Imperva Web Application Firewall (WAF) v14.7P20

Security Target

Version 1.8

11 September 2023

Prepared for:

One Curiosity Way, Suite 203
San Mateo, CA 94403
United States

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Table of Contents

List of Figures and Tables

1 Security Target Introduction

This Security Target (ST) describes the objectives, requirements, and rationale for the Imperva Web Application Firewall (WAF) software. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target, Target of Evaluation and Common Criteria Identification

ST Title: Imperva Web Application Firewall (WAF) v14.7P20 Security Target

ST Version: Version 1.8

ST Date: 2023-09-11

TOE Identification: Imperva Web Application Firewall (WAF) v14.7P20

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017
  - Part 3 Conformant.

This ST and the TOE it describes are conformant to the following package:

- EAL2 augmented (ALC_FLR.1 Basic flaw remediation)

1.3 Conventions

The following conventions are used in this document:

- Security Functional Requirements - Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration; selection; assignment; and refinement.
  - Iteration - allows a component to be used more than once with varying operations. In this ST, iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
  - Selection - allows the specification of one or more elements from a list. Selections are indicated as underlined text and are enclosed by brackets (e.g., [selection]).
  - Assignment - allows the specification of an identified parameter. Assignments are indicated using italicized text and are enclosed by brackets (e.g., [*assignment*]). An assignment within a selection is identified in underlined italics and with italicized embedded brackets (e.g., [*[selected assignment]*]).

  - Refinement - allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST - other sections of the ST use bolding and/or different fonts (such as Courier) to highlight text of special interest, such as captions, commands, or filenames specific to the TOE.

1.4 Keywords

Web application firewall, threats, risk, collection, analysis.

1.5 TOE Overview

1.5.1 TOE Type

Imperva WAF v14.7P20 protects Web servers by analyzing network traffic flowing to and from protected servers and applications, detecting requests that may be indicative of intrusion, and reacting by reporting the events and/or blocking the suspected traffic.

A sampling of attacks WAF is capable of detecting is:

- Buffer Overflow,
- Denial of Service,
- SQL Injections,
- Cross-site Scripting,
- Parameter Tampering,
- Brute-force,
- Automated Bot attack,
- Scraping attack,
- Cookie Poisoning,
- Session Hijacking,
- Takeover of Server,
- Protocol Violation,
- Directory Traversal,
- Stealth Commanding,
- Site Probing.

In this Security Target, the Target of Evaluation is categorized as an IDS/IPS product. The WAF IDS System collects the following information from the targeted IT System resource(s): service requests, network traffic, detected known vulnerabilities. The IDS then performs various analysis functions on the IDS data in order to make intrusion and vulnerability determinations, and provide a response capability.

The product underwent a re-branding in 2021/2 but some old references to "SecureSphere" are still present in the vendor's manuals and online documentation. Any references to "SecureSphere" in any document or manual are the same as references to "WAF GW" or simply "WAF". The TOE's SOM

(SecureSphere Operation Manager) is referred to as Management Server Manager in some of the manuals.

1.5.2 TOE Usage and Major Security Features

Imperva WAF v14.7P20 provides protection from attacks against Web and Web Services asset, both within the organization (insider attacks) and from without. Imperva WAF protects Web servers by analyzing network traffic flowing to and from protected servers and applications, detecting requests that may be indicative of intrusion, and reacting by reporting the events and/or blocking the suspected traffic. 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) (Figure 1 below).

The TOE provides protection from attacks against 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), an Imperva WAF appliance monitors application-level protocols for attacks and reacts by blocking the attacks and/or reporting them to a centralized management server, MX Management Server.

The product is deployed as one or more WAF instances (physical, virtual, or cloud), controlled by an Imperva Management Server (MX) appliance. In multi-tier management configurations, one or more MXs may in turn be managed by an Imperva SecureSphere Operation Manager (SOM). Administrators connect to the MX using a standard Web browser (Figure 1 below) or using OpenAPI. They are required to authenticate their identity before being allowed any further action.

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.

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

Imperva's Dynamic Profiling technology automatically builds a model of legitimate application behavior that is used by the product to identify illegitimate traffic. In addition, attack signatures are preconfigured into the product and can be periodically updated from an external Application Defense Center (ADC). The ADC also provides ADC Insights – these are pre-packaged security policy rules and reports for commonly used applications. Imperva also provides a ThreatRadar service that provides categorized reputation-based IP blocking lists in near real-time.

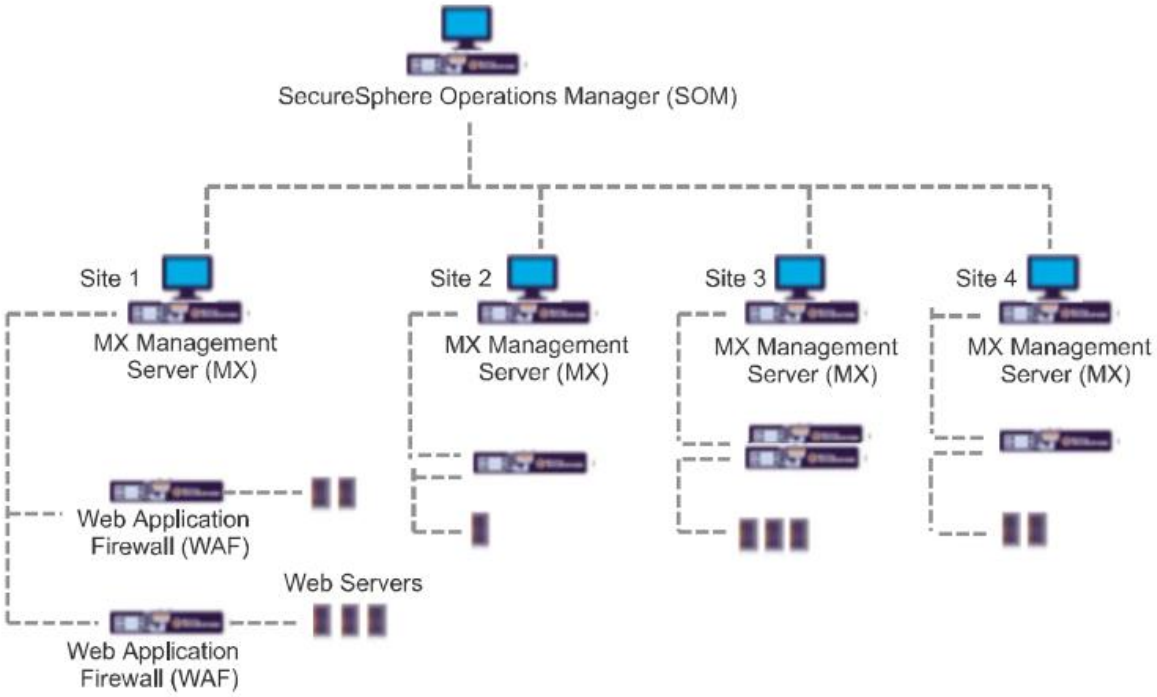


Figure 1: Multi-domain Environment Managed by SecureSphere Operation Manager (SOM)

1.5.3 Non-TOE Hardware/Software/Firmware Required by the TOE

The figure below depicts the TOE protecting Web servers. The Imperva WAF v14.7P20 software (TOE) is installed on Imperva appliances in front of the protected resources. They are connected to the MX Management Server using dedicated out of band (OOB) management network interfaces, so that the communication between the gateways and the MX Management Server is not exposed to any internal or external users.

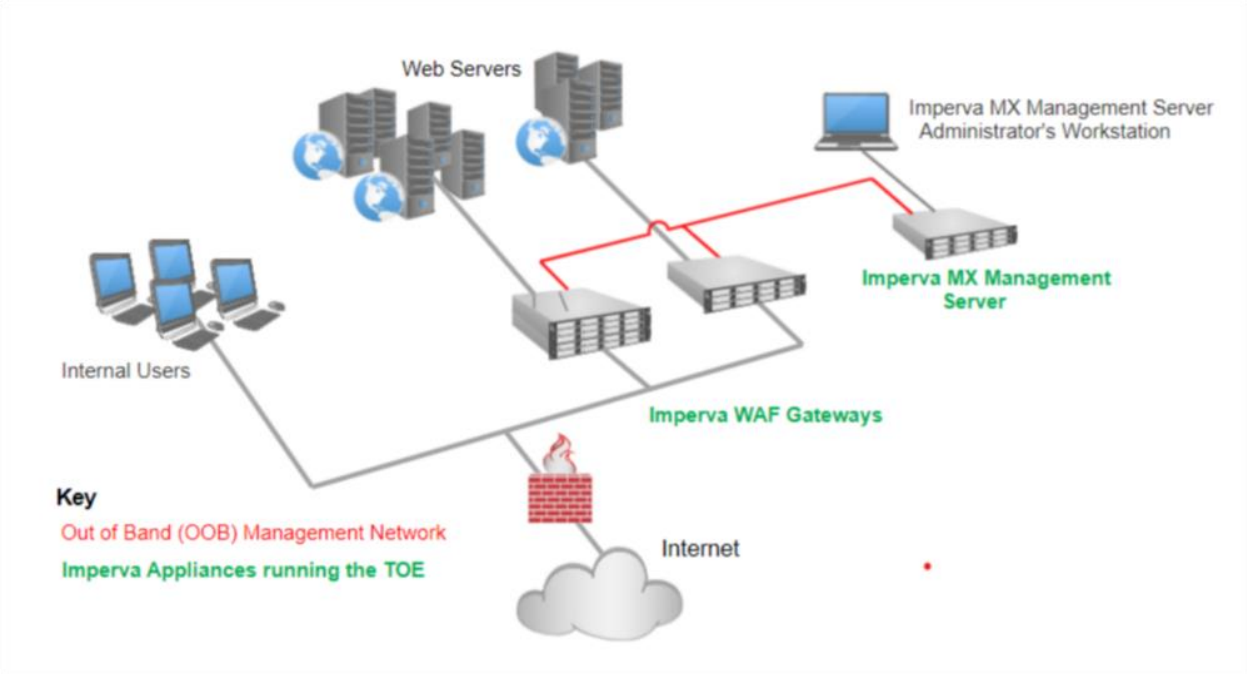


Figure 2: Typical TOE Deployment

1.5.3.1.1 Web Browser for Imperva GUI Management Interface

Administrators manage and monitor the TOE by connecting to the TOE's GUI or via OpenAPI which is resident on the MX Management Server. Imperva WAF accepts the following Web browsers:

- Microsoft Internet Explorer: 10 - 11
- Mozilla Firefox: Most recent stable version.
- Google Chrome: Most recent stable version.
- Microsoft Edge: Most recent stable version.
- Safari : Most recent stable version.
- Opera: Most recent stable version.

1.5.3.1.2 Network Time Protocol (NTP) Server

The TOE requires a reliable time source. This is accomplished by requiring the environment to provide a NTP implementation. The MX Management Server is configured to communicate to the server and in turn supplies the time to the WAF GWs.

