



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

Diseño e implementación de un firewall de aplicaciones web que permita optimizar la seguridad de los sites de un organismo adscrito al ministerio de energía y minas del Perú en el año 2021

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Omar Oswar MAIZ ORDOÑEZ

ASESOR

Mg. Juan Antonio APESTEGUIA INFANTES

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Maiz, O. (2024). *Diseño e implementación de un firewall de aplicaciones web que permita optimizar la seguridad de los sites de un organismo adscrito al ministerio de energía y minas del Perú en el año 2021*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Omar Oswar Maiz Ordoñez
Tipo de documento de identidad	DNI
Número de documento de identidad	76652540
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Juan Antonio Apesteguia Infantes
Tipo de documento de identidad	DNI
Número de documento de identidad	10423762
URL de ORCID	https://orcid.org/0000-0003-2545-0764
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Manuel Francisco Bermeo Noriega
Tipo de documento	DNI
Número de documento de identidad	08437735
Miembro del jurado 1	
Nombres y apellidos	Oscar Armando Casimiro Pariasca
Tipo de documento	DNI
Número de documento de identidad	06592392
Miembro del jurado 2	
Nombres y apellidos	Jean Carlos Malca Fernandez
Tipo de documento	DNI
Número de documento de identidad	45535181
Datos de investigación	
Línea de investigación	
Grupo de investigación	No Aplica
Agencia de financiamiento	No Aplica

Ubicación geográfica de la investigación	Edificio: Instituto Geológico, Minero y Metalúrgico País: Perú Departamento: Lima Provincia: Lima Distrito: San Borja Latitud: -12.08484 Longitud: -77.00909
Año o rango de años en que se realizó la investigación	Agosto 2021 – Diciembre 2021
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica https://purl.org/pe-repo/ocde/ford#2.02.01 Robótica, Control automático https://purl.org/pe-repo/ocde/ford#2.02.02 Sistemas de automatización, Sistemas de control https://purl.org/pe-repo/ocde/ford#2.02.03 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Telecomunicaciones https://purl.org/pe-repo/ocde/ford#2.02.05 Hardware, Arquitectura de computadoras https://purl.org/pe-repo/ocde/ford#2.02.06



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima I – Perú



ACTA DE SUSTENTACIÓN TRABAJO DE SUFICIENCIA PROFESIONAL

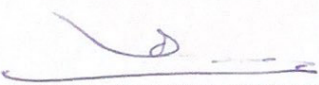
ACTA N°019/FIEE-CTGT/2024

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 01 de abril del 2024, como presidente de Jurado el **MG. MANUEL FRANCISCO BERMEO NORIEGA**, integrado por el Miembro de Jurado el **ING. OSCAR ARMANDO CASIMIRO PARIASCA**, el Miembro de Jurado **MG. JEAN CARLOS MALCA FERNANDEZ** y Miembro Asesor el **MG. JUAN ANTONIO APESTEGUIA INFANTES**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del Bach. **OMAR OSWAR MAIZ ORDOÑEZ** con código N° **14190091** que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL DE APLICACIONES WEB QUE PERMITA OPTIMIZAR LA SEGURIDAD DE LOS SITES DE UN ORGANISMO ADSCRITO AL MINISTERIO DE ENERGÍA Y MINAS DEL PERÚ EN EL AÑO 2021**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió aprobar otorgándole el calificativo de **17 (Diecisiete)**

Ciudad Universitaria, 01 de abril del 2024


MG. MANUEL FRANCISCO BERMEO NORIEGA

Presidente Jurado


ING. OSCAR ARMANDO CASIMIRO PARIASCA

Miembro Jurado


MG. JEAN CARLOS MALCA FERNANDEZ

Miembro jurado


MG. JUAN ANTONIO APESTEGUIA INFANTES

Miembro Asesor



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Vicerrectorado de Investigación y Posgrado



CERTIFICADO DE SIMILITUD

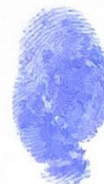
Yo Juan Antonio Apesteguía Infantes en mi condición de asesor acreditado con el Acta de Sustentación de Trabajo de Suficiencia Profesional: DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL DE APLICACIONES WEB QUE PERMITA OPTIMIZAR LA SEGURIDAD DE LOS SITIOS DE UN ORGANISMO ADSCRITO AL MINISTERIO DE ENERGÍA Y MINAS DEL PERÚ EN EL AÑO 2021, presentado por el bachiller Omar Oswar Maiz Ordoñez, para optar al título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 7% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**. Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado correspondiente.


Firma del Asesor

DNI: 10423762

Nombres y apellidos del asesor:

MG. JUAN ANTONIO APESTEGUIA INFANTES



DEDICATORIA

Este trabajo está dedicado a mis padres por su amor, paciencia y sacrificio durante todos estos años y por inculcarme el ejemplo de esfuerzo y valentía de afrontar las adversidades de la vida porque dios está conmigo.

A Bengy por ser siempre el hermano mayor que necesité, por mostrarme una nueva apreciación del significado y la importancia de la amistad y a mi hermanito Johan por estar siempre presente, sus existencias me mantuvieron soñando cuando quise rendirme. Los querré por siempre.

AGRADECIMIENTOS

A Dios por ser siempre mi soporte en mis metas y retos.

A mis padres y hermanos, por ser mi motivación para salir adelante aun así las cosas parecían imposibles.

A la Universidad Nacional Mayor de San Marcos, por brindarme muchas oportunidades y enriquecerme en conocimiento.

Esta es mi pequeña retribución.

A mi asesor, Dr. Juan Apesteguia, por su apoyo incondicional durante el desarrollo de la investigación.

Al Ing. Marco Quispe por las sugerencias y esclarecimientos.

A Jhessica mi compañera de universidad, de corazón y ahora de vida.

A todas las personas que me apoyaron en la realización de mi anhelo más deseado.

RESUMEN

En el presente trabajo de suficiencia profesional (TSP) se describe el desarrollo del diseño e implementación de un Firewall de Aplicaciones Web (WAF) en el Instituto Geológico, Minero y Metalúrgico (INGEMMET) con el objetivo de fortalecer la protección contra ciberamenazas.

La metodología del proyecto es aplicativa, tecnológica y analítica, enfocada en diseñar e implementar un WAF para fortalecer la seguridad en el INGENMET. Se ponderó la importancia de proteger el servidor web, aplicaciones e información asociada. El diseño del WAF incluye un modo de implementación para maximizar la compatibilidad e integración con la postura de seguridad actual en la red del INGENMET.

Se implementó el WAF en el INGENMET, siguiendo buenas prácticas y recomendaciones del fabricante. Se crearon sitios, grupos y aplicaciones, configurando políticas de seguridad. El sistema operó en modo simulación para monitorear violaciones y alertas, corrigiendo falsos positivos. Finalmente, se habilitó el modo activo para los servidores protegidos.

Como resultado, se obtuvo una protección óptima de las páginas y aplicativos webs del INGENMET, considerando las buenas prácticas en las políticas de seguridad del WAF. El trabajo actual detalla las consideraciones esenciales para un diseño e implementación adecuados de un WAF en una entidad gubernamental.

Palabras claves: waf, buenas prácticas, gateway, sites, ciberamenazas.

ABSTRACT

In this present Professional Sufficiency Project (PSP), the development of the design and implementation of a Web Application Firewall (WAF) at the Geological, Mining, and Metallurgical Institute (INGEMMET) is described with the aim of enhancing protection against cyber threats.

The project methodology is applied, technological, and analytical, focused on designing and implementing a WAF to strengthen security at INGEMMET. The significance of safeguarding the web server, applications, and associated information was emphasized. The WAF design includes an implementation mode to maximize compatibility and integration with the current security posture in INGEMMET's network.

The WAF was implemented at INGEMMET, following best practices and manufacturer recommendations. Sites, groups, and applications were created, and security policies were configured. The system operated in simulation mode to monitor violations and alerts, correcting false positives. Finally, the active mode was enabled for the protected servers.

As a result, optimal protection of INGEMMET's web pages and applications was achieved, considering best practices in WAF security policies. This work details essential considerations for a proper design and implementation of a WAF in a government entity.

Keywords: waf, the best practices, gateway, sites, cyber threats.

TABLA DE CONTENIDO

RESUMEN	IV
ABSTRACT	V
TABLA DE CONTENIDO	VI
LISTA DE FIGURAS	VIII
LISTA DE TABLAS	X
CAPÍTULO I: INTRODUCCIÓN	1
CAPÍTULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD	3
2.1. Institución – Actividad que desarrolla	3
2.2. Periodo de duración de la actividad.	3
2.3. Finalidad y objetivos de la entidad	3
2.4. Razón social	4
2.5. Dirección postal	4
2.6. Correo electrónico del profesional a cargo.	4
CAPÍTULO III DESCRIPCIÓN DE LA ACTIVIDAD	5
3.1. Organización de la actividad	5
3.2. Finalidad y objetivos de la Actividad	5
3.2.1. Finalidad	5
3.2.2. Objetivos	6
3.3. Problemática	6
3.3.1. Problema General	6
3.3.2. Problemas Específicos	7
3.4. Justificación e importancia de la investigación	7
3.5. Metodología	7
3.5.1. Bases teóricas	8
3.5.2. Marco conceptual	10
3.6. Procedimiento	16

3.6.1. Recopilación de información del INGEMMET	16
3.6.2. Diseño e Implementación del WAF en la infraestructura del INGEMMET	18
3.6.3. Monitoreo de las Alertas y violaciones	34
3.6.4. Validaciones de adecuada protección	39
3.6.5. Organigrama de responsabilidad de administración del WAF	42
3.7. Resultado de la actividad	44
CAPÍTULO IV: CONCLUSIONES	46
4.1. Justificación	46
4.2. Evaluación económica	46
4.3. Conclusiones	48
4.4. Recomendaciones	49
CAPÍTULO V: BIBLIOGRAFÍA	50
CAPÍTULO VI: ANEXOS	52

