Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Imperva Web Application Firewall (WAF) v14.7P20

Version 1.0, 11 Dec 2023

Document reference: AISEP-CC-CR-2023-EFT-T038-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Imperva Web Application Firewall (WAF) v14.7P20 against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is Imperva Web Application Firewall (WAF) v14.7P20. The TOE is a software product or network appliance that can perform an intrusion detection system (IDS) or intrusion prevention system (IPS) role.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP).

The evaluation was performed by Teron Labs and was completed on 28 November 2023.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends:

- that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the vendor's supplementary guidance
- users should carefully consider the different deployment modes of the TOE to ensure that each desired feature is available in the chosen deployment
- users should carefully consider the firewall policies configured and verify their behaviour is as expected before depending on the security features they provide
- users should periodically reassess the TOE's firewall policies and ensure that they are configured to provide the best protection by considering the nature of recent security vulnerabilities, latest CVEs, and the IT resources that the TOE protects
- users should periodically download the latest Imperva ADC content, review the attack signatures and assess if they are relevant in protecting the user's IT assets
- users must maintain the confidentiality, integrity, and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE
- auditors should review the audit trail generated and exported by the TOE frequently
- users should verify the integrity of the TOE software prior to installation by comparing the SHA256 hash of the downloaded software against the value available from the guidance documentation.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [6] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Imperva Web Application Firewall (WAF) v14.7P20.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Imperva Web Application Firewall (WAF)
Software version	V14.7P20
Security Target	*Imperva Web Application Firewall (WAF) v14.7P20 Security Target Version 1.8 11 September 2023*
Evaluation Technical Report	*Evaluation Technical Report Imperva WAF 1.0 dated 28 November 2023* Document reference EFT-T038-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	EAL 2 augmented with ALC_FLR.1 (Basic flaw remediation)
Developer	Imperva Inc. One Curiosity Way, Suite 203 San Mateo, CA 94403

	United States
Evaluation facility	Teron Labs Pty Ltd Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Imperva Web Application Firewall (WAF) v14.7P20.

Imperva Web Application Firewall (WAF) v14.7P20 provides protection from attacks against Web and Web Services asset, both within the organization (insider attacks) and from outside the organisation. Imperva WAF protects Web 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. The product is deployed as one or more WAF appliances (physical, virtual, or cloud) and controlled by a management system, MX Management Server (MX) appliance. In a multi-tier management configuration, one or more MXs may be managed by a SecureSphere Operation Manager (SOM).

The different appliance models all run the same WAF v14.7P20 software and provide all claimed security functionality but may differ in throughput and storage capacity. Imperva WAF software (including both management and/or WAF components) may alternatively be installed on a Virtual Machine (VM) hosted by a VMware ESX/ESXi Hypervisor. The Virtual Machine emulates the WAF v14.7P20 appliance hardware. The VMware Hypervisor and underlying hardware is considered to be outside of the boundaries of the Target of Evaluation.

Virtual appliances are listed in the Table below:

	WAF Gateway Appliances				Management Appliance
Model	V6500	V4500	V2500	V1000	VM150
CPU	8	8	4	2	4
Memory	32 GB	16 GB	8 GB	8 GB	8 GB
Minimum Disk	250 GB	160 GB	160 GB	160 GB	160 Gb

Physical appliances are listed in the Table below:

Product Generation	Model	Throughput	Form Factor	Fault Tolerant	Management Server
5G	X1010	100 Mbps	1U	No	M110
	X2010	500 Mbps	1U	No	
	X2510	500 Mbps	2U	Yes	M160

Product Generation	Model	Throughput	Form Factor	Fault Tolerant	Management Server
	X4510	1 Gbps	2U	Yes	
	X6510	2 Gbps	2U	Yes	
	X8510	5 Gbps	2U	Yes	
	X10K	10 Gbps	2U	Yes	
6G	X1020	100 Mbps	1U	No	M120
	X2020	500 Mbps	1U	No	
	X2520	500 Mbps	2U	Yes	M170
	X4520	1 Gbps	2U	Yes	
	X6520	2 Gbps	2U	Yes	
	X8520	5 Gbps	2U	Yes	
	X10k2	10 Gbps	2U	Yes	

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6.4 of the Security Target [6].

TOE physical boundary

The TOE physical boundary is described in section 1.6.2 of the Security Target [6].

TOE Architecture

Imperva WAF can be run in different configurations depending on user requirements. In the evaluated configuration the Imperva WAF Gateway(s) are managed by the Imperva MX Management Server(s) and the Imperva MX Management Server(s) are optionally managed by a SecureSphere Operation Manager (SOM).