1.5.3.1.3 Models

The TOE is a software application which runs on the following Imperva physical and virtual appliances.

Table 1: Imperva WAF Gateway and MX Management Server Virtual Appliances

	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

Virtual appliances are supported on the following hypervisors:

- VMware ESX/ESXi (5.5 and later)
- KVM (Linux)
- Microsoft Azure
- Microsoft Hyper-V
- Amazon AWS

Table 2: : Imperva WAF Gateway and MX Management Server Physical Appliances

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
	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	

1.6 TOE Description

1.6.1 Introduction

Imperva WAF v14.7P20 provides a broad range of services, features and capabilities. This ST makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality. The evaluated configuration must be established in accordance with the evaluated configuration guidance.

This part of the ST describes the physical and logical scope and boundaries of the Target of Evaluation (TOE). This description effectively partitions product functionality into three classes:

- Claimed security functionality that is evaluated in the context of this ST.
- Excluded functionality that is not available in the TOE's evaluated configuration.

- Other functionality that is in the TOE but is not evaluated in the context of this ST except for the determination that it cannot compromise any claimed security functionality.

1.6.2 Physical Boundary

The TOE is distributed as a software distribution, Imperva WAF v14.7P20, that includes the software, operating system, crypto-libraries, and additional libraries to operate the WAF Gateways, MX Management Server, and the SecureSphere Operation Manager (SOM). The bundle includes:

- the Imperva WAF v14.7P20 software,
- the MX Management Server v14.7P20 software (includes OpenAPI 3.0),
- the SecureSphere Operation Manager (SOM) v14.7P20 software,
- CentOS 7.5, the operating system for appliances,
- Security-Enhanced Linux (SELinux) - a kernel module that provides a mechanism for supporting access control security policies,
- the Bouncy Castle v1.71 crypto library used with the MX Management Server software, and
- the OpenSSL v1.1.1n crypto library used with the WAF Gateway software.

The specific evaluated Imperva software version is 14.7.0.20_0.44105. The TOE is delivered to customers in the form of pre-installed hardware appliances via courier delivery and Virtual Appliance images (.ovf) via web site download. The TOE includes the guidance documentation identified in Section 1.7. The guidance documentation can be obtained and downloaded from the Imperva FTP site.

Installation procedures prompt the installer which product to install. The complete Imperva WAF v14.7P20 distribution is included in the TOE boundary with one exception. The TOE appliances support local console access and remote access to appliance operating system-level installation and configuration CLI over the SSH protocol. The CLI is used solely for initial configuration, once an appliance is correctly configured and operational, the SSH channel used for this configuration is disabled and all management should be performed via Imperva GUI or the OpenAPI interface. Therefore, the evaluated configuration excludes the CLI.

1.6.3 Evaluated Configuration

The evaluated configuration is the TOE (software) installed on one WAF Gateway appliance and one MX Management Server physical appliance, and a virtual SOM installed on VMware ESXi 6.7.

1.6.4 Summary of TOE Security Functionality

1.6.4.1 IDS Component

Imperva WAF is an IDS/IPS that monitors web 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. Available configurable alarms are sending a syslog message to a syslog server or creating an SNMP trap and sending the trap to an SNMP destination.

1.6.4.2 Security Management, Identification and Authentication and Trusted Path

Administrators manage system configuration settings using the Imperva GUI, a web-based interface provided by the MX Management Server or OpenAPI. Administrators log in to the MX Management Server and are authenticated using a password. The server provides a trusted path for the management session using the TLS protocol. A role-based scheme is used to define administrator authorizations. Only designated authorized System administrators may modify the behavior of IDS System data collection, analysis and reaction capabilities. Other authorized administrators may only query System and audit data and modify other TOE data.

1.6.4.3 Security Audit

The TOE records TOE events related to ADC content updates, administrator logins, changes to configuration, activation of settings, building profiles, automatic profile updates, server start/stop, etc. in an audit trail. Administrators are provided with reporting tools to review audit trail and System data. The TOE provides protection against modification and unauthorized deletion of audit records and System data, as well as storage exhaustion.

1.6.4.4 Protection of the TSF

The TOE protects itself and its data from tampering. Transfer of information between the gateways and the Management Server is physically separated from other information flows by the use of the dedicated OOB management network interface. Audit data that is stored on an archive outside of the TOE is cryptographically protected from disclosure or tampering. ADC content updates are provided over a secure channel using TLS, ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. WAF also protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE includes its own time clock to ensure that reliable time information is available (e.g., for log accountability) but requires an NTP Server in the operational environment in order to synchronize its clock with that of the external time server. The TOE uses HTTPS to protect communications between distributed TOE components and with the users.

1.6.4.5 Cryptographic Support

The TOE provides a FIPS mode of operation, which must be enabled in the evaluated configuration. The TOE includes FIPS-approved algorithms providing supporting cryptographic functions. The TOE uses the Bouncy Castle v1.71 and OpenSSL v1.1.1n for all of the cryptographic functionality. The modules provide key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of higher level cryptographic protocols, including TLS and HTTP over TLS.

1.6.5 Imperva WAF Deployment Scenarios

Imperva Web Application Firewall (WAF) v14.7P20 appliances support both non-inline (sniffing), inline (bridge), and reverse proxy 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 reverse proxy gateway terminates the connections and therefore is the most invasive mode, as a result, it provides more capabilities and features than an inline gateway.

In all modes, system administrators shall ensure that the connection between WAF GW and MX is over an OOB network and that there is IP connectivity between the WAF GWs, the MX, and the optional SOM.

1.6.5.1 Inline (Bridge)

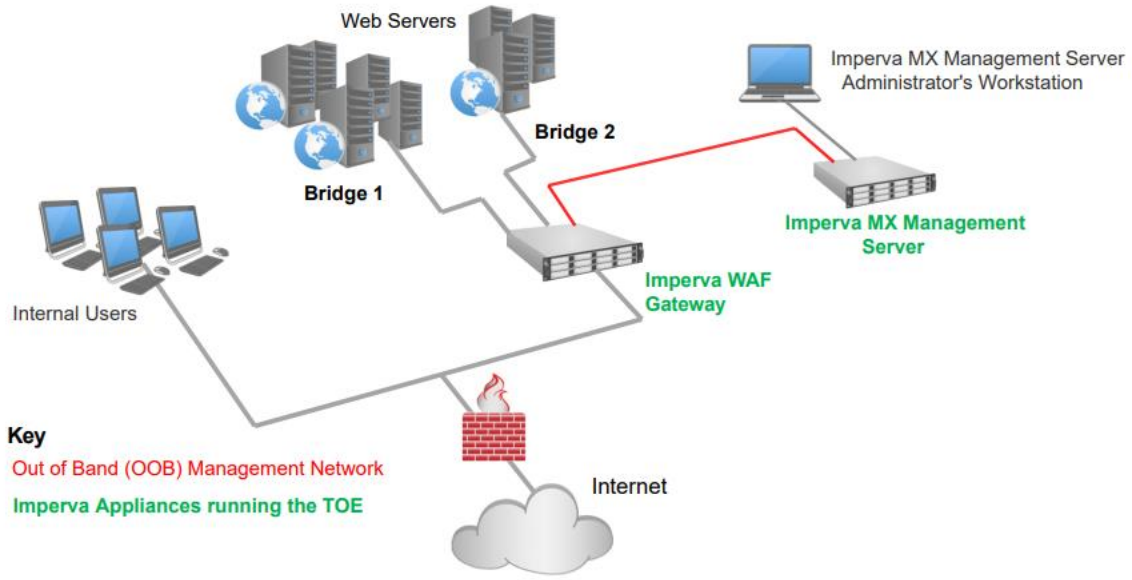


Figure 3: A Typical Imperva WAF Inline (Bridge) *Deployment*

In the inline scenario, the WAF gateway acts as a bridging device between the external network and the protected network segment. The gateway will block malicious traffic inline (i.e., drop packets). A single inline gateway protects one or two network segments. It has six network interface cards. Two of the cards are used for management: one to connect to the management server and the other is optional. The other four cards are part of two bridges that are used for inline inspection of up to two different protected network segments. Each bridge includes one card for the external network and one for the protected network. The figure above depicts a sample inline deployment.

1.6.5.2 Non-Inline (Sniffing Mode)

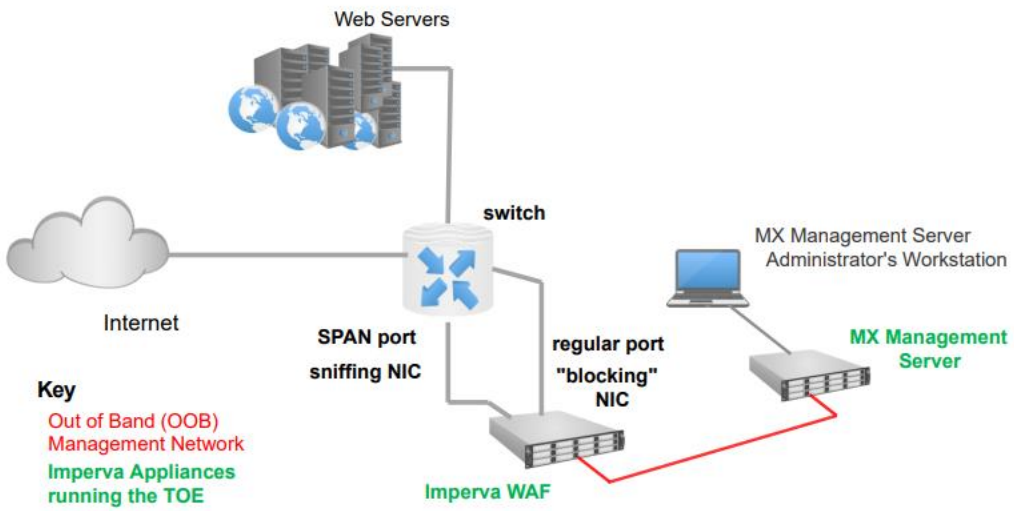


Figure 4: A Typical Imperva WAF Non-Inline (Sniffing) Deployment

A sniffing gateway is a passive sniffing device. It connects to corporate hubs and switches and taps the traffic sent to and from protected servers, using a SPAN (mirror) port on the switch, or a dedicated TAP device. Traffic is copied to it instead of passing directly through it. TCP resets are transmitted over a "blocking" NIC. The above figure depicts a sample sniffing deployment.

1.6.6 Reverse Proxy

In a Reverse Proxy deployment, the client begins the session by sending packets to the WAF Gateway's inbound IP address. The WAF Gateway inspects the packets and based on the rules, opens a second connection to the server, changing the packet's source IP address to the WAF Gateway's outbound IP address and the destination IP address to the real IP address of the server. The following figure depicts a Reverse Proxy Deployment.