ÍNDICE DE FIGURAS

FIGURA 1: THE SITES TREE.	13
FIGURA 2: IMPLEMENTACIÓN DE MODO SNIFFING.	14
FIGURA 3: IMPLEMENTACIÓN DE MODO BRIDGE.	15
FIGURA 4: IMPLEMENTACIÓN DE MODO PROXY.	15
FIGURA 5: CUADRANTE MÁGICO PARA WAF.	18
FIGURA 6: TOPOLOGÍA REFERENCIAL DE LA UBICACIÓN DEL WAF.	24
FIGURA 7: EJEMPLO DE UN NUEVO SERVIDOR DESCUBIERTO Y ACEPTADO.	24
FIGURA 8: POLÍTICA APLICADO A UN SERVER GROUP.	25
FIGURA 9: POLÍTICA WEB APLICADO A UN SERVICIO.	25
FIGURA 10: POLÍTICA WEB APLICADO A LAS APLICACIONES.	25
FIGURA 11: UMBRALES DE APRENDIZAJE DE LOS PARÁMETROS DE CAMBIO A MODO PROTECCIÓN.	27
FIGURA 12: PROGRAMACIÓN DE ACTUALIZACIÓN DE THREATRADAR - PHISHING URLs.	27
FIGURA 13: ACTIVOS WEB PROTEGIDOS POR THREATRADAR - PHISHING URL.	28
FIGURA 14: POLÍTICA DE SEGURIDAD DE THREATRADAR.	28
FIGURA 15: CRITERIO DE COINCIDENCIA PARA APLICACIONES INFORMATIVAS.	29
FIGURA 16: POLÍTICA DE BLOQUEO POR INTENTOS DE INICIO DE SESIÓN INTERNACIONALES.	30
FIGURA 17: CONFIGURACIÓN DE ENMASCARAMIENTO.	30
FIGURA 18: CONFIGURACIÓN DE CAPTCHA.	31
FIGURA 19: POLÍTICAS DE THREATRADAR EMERGENCY FEED.	32
FIGURA 20: MODO ACTIVO EN UN SERVER GROUP.	33
FIGURA 21: PANEL DE ALERTAS.	34
FIGURA 22: CONFIGURACIÓN DE NOTIFICACIÓN DE ERROR AL DESCIFRAR EL TRÁFICO WEB.	35
FIGURA 23: EJEMPLO DE ERROR DE CERTIFICADO WEB.	36
FIGURA 24: EJEMPLO DE CIFRADO DH NO SOPORTADO.	36

FIGURA 25: PERFIL DE OPTIMIZACIÓN.	39
FIGURA 26: BLOQUEO DE IPs MALICIOSAS POR THREATRADAR.	40
FIGURA 27: BLOQUEO DE SQL INJECTION. FUENTE. INGEMMET 2021	40
FIGURA 28: VALIDACIÓN DE CORRECTO BLOQUEO CON HERRAMIENTA DE BLACKLIST DE MX TOOLBOX.	41
FIGURA 29: ESCANEO DE PÁGINA WEB DE INGEMMET CON EL WAF EN MODO SNIFFING.	41
FIGURA 30: ESCANEO DE PÁGINA WEB DE INGEMMET CON EL WAF EN MODO BRIDGE.	42
FIGURA 31: RESPUESTA DEL WAF EN MODO BRIDGE.	42
FIGURA 32: ORGANIGRAMA DE LA OSI- ADMINISTRADORES DEL WAF.	43

ÍNDICE DE TABLAS

TABLA 1: CARACTERÍSTICAS DISPONIBLES DE CADA MODO DE DESPLIEGUE	21
TABLA 2: IMPERVA BEST PRACTICE- OCCURRENCES SETTINGS FOR SWITCHING TO PROTECT MODE THRESHOLDS	26
TABLA 3: REPORTE DE LOS ÚLTIMOS 3 MESES AL CENTRO NACIONAL DE SEGURIDAD DIGITAL CON EL WAF EN MODO SNIFFING	44
TABLA 4: REPORTE DE LOS ÚLTIMOS 3 MESES AL CENTRO NACIONAL DE SEGURIDAD DIGITAL CON EL WAF EN MODO BRIDGE	45
TABLA 5: COMPARATIVA DE RESULTADOS DE ESCANEEO DE PÁGINAS WEB DEL INGEMMET.	45
TABLA 6: LISTA DE COSTOS DE EGRESOS	47
TABLA 7: LISTA DE COSTOS DE INGRESOS	47

CAPÍTULO I: INTRODUCCIÓN

Actualmente existen diversas soluciones de seguridad para la protección de ciberamenazas que atacan las páginas y aplicativos webs a nivel de capa de aplicación. Integrando un WAF de forma adecuada a la red de seguridad se puede mitigar los ciberataques.

El WAF Imperva permite la opción de brindar diferentes modos de operación según las necesidades del cliente, el modo proxy inverso, aplicado a la configuración del cliente INGEMMET, permite vigilar y bloquear el tráfico HTTP/S malicioso e impide que se filtre alguna información no autorizada.

El objetivo general es diseñar e implementar un WAF que permita optimizar la seguridad de los sites del INGEMMET. La pregunta central del trabajo es ¿De qué manera el diseño e implementación de un Firewall de Aplicaciones Web, permite optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú? La hipótesis está basada en que el diseño e Implementación de un WAF en modo proxy inverso permite optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.

El presente trabajo de suficiencia profesional (TSP) se desarrolló en base a los capítulos descritos a continuación:

En el capítulo 1, se describirá de forma general y resumida la problemática, objetivos, desarrollo, conclusiones y recomendaciones del trabajo de suficiencia profesional.

En el capítulo 2, se brindará la información pertinente del lugar donde se desarrolló la actividad, el periodo de duración del diseño e implementación del equipo de seguridad en las instalaciones del cliente, así como el personal a cargo del proyecto.

En el capítulo 3, se indicará de forma puntual los objetivos y problemática del presente trabajo con la finalidad de definir la estructura del enfoque y desarrollo del mismo. Asimismo, se detallarán los aspectos que se tomó en cuenta para el diseño e implementación de un firewall de aplicaciones web en el Instituto Geológico, Minero y Metalúrgico, las bases teóricas donde respaldamos las buenas prácticas aplicadas en las configuraciones tomando en cuenta la evaluación de riesgos y estrategias de mitigación ante nuevas y conocidas vulnerabilidades.

Finalmente, en los siguientes capítulos, se presentarán las conclusiones y recomendaciones donde se indica que ante las pruebas realizadas se evidencia que existe una seguridad eficiente de los sites del cliente.

CAPÍTULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

En el presente capítulo se detalla la información de la empresa que desarrolló la actividad y donde se desarrolla la actividad.

2.1 Institución – Actividad que desarrolla

La institución donde se desarrolló la actividad es el Instituto Geológico, Minero y Metalúrgico, y quien realizó las actividades fue Imperia Soluciones Tecnológicas S.A.C.

2.2 Periodo de duración de la actividad.

La actividad se desarrolló durante el periodo del 15 de agosto del 2021 hasta el 15 de diciembre del 2021.

2.3 Finalidad y objetivos de la entidad

Imperia Soluciones Tecnológicas, es una empresa con amplia experiencia en el rubro de la tecnología y la ciberseguridad, emplean la disciplina, pasión y lealtad como pilares para brinda servicios de soporte, implementación, gestión

TI y gestión de ciberseguridad, su objetivo principal es de brindar soluciones tecnológicas que permitan optimizar y garantizar los procesos de sus clientes con la finalidad de mantener una alta calidad de servicios y garantizar su crecimiento.

2.4 Razón social

Imperia Soluciones Tecnológicas S.A.C con número de RUC 20552075341.

2.5 Dirección postal

La dirección de la empresa Imperia Soluciones Tecnológicas S.A.C es en la Av. Abel B Du Petit Thouars Nro. 1775 Int. 804

2.6 Correo electrónico del profesional a cargo.

El trabajo fue realizado por Imperia Soluciones Tecnológicas S.A.C a cargo de Hector Pessolano Tay con el correo electrónico hector.pessolano@imperia.com.pe.

CAPÍTULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

Las actividades en la entidad gubernamental se desarrollaron cumpliendo los plazos descritos en las bases integradas de la siguiente manera:

- Levantamiento de información sobre infraestructura interna, rubro de la entidad y antecedentes del mismo.
- Diseño e implementación del WAF de acorde a las necesidades del cliente.
- Descubrimiento y aseguramiento de servidores previamente desconocidos en la red.
- Aplicación de buenas prácticas en las configuraciones del WAF.
- Ajuste de los límites iniciales de aprendizaje para más exactitud en la creación de perfiles de protección para el tráfico web.
- Monitoreo de las alertas y violaciones de seguridad en los sites del cliente.
- Corroborar y verificar los resultados de la eficiencia de seguridad de los sites de INGEMMET.

3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

La finalidad del presente trabajo es optimizar la seguridad de las páginas y aplicativos internos de INGEMMET teniendo en consideración sus

necesidades y el rubro en el que se desempeña para proteger a la entidad de ataques cibernéticos.

3.2.2 Objetivos

A. Objetivo General.

Diseñar e Implementar un Firewall de Aplicaciones Web para optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.

B. Objetivos Específicos.

- Recolección de información previa para el diseño del WAF.
- Implementar las políticas de seguridad de cada aplicativo web
- Evaluar las mejores prácticas en el diseño e implementación de un WAF.

3.3 Problemática

3.3.3 Problema General

¿De qué manera el diseño e implementación de un Firewall de Aplicaciones Web, permite optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú ante un continuo incremento de ataques cibernéticos?

3.3.4 Problemas Específicos

- ¿Cómo obtener los parámetros necesarios para realizar el diseño de un WAF?
- ¿Qué consideraciones se deben de tomar para configurar las políticas de seguridad de los aplicativos webs?
- ¿Cómo realizar las mejores prácticas en el diseño e implementación de un WAF?

3.4 Justificación e importancia de la investigación

La justificación e importancia del desarrollo del presente trabajo es de carácter práctico por la necesidad de la protección de las páginas y aplicativos webs del INGEMMET ante un crecimiento abrupto de ataques cibernéticos y exposición de nuevas vulnerabilidades, en base a las necesidades del cliente se diseñó e implementó un WAF en modo transparent reverse proxy con el fin proteger los servidores web de algún agente malicioso. Tiene implicaciones trascendentales para salvaguardar la información tomando como base la triada CID (confidencialidad, integridad y disponibilidad) y aplicada a los servidores web y los SITES que contienen.

3.5 Metodología

La metodología y técnicas de recolección de datos que formaron parte de la realización de este proyecto y posteriormente análisis e identificación de los puntos críticos de vulnerabilidades en la red interna de la entidad INGEMMET es de tipo aplicativa, tecnológica y analítica. Se realizó la recopilación de información bibliográfica nacional e internacional para mostrar el enfoque de otros autores y el estado actual del conocimiento en el diseño e

implementación de un WAF que permita optimizar la seguridad a nivel de capa de aplicación. Para el diseño de la integración del WAF se tomó en consideración la importancia y criticidad que implica la protección del servidor web, aplicaciones que contienen y la información que resguardan, para integrar un modo de implementación que maximice la compatibilidad y la integración en la postura de seguridad existente de la red con el WAF.

