- *Intrusion Detection System System Protection Profile*, *Version 1.6*, April 4, 2006

Security Target:

- *Security Target for Common Criteria: Imperva SecureSphere 6, version 1.6*, February 5, 2009.