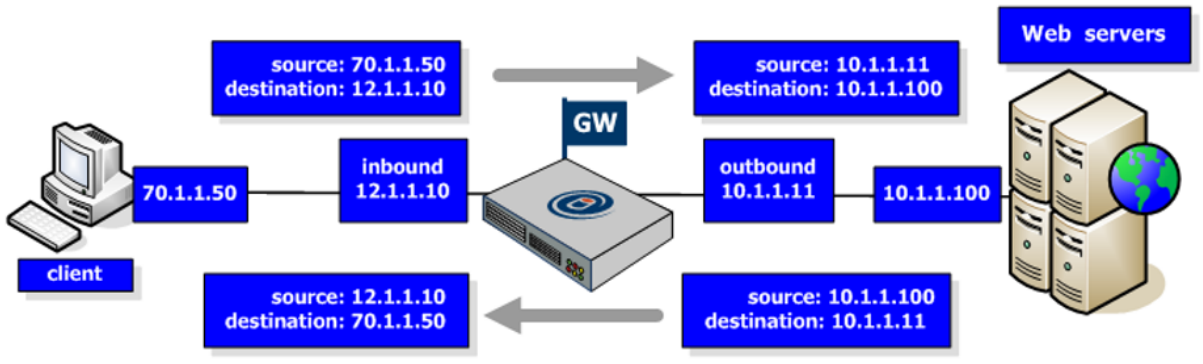


Figure 5: A Typical Reverse Proxy Deployment

A Reverse Proxy configured WAF Gateway can be deployed as a cluster of gateways behind a load balancer. The following figure depicts an example of a cluster gateway configuration. In this case, from the client's point of view, the server is the load balancer's inbound IP address. The server sends the return packets to the WAF Gateway, which inspect the packets and forwards them to the client, changing the source IP address to the Gateway's inbound IP addresses, and the destination IP address to that of the client. From the client's point of view, the server is the Gateway's inbound IP address. From the server's point-of-view, the client is the Gateway's outbound IP address.

A reverse proxy gateway can be deployed as a cluster of gateways behind a load balancer. In this case, from the client's point of view, the server is the load balancer's inbound IP address.

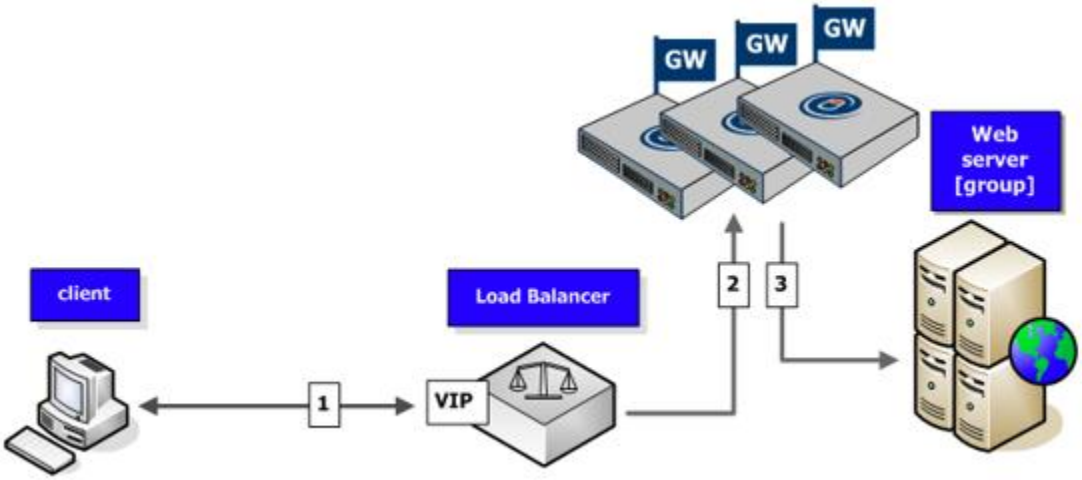


Figure 6: Reverse Proxy Deployed as a Cluster Behind a Load Balancer

1.6.6.1 Management Network

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

Separation between the production traffic and the OOB management network is achieved by allocating a separate (onboard) NIC for this purpose on WAF GWs. The WAF GWs operating system does not bridge or route packets between production NICs and Management NICs.

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

1.6.7 Web Application Firewall Functionality

1.6.7.1 Network Traffic Data Collection Modes

WAF v14.7P20 collects and records network traffic using either the sniffing, inline, or reverse proxy topologies described above. The traffic is analyzed using the TOE's IDS functionality. This section describes these different configurations.

1.6.7.1.1 Non-Inline (Sniffing)

When configured in sniffing topology, Imperva WAF is configured with one or more NICs in sniffing mode. Sniffing mode allows the appliance to read all frames transmitted on the monitored network segment. Frames picked up from the network are then passed to the appliance's analysis and reaction logic.

1.6.7.1.2 Inline (Bridge)

When configured in inline topology, WAF v14.7P20 appliances can be configured to bridge pairs of NICs. When bridging, frames are picked up from one network segment, and if the destination MAC address belongs to the paired segment, and the frame is not blocked by the analysis and reaction logic, the frame is transmitted it on the paired segment. This mode is known as "Transparent Bridge".

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

1.6.7.1.3 Transparent Reverse Proxy

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

This data collection mode can be used in bridge mode. In this case it is known as "Transparent Reverse Proxy in bridge mode."

1.6.7.1.4 Reverse Proxy (NGRP)

In non-Transparent mode, the gateway is assigned an IP address, and HTTP clients proxy traffic through the gateway. Reverse Proxy configurations are used to provide support for HTTP translation rules (e.g., URL rewriting). This mode is written completely in user space and uses OpenSSL v1.1.1n for cryptography purposes.

1.6.7.1.5 Fail-Safe Modes

WAF 14.7P20 Gateway appliances in inline topology can be configured to either block all traffic in the event of a software, hardware, or power failure, or to allow all traffic to pass transparently through the gateway. By default, the TOE uses safe mode.

1.6.7.2 Analysis and Reaction

Imperva WAF applies different layers of intrusion detection logic to analyzed network traffic. Some of these layers are applicable to all network traffic; some are relevant only for Web traffic. In addition, Imperva's Correlated Attack Validation (CAV) technology examines sequences of events and identifies suspicious traffic based on a correlation of multiple analysis layers. Identified malicious traffic is blocked.

Imperva WAF supports the following blocking methods:

- TCP Reset (sniffing topology): Imperva WAF can signal protected servers to disconnect malicious users using TCP reset, a special TCP packet that signals TCP peers to close the TCP session. Imperva WAF spoofs a TCP reset packet and sends it to the protected server. It is assumed that a standards-conformant server would immediately drop the attacker's session on receipt of the TCP reset packet. Note: TCP reset is considered inferior to inline blocking (see below) because it does not actively block the malicious traffic from reaching the server; blocking depends on the server's correct and timely session termination behavior.
- Inline Blocking: the WAF appliance drops the packet, so that it doesn't reach its intended destination, and sends a TCP reset to the server. Note: When Imperva WAF blocks a web connection, it can be configured to display an error page to the blocked user.
- Reverse Proxy Blocking: the WAF drops the packet and closes the connection with the server. To the blocked client, the WAF will send a pre-defined HTML error page and then close the connection.

1.7 TOE Documentation

The physical boundary includes the following guidance documentation.

- *Imperva 14.7 WAF Administration Guide, version 1, May 2023*
- *Imperva 14.7 WAF Management Server Manager User Guide, version 1, May 2023*
- *Imperva 14.7 WAF API Reference Guide, version 1, May 2023*
- *Imperva Application Firewall User Guide, version 1, May 2023*
- *Imperva WAF GW 14.7 Evaluated Configuration Guidance v1.2, 2023-07-17*
- *Imperva v14.7 WAF System Events Reference Guide, Version 1, May 2023*

2 Security Problem Definition

2.1 Introduction

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

A. The TOE usage assumptions in the suggested operational environment.
B. The alleged known threats that will be countered by the TOE
C. The organizational security policies that the TOE must adhere to

2.2 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

2.2.1 Intended Usage Assumptions

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

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

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

A.TIME The NTP server configured in the TOE for synchronization must be accurate and reliable so when the TOE acts as a server itself, it will provide good timestamps.

2.2.2 Physical Assumptions

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

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

2.2.3 Personnel Assumptions

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

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

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

2.3 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment. Threats are identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides.

2.3.1 TOE Threats

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

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.FACCNT An unauthorized user's attempts to access TOE data or security functions goes undetected.

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions of the monitored IT System 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.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 TOE'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

2.3.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity, allowing unauthorized or malicious users to exploit vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources, allowing unauthorized or malicious users to exploit vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source, allowing unauthorized or malicious users to exploit

vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors, allowing careless or unauthorized users to access or adversely manipulate protected data undetected.

T.MISUSE Undetected authorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors, allowing unauthorized or malicious users to exploit weaknesses in the system or gain unauthorized access to protected data.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors, allowing unauthorized or malicious users to exploit weaknesses in the system or gain unauthorized access to protected data.

2.4 Organizational Security Policies

The organizational security policies are defined as follows.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.MANAGE The TOE shall only be managed by authorized users.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3 Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 2.

3.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.AUDIT_PROT	The TOE must provide the capability to protect audit information
O.AUDIT_SORT	The TOE must provide the capability to sort the audit information
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must collect system data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSCAN	The TOE must collect and store system data information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.SDC	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.TIME	The TOE must provide a reliable time source.

3.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE:

OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected with competency and trustworthiness in mind and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that the software of the TOE and the hardware where it runs is protected from any physical attack, including administrator workstations and OOB network.
OE.TIME	The IT Environment (external NTP server and hardware clock sources) will provide reliable timestamps to the TOE.

4 Extended Components Definition

This ST defines the following extended components for use within this ST.

4.1 Class FAU: Security audit

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

4.1.1 Security audit event storage (FAU_STG)

Family behaviour

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

Component levelling

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

Management: FAU_STG.5

There are no management activities foreseen.

Audit: FAU_STG.5

There are no auditable events foreseen.

FAU_STG.5 Audit export and purge

Hierarchical to:

No other components.

Dependencies:

FAU_GEN.1

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

4.2 Class FCS: Cryptographic support

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

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

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

4.2.1 HTTPS (FCS_HTT)

Family behaviour

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

Component leveling

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

Management: FCS_HTT.1

There are no management activities foreseen.

Audit: FCS_HTT.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:

a) Basic: Failure to establish a session.

b) Basic: Establishment/termination of a session.

FCS_HTT.1: HTTPS

Hierarchical to:

No other components.

Dependencies:

FCS_TLS.1

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

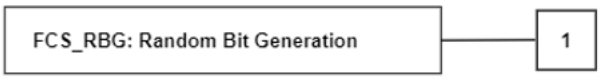
FCS_HTT.1.2 ***The TSF shall implement HTTPS using TLS as specified in FCS_TLS.1.***

4.2.2 Random Bit Generation (FCS_RBG)

Family behaviour

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

Component leveling



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

Management: FCS_RBG.1

There are no management activities foreseen.

Audit: FCS_RBG.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:

a) Basic: Failure of the randomization process.

FCS_RBG Random Bit Generation

Hierarchical to:

No other components.

Dependencies:

No dependencies.