3.5.5 Bases teóricas

A. Antecedentes internacionales

En el año 2020, el estudiante Cabezas Cedeño, Natalie de la PUCESE de Ecuador configuró el WAF Modsecurity de código abierto para fortalecer la seguridad y reducir las vulnerabilidades en un servidor web, implementó un ambiente de pruebas para probar la efectividad de protección ante diversos ataques cibernéticos, esto desarrollado en su proyecto de tesis titulada “CONFIGURACIÓN DEL FIREWALL DE APLICACIONES WEB MODSECURITY PARA PREVENIR DIVERSOS ATAQUES HACIA APLICACIONES WEB ALOJADOS EN SERVIDORES OPEN SOURCE” (Cabeza, 2020). El autor concluyó que la recopilación de información utilizando los comandos de nikto y nmap ayudaron a identificar los puertos abiertos, así mismo, la herramienta ssl labs permitió identificar los certificados y cifrados de los que carecía la página web del servidor. También se concluyó que la aplicación de los módulos de seguridad de MODSECURITY mitigaron los ataques DoS y DDoS que se realizaron con fines de prueba.

En el 2022, Ramírez Márquez, Jimmy F. en su tesis “ANÁLISIS, DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL FORTALECIMIENTO DE VULNERABILIDADES E INTEGRIDAD DE APLICACIONES WEB ACADÉMICAS”, tuvo como objetivo fortalecer la seguridad e integridad de aplicaciones web en la UTELVT, es por ello que en el desarrollo del presente trabajo en mención se implementó un ambiente de pruebas basados en la situación actual de los sites de la UTELVT y se realizó

un escaneo de vulnerabilidades orientados en la metodología OWASP usando herramientas de pentesting, identificando 3 vulnerabilidades críticas y desarrollando un sistemas que ayude a proteger las páginas internas y reducir las probabilidades de ocurrencia de fallo (Ramirez, 2022). El autor concluyó que la aplicación de la metodología OWASP reduce en más de un 98% las vulnerabilidades que tiene las aplicaciones web académicas.

En el 2021, Luque Tovar, Angela L. y Bravo Builes, Cristian B. en su tesis “DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE PROTECCIÓN CONTRA EL ATAQUE DE INYECCIÓN SQL, EN UN SERVIDOR VULNERABLE UTILIZANDO HERRAMIENTAS OPEN ACCESS”, analizaron y evaluaron las vulnerabilidades a las que se encontraba expuesta un servidor DVWA (Damn Vulnerable Web Application) al ejecutar diversos tipos de ataques de Inyección SQL, como resultado se concluyó que sin una solución dedicada de protección como lo es un WAF, el servidor estaba expuesto a robo de información sensible. Al realizar pruebas de pentesting con la implementación de 3 WAFs Open Source de diversas marcas, se evidenció que solo uno de ellos era el más viable y eficaz debido a que reconoció todos los intentos de vulneraciones como maliciosos y soportó múltiples ataques simultáneos, bloqueando el acceso no permitido. (Luque, 2021)

B. Antecedentes nacionales

En el 2019, Morocho Maldonado, Vicente en su investigación titulada “IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL EN LA RED DE DATOS DEL HOSPITAL NACIONAL DANIEL ALCIDES CARRIÓN”, donde describe el análisis y el desarrollo que se realizó para diseñar e implementar una infraestructura de red amparada en normas técnicas y buenas prácticas. En base al análisis situacional de la institución como su sistema de seguridad perimetral se determinó que se requiere una reestructuración física y lógica de la seguridad perimetral y los accesos permitidos por la institución. (Morocho, 2019). El autor concluyó que el uso de diversas soluciones de seguridad con limitaciones de licencia, hardware obsoleto y falta de mantenimientos lógicos

y físicos no hacen más que obstaculizar la aplicación de perfiles de seguridad a la red de datos del Hospital Daniel Alcides Carrión.

En el 2020, Taipe Domínguez, Daniel I. en su trabajo de investigación titulada “LA AUDITORÍA DE SEGURIDAD INFORMÁTICA Y SU RELACIÓN EN LA CIBERSEGURIDAD EN EL SECTOR PÚBLICO AÑO 2018”, analiza la implicancia que tienen las auditorias en la ciberseguridad de una entidad pública, haciendo uso de herramientas de ethical hacking para descubrir y posteriormente subsanar vulnerabilidades, las cuales guían a las instituciones a mantener sus activos de información más sensibles protegidas ante eventuales ataques cibernéticos. Concluyendo el presente trabajo descrito, se determinó que las entidades en el año 2018 no contaban con concientización de ciberseguridad y esto evidenciado en el análisis de riesgos realizadas en cada entidad. (Taipe, 2020)

En el 2021, Palacios Gallardo, Margaret L. en su trabajo de investigación titulada “APLICACIÓN DE PENTESTING EN EL ANÁLISIS DE VULNERABILIDADES DEL SISTEMA WEB DE GESTIÓN ADMINISTRATIVA DE LA EMPRESA DEVHUAYRA SAC HUANCAYO”, realizó pruebas de penetración, pentest, donde identificó y categorizó las vulnerabilidades encontradas en el sistema web de administración de una empresa privada obteniendo una matriz de riesgos que se utilizó para subsanar las vulnerabilidades encontradas en la entidad y garantizar los principios de seguridad (disponibilidad, integridad y confidencialidad) de sus activos. (Palacios, 2021).

3.5.6 Marco conceptual

A. Conceptos generales de seguridad

a) OWASP

OWASP es un proyecto gratuito dedicado a la búsqueda y lucha contra vulnerabilidades en software. Ofrece documentación, herramientas y foros para mejorar la seguridad en aplicaciones web, y su proyecto más importante es el informe OWASP Top 10, que presenta los 10 riesgos más importantes.

A continuación, se muestra el listado del top 10 de los riesgos de seguridad de las aplicaciones web según OWASP:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

b) Test de penetración o intrusión (Pentesting)

El Pentesting es una técnica de seguridad que busca identificar brechas en una organización mediante la realización de ataques consentidos. Existen tres tipos de pentesting: BlackBox, GrayBox y WhiteBox. El proceso se divide en cinco fases: Reconocimiento, Escaneo, Explotación, Post Explotación e Informe.

c) Herramientas para test de penetración

El pentesting requiere conocimientos avanzados de ciberseguridad y herramientas específicas para cada fase de la prueba. Para la fase de reconocimiento se utilizan herramientas como HTTRACK, WHOIS, NETCRAFT, RECON-NG; para la fase de escaneo de vulnerabilidades se usan NMAP, WIRESHARK, OPENVAS; y para la explotación de vulnerabilidades, herramientas como METASPLOIT, inyecciones SQL, XSS.

B. WAF.

Un Firewall de Aplicaciones Web (WAF) es una herramienta dedicada a la protección de tráfico web, nace con la necesidad de proteger a los servidores y las páginas web de ataques enfocados al protocolo HTTP y HTTPS, ataques como SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Skript injection, Cookie Poisoning y muchos más, estos tipos de ataques no pueden ser detectados ni por un Firewall ni por un IPS.

C. Gateway y MX

Un WAF está conformado por un Gateway y un centralizador de administración y generación de reportes conocido como MX. Ambas herramientas se sincronizan y trabajan en conjunto para proteger los activos web. Un MX contiene una base datos con todas las configuraciones realizadas, el Gateway inspecciona y aplica las configuraciones obtenidas del MX al tráfico web y reenvía al MX los eventos que hacen match con las políticas de seguridad, el MX analiza y alerta en función a los eventos compartidos por el Gateway, también almacena las violaciones de seguridad, alarmas del sistema, logs de auditoría y proporciona reportes.

D. Sites

Un Site es la agrupación de Servers Groups que contienen páginas y aplicativos webs que serán protegidos, representan el ambiente donde se encuentran los Servidores webs. Cada Server Group puede contener varias IPs de servidores que tengan afinidad entre ellos, como estar en cluster, ser idénticos, estar en alta disponibilidad, que contengan la misma aplicación web o base de datos o se encuentren en el mismo servidor. A la vez, el Server Group protege los recursos de las aplicaciones que contienen, como puede ser la IP del servidor, puertos, URLs, tabla de base de datos y otras características. (Imperva, 2022)

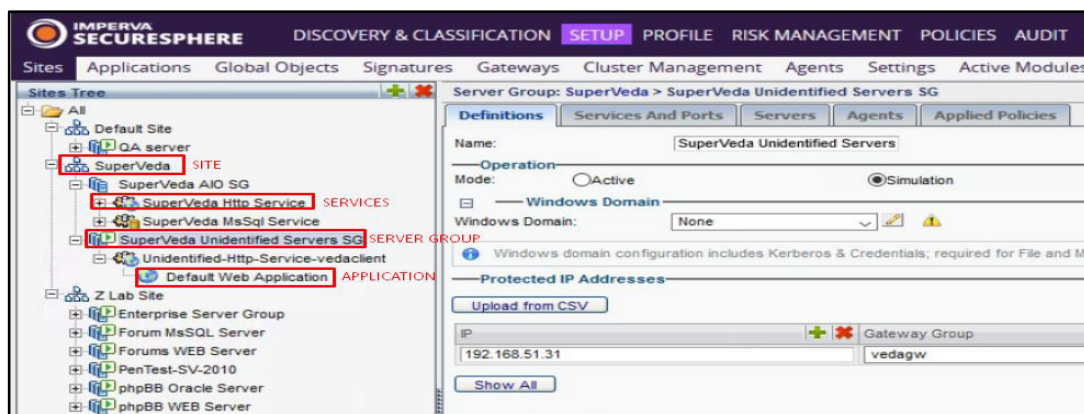


Figura 1: The Sites Tree. Fuente: Elaboración propia

E. Modos de operación del Server Group

El modo de operación del Server Group define la acción que realizará el Gateway con respecto al tráfico monitoreado, cada Server Group puede ser configurado para operar con un modo diferente. Existen tres modos de operación; Mode Disabled, donde se suspende el monitoreo y las acciones sobre ese Server Group, se utiliza para realizar troubleshooting, Mode Simulation, donde se monitorea y genera alertas de violaciones de seguridad, pero no se aplican acciones sobre el tráfico, se utiliza cuando el SecureSphere está aprendiendo, y Mode Active, donde se monitorea y aplican las acciones de las políticas configuradas en el servidor protegido. (Imperva, 2022)

F. Modos de operación del Gateway

La arquitectura del Gateway Imperva permite varios modos de implementación, brindando la posibilidad de integrar el equipo en redes ya existentes con mínimas interrupciones y cambios en la topología. Los modos de implementación son: Sniffing, Bridge y Proxy.