Various ways that the TOE can be used include:

- Imperva WAF Gateways deployed inline, suitable for blocking
- Imperva WAF Gateways deployed non-inline suitable for sniffing
- Imperva WAF Gateways deployed in reverse proxy mode.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [6].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [6] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

Instructions for using the TOE in the evaluated configuration are provided in the *Evaluated Configuration Guidance* [5].

Software delivery procedures

The TOE is delivered to customers in the form of pre-installed hardware appliances via courier delivery or via downloaded Virtual Appliance images (.iso, .ovf or .vmdk) from the Imperva FTP web site. The Imperva FTP site supports FTPS (FTP over SSL), which is more secure than plain FTP and should be used for the download. The *Evaluated Configuration Guidance* [5] documentation that is also part of the TOE can be obtained from the Imperva FTP web site with credentials provided by Imperva.

- When delivered as hardware appliances with pre-installed software the customer examines the packaging and the appliance and compares against the order.
- After download from the Imperva FTP web site the install image can be verified against the SHA256 hashes listed in the *Evaluated Configuration Guidance* [5].

Installation of the TOE

The *Evaluated Configuration Guidance* [5] contains all relevant information for the secure configuration of the TOE.

Version verification

The Imperva software version evaluated is described as v14.7P20 but it should be noted that in full detail the version shows as 14.7.0.20_0.44105. The version string "14.7.0.20_0.44105" is expected in the appliance image filenames. After initial installation the version can be checked using the appliance's SSH CLI interface at the `SecureSphere>` prompt via the `version --verbose` command.

Documentation and guidance

The *Evaluated Configuration Guidance* [5] is available from the Imperva FTP web site with credentials provided by Imperva. The Imperva FTP site supports FTPS (FTP over SSL), which is more secure than plain FTP and should be used for the download.

Generic Common Criteria information is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4].

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

- The TOE has access to all attack signatures it needs to perform its functions.
- The TOE has adequate compute capability for the systems it serves.
- The TOE is managed in a way that adjusts to changes in the protected systems.
- The NTP server configured in the TOE is accurate and reliable.
- The TOE hardware is secure.
- The TOE hardware and software is protected from unauthorized physical modification.
- The TOE administrators are not careless, negligent or hostile.
- The TOE can only be accessed by authorized users.
- There are one or more competent individuals assigned to manage the TOE.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [9]. In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [8].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators found that the developer tests covered all Security Functional Requirements specified in the ST.

The evaluators examined the TOE prior to testing and determined that the test configuration was consistent with the configuration under evaluation as specified in the ST. The evaluators followed the user installation and configuration guidance to ensure that the TOE had been installed correctly and was in a known state prior to conducting testing.

The evaluators drew upon the developer testing evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators also devised and conducted additional functional testing.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by providing a full Security Target and an analysis of the Security Functional Requirements (SFRs) in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [6] and **has met** the requirements of Common Criteria EAL2 augmented with ALC_FLR.1 (Basic flaw remediation).

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of Imperva Web Application Firewall (WAF) v14.7P20 performed by the Australian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends:

- that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the vendor's supplementary guidance

- users should carefully consider the different deployment modes of the TOE to ensure that each desired feature is available in the chosen deployment
- users should carefully consider the firewall policies configured and verify their behaviour is as expected before depending on the security features they provide
- users should periodically reassess the TOE's firewall policies and ensure that they are configured to provide the best protection by considering the nature of recent security vulnerabilities, latest CVEs, and the IT resources that the TOE protects
- users should periodically download the latest Imperva ADC content, review the attack signatures and assess if they are relevant in protecting the user's IT assets
- users must maintain the confidentiality, integrity, and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE
- auditors should review the audit trail generated and exported by the TOE frequently
- users should verify the integrity of the TOE software prior to installation by comparing the SHA256 hash of the downloaded software against the value available from the guidance documentation.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
5. *Imperva WAF GW 14.7 Evaluated Configuration Guidance v1.2, 2023-07-17*
6. *Imperva Web Application Firewall (WAF) v14.7P20, Security Target, Version 1.8, 11 September 2023*
7. *Evaluation Technical Report - EFT-T038 ETR V1.0 dated 28 November 2023*
8. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*
9. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*

Abbreviations

ADC	Imperva Application Defense Center
AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CCRA	Common Criteria Recognition Arrangement
FTPS	FTP over SSL
.iso	File extension for binary image file that can be written to DVD disc or USB drive
OVF	Open Virtualization Format – packaging for virtual machines
SFR	Security Functional Requirement
TOE	Target of Evaluation
VMDK	Virtual Machine DisK – format for virtual appliances