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

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

4.2.3 TLS (FCS_TLS)

Family behaviour

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

Component leveling

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

Management: FCS_TLS.1

There are no management activities foreseen.

Audit: FCS_TLS.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:

a) Basic: Failure to establish a session.

b) Basic: Establishment/termination of a session.

FCS_TLS.1 TLS

Hierarchical to:

No other components.

Dependencies:

FCS_COP.1

FCS_TLS.1.1 ***The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246), TLS1.3 (RFC 8446)] supporting the following ciphersuites: [assignment (ciphersuite supported)].***

4.3 Class IDS: Intrusion Detection System

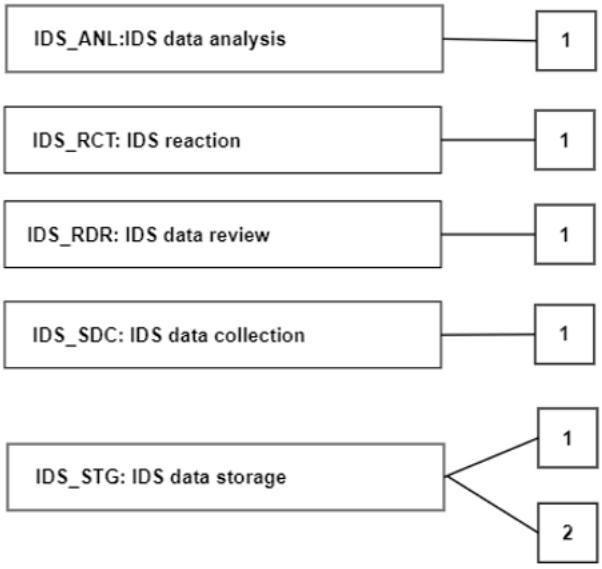
Introduction

This class is used to satisfy security objectives that pertain to intrusion detection and prevention (IDS/IPS) systems. These include data collection and analysis, automatic reaction capabilities, review, and IDS data analysis (IDS_ANL).

Informative notes

A class of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose

of this class of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing, and managing the data.

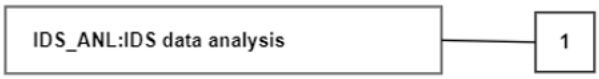


4.3.1 IDS data analysis (IDS_ANL)

Family behaviour

This family defines requirements for automated means that analyze IDS System data looking for possible or real security violations. The actions to be taken based on the detection can be specified using the IDS reaction (IDS_RCT) family as desired.

Component leveling



In IDS_ANL.1 Analyser analysis, statistical, signature, or integrity-based analysis is required.

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the parameters of the analytical functions.

Audit: IDS_ANL.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:

b) Minimal: Enabling and disabling of any of the analysis mechanisms.

IDS_ANL.1 IDS data analysis

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

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

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

4.3.2 IDS reaction (IDS_RCT)

Family behaviour

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

Component leveling

At IDS_RCT.1 IDS reaction, the TSF shall send an alarm and take action when an intrusion is detected.

Management: IDS_RCT.1

The following actions could be considered for the management functions in FMT:
a) the management (addition, removal, or modification) of actions.

Audit: IDS_RCT.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:
a) Minimal: Actions taken due to detected intrusions.

IDS_RCT.1 IDS reaction

Hierarchical to:

No other components.

Dependencies:

IDS_ANL.1

IDS_RCT.1.1 ***The System shall send an alarm to [assignment: alarm destination] and take [assignment: appropriate actions] when an intrusion is detected.***

4.3.3 IDS data review (IDS_RDR)

Family behaviour

This family defines the requirements for tools that should be available to authorised users to assist in the review of IDS System data.

Component leveling

IDS data review, provides the capability to read information from the System data and requires that there are no other users except those that have been identified as authorised users that can read the information.

Management: IDS_RDR.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data.

Audit: IDS_RDR.1

The following actions should be auditable if FAU_GEN is included in the PP/ST:

a) Basic: Reading of information from the System data.

b) Basic: Unsuccessful attempts to read information from the System data.

IDS_RDR.1 IDS data review

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

IDS_RDR.1.1 ***The System shall provide [assignment: authorised users] with the capability to read [assignment: list of System data] from the System data.***

IDS_RDR.1.2 ***The System shall provide the System data in a manner suitable for the user to interpret the information.***

IDS_RDR.1.3 ***The System shall prohibit all users read access to the System data, except those users that have been granted explicit read access.***

4.3.4 IDS data collection (IDS_SDC)

Family behaviour

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

Component leveling

IDS data collection defines the information to be collected from the targeted IT System resource(s), and specifies the data that shall be recorded in each record.

Management: IDS_SDC.1

There are no management activities foreseen.

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 IDS data collection

Hierarchical to:

No other components.

Dependencies:

FPT_STM.1

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

a) [selection*: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability, policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.1.2 **At a minimum, the System shall collect and record the following information:**

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) [assignment: *other additional information*].

4.3.5 IDS data storage (IDS_STG)

Family behaviour

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

Component leveling

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

Prevention of System data loss specifies actions in case of exceeded storage capacity.

Management: IDS_STG.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the actions to be taken in case of storage failure.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 Guarantees of System data availability

Hierarchical to:

No other components.

Dependencies:

IDS_SDC.1

IDS_STG.1.1 ***The System shall protect the stored System data from unauthorized deletion.***

IDS_STG.1.2 ***The System shall protect the stored System data from modification.***

IDS_STG.1.3 ***The System shall ensure that [assignment: metric for saving System data] System data will be maintained when the following conditions occur: [selection: System data storage exhaustion, failure, attack].***

IDS_STG.2 Prevention of System data loss

Hierarchical to:

No other components.

Dependencies:

IDS_STG.1

IDS_STG.2.1: ***The System shall [selection: 'ignore System data', 'prevent System data, except those taken by the authorised user with special rights', 'overwrite the oldest stored System data'] and [assignment: other actions to be taken in case of storage failure] if the storage capacity has been reached.***

5 Security Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 5, and from the extended components defined in Section 4.3 above.

5.1 TOE Security Functional Requirements

Table 3: TOE Security Functional Components

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.2 Guarantees of audit data availability
	FAU_STG.4 Prevention of audit data loss
	FAU_STG.5 Audit export and purge
FCS: Cryptographic support	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.2 Cryptographic key distribution
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic operation
	FCS_HTT.1 HTTPS
	FCS_RBG.1(1) Random Bit Generation (WAF Gateway)
	FCS_RBG.1(2) Random Bit Generation (Management Server)
	FCS_TLS.1(1) TLS (Traffic Connections)
	FCS_TLS.1(2) TLS (HTTP GUI)
	FCS_TLS.1(3) TLS (ADC Content)
	FCS_TLS.1(4) TLS (Inter-TOE)
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
FMT: Security management	FMT_MOF.1 Management of security functions behaviour
	FMT_MTD.1 Management of TSF data
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles

Requirement Class	Requirement Component
FPT: Protection of the TSF	FPT_ITT.1 Basic internal TSF data transfer protection
	FPT_STM.1 Reliable time stamps
FTP: Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel
	FTP_TRP.1 Trusted path
IDS: Intrusion Detection	IDS_ANL.1 IDS Analyser analysis
	IDS_RCT.1 IDS Analyser react
	IDS_RDR.1 IDS Restricted data review
	IDS_SDC.1 IDS System data collection
	IDS_STG.1 Guarantees of System data availability
	IDS_STG.2 Prevention of System data loss

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

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

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

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

c) [

- *All configuration changes. This includes all actions (CUD = Create, Update, Delete) on all entities (policies, users, roles, authentication schema, authorization schema, permissions, access or communication keys, certificates, lists of signatures, lists of IP addresses).*
- *Export of information from WAF.*
- *Purge of information.*
- *All actions related to patch and version changes – availability of a new version, installation on a machine, failure to install.*
- *WAF deployment changes.*
- *Failover events, MXs registration and removal from SOM, adding or removing gateways, gateway move within group/cluster or out of it.*
- *All actions related to users and permissions – including the above (CUD) – and also accessing these screens.*
- *Access to the audit screens.*

].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

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

5.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*Administrators with appropriate permissions*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_SAR.2 Restricted audit review

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

5.1.1.4 FAU_SAR.3 Selectable audit review

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

5.1.1.5 FAU_STG.2 Guarantees of audit data availability

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

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

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

5.1.1.6 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [**"**overwrite the oldest stored audit records**"**] and [*send an alarm*] if the audit trail is full.

5.1.1.7 FAU_STG.5 Audit export and purge

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

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*IFC Key Pair Generation, ECC Key Pair Generation*] and specified cryptographic key sizes [*2048 or more bits for IFC Key Pairs; 256, 384 or 521 bits for ECC Key Pairs*] that meet the following: [*FIPS PUB 186-4, "Digital Signature*

Standard (DSS)" Appendix B.3; FIPS PUB 186-4, "Digital Signature Standard (DSS) Appendix B.4].

5.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall **establish** ~~distribute~~ cryptographic keys in accordance with a specified cryptographic key **establishment** ~~distribution~~ method [*FFC Schemes using "safe-prime" groups, elliptic curve schemes*] that meets the following: [*NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"; NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, and groups listed in RFC 3526*].

5.1.2.3 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwriting with zeroes*] that meets the following: [*FIPS 140-2 level 1*].

5.1.2.4 FCS_COP.1 Cryptographic operation (symmetric cryptography)

FCS_COP.1.1 The TSF shall perform [*the cryptographic operations listed in the table below*] in accordance with a specified cryptographic algorithm [*listed in the table below*] and cryptographic key sizes [*listed in the table below*] that meet the following: [*FIPS 140-2 level 1 and the standards identified in the table below*].

Table 4: Cryptographic Operations

Operation	Algorithm	**Key Size**	**Standard**
encryption and decryption	AES-CBC, AES-GCM	128 and 256 bits	AES as specified in ISO 18033-3, CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772
	AES-CTR	128, 192 and 256 bits	
cryptographic signature services	RSA Digital Signature Algorithm (rDSA)	2048 bits or greater	FIPS Pub 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5
	Elliptic Curve Digital Signature Algorithm (ECDSA)	256, 384 and 521 bits	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D; ISO/IEC 14888-3, Section 6.4

Operation	Algorithm	**Key Size**	**Standard**
cryptographic hashing services	SHA-1, SHA-256, SHA-384, SHA-512	160, 256, 384 and 512 bits	FIPS Pub 180-4, 'Secure Hash Standard.'
keyed-hash message authentication	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384 and 512 bits	FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-4, 'Secure Hash Standard.'

5.1.2.5 FCS_HTT.1 HTTPS

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

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

5.1.2.6 FCS_RBG.1(1): Random Bit Generation (WAF Gateway)

FCS_RBG.1.1(1) The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using CTR_DRBG (AES)] seeded by an entropy source that accumulates entropy from [a software-based noise source].

FCS_RBG.1.2(1) The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application note: Iteration (1) applies to the WAF Gateway.

5.1.2.7 FCS_RBG.1(2): Random Bit Generation (Management Server)

FCS_RBG.1.1(2) The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using HMAC DRBG (any)] seeded by an entropy source that accumulates entropy from [a TSF-hardware-based noise source].