Modo Sniffing, se configura el equipo para recibir una copia del tráfico del servidor web para inspeccionarlo. Si el Gateway determina que los eventos

analizados son de carácter malicioso, envía un reset packet al servidor para que se corte la conexión con el cliente. (Imperva, 2022)

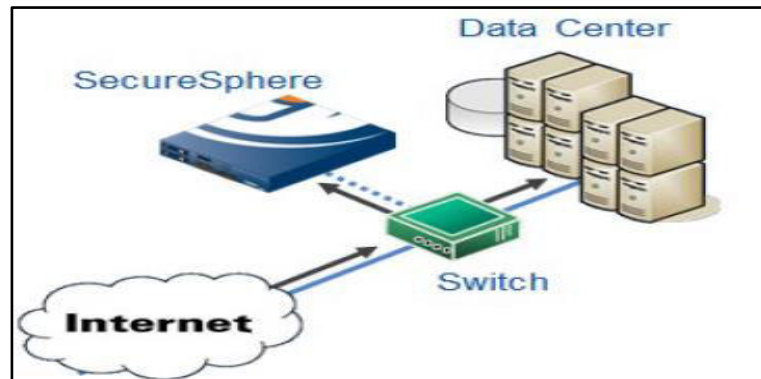


Figura 2: Implementación de modo sniffing. Fuente. Imperva (2022)

Modo bridge, el GW se integra entre el servidor y el cliente, analizando el tráfico pasante y enviando un RST packet al servidor protegido si detecta una acción maliciosa. Adicional a esto, envía una página de error al cliente con quien se tiene establecida la sesión y descarta todos los paquetes del mismo. (Imperva, 2022)

Así mismo, cuando se configura el WAF Imperva para trabajar en modo Bridge, también se puede habilitar la opción de trabajar por cada server Group como un TRP (Transparent Reverse Proxy). Con TRP habilitado, el WAF intercepta todas las solicitudes de los clientes y las redirige a la aplicación web. El WAF también intercepta las respuestas de la aplicación web y las envía de vuelta a los clientes. El tráfico de red se enruta a través del WAF de forma transparente, como si el WAF no estuviera allí.

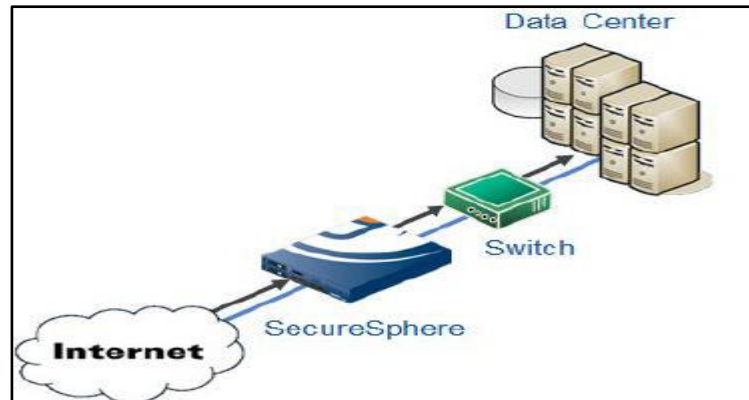


Figura 3: Implementación de modo bridge. Fuente. Imperva (2022)

En modo proxy, más conocido como reverse proxy, el Gateway establece conexiones independientes con el cliente y el servidor web protegido. De esta forma funciona como intermediario cuando el usuario realiza peticiones HTTP/S a los servidores web. (Imperva, 2022)

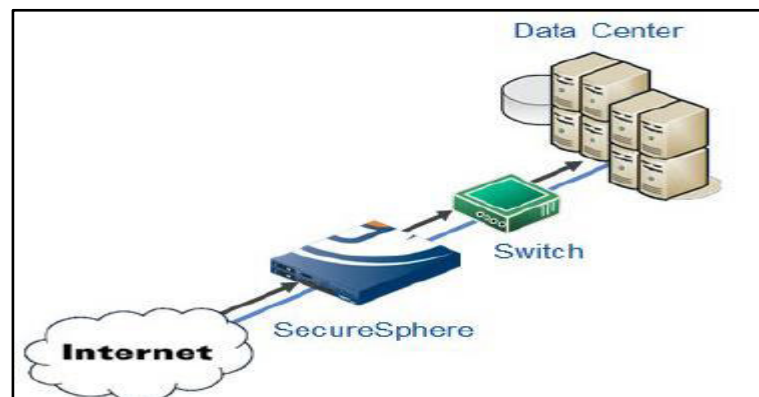


Figura 4: Implementación de modo proxy. Fuente. Imperva (2022)

G. ADC

Application Defense Center (ADC) es una organización que tiene como principal función brindar protección avanzada contra amenazas cibernéticas. El ADC en conjunto con Snorp proporcionan la protección más actualizada contra amenazas, así como las mejores prácticas de cumplimiento normativo más recientes. El centro de ADC brinda actualización sobre amenazas y

vulnerabilidades encontradas con una frecuencia de 2 semanas. (Imperva, 2020)

H. ThreatRadar

Es la principal fuente de información de amenazas para un WAF Imperva, provee 5 categorías de protección las cuales se enfocan en proporcionar información relevante contra las amenazas más recientes y problemáticas. ThreatRadar tiene suscripciones en Intelligence Reputation Services, Intelligence Community Defense, Anti Automation Bot Protection, Emergency Feed y Account Takeover Protection.

3.6 Procedimiento

El presente capítulo detalla el procedimiento del diseño e Implementación de un WAF en la sede principal del INGEMMET ubicado en la provincia de Lima y distrito de San Borja. El presente trabajo ha sido estructurado en 5 etapas:

3.6.7 Recopilación de información del INGEMMET

El primer paso para la implementación de un WAF es definir con exactitud que activos web se va proteger, esto es tan importante como la ubicación que debe tener la solución dentro de la topología del cliente y en qué modo de operación va a funcionar.

Para este proceso se solicita información detallada de los activos web como los descritos a continuación:

- El estado actual de sus activos web (Ejemplo: En desarrollo, en producción, otros).
- Cantidad de páginas y/o aplicativos webs de acceso interno y/o externo a proteger.

- Criticidad de los activos web.
- Dirección IP de servidores web donde se alojan las aplicaciones y sus CNAME (nombre de dominio).
- URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos HTTP, elementos XML / JSON y acciones SOAP / REST de cada uno de sus activos web a proteger.
- Enfoque de desarrollo de las páginas web.
- Activos web que cuentan con un balanceador o proxy.
- Puertos que tienen abiertos en cada servidor y aquellos que se permitirán o denegarán por cada uno de estos.
- IPs de los escáneres de vulnerabilidades u otras direcciones que se consideraran para una White list, entre otros.
- Certificados SSL.
- Área responsable del desarrollo y administración de los activos web.
- ¿Se cuenta con un WAF? En caso de contar con un equipo previo, brindar marca, modelo y modo de trabajo del WAF.
- Antecedentes de violaciones de seguridad sobre sus activos web.

Esta etapa es muy crítica ya que se validan posibles vulnerabilidades en la etapa de desarrollo del aplicativo, se recomiendan las acciones inmediatas en cuanto se detecte una brecha de seguridad en sus activos web.

A. Situación actual

El Ingemmet cuenta con un WAF Imperva desplegado en modo Sniffing el cual solo cumple con la funcionalidad de monitorear y alertar ante cualquier evento de vulneraciones hacia los aplicativos webs.

Los eventos de violaciones de seguridad no son bloqueados por el WAF, se alertan para que se pueda aplicar alguna acción correspondiente por otro equipo de seguridad o se corrija el inconveniente en el mismo site.

Los tiempos de respuesta para la mitigación de ataques dependen de un personal Humano y la solución que este provea.

3.6.8 Diseño e Implementación del WAF en la infraestructura del INGEMMET

Para realizar el diseño e implementación del WAF dentro de una topología existente, se debe tener en consideración los equipos de seguridad con los que interactuará el Gateway, las necesidades del cliente en base al TDR brindado y la información recolectada, como se vio en el capítulo anterior (3.6.7). A continuación, se presentan los procesos a tener en consideración para el diseño e implementación del WAF.

A. Comparativa de los proveedores de la solución WAF en el mercado

El cuadro de Gartner mostrado en la gráfica siguiente clasifica a los proveedores de soluciones WAF en función de su capacidad de ejecución y su visión estratégica. Esto se representa en cuatro cuadrantes: Líderes, Desafiadores, Jugadores de Nicho y Visionarios. Cada cuadrante representa un enfoque y características distintas de los proveedores, donde se observa que la solución Imperva, Cloudflare y Akamai son los líderes de este mercado y son quienes ofrecen soluciones completas y bien establecidas.



Figura 5: Cuadrante mágico para WAF. Fuente: Gartner, 2022

a) Comparativa de características de los vendors Akamai, Cloudflare e Imperva

Imperva

- **Amplia cobertura de seguridad:** Ofrece una amplia gama de capacidades de protección contra amenazas, incluyendo mitigación de ataques DDoS, prevención de bots y protección contra vulnerabilidades conocidas, como SQL Injection y Cross-Site Scripting (XSS).
- **Analítica avanzada:** Proporciona capacidades de análisis y reporte detalladas para identificar patrones de tráfico malicioso y mejorar la seguridad.
- **Integración con otros productos:** Imperva ofrece una suite de productos de seguridad en la nube, lo que permite una integración más estrecha con otras soluciones de seguridad para una protección más completa de las aplicaciones.
- **Costos:** Imperia al ser partner de Imperva y por la cantidad de años que viene trabajando de la mano con este vendor, obtiene descuentos muy favorables.
- **Interfaz de administración:** Imperva ofrece una interfaz de administración centralizada y amigable que permite configurar y gestionar las políticas de seguridad de manera intuitiva. Proporciona paneles de control, informes detallados y herramientas de análisis para facilitar la administración. Además, el Ingemmet contaba con una solución WAF en la marca Imperva así que la interfaz de administración ya le es familiar.
- **Distribución en el mercado peruano:** Imperva tiene presencia global y acapara más de un 50% del mercado peruano.

Akamai

- **Escalabilidad global:** La solución de WAF de Akamai se basa en su amplia red de distribución de contenido (CDN), lo que les permite proporcionar una protección escalable en todo el mundo.

- **Optimización de rendimiento:** Además de la seguridad, Akamai se enfoca en mejorar el rendimiento de las aplicaciones web al aprovechar su CDN y ofrecer optimización de contenido.
- **Gestión centralizada:** Proporciona una plataforma centralizada para administrar y configurar políticas de seguridad en múltiples aplicaciones y ubicaciones.

Cloudflare

- **Protección en la nube:** La solución de WAF de Cloudflare se ejecuta en su red global, lo que permite una protección distribuida y eficiente contra amenazas.
- **Fácil configuración:** Cloudflare se enfoca en la facilidad de uso y ofrece configuraciones predeterminadas para una implementación rápida, además de permitir personalizaciones según las necesidades específicas.
- **Capacidad de CDN:** Junto con la seguridad de aplicaciones web, Cloudflare ofrece servicios de CDN para acelerar la entrega de contenido y mejorar el rendimiento.

La solución seleccionada combina características particulares, una sólida distribución en el mercado peruano y una familiaridad previa con la plataforma. Lo que convierte a Imperva en la opción más adecuada para satisfacer las necesidades y objetivos del cliente.

B. Comparativa de los modos de operación del Gateway

A continuación, se mostrará una tabla con las principales características diferenciadas para los modos de operación del Gateway.

Tabla 1: Características disponibles de cada modo de despliegue

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes	
			Trans. RP	Kernel RP
Inspect TCP handshake	SI	SI	SI	SI
Latencia de bloqueo de tráfico	NO	SI	NO	NO
Session / cookie protection	SI	SI	SI	SI
Validación de entrada (lista blanca)	SI	SI	SI	SI
Detección de ataques (lista negra, incluidos ataques a aplicaciones, redes, servidores web y sistemas operativos)	SI	SI	SI	SI
Validación de ataques correlacionados	SI	SI	SI	SI
Bloquear ataques	SI	SI	SI	SI
Bloqueo de fugas de información (inspeccione el tráfico saliente en busca de datos confidenciales, números de tarjetas de crédito y datos que coincidan con firmas personalizadas)	SI	NO	SI	SI
Reescribir contenido	NO	NO	SI	SI
Aplicación de políticas de seguridad a nivel de firewall y protocolo de red	SI	NO	NO	NO
Redirigir al cliente a una página de error	SI	NO	SI	SI

Fuente: (Imperva, 2022).

Se puede ver con mucho más detalle otras características de cada modo de despliegue en los anexos 2, 3 y 4.

De lo observado en la *Tabla 1* y en los anexos 2, 3 y 4 se puede concluir que la mejor opción es el modo de trabajo Transparent Bridge, así mismo, hacer mención que en este modo de despliegue del gateway se puede habilitar el modo Transparent Reverse Proxy (TRP).

A continuación, se mostrará una comparación de las ventajas y desventajas del modo de despliegue actual y el que se consideró como la mejor opción según la Tabla 1.

a) Ventajas y desventajas del modo Bridge

Ventajas

- No requiere cambios de configuración en la red, lo que facilita su implementación.
- Permite la identificación y bloqueo de ataques en tiempo real sin afectar la disponibilidad de los recursos de red.
- Puede adoptar las funcionalidades y características de un TRP.

Desventajas

- Introduce latencia en el tráfico hacia una página web o base de datos.
- No puede bloquear el tráfico malicioso que no pasa por el dispositivo WAF.
- Puede afectar el rendimiento de la red si no se implementa correctamente.

b) Ventajas y desventajas del modo Sniffing (Actual)

ventajas

- La ventaja de usar un WAF en modo Sniffing es que no introduce latencia en la comunicación de un servidor y cliente de una página web o base de datos.
- No requiere cambios en la arquitectura de la red existente.

Desventajas

- El envío de TCP reset no es tan seguro como dropear paquetes cuando se quiere bloquear el tráfico de red. Puesto que el equipo fue desplegado con el único objetivo de monitorear y alertar no realiza bloqueos de tráfico.

- En ocasiones, cuando hay exceso de carga en los puertos SPAN estos pueden desechar paquetes, lo cual implica que SecureSphere no los podrá analizar.
- Este modo de operación es menos confiable ya que depende de los recursos del Switch, lo que implica que pueda haber perdidas de paquetes.
- El modo de sniffing puede no ser suficiente para identificar amenazas complejas que ocultan su comportamiento malicioso en el tráfico cifrado

Concluyendo de la información descrita anteriormente que la solución WAF Imperva en modo bridge es la opción más eficiente en términos de rendimiento, visibilidad, facilidad de implementación y protección más robusta contra las amenazas actuales y emergentes.

C. Ubicación del Gateway en la infraestructura del INGEMMET

Para diseñar e implementar un WAF, el primer procedimiento a realizar es ubicar la solución en la topología del cliente. El Ingemmet adquirió una solución ON PREMISE según las Bases solicitadas en el OSCE, es por ello que solo se debe de tener en consideración el modo de operación del Gateway para realizar la ubicación de la solución, por este motivo se le indicó las ventajas y desventajas que tienen el modo de operación del Gateway, siendo estos Sniffing, Bridge y Proxy, descritos con mayor detalle en el capítulo (3.5.6F).

El Ingemmet optó por la implementación del WAF en modo Bridge por las ventajas que proveía este modo de despliegue, de esta forma no se requirió asignar una IP a las interfaces para responder las peticiones web ya que lo harían los mismos servidores web.

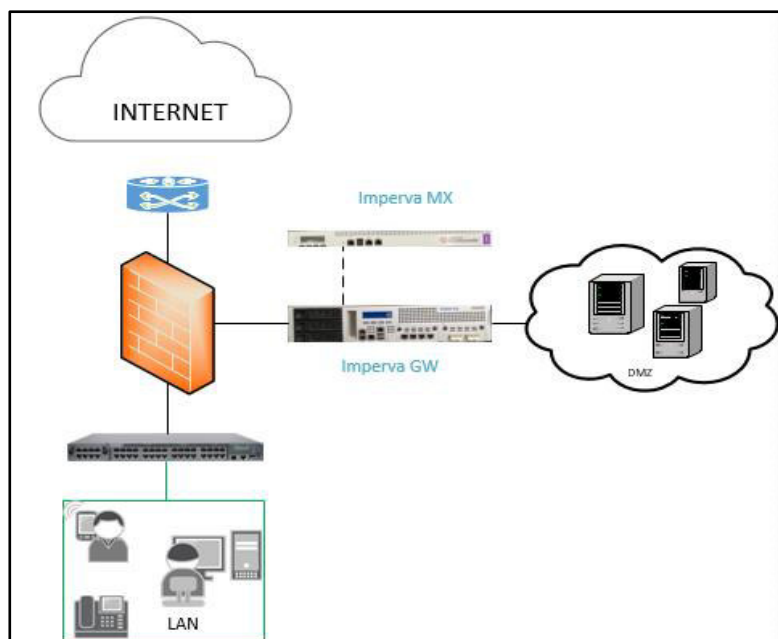


Figura 6: Topología referencial de la ubicación del WAF. Fuente. Propia

D. Escaneo de servidores con servicio HTTP/S

Imperva On-Prem WAF ofrece una función llamada Service Discovery Scans que permite a los administradores realizar el descubrimiento y aseguramiento de servidores previamente desconocidos en la red y que pueden presentar amenazas de seguridad si no se protegen. Los escaneos buscan respuesta de puertos específicos y protocolos específicos, por ejemplo, para aplicaciones web enfocados en protocolos HTTP, HTTPS y para aplicaciones de base de datos puertos como el 3306 o 1433. Adicionalmente, los servidores escaneados que se agregan en lo sites, se deben especificar que se añadan a la lista de IPs protegidas.

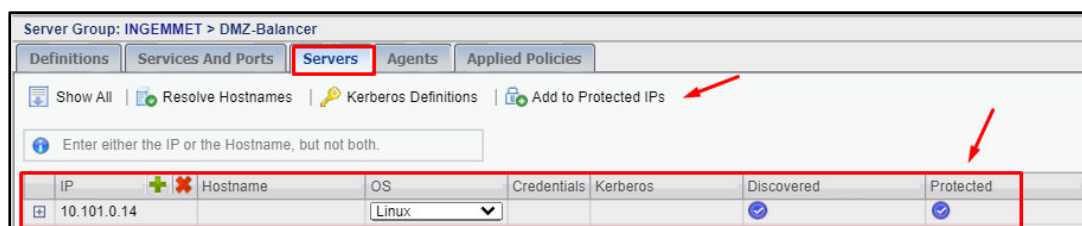


Figura 7: Ejemplo de un nuevo servidor descubierto y aceptado. Fuente. Propia.

E. Configuración de perfiles de seguridad para los sites del INGEMMET

SecureSphere tiene políticas predefinidas que protegen contra ataques y amenazas en aplicaciones web. Estas políticas se aplican automáticamente durante la configuración inicial y son actualizadas por el equipo del Centro de defensa de aplicaciones de Imperva (ADC). Estas políticas predefinidas tienen modificaciones limitadas y garantizan una protección eficaz.