FCS_RBG.1.2(2) The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application note: Iteration (2) applies to the Management Server.

5.1.2.8 FCS_TLS.1(1): TLS (Traffic Connections)

FCS_TLS.1.1(1) The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246), TLS.1.3 (RFC 8446)] supporting the following ciphersuites: [

- *TLS_RSA_WITH_AES_256_CBC_SHA,*
- *TLS_RSA_WITH_AES_128_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA256,*

- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*].

Application note: Iteration (1) applies to the traffic connections in reverse proxy mode.

5.1.2.9 FCS_TLS.1(2): TLS (HTTP GUI)

FCS_TLS.1.1(2) The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- *TLS_RSA_WITH_AES_128_CBC_SHA,*
- *TLS_RSA_WITH_AES_128_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA*].

Application note: Iteration (2) applies to the HTTPS GUI connection.

5.1.2.10 FCS_TLS.1(3): TLS (ADC Content)

FCS_TLS.1.1(3) The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- *TLS_RSA_WITH_AES_128_CBC_SHA,*
- *TLS_RSA_WITH_AES_256_CBC_SHA,*
- *TLS_RSA_WITH_AES_128_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA256,*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA,*
- *TLS_DHE_DSS_WITH_AES_128_CBC_SHA,*
- *TLS_DHE_DSS_WITH_AES_256_CBC_SHA*].

Application note: Iteration (3) applies to the ADC Content update connection.

5.1.2.11 FCS_TLS.1(4): TLS (Inter-TOE)

FCS_TLS.1.1(4) The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- *TLS_RSA_WITH_AES_128_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA256,*
- *TLS_RSA_WITH_AES_256_CBC_SHA,*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*].

Application note: Iteration (4) applies to the inter-TOE communications.

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*user identity, authentication data, and authorisations*].

5.1.3.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.3 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of security functions behaviour

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

5.1.4.2 FMT_MTD.1 Management of TSF Data

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

5.1.4.3 FMT_SMF.1 Specification of Management Functions

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

Table 5: Specification of Management Functions

SFR	Management Function	Required Authorisations	Management Functionality
FMT_MOF.1	Modify the behaviour of the functions of System data collection, analysis and reaction	Authorised System administrator	Authorised System administrators use the Imperva GUI or via OpenAPI interface to modify Server Group definitions, define Action Interfaces and Action Policies, configure Security Rules for each Server Group, enable collection, analysis and reaction capabilities, and manage Profiles and Signatures.

SFR	Management Function	Required Authorisations	Management Functionality
FMT_MTD.1	Query audit data	Authorized administrator with appropriate permissions	Audit records are stored as System Events and may be reviewed using the Imperva GUI or via OpenAPI. Format or as System Events reports.
	Query and add System data	Authorised administrator with View permission on applicable objects	Authorised administrators can use the WAF GUI or via OpenAPI interface to review System data for which they have View permission, to update Profiles and Signatures and to invoke assessments.
	Query (export) and modify (create, delete, import) audit archive protection keys	Authorised administrator with Settings permission	Authorised administrators with Settings permission can use the OpenAPI or Imperva GUI interface to create, delete, import and export and to set the default RSA keys used for signing and encrypting archived audit data.
	Query and modify all other (non-System and audit) TOE data	Authorised administrator	Authorised administrators can use the OpenAPI or WAF GUI interface for reviewing and modifying all other TOE data (e.g., jobs or tasks).
FMT_SMR.1	Modify the group of users that are part of a Imperva WAF role	Authorised System administrator	Imperva GUI or via OpenAPI allows authorised administrators belonging to the Administrators group with access to the Users and Roles screen, providing the ability to add, edit, and delete user accounts, and reset their passwords.

5.1.4.4 FMT_SMR.1 Security roles

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

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

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

5.1.5.2 FPT_STM.1 Reliable time stamps

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

Application note: This SFR is implemented by the TOE using an NTP server used by the MX Management Server which provides reliable timestamps to its WAF GWs.

5.1.6 Trusted Path/Channels (FTP)

5.1.6.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[**the TSF**]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*ADC Content*].

5.1.6.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, *[all subsequent user interactions]*].

5.1.7 Intrusion Detection (IDS)

5.1.7.1 IDS_ANL.1 IDS data analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received: a**)** [signature, integrity] ; and b) [*Matching traffic with ThreatRadar Block Lists, Protocol violations, Profile violations, Correlated Attack Validation*].

IDS_ANL.1.2 The System shall record within each analytical result at least the following information: a) Date and time of the result, type of result, identification of data source; and b) [*destination server Group and username*].

5.1.7.2 IDS_RCT.1 IDS reaction

IDS_RCT.1.1 The System shall send an alarm to [*MX Server, syslog server, SNMP trap*] and take [*action to block and/or monitor application network traffic*] when an intrusion is detected.

5.1.7.3 IDS_RDR.1 IDS data review

IDS_RDR.1.1 The System shall provide [*authorized Administrators*] with the capability to read [*Alerts, audit records, collected application profiles, System configuration and Gateway Status*] from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read access.

5.1.7.4 IDS_SDC.1 IDS data collection

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s): [service requests, network traffic, detected known vulnerabilities] ; and b) [*none*].

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

Table 5: System Data Collection Events and Details

Event	Details
Service requests	Specific service, source address, destination address
Network traffic	Protocol, source address, destination address
Detected known vulnerabilities	Identification of the known vulnerability

5.1.7.5 IDS_STG.1 Guarantees of System data availability

IDS_STG.1.1 The System shall protect the stored System data from unauthorised deletion.

IDS_ STG.1.2 The System shall protect the stored System data from modification.

IDS_ STG.1.3 The System shall ensure that [*250,000 Alert records*] System data will be maintained when the following conditions occur: [System data storage exhaustion].

5.1.7.6 IDS_STG.2 Prevention of System data loss

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

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

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL2 augmented with ALC_FLR.1 Basic flaw remediation components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components. The assurance requirements are identified in the following table. These requirements reference Part 3 of the *Common Criteria for Information Technology Security Evaluation*. The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2.

Table 6: Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.1: Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims
	ASE_ECD.1: Extended components definition
	ASE_INT.1: ST introduction
	ASE_OBJ.2: Security objectives
	ASE_REQ.2: Derived security requirements
	ASE_SPD.1: Security problem definition
	ASE_TSS.1: TOE summary specification
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

5.2.1 Development (ADV)

5.2.1.1 ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 ADV_FSP.2 Security-enforcing functional specification

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 ADV_TDS.1 Basic design

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance Documents (AGD)

5.2.2.1 AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle Support (ALC)

5.2.3.1 ALC_CMC.2 Use of a CM system

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 ALC_CMS.2 – Parts of the TOE CM coverage

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 ALC_DEL.1 Delivery procedures

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.4 ALC_FLR.1 Basic flaw remediation

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target Evaluation (ASE)

5.2.4.1 ASE_CCL.1 Conformance claims

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 ASE_ECD.1 Extended components definition

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

5.2.4.3 ASE_INT.1 ST introduction

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

5.2.4.4 ASE_OBJ.2 Security objectives

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.5 ASE_REQ.2 Derived security requirements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.6 ASE_SPD.1 Security problem definition

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.7 ASE_TSS.1 TOE summary specification

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Tests (ATE)

5.2.5.1 ATE_COV.1 Evidence of coverage

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 ATE_IND.2 Independent testing – sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability Assessment (AVA)

5.2.6.1 AVA_VAN.2 Vulnerability analysis

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.1C The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6 TOE Summary Specification

This section describes the following security functions implemented by the TOE to satisfy the SFRs claimed in Section 5.

6.1 FAU: Security audit

6.1.1 FAU_GEN.1

The MX Management Server hosts a database that is used for storing audit records (System Events), IDS System data (Alerts), application Profiles, user attributes and configuration information.

The System Events Log includes activities related to

- changes to configuration,
- ADC content updates,
- activation of settings,
- building profiles,
- automatic profile updates,
- server start/stop,
- OpenAPI and GUI logins/logouts, and
- user administration operations.

For each event, the following attributes are recorded in the MX database on the MX Management Server:

- Event Time: Date and time of the event.
- Sub System: The subsystem that generated the log entry, e.g., User, platform, ADC, security etc.
- Severity: One of: high, medium, low, info.
- Message: A description of the event. For administrator login events, this includes the user's IP address.
- User: The username that generated this event. If the event was generated by the WAF system, the username is 'System'.

Each system log record includes the following information: date and time of the event, type of event, subject identity, Severity, and object IDs (primary URI) where applicable. Location is identified by the administrator's IP address. The outcome (success or failure) of the related event is implied from the event Type.

The SOM administrator can pre-select System Event types that will be automatically forwarded from the MX server to the SOM for storage and audit review by the SOM administrator. System Events are also generated by the SOM (e.g., for SOM administrator logins and SOM user account management) and are stored locally on the SOM server.

6.1.2 FAU_SAR.1 and FAU_SAR.2

The Imperva GUI and the OpenAPI interface allows users to read audit information from the audit records using a Web-based interface. Users without access authorisations to OpenAPI or Imperva GUI cannot view audit records.

6.1.3 FAU_SAR.3

Imperva GUI and the OpenAPI interface allow authorised administrators to perform sorting of audit data based on date and time, subject identity (username), and event type. The success or failure of the related event is implied from the event type.

6.1.4 FAU_STG.2, FAU_STG.4, FAU_STG.5

System Events log records are stored in a MX Management Server database table and may also be forwarded for storage on a corresponding SOM database. The TOE does not provide any interface for modifying audit records. Audit records can only be archived and purged by an authorized System administrator via the Imperva GUI management interface.

By default, the MX Management Server retains up to 100,000 System Event records and purges the oldest records when this configurable threshold is exceeded. An authorized System administrator with appropriate permissions can modify this threshold or specify a time period for which System Event records must be retained. System Event records can also be archived to external storage before being purged on a defined schedule. An alarm can be configured to be sent to an Action Interface if the audit trail is full.

The authorised administrator may schedule automatically generated recurring reports that are sent from the MX Management Server in CSV or PDF format to an administrator-specified email address, containing all or a subset of the stored audit records.

6.2 FCS: Cryptographic support

6.2.1 FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1, FCS_HTT.1, FCS_RBG.1(1), FCS_RBG.1(2), FCS_TLS.1(1), FCS_TLS.1(2), FCS_TLS.1(3), FCS_TLS.1(4)

Passwords
Administrator passwords for locally defined users are stored using BcryptPasswordEncoder version $2a hashes in a database located on the MX Management Server.

Random Number Generation (FCS_RBG.1(1), FCS_RBG.1(2))
The WAF Gateways implement a software-based deterministic random bit generator that complies with NIST SP 800-90, using CTR_DRBG (AES) seeded with 256 bits of entropy. On the X10K2, X8520, X6520, X4520, X2520, X10K, X8510, X6510 and X2510 appliances, the entropy source is the RDRAND instruction provided by Intel Ivy Bridge-based processors, which is assumed to provide 0.5 bits of entropy per bit sample. The same entropy source is also used on virtual gateway appliances, which require an Ivy Bridge-based processor on the hosting hardware. On X4510 appliances, the entropy

source is an Infineon SLB96xx Trusted Platform Module (TPM) processor, which is assumed to provide 1 bit of entropy per bit sample (i.e., full entropy).