A continuación, se muestran las políticas configuradas para el Ingemmet:

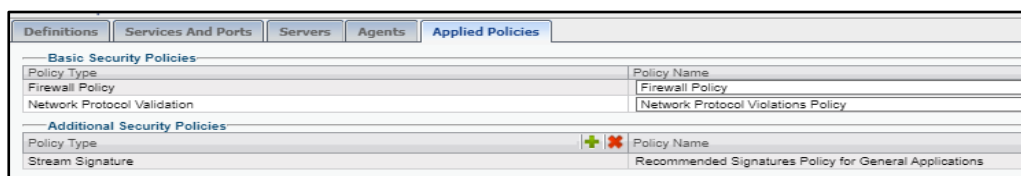


Figura 8: Política aplicado a un server group. Fuente. Ingemmet 2021

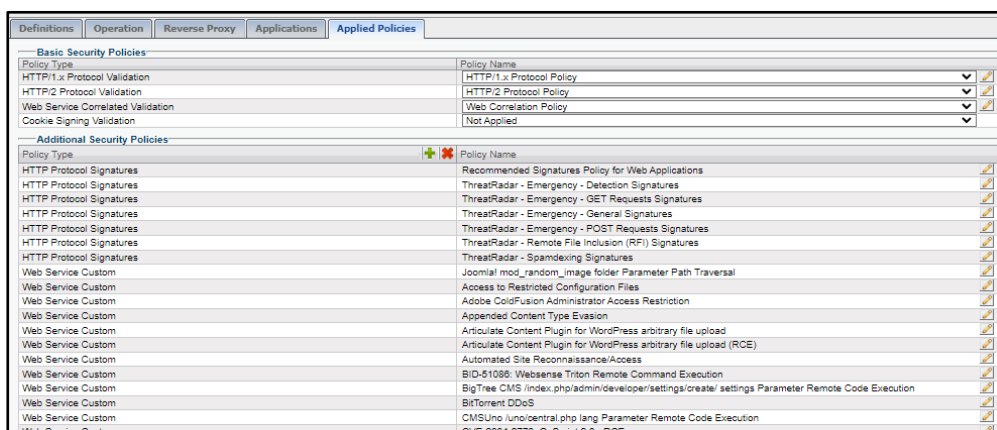


Figura 9: Política web aplicado a un servicio. Fuente. Ingemmet 2021

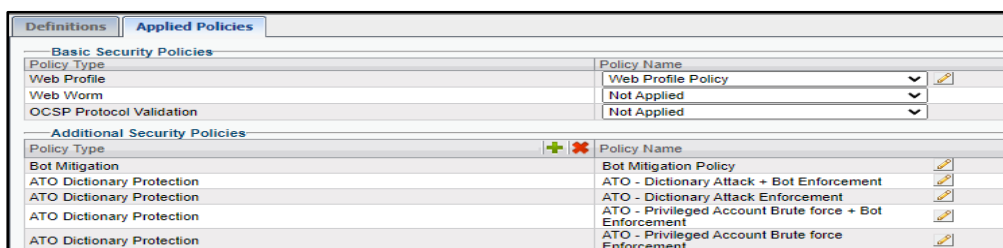


Figura 10: Política web aplicado a las aplicaciones. Fuente. Ingemmet 2021

Se puede tener mayor detalle sobre la funcionalidad de las políticas en los anexos 5,6,7,8 y 9

F. Best Practice para un despliegue exitoso

Se recomienda renombrar la aplicación por defecto al crear un nuevo Server Group. Si se cuenta con diversas aplicaciones web alojadas en el servidor protegido, se recomienda crear diferentes aplicaciones según la sensibilidad de cada uno. (Imperva, 2022, págs. 67-76)

Los valores por defecto del umbral de aprendizaje de las aplicaciones pueden ser muy agresivos o insuficientes para aplicaciones web más grandes que requieran mayor tiempo de aprendizaje, es por ello que el Fabricante recomienda ajustar la configuración basado en el tamaño y volumen de actividad de las aplicaciones web del cliente. (Imperva, 2022, pág. 76) Para el aprendizaje de cookies y URLs se recomienda modificar el parámetro por lo menos a 720 horas. (Imperva, 2022, pág. 77)

Con el propósito de proteger los recursos de un cliente, es imperativo que todo el tráfico dirigido a sus servidores WEB atraviese inicialmente por el Firewall de Aplicaciones Web (WAF) para someterse a un proceso de evaluación exhaustiva. Esta medida es esencial, ya que el WAF debe ser capaz de identificar peticiones HTTP/HTTPS potencialmente dañinas con el fin de aplicar medidas de mitigación adecuadas, según los perfiles de seguridad configuradas. (Imperva, 2022)

Tabla 2: Imperva Best Practice- Occurrences settings for Switching to Protect Mode Thresholds

Threshold Setting	Protected Application Size		
	small	Medium	Large and Highly Active
Minimum occurrences required to switch a cookie into protect mode	2000	5000	10000

Number of occurrences required to determine if a parameter is read-only			
---	--	--	--

Fuente, (Imperva, 2022, pág. 78)

La siguiente imagen muestra los umbrales de aprendizaje configurados en el WAF de clientes con un tamaño y volumen de actividad baja de sus aplicaciones web.

Switching to "Protect" Mode Thresholds (Web)	
Name	Value
☒ Traceability Percentage required to switch a cookie into partial protect mode	95.0
☒ Traceability Percentage required to switch a cookie into full protect mode	95.0
☒ Duration (in hours) required to switch all Cookies to protect or ignored mode	720
☒ Minimum occurrences required to switch a cookie into protect mode	100
☒ Duration (in hours) required to switch all URLs to protect mode	720
☒ Success rate required to set a specific parameter as read-only	99.9
☒ Number of occurrences required to determine if a parameter is read-only	100

Figura 11: Umbrales de aprendizaje de los parámetros de cambio a modo protección. Fuente. Imperva (2021)

G. Perfilamiento de ThreatRadar

Una de las primeras configuraciones para los perfiles de protección de ThreatRadar es la frecuencia con la que se realizará una validación de actualización de la base de información. La consideración de la periodicidad se realiza en comunicación con el centro de defensa de aplicaciones (ADC). Por ejemplo, la siguiente imagen muestra la frecuencia en la que sea realizará las actualizaciones de información de URLs de Phishing.

Figura 12: Programación de actualización de ThreatRadar - Phishing URLs. Fuente. Imperva (2021)

La fuente de URLs de Phishing de ThreatRadar requiere de una configuración previa de los activos web que están siendo protegidas por el WAF para recibir actualizaciones.

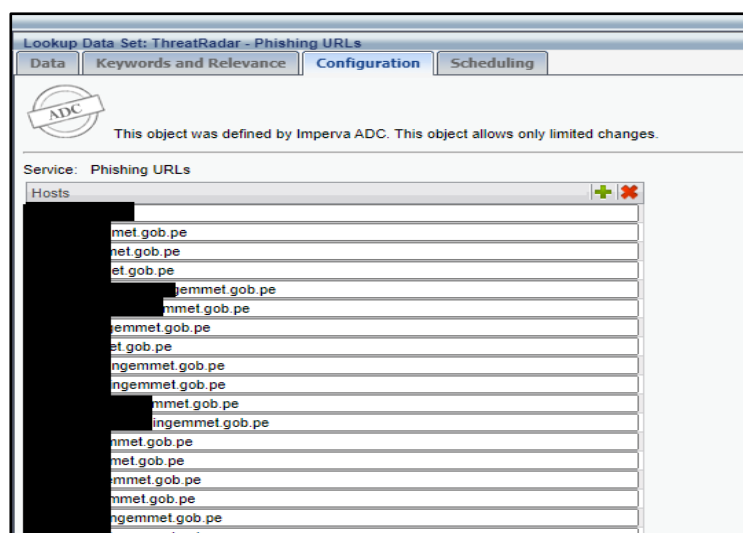


Figura 13: Activos webs protegidos por ThreatRadar - Phishing URL. Fuente. Imperva (2021)

Las políticas de seguridad de ThreatRadar tienen configuradas por defecto una acción de NONE, sin embargo, posterior a un periodo apropiado de corrección de falsos positivos se recomienda cambiar la acción de las políticas por BLOCK, como muestra la siguiente imagen adjunta.

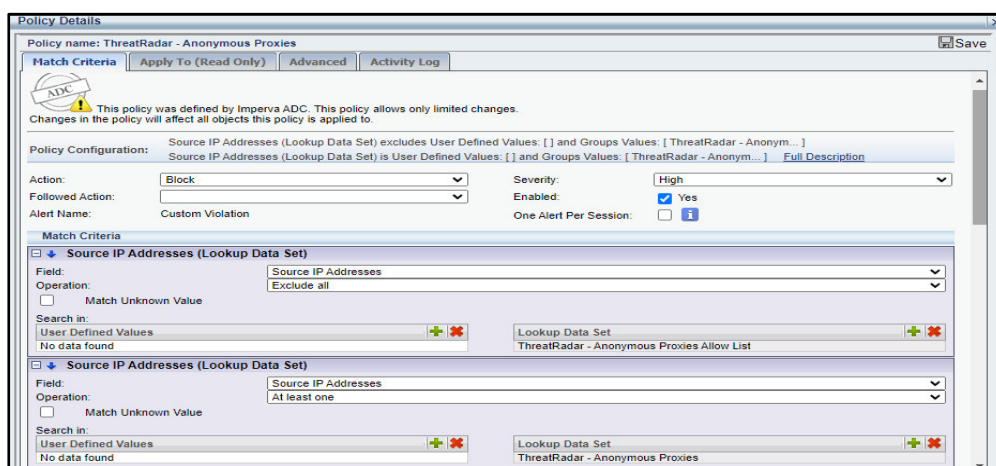


Figura 14: Política de seguridad de ThreatRadar. Fuente. Imperva (2021)

Sin embargo, para algunas aplicaciones se tiene que mantener un criterio diferente al aplicar el modo de bloqueo en las políticas de seguridad de ThreatRadat, por ejemplo, en la siguiente imagen se muestra una política de bloqueo adecuado para una aplicación más enfocada a brindar información o noticias sobre la entidad. El criterio aplicado indica que cincuenta infracciones graves en un minuto desde un proxy anónimo o una dirección IP de TOR será detectado como un evento malicioso y se aplicará el bloqueo a estas direcciones sospechosas, esto con el fin de evitar falsos positivos.

Figura 15: Criterio de coincidencia para aplicaciones informativas.
Fuente. Imperva (2021)

Otro de los criterios a tener en consideración son los países que pueden registrar un evento de login en las aplicaciones protegidas, para el desarrollo de esta política se requiere considerar el alcance que tiene el aplicativo para zonas geográficas externas.

Policy name: ThreatRadar Geolocation and IP Forensics Custom

Match Criteria | Apply To | Advanced | Activity Log

Policy Configuration:

Authentication URL is [Yes]
 URL is [redacted] [admin...]
 Source GeoLocation is at least one of [redacted] [Full Description](#)

Action: Block
 Severity: High
 Followed Action:
 Enabled: ☒ Yes
 Alert Name: Custom Violation
 One Alert Per Session: ☐ [i](#)

Match Criteria

☒ Authentication URL
 Equals Yes

☒ HTTP Request URL
 Match: Exact URLs
 Operation: At Least One
 Value: dminlogin

☒ Source GeoLocation
☐ Apply this rule to unidentified locations
 Operation: At least one
 Countries: [redacted] Selected: [redacted]

Figura 16: Política de bloqueo por intentos de inicio de sesión internacionales. Fuente. Imperva (2021)

Para adquirir licenciamiento de ThreatRadar Intelligence Community Defense de forma gratuita se tiene que proporcionar información de ataques que sufre la entidad, es por ello que Imperva brinda total control de enmascaramiento sobre la información que se envía. Hay tres tipos de acciones para proteger la confidencialidad de la información compartida, la primera correspondo a usar un HASH, la segunda permite enmascarar los 12 primeros caracteres y la última remueve la información a enviar. Estas tres opciones evitan la exposición de información potencialmente sensible.