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

HTTP/TLS (FCS_HTT.1, FCS_TLS.1(2))
Imperva GUI is a browser-based interface to the MX that allows authorised administrators to access TOE management functions. It is implemented by a Web server component on the MX. The TOE's HTTPS protocol complies with RFC 2818 and is implemented using TLS 1.2 (RFC 5246) supporting the following ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, and TLS_RSA_WITH_AES_256_CBC_SHA.

Key agreement supports DH with FFC schemes using "safe-prime" groups and elliptic curve schemes. For FFC, key sizes of 2048 bits and greater are supported. For elliptic curve, P-256 and P-384 are supported.

HTTP over TLSv1.2 as well as the same ciphersuites are also used for the internal TOE component communications.

TLS WAF GW Traffic in Reverse Proxy mode (FCS_HTT.1, FCS_TLS.1(1))
The TOE's TLS protocol complies with RFC 2818 and is implemented using TLS v1.2 (RFC5246) and TLSv1.3 (RFC 8446) supporting the following ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384.

Key agreement supports DH with FFC schemes using "safe-prime" groups and elliptic curve schemes. For FFC, key sizes of 2048 bits and greater are supported. For elliptic curve, P-256, P-384 and P-521 are supported.

ADC content updates (FCS_TLS.1(3))

The TOE retrieves ADC content updates from the trusted Imperva Server using a secure TLS v1.2 (RFC5246) channel supporting the following ciphersuites: TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA .

Inter-TOE communication (FCS_TLS.1(4))

The TOE uses TLS v1.2 to secure communications between the separate TOE components and supports the following ciphersuite: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

Key agreement supports RSA with key sizes of 2048 bits and greater and elliptic curve with P-256, P-384, and P-521.

Sending audit (FCS_COP.1)
An authorised administrator can configure the TOE to automatically archive and/or purge the audit files on a defined schedule. Archiving sends the audit files in CSV format to an external audit server. To protect the archived audit data from unauthorised read access or modification, the TOE encrypts and signs the files.

The TOE uses the following cryptographic operations in support of higher level protocols such as HTTPS and TLS as well as for protecting the archived audit data.

Table 7: Cryptographic Operations

Function	Algorithm	Options
Random Number Generation. Symmetric key generation	[SP 800--90] DRBG Prediction resistance	HMAC DRBG, no reseed CTR DRBG (AES), no derivation function
Encryption/Decryption	[FIPS 197] AES	128/256 CBC and GCM
		128/192/256 CTR
Hash	[FIPS 180-4]	SHA-1, SHA-2 (256, 384, 512)
Keyed Hash	[FIPS 198-1] HMAC	SHA-1, SHA-2 (256, 384, 512)
Digital Signature	[FIPS 186-4] RSA	SigGen PKCS1.5/PSS, SigVer PKCS1.5/PSS
	[FIPS 186-4] ECDSA	SigGen/SigVer P-256, P-384,P-521
Asymmetric Key Generation	[FIPS 186-4] RSA	KeyGen Mode B.3, 2048
	[FIPS 186-4] ECDSA	KeyGen P-256,P-384, P-521

The TOE is designed to cryptographically destroy (zeroization) secret and private keys when they are no longer required by the TOE. The TOE performs all zeroization automatically by calling Bouncy Castle APIs that perform an “Overwrite with a fixed string of zeroes; then delete”. The zeroization applied to keys stored on RAM disk refers to the fixed data structures in the file system where the keys permanently reside, until they are no longer needed and subsequently deleted. The TOE’s zeroization method ensures Keys and CSPs zeroized from the storage locations as identified in the table below are unrecoverable.

Table 8: Key/CSP Zeroization Summary

#	Key/ CSP Name	Generation/ Algorithm	Description	Storage
CSP1	RSA private keys	RSA(2048 bits)	Identity certificates for the security appliance itself and also used in TLS negotiations	Key Store on Disk RAM (plain text)
CSP2	CA Certificates	RSA(2048 bits)	Trusted CAs	Trust Store on Disk RAM (plain text)
CSP3	Proxy Credentials	Secret (plain text)	Usernames and passwords for protected machines	Transit (TLS with secrets generated by RSA-2048 private keys)
CSP4	SIEM Credentials	Secret	Used for sending syslog messages	See CSP3
CSP5	External Machines Certificates	Various, can be shared secrets of any kind	Public Keys of machines for integration authentication	See CSP3
CSP6	Machine	Secret	admin login	Stored encrypted as a Linux Hash saved on disk

6.3 FIA: Identification and authentication

6.3.1 FIA_ATD.1

The Imperva application on the MX Management Server maintains the following required security attributes in the MX database (described above for FAU_GEN.1) for each authorised administrator user, as follows:

- User identity – Username
- Authentication data –Hashed Password
- Authorisations – Role assignments, user-specific permissions

6.3.2 FIA_UAU.2 and FIA_UID.2

The Web Server component on the MX Management Server requires identification and authentication for all Imperva GUI and OpenAPI requests. The Web Server requires HTTP Basic Authentication from the user and sends the user's password to the Imperva application on the MX Management Server for validation against the authentication data stored in the database.

6.4 FMT: Security management

6.4.1 FMT_MOF.1, FMT_MTD.1, FMT_SMR.1

As explained above for FIA_ATD.1, each authorised administrator may be associated with role(s) and user-specific permissions in the OpenAPI and Imperva GUI.

Roles are associated with permissions. Users associated with the role inherit these permissions in addition to any user-specific permissions they have been allocated. Permissions are evaluated for each user when the user logs in. They are associated with the user's session, and affect which objects are displayed and which operations may be performed.

The predefined Administrator role is granted all permissions and is the only out-of-the-box role that is allowed to access the Imperva GUI Admin workspace in order to manage MX server users, roles, and authorisations.

Permissions are defined on managed objects (Applications, Policies, Gateways, Sites, Servers, and Global Objects), as View, Edit, or Create. Edit permission implies View permission. Create permission implies Edit permission. An authorised administrator is defined in this ST (see FMT_SMR.1) to be an authorised System administrator for a subset of System data if assigned Edit permissions to the corresponding System objects. In particular, the predefined Web Security Admin role provide authorized System administrator permissions to the corresponding functional subsets of System data.

Special permissions allow users to activate settings and navigate to certain pages, e.g., the Alerts permissions allow access to the Alerts viewer or for viewing Alerts reports. In this example, users assigned with this special permission will only see report data regarding alerts generated on Server Groups for which they have View permission. In particular, the Settings permission is required for access to database audit archiving configuration and key management interfaces.

6.4.2 FMT_SMF.1

The Imperva GUI and OpenAPI interface is used by authorised administrators to manage all IDS/IPS System and audit capabilities as described in the following table.

Table 9: Management Functions

	Requirement Class	**Requirement Component**
FMT_MOF.1	Modify the behaviour of the functions of System data collection, analysis, and reaction	Authorised System administrators use the OpenAPI or Imperva GUI interface to modify Server Group definitions, define Action Interfaces and Action Policies, configure Security Rules for each Server Group, enable collection, analysis and reaction capabilities, and manage Profiles and Signatures.
FMT_MTD.1	Query audit data	Audit records are stored as System Events and may be reviewed using the Imperva GUI in an online tabular format or as System Events reports.

	Requirement Class	Requirement Component
	Query and add System data	Authorised administrators can use the Imperva GUI interface to review System data for which they have View permission, to update Profiles and Signatures and to invoke assessments.
	Query (export) and modify (create, delete, import) audit archive protection keys	Authorised administrators with Settings permission can use the OpenAPI or Imperva GUI interface to create, delete, import and export and to set the default RSA keys used for signing and encrypting archived database audit data.
	Query and modify all other (non-System and audit) TOE data	Authorised administrators can use the OpenSSL or Imperva GUI interface for reviewing and modifying all other TOE data (e.g., Tasks).
FMT_SMR.1	Modify the group of users that are part of a role	Imperva GUI allows authorised administrators belonging to the Administrators group with access to the Users and Roles screen, providing the ability to add, edit, and delete user accounts, and reset their passwords.

6.5 FPT: Protection of the TSF

6.5.1 FPT_ITT.1

The internal TOE transfer of TSF data is protected by the allocation of a physically separate NIC on both MX Management Server and WAF gateways for Gateway-Management Server communication, as explained in the ST introduction.

Neither the MX Management Server nor the WAF gateways route or bridge network traffic between the Management NIC and the production NICs. This separation provides a separate network domain for the Out of Band (OOB) management network, protecting all Gateway-MX Management Server communication from any access by authorised or unauthorised users.

ST introduction describes supported Imperva WAF deployment configurations. In both sniffing and bridging configurations (except for non-transparent reverse proxy configurations), Imperva Gateways do not have an assigned IP address on all sniffing/bridging network interface cards (NICs), so that the gateways cannot be directly attacked over the network.

FPT_ITT.1 requires protection of TSF data when it is transmitted between separate parts of the TOE, i.e., while it is in transit outside of the TOE. For protection between the TOE components, TLS v1.2 is used. In the case of audit archiving, the MX Management Server is sending the TSF data outside the TOE through untrusted media (the audit archive server) for later retrieval by same MX Management Server. The audit archive server does not have to be trusted to protect the data while it is outside the TOE – it is prevented from disclosing or modifying the data by the cryptographic protection applied to the data by

the TOE, as described for FCS_COP.1. The FPT_ITT term “separate parts of the TOE” is interpreted in this context to mean that there is a gap (of potential insecurity) that is traversed by the data.

6.5.2 FPT_STM.1

The MX Management Server and WAF gateways use the system real time clock that provides reliable timestamps for recorded System data. The MX Management Server synchronizes the gateways’ clocks with its own using the NTP protocol over the OOB management network. The MX Management Server’s clock can be synchronized with an external NTP server. An external NTP server providing a reliable time source is required.

6.6 FTP: Trusted path/channels

6.6.1 FTP_ITC.1

The TOE provides a trusted channel for the TOE to retrieve ADC content updates from the trusted Imperva Server. The channel is secured using TLS v1.2.

6.6.2 FTP_TRP.1

The TOE provides a trusted path for authorised administrator sessions to the OpenAPI and Imperva GUI. The MX Management Server allows remote users to initiate communication via the trusted path by establishing TLSv1.2 sessions, using RSA for Management Server authentication and a password for authenticating the administrator. This is required for all administrator sessions.

6.7 IDS: Intrusion Detection

6.7.1 IDS_ANL.1

Events that are matched by any of the ID analysis engines are recorded as an Alert. Security Rules applied when an Alert is generated are defined per Server Group. There are six categories of Security Rules, defined by the type of ID analysis layer that generated the Alert:

- Network Firewall Rules,
- Signature Rules,
- Protocol Violation Rules,
- Web Worm Defender Rules,
- Profile Violation Rules, and
- Correlation Rules.