Summary | Manage

Settings:

☒ Collect Violation Information
☒ Send Collected Information

Cloud Communication Parameters

Key ID: [redacted]
 Key: [redacted]
 Cloud Customer ID: [redacted]
 New Key Generation: [Generate](#)

Masking Configuration

Masking Configuration: [Edit](#) [i](#)

Data Sample

Data Sample: [Show](#) [i](#)

Figura 17: Configuración de enmascaramiento. Fuente. Imperva (2021)

Una de las formas más eficaces de proteger tus activos web de los Bad BOTS es el CAPTCHA. Para configurar la opción de verificación previa de CAPTCHA para ingresar a tu activo web protegido se requiere contar con licencia en ThreatRadar Bot Protection y una subscripción previa en google reCAPTCHA. En la siguiente imagen se muestra la configuración de parámetros de CAPTCHA.

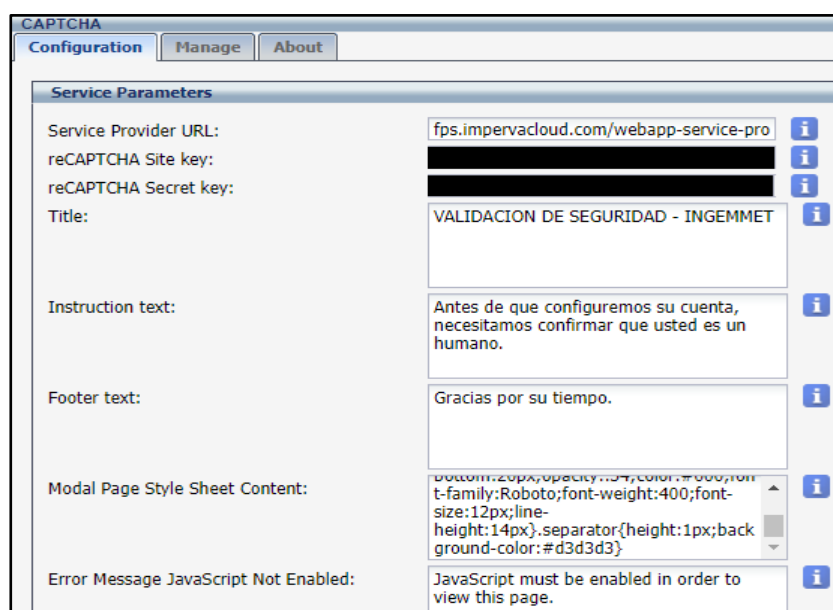


Figura 18: Configuración de CAPTCHA. Fuente. Imperva (2021)

ThreatRadar Emergency Feed equilibra la rapidez en la respuesta de las amenazas emergentes y la garantía de la precisión de las firmas proporcionadas, sin embargo, los servicios y las políticas de seguridad de ThreatRadar Emergency Feed vienen deshabilitados por defecto, es por ello que se tiene que considerar la habilitación y/o customización de una política de seguridad adaptado según el volumen de tráfico y requisitos de cada aplicación web protegida. En la siguiente imagen se muestra una política customizada para un activo web.

Policy name: ThreatRadAr Emergency Feed Save					
Policy Rules Apply To Advanced Activity Log					
Dictionary Name	Enabled	Severity	Action	Followed Action	
☐ ThreatRadAr - Emergency - Authenticated Sessions	☒	High	Block	To SEM	
☐ ThreatRadAr - Emergency - Detection	☒	High	Block	To SEM	
☐ ThreatRadAr - Emergency - GET Requests	☒	High	Block	To SEM	
☐ ThreatRadAr - Emergency - General	☒	High	Block	To SEM	
☐ ThreatRadAr - Emergency - POST Requests	☒	High	Block	To SEM	

Figura 19: Políticas de ThreatRadAr Emergency Feed. Fuente. Imperva (2021)

H. Configuraciones complementarias

El WAF de Imperva puede ser configurado para responder automáticamente ante cualquier evento que ocurra. Para modelar estas respuestas se tienen que realizar 3 configuraciones, Action Interfaces, Actions Sets y Followed Actions.

A continuación, se detallan algunas configuraciones que un administrador puede configurar para obtener respuestas automáticas.

- Transferir archivos (MX Backups, Audit Archives, Reports) via FTP, SFTP, SCP, CIFS, or NFS
- Enviar información a Syslogs externos o SIEM
- Enviar un SNMP traps
- Enviar correos (reportes, notificaciones genéricas)
- Notificar eventos de seguridad
- Correr un comando o script en el OS

Una configuración indispensable en la implementación del WAF es la customización de los reportes por cada Server Group y/o aplicación protegida, también se debe de tener en consideración el envío de los reportes a un servidor FTP externo y la eliminación de aquellos de mayor antigüedad en base a la disponibilidad de espacio del directorio guardado en el MX.

I. Ejecución del Modo Activo en el GROUP SERVER

Se considera un procedimiento de 5 pasos para cambiar del modo simulación al modo activo en un WAF. A continuación, se describen cada uno de los pasos:

1. **Pruebas exhaustivas:** Donde se realiza pruebas completas en modo de simulación para asegurarte de que las reglas y políticas del WAF estén configuradas correctamente y evitar falsos positivos.
2. **Monitoreo continuo:** Se vigila el tráfico y los registros del WAF para detectar bloqueos incorrectos o actividad sospechosa una vez en modo activo.
3. **Ajuste gradual:** Se cambia al modo activo gradualmente, comenzando con un conjunto limitado de reglas y agregando más según sea necesario.
4. **Pruebas de carga:** Evalúa el rendimiento del WAF en condiciones de carga de tráfico real antes de cambiar al modo activo por completo.
5. **Respuesta a incidentes:** Ten un plan de respuesta a incidentes en su lugar para investigar y responder rápidamente a eventos de seguridad una vez que el WAF esté en modo activo.

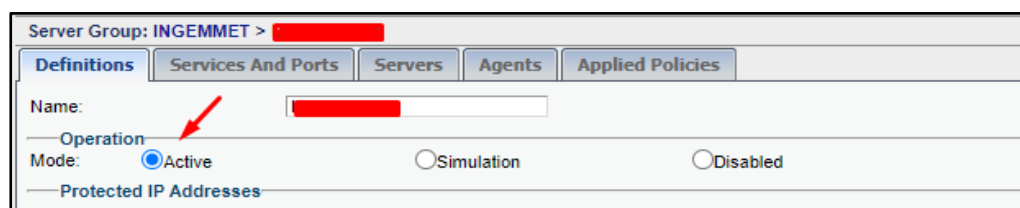


Figura 20: Modo activo en un server Group. Fuente. Ingemmet 2021

3.6.9 Monitoreo de las Alertas y violaciones

La siguiente imagen muestra el panel de alertas en un WAF, diferenciadas por el color rojo aquellas que tienen una acción de bloqueo por la infracción reconocida y las de color negro aquellas que tienen como objetivo notificar al cliente de una acción sospechosa y/o posiblemente peligrosa. Cada alerta tiene una descripción de las infracciones cometidas y las políticas que notificaron estas actividades sospechosas.

The screenshot displays a WAF alert management interface. On the left, a table lists alerts with columns for ID, time, severity, and description. Alerts are color-coded: red for blocking actions and black for notifications. On the right, a detailed view of alert 2100988 is shown, including its title 'ThreatRadar - Malicious IPs', actions like 'Immediate Block', policy details, event information, and connection data.

Alert ID	Time	Severity	Description
2100991	19:19:14	1	ThreatRadar - Malicious IPs
2100841	19:19:14	551	Unauthorized Method HEAD for [redacted]
2100988	19:19:13	1	ThreatRadar - Malicious IPs
2100989	19:19:13	1	ThreatRadar - Malicious IPs
2100987	19:19:11	1	ThreatRadar - Malicious IPs
2100978	19:18:51	6	Unauthorized Content Type for [redacted]
2100924	19:18:15	16	Multiple Post Request - Missing Content Type: 'none'
2100986	19:18:15	1	SSL Untraceable Connection - Unsupported Cipher
2100934	19:17:44	6	Unauthorized Content Type for [redacted]
2100935	19:17:44	492	Multiple Extremely Long Parameter from 190.239.28.132
2100985	19:17:43	1	SOAP Access to a Non-SOAP URL [redacted]
2100961	19:16:31	6	Untraceable SSL Sessions: Unsupported Cipher
2100982	19:16:06	3	Unauthorized Content Type for [redacted]
2100877	19:15:13	20	Unauthorized Method HEAD for [redacted]
2100903	19:15:13	14	Unauthorized Method HEAD for [redacted]
2100876	19:15:13	20	Unauthorized Method HEAD for [redacted]
2100878	19:15:13	20	Unauthorized Method HEAD for [redacted]
2100902	19:15:13	14	Unauthorized Method HEAD for [redacted]
2100775	19:15:09	15	Multiple IP - Too Small TTL from [redacted]
2100724	19:15:09	21	Multiple IP - Too Small TTL from [redacted]
2100897	19:14:31	14	Multiple IP - Too Small TTL from [redacted]
2100875	19:14:01	20	Suspicious Response Code
2100797	19:12:44	458	IP - Too Small TTL 1
2068789	19:12:44	50584	Multiple IP - Too Small TTL from [redacted]
2100981	19:11:22	2	Distributed Unauthorized Method for Known URL on [redacted]
2058794	19:09:48	50354	Multiple IP - Too Small TTL from [redacted]
2068790	19:09:46	50359	Multiple IP - Too Small TTL from [redacted]
2100980	19:07:36	2	Suspicious Response Code
2100979	19:05:48	1	Unauthorized Method HEAD for [redacted]
2100953	18:59:57	18	Unauthorized Content Type for [redacted]
2100955	18:59:25	13	Unauthorized Content Type for [redacted]
2100907	18:58:33	615	Distributed Required Parameter Not Found on [redacted]
2100956	18:58:33	111	Unauthorized Content Type for [redacted]
2100971	18:45:01	4	Unauthorized Content Type for [redacted]

Alert 2100988: ThreatRadar - Malicious IPs

Actions: Immediate Block
 Book-IPs_Malicious: An email was sent to [redacted] (September 18, 2022 7:19:13 PM)
 Book-IPs_Malicious: IP was blocked. Duration: 5184000 seconds (September 18, 2022 7:19:13 PM)

Policy: ThreatRadar - Malicious IPs (Policy Description)
[Edit Policy](#) [Knowledge Base](#)

Event: 7138166862054083293: Custom Rule Violation

Key	Value
Violation Type	Http
Severity	High
Policy Name	ThreatRadar - Malicious IPs (Policy Description)
Alert Number	2100988
Violation Description	ThreatRadar - Malicious IPs
Violated Item	Custom Violation
Immediate Action	Block
Matched Patterns	

Event Details:

Event Time	Gateway
September 18, 2022 7:19:09 PM	[redacted]

Server Group: [redacted] Service: [redacted] Application: [redacted]

Host: [redacted] Source GeoLocation: Germany

Connection: [redacted]

User: [redacted] Session: [redacted]

Response Code	Response Size	Response Time
N/A	Bytes	N/A msec.