Alert attributes include the following relevant fields:

- Alert Severity: Informative or Low, Medium, or High Severity.
- Time: date and time when the Alert was generated.
- Type:
  - Firewall,
  - Signature,
  - HTTP Worm,

  - Protocol Violation,
  - Profile Violation,
  - Correlation.
- Aggregated: Alert record is an aggregation of multiple network-level events.
- Source IP: the source IP address that generated the alert.
- Server Group: the name of the destination Server Group.
- Description: Alert identification
- Immediate Action: Blocked if the corresponding connection was blocked.
- User identity: The identity of the user associated with the event (if available).

In addition, Alert Type-specific information is recorded. Among other attributes, this may include source and destination ports, protocol (TCP/UDP/ICMP), service name (if recognized), and packet contents.

6.7.2 IDS_RCT.1

For each Security Rule, the Action Policy defined by the authorised System administrator can invoke two types of actions:

- Immediate Actions: actions taken as an immediate response to an attack. Imperva WAF can be configured to immediately react to a specific identified intrusion type by blocking the network packet that generated the security event (by dropping it when in inline topology), by closing the HTTP connection in reverse proxy topology, or by sending a TCP reset to the attacked server (when in sniffing topology) to cause it to disconnect the corresponding session.

- Followed Actions: follow-up actions taken by the System. An Action Set defines a set of actions and operations that are executed by Imperva WAF v14.7P20 as a result of an ID analysis. Configurable actions include:

  - Blocking Attacking IP: Blocking subsequent IP packets with a presumed source address equal to that recorded for the event, for a specified period of time.
  - Blocking Attacking Session: Blocking subsequent HTTP requests with the same session identifier as was recorded for the event, for a specified period of time.
  - Block User: Block subsequent requests associated with the same user as was identified for the event, for a specified period of time.
  - Dispatch Alert: Send alarm to specified Action Interfaces including relevant Alert details.
  - Start Monitoring-Record all requests/responses from the IP or session recorded for the event, for a specified period of time.

The available configurable alarms are: sending a syslog message to a syslog server or creating and sending an SNMP trap to an SNMP destination.

6.7.3 IDS_RDR.1

The Imperva GUI capability provides authorised administrators with the capability to read System data using a Web-based interface. Authorised administrator permissions are described for FMT_SMR.1.

Audit data archived outside the TOE is cryptographically protected as described for FCS_COP.1, preventing unauthorized access to the data

6.7.4 IDS_SDC.1

In both sniffing and bridging topologies, Imperva WAF collects all IP network traffic flowing between external and internal networks. Collected IP packets are recognized as UDP datagrams, TCP sessions, or other IP protocols, and forwarded to the TOE's analysis and reaction logic. As described above for IDS_ANL.1. Alerts may be generated by the analysis logic; these may be an indication of suspicious activity, or a result of an administrator request to monitor specified events.

In addition to collecting network traffic, the TOE provides application-level monitoring for service requests for Web resources (over HTTP and HTTPS protocols).

The TOE can identify HTML form-based Web identification and authentication events and associate the user's identity with the session. Because Web access often involves multiple HTTP sessions to the Web server for a single user session, the TOE can track Web session identifiers passed as HTTP parameters or in HTTP cookies, allowing it to trace users' activity more accurately across HTTP sessions.

6.7.5 IDS_STG.1, IDS_STG.2

Alerts and system data are sent by the Gateway that generates the Alert to the MX Management Server and stored in the Imperva database in a table that can hold up to 250,000 Alert records. When the table fills up, the MX Management Server switches to a second table of the same capacity, erasing its previous contents and overwriting them with new Alert records. The MX Management Server switches back to the first table when the second table fills up. This process guarantees that at the least the most recent 250,000 Alert records will be retained at any given point in time. An Alarm can be configured to be sent to a syslog server in the IT environment after a table switch is performed.

Recorded System data is reviewed by authorized Administrators via the Imperva GUI. Authorized Administrators can selectively delete System data but have no interface for modifying stored data. The TOE does not provide any interface for unauthorized users to access System data. The TOE extends protection to archived audit files by signing the files, allowing the TOE to detect any unauthorized modification of these files while outside the TOE. The TOE cannot prevent unauthorized deletion of data stored outside the TOE.

System data storage capacity is described for IDS_SDC.1. An authorized administrator may schedule automatically generated recurring reports that are sent from the MX Management Server in CSV or PDF format to an administrator-specified email address, containing all or a subset of the stored Alerts records. Audit files can be archived outside the TOE, either manually by the administrator or on an administrator-defined schedule.

7 TOE Rationale

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions, threats and policies are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

Table 10: Security Problem Definition to Security Objective Correspondence

Objectives / Threats	O.ACCESS	O.AUDITS	O.AUDIT_PROT	O.AUDIT_SORT	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.SDC	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.TIME
T.COMDIS	✓						✓					✓								
T.COMINT	✓						✓			✓		✓								
T.FACCNT		✓																		
T.IMPCON	✓				✓		✓								✓	✓		✓	✓	
T.INFLUX											✓									
T.LOSSOF	✓						✓			✓		✓								
T.NOHALT	✓					✓	✓	✓	✓						✓	✓		✓	✓	
T.PRIVIL	✓						✓					✓			✓	✓		✓	✓	
T.FALACT													✓							
T.FALASC						✓														
T.FALREC						✓														
T.INADVE		✓							✓											
T.MISUSE		✓							✓											
T.SCNVUL								✓												
P.ACCACT		✓		✓			✓							✓						✓
P.ACCESS	✓		✓				✓					✓								
P.ANALYZ						✓														
P.INTGTY										✓										
P.MANAGE	✓				✓		✓					✓			✓	✓		✓		
P.PROTCT											✓								✓	
A.ACCESS																	✓			

Objectives / Threats	O.ACCESS	O.AUDITS	O.AUDIT_PROT	O.AUDIT_SORT	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.SDC	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.TIME
A.ASCOPE																	✓			
A.DYNMIC																	✓	✓		
A.TIME																		✓		✓
A.LOCATE																			✓	
A.PROTCT																			✓	
A.NOEVIL																✓		✓		
A.NOTRST															✓				✓	
A.MANAGE																		✓		

7.1.1 Threats

This section shows that all threats are completely countered by the security objectives for the TOE or operational environment.

7.1.1.1 TOE Threats

T.COMDIS

An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

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

T.COMINT

An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

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

T.FACCNT

An unauthorized user's attempts to access TOE data or security functions goes undetected.

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

T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions of the monitored IT System to go undetected.

- The **OE.PERSON**, **OE.CREDEN**, **OE.PHYCAL** and **OE.INSTAL** security objectives for the operational environment together provides mitigation to this threat with responsible administrators and forbidden physical access to the TOE.
- The **O.EADMIN** objective ensures the TOE has all the necessary administrator functions to manage the product.
- The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses.
- The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX

An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

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

T.LOSSOF

An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

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

T.NOHALT

An unauthorized user may attempt to compromise the continuity of the TOE's collection and analysis functions by halting execution of the TOE.

- **OE.PERSON, OE.CREDEN, OE.PHYCAL and OE.INSTAL** security objectives for the operational environment together provides mitigation to this threat with responsible, trusted administrators and forbidden physical access to the TOE.
- The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses.
- The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- The **O.IDSCAN**, **O.SDC**, and **O.IDANLZ** objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE.

T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

- The **OE.PERSON**, **OE.CREDEN**, **OE.PHYCAL** and **OE.INSTAL** security objectives for the operational environment together provides mitigation to this threat with responsible administrators and forbidden physical access to the TOE.
- The **O.IDAUTH** objective provides for authentication of users prior to any TOE function accesses.
- The **O.ACCESS** objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- The **O.PROTCT** objective addresses this threat by providing TOE self-protection.

7.1.1.2 IT System Threats

T.FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity, allowing unauthorized or malicious users to exploit vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

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

T.FALASC

The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources, allowing unauthorized or malicious users to exploit vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

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

T.FALREC

The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source, allowing unauthorized or malicious users to exploit vulnerabilities in the monitored IT System or gain unauthorized access to protected data.

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

T.INADVE

Inadvertent activity and access may occur on an IT System the TOE monitors, allowing careless or unauthorized users to access or adversely manipulate protected data undetected.

- The **O.AUDITS** and **O.SDC** objectives address this threat by requiring a TOE to collect audit and system data.

T.MISUSE

Undetected authorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors, allowing unauthorized or malicious users to exploit weaknesses in the system or gain unauthorized access to protected data.

- The **O.AUDITS** and **O.SDC** objectives address this threat by requiring a TOE to collect system and audit data.

T.SCNVUL

Vulnerabilities may exist in the IT System the TOE monitors, allowing unauthorized or malicious users to exploit weaknesses in the system or gain unauthorized access to protected data.

- The **O.IDSCAN** objective counters this threat by requiring a TOE to collect and store system information that might be indicative of a vulnerability.

7.1.2 Organizational Security Policies

This section shows that all security policies are completely countered by the security objectives for the TOE or operational environment.

P.ACCACT

Users of the TOE shall be accountable for their actions within the IDS.

- The **O.AUDITS** objective implements this policy by requiring auditing of all data accesses and use of TOE functions.
- The **O.IDAUTH** objective supports this objective by ensuring each user is uniquely identified and authenticated.
- **O.AUDIT_SORT** supports this objective by allowing the administrator to sort audit data providing for user accountability
- **OE.TIME** and **O.TIME** together supports this OSP providing an accurate time and date.

P.ACCESS

All data collected and produced by the TOE shall only be used for authorized purposes.

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

P.**ANALYZ**

Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

- The **O.IDANLZ** objective requires analytical processes be applied to collected system data.

P.INTGTY

Data collected and produced by the TOE shall be protected from modification.

- The **O.INTEGR** objective ensures the protection of data from modification.

P.MANAGE

The TOE shall only be managed by authorized users.

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

P. PROTCT

The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

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

7.1.3 Assumptions

This section shows that all secure usage assumptions are completely covered by security objectives for the TOE or operational environment.

7.1.3.1 Intended Usage Assumptions

A.ACCESS

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

- The **OE.INTROP** objective ensures the TOE has the needed access.

A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

- The **OE.INTROP** objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.DYNMIC

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

- The **OE.INTROP** objective ensures the TOE has the proper access to the IT System.
- The **OE.PERSON** objective ensures that the TOE will be managed appropriately.

A.TIME

The NTP server configured in the TOE for synchronization must be accurate and reliable so when the TOE acts as a server itself, it will provide good timestamps.

- The **OE.PERSON** and **OE.TIME** ensures time is correctly configured for the TOE.

7.1.3.2 Physical Assumptions

A.LOCATE

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

- The **OE.PHYCAL** provides for the physical protection of the TOE.

A.PROTCT

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

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

7.1.3.3 Personnel Assumptions

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.

- The OE.PERSON objective ensures that the TOE administrators are carefully selected with competency and trustworthiness in mind and trained for proper operation of the System.
- The **OE.INSTAL** objective provides administrators with the instructions they are expected to abide by.

A.NOTRST

The TOE can only be accessed by authorized users.

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

A.MANAGE

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

- The **OE.PERSON** objective ensures all authorized administrators are qualified and trained to manage the TOE

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this ST are fully addressed in this section and each is mapped to the objective it is intended to satisfy. The following table summarizes the correspondence of functional requirements to TOE security objectives.

Table 11: SFR to Security Objective Correspondence

Objectives / SFRs	O.ACCESS	O.AUDITS	O.AUDIT_PROT	O.AUDIT_SORT	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.SDC	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME
FAU_GEN.1		✓												
FAU_SAR.1					✓									
FAU_SAR.2	✓						✓							
FAU_SAR.3				✓										
FAU_STG.2	✓		✓				✓			✓	✓	✓		
FAU_STG.4		✓									✓			
FAU_STG.5		✓									✓			
FCS_CKM.1	✓									✓		✓		
FCS_CKM.2	✓									✓		✓		
FCS_CKM.4	✓									✓		✓		
FCS_COP.1	✓									✓		✓		
FCS_HTT.1	✓									✓				
FCS_RBG.1(1)												✓		
FCS_RBG.1(2)	✓									✓		✓		
FCS_TLS.1(1)										✓		✓		
FCS_TLS.1(2)	✓											✓		
FCS_TLS.1(3)												✓		
FCS_TLS.1(4)												✓		
FIA_ATD.1							✓							
FIA_UAU.2	✓						✓							
FIA_UID.2	✓						✓							
FMT_MOF.1	✓						✓					✓		
FMT_MTD.1	✓						✓			✓		✓		
FMT_SMF.1	✓				✓		✓					✓		
FMT_SMR.1							✓							
FPT_ITT.1										✓		✓		

Objectives / SFRs	O.ACCESS	O.AUDITS	O.AUDIT_PROT	O.AUDIT_SORT	O.EADMIN	O.IDANLZ	O.IDAUTH	O.IDSCAN	O.SDC	O.INTEGR	O.OFLOWS	O.PROTCT	O.RESPON	O.TIME
FPT_STM.1														✓
FTP_ITC.1												✓		
FTP_TRP.1												✓		
IDS_ANL.1						✓								
IDS_RCT.1													✓	
IDS_RDR.1	✓				✓		✓							
IDS_SDC.1								✓	✓					
IDS_STG.1	✓						✓			✓	✓	✓		
IDS_STG.2											✓			

O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data.

- **FIA_UID.2**, **FIA_UAU.2:** Users authorized to access the TOE are defined using an identification and authentication process.
- **FMT_MOF.1**, **FMT_SMF.1:** The TOE is required to provide the ability to restrict managing the behaviour of functions of the TOE to authorized users of the TOE.
- **FMT_MTD.1:** Only authorized administrators of the System may query and add System and audit data, and authorized administrators may query and modify all other data.
- **FCS_HTT.1**, **FCS_TLS.1(2), FCS_CKM.1, FCS_CKM.2, FCS_CKM.4**, **FCS_RBG.1(2):** The connection to the user interface cannot be modified or intercepted because secure access mechanisms are implemented.
- **FAU_SAR.2:** The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- **IDS_RDR.1, FCS_CKM.1**, **FCS_COP.1:** The System is required to restrict the review of System data to those granted with explicit read access.
- **FCS_CKM.1**, **FCS_COP.1:** System archived audit data is encrypted.
- **FAU_STG.2:** The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure, or attack.
- **IDS_STG.1:** The System is required to protect the System data from any modification and unauthorized deletion.

O.AUDITS

The TOE must record audit records for data accesses and use of the System functions.

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

O.AUDIT_PROT

The TOE must provide the capability to protect audit information.

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

O.AUDIT_SORT

The TOE must provide the capability to sort the audit information.

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

O.EADMIN

The TOE must include a set of functions that allow effective management of its functions and data.

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

O.IDANLZ

The TOE must collect system data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

- **IDS_ANL.1:** The TOE is required to perform intrusion analysis and generate conclusions.

O.IDAUTH

The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

- **FAU_SAR.2:** The TOE is required to restrict the review of audit data to those granted with explicit read access.
- **IDS_RDR.1:** The System is required to restrict the review of System data to those granted with explicit read access.
- **FAU_STG.2:** The TOE is required to protect the stored audit records from unauthorized deletion.
- **IDS_STG.1:** The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack.
- **FIA_ATD.1:** Security attributes of subjects use to enforce the authentication policy of the TOE must be defined.

- **FIA_UID.2**, **FIA_UAU.2:** Users authorized to access the TOE are defined using an identification and authentication process.
- **FMT_MOF.1**, **FMT_SMF.1:** The TOE is required to provide the ability to restrict managing the behaviour of functions of the TOE to authorized users of the TOE.
- **FMT_MTD.1:** Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
- **FMT_SMR.1:** The TOE must be able to recognize the different administrative and user roles that exist for the TOE.

O.IDSCAN

The TOE must collect and store system data information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

- **IDS_SDC.1:** The TOE is required to collect and store system data information.

O.SDC

The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

- **IDS_SDC.1:** The TOE is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System.

O.INTEGR

The TOE must ensure the integrity of all audit and System data.

- **FAU_STG.2:** The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack.
- **IDS_STG.1** The System is required to protect the System data from any modification and unauthorized deletion.
- **FMT_MTD.1:** Only authorized administrators of the System may query or add audit and System data.
- **FPT_ITT.1**, **FCS_COP.1**, **FCS_TLS.1(1)**, FCS_TLS.1(2), **FCS_CKM.4**, **FCS_CKM.1 (MX), FCS_CKM.2 (MX):** The System must protect the collected data from modification and ensure its integrity when the data is transmitted internally and to remote IT systems.
- **FCS_COP.1**, **FCS_TLS.1(1)**, **FCS_HTT.1**, **FCS_RBG.1(2) (accessed by users):** The System must protect the collected data from modification and ensure its integrity when the data is transmitted internally and to remote IT systems.

O.OFLOWS

The TOE must appropriately handle potential audit and System data storage overflows.

- **FAU_STG.2:** The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack.
- **FAU_STG.4**, **FAU_STG.5:** The TOE must prevent the loss of audit data in the event its audit trail is full.

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

O.PROTCT

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

- **FAU_STG.2:** The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure, or attack.
- **IDS_STG.1:** The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack.
- **FMT_MOF.1**, **FMT_SMF.1:** The TOE is required to provide the ability to restrict managing the behaviour of functions of the TOE to authorized users of the TOE.
- **FMT_MTD.1:** Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
- **FTP_ITC.1**: The TOE provides a trusted channel to obtain ADC content updates from the trusted Imperva Server using TLS v1.2.
- **FTP_TRP.1:** The TOE provides a trusted path for remote users initiating communication for administrator sessions, protecting OpenAPI and Imperva GUI data and functions from unauthorized access over the network.
- **FPT_ITT.1**: It also prevents unauthorized modifications and access for TSF data transmitted between the separate parts of the TOE.
- **FCS_CKM.1, FCS_CKM.2**, , **FCS_TLS.1(1)**, **FCS_TLS.1(2), FCS_TLS.1(3), FCS_TLS.1(4)**, **FCS_CKM.4**, **FCS_COP.1**, **FCS_RBG.1(1), FCS_RBG.1(2):** This requires some cryptographic capabilities.

O.RESPON

The TOE must respond appropriately to analytical conclusions.

- **IDS_RCT.1:** The TOE is required to respond accordingly in the event an intrusion is detected.

O.TIME

The TOE must provide a reliable time source.

- **FPT_STM.1**: The NTP server in the management server provides a reliable time source

7.3 Security Assurance Requirements Rationale

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is intended for use in an environment with good physical access security where it is assumed that attackers will have Basic attack potential. The target assurance level of EAL2 is appropriate for such an environment. Augmentation was chosen to provide the added assurance that is gained by defining flaw remediation procedures. Therefore, the target assurance level of EAL2 augmented with ALC_FLR.1 is appropriate for such an environment.

7.4 SFR Component Hierarchies and Dependencies Rationale

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 12: TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied because FAU_STG.2 is hierarchical to FAU_STG.1
FAU_STG.5	No other components.	FAU_GEN.1	Satisfied
FCS_CKM.1	No other components.	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	FCS_COP.1 Satisfied FCS_CKM.4 Satisfied
FCS_CKM.2	No other components.	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.1 Satisfied FCS_CKM.4 Satisfied
FCS_CKM.4	No other components.	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1 Satisfied
FCS_COP.1	No other components.	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4,	FCS_CKM.1 Satisfied FCS_CKM.4 Satisfied
FCS_HTT.1	No other components.	FCS_TLS.1	Satisfied
FCS_RBG.1	No other components.	None	n/a
FCS_TLS.1	No other components.	FCS_COP.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	FIA_UID.1 is satisfied because FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UID.2	FIA_UID.1	None	n/a
FMT_MOF.1	No other components.	FMT_SMR.1, FMT_SMF.1	Satisfied, Satisfied
FMT_MTD.1	No other components.	FMT_SMR.1, FMT_SMF.1	Satisfied, Satisfied
FMT_SMF.1	No other components.	None	n/a

SFR	Hierarchical To	Dependency	Rationale
FMT_SMR.1	No other components.	FIA_UID.1	FIA_UID.1 is satisfied because FIA_UID.2 is hierarchical to FIA_UID.1
FPT_ITT.1	No other components.	None	n/a
FPT_STM.1	No other components.	None	n/a
FTP_ITC.1	No other components.	None.	n/a
FTP_TRP.1	No other components.	None	n/a
IDS_ANL.1	No other components.	IDS_SDC.1	Satisfied
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_SDC.1	Satisfied
IDS_SDC.1	No other components.	FPT_STM.1	Satisfied
IDS_STG.1	No other components.	IDS_SDC.1	Satisfied
IDS_STG.2	No other components.	IDS_STG.1	Satisfied

8 Abbreviations and Acronyms

Table 13: Abbreviations and Acronyms

Abbreviation and Acronyms	Definition
ADC	Application Defense Center
AES	Advanced Encryption Standard—a symmetric encryption algorithm
API	Application Programming Interface
CAV	Correlated Attack Validation
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CSV	Comma Separated Values
EAL	Evaluation Assurance Level
GCM	Galois/Counter Mode—a mode of operation for AES
GUI	Graphical User Interface
GW	Gateway
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ID	Intrusion Detection
IDS	Intrusion Detection System
IT	Information Technology
NGRP	Next Generation Reverse Proxy
NIC	Network Interface Card
NTP	Network Time Protocol
OOB	Out of Band
OSP	Organizational Security Policy
PDF	Portable Document Format
RSA	Rivest-Shamir-Adleman—an asymmetric cryptographic algorithm
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Function
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management

Abbreviation and Acronyms	Definition
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TAP	Terminal Access Point
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UDP	User Datagram Protocol