Request:

GET / HTTP/1.1
 Host: 143.137.145.48
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Encoding: deflate,gzip,*/*

Figura 21: Panel de alertas. Fuente. Ingemmet (2021)

Tanto las alertas como las violaciones se almacenan en registros llamados “Tabletas” acompañados de parámetros que indican, el tiempo, el colector y un dígito que evita que la información se sobrescriba. El tamaño de cada archivo es de 10 MB y el tiempo de almacenamiento depende del espacio y rendimiento del equipo de seguridad, así mismo se toma en cuenta el flujo de tráfico y cantidad de infracciones de las aplicaciones protegidas. (Imperva, 2022)

A. Ajustes de perfiles de protección del grupo de servidores

El ajuste o afinamiento es uno de los procesos más importantes en la implementación del WAF, tiene como objetivo mejorar el rendimiento y la precisión del Gateway al momento de inspeccionar y aplicar una acción al tráfico web.

A continuación, se mencionan los ajustes más comunes y los recomendados por el fabricante Imperva.

- Verifique que SecureSphere descifre correctamente el tráfico SSL.
- Excluya el tráfico legítimo con restricciones de origen
- Ajuste del perfil de la aplicación web
- Ajuste de alertas y violaciones

a) Descifrado del tráfico SSL

Para que el Gateway pueda inspeccionar el tráfico SSL necesita descifrarlo, además el cifrado del tráfico debe ser compatible con el modo de operación del Gateway. Cuando el GW no puede descifrar de forma adecuada el tráfico web muestra el evento “Untraceable SSL Sessions”, esto previamente configurado en las políticas aplicadas al Server Group.

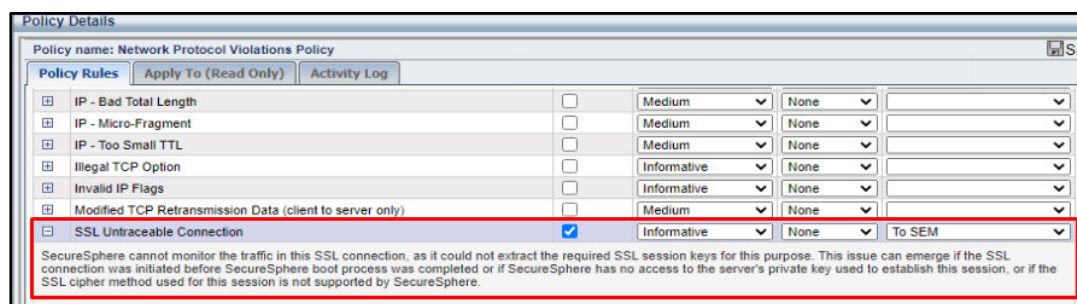


Figura 22: Configuración de notificación de error al descifrar el tráfico web. Fuente. Imperva (2021)

Existen 3 posibles razones por las cuales el GW muestre el error “Untraceable SSL Sessions”:

1. El GW no vio el inicio de sesión SSL.
2. El GW no cuenta con el certificado web del servidor.
3. El GW no soporta el cifrado utilizado en el tráfico de inspección.

A continuación, se muestran algunos casos de problemas en la inspección de tráfico SSL.

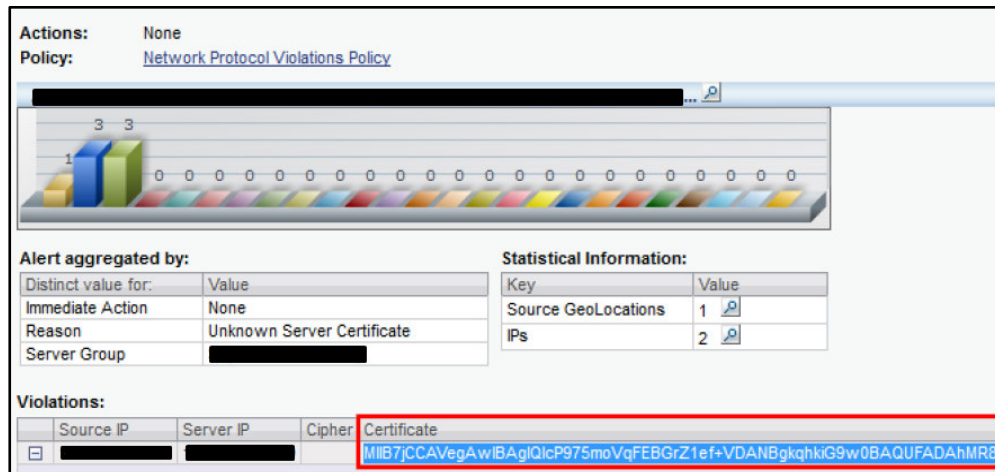


Figura 23: Ejemplo de error de certificado web. Fuente. Imperva (2021)

Para corregir esta situación se debe cargar de forma adecuada el certificado del servidor web protegido. Así mismo, se puede corroborar los cifrados soportados por modo de Gateway en las tablas mostradas en el Anexo 10.

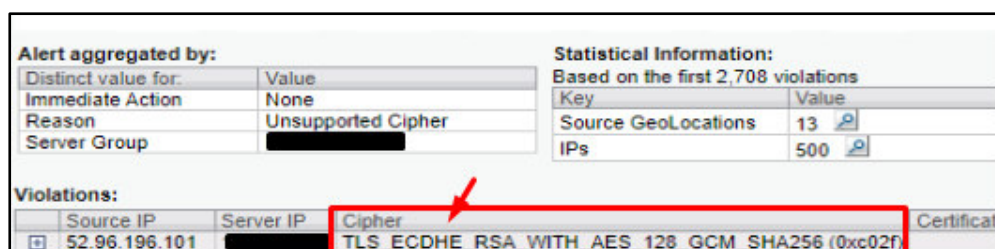


Figura 24: Ejemplo de cifrado DH no soportado. Fuente. Imperva (2021)

b) Corrección de falsos positivos en el periodo de modo simulación

La corrección de falsos positivos se realiza en base a las infracciones de seguridad detectados en el tráfico inspeccionado hacia los activos webs protegidos.

Análisis de las alertas por los escenarios

Para altos números de eventos agregados en una alerta, se puede interpretar de dos formas dependiendo de la política en la que está haciendo match, la primera circunstancia corresponde a un falso positivo en el contexto de que la actividad de ataques es un portaje minoritario de la actividad web, el segundo escenario corresponde a un ataque masivo o sucesivo como lo puede ser un ataque DDoS, escaneos de sitios web, ataques de fuerza bruta, etc.

Las alertas identificadas como distribuidas por la diversidad de IPs públicas que se pueden mostrar en dicha alerta, se plantean 2 escenarios, el primero corresponde a un falso positivo en el contexto de que los ataques desde múltiples direcciones IP son más difíciles de ejecutar y por lo tanto se evidencian con menos frecuencia. El segundo escenario corresponde a un ataque de DDoS, escaneos de sitios web distribuida, ataques de fuerza bruta distribuida, etc.

La periodicidad de los ataques mostradas en las gráficas de las alertas es otro indicativo a tener en cuenta, teniendo en consideración que los atacantes varían el tipo de ataque con respecto al tiempo en el que son aplicados, visualizar una alta frecuencia de eventos en las alertas puede significar un falso positivo, sin embargo, los ataques a inicio de sesión, registros, compra y otros o ataques de exploración o fuzzing (testeo de errores o vulnerabilidades en las aplicaciones web) pueden mostrar este mismo comportamiento.

Excepciones de tráfico de confianza

En muchas organizaciones se cuentan con escáneres de vulnerabilidades confiables para identificar brechas o debilidades de seguridad, es por ello que cuando se implementa un WAF, es necesario configurar una excepción ya

que de no hacerlo perjudica la visibilidad de los escáneres y a la vez interfiere con el aprendizaje y la sensibilidad de las políticas de seguridad en la red Interna y/o externa.

Problemas comunes en el perfilamiento Web

Los problemas más conocidos son provocados por los falsos positivos generados por configuraciones por defecto, inadecuado manejo de las políticas o falta de afinamiento de los parámetros aprendidos. Es por ello que se recomienda que dentro del cronograma de despliegue de la solución se encuentre el perfilamiento de configuraciones. Son dos los problemas más comunes que se presentan cuando se realiza una implementación de un WAF; estos son:

Ajuste de perfiles de aplicaciones web

El principal inconveniente que tienen los administradores del WAF son los falsos positivos que se tiene cuando culmina el periodo de aprendizaje de las URLs de las aplicaciones protegidas. Si el perfil web no fue afinado durante el proceso de aprendizaje conlleva a problemas como protección de URLs incompletas o incorrectas.

Para realizar el afinamiento del perfil de aplicaciones web se tiene que seguir una serie de pasos en base al análisis de las alertas y violaciones.

- Identificar oportunidades de ajuste en base al comportamiento de las alertas.
- Descartar ataques

Identificar tipo de alerta y cantidad de eventos

Analizar los detalles de la alerta en búsqueda de actividades sospechosa

Filtre las direcciones IPs, tipo de alerta y/o comportamientos en búsqueda de algún patrón de ataque.

- Determine si es o no un falso positivo y ajústelo al perfil.

Incompleto o inexacto aprendizaje de URLs de las aplicaciones protegidas

La corrección de los falsos positivos de las URLs y parámetros aprendidos es sencillo, basta con ingresar a la alerta y presionar el botón de “agregar al perfil”

para introducirlo dentro del registro de las URLs en protección, sin embargo, este proceso se hace más complejo a mayor cantidad de URLs que contiene una aplicación web, lo recomendable es que se trabaje en conjunto con el desarrollador web para realizar los ajustes de aprendizaje de URLs y parámetros que deben ser aceptados en el perfil web.

Imperva SecureSphere tiene una herramienta que ayuda a la optimización del perfil web, tiene como función analizar automáticamente el perfil en busca de problemas de aprendizaje y sugiere soluciones, esta herramienta es de mucha ayuda cuando un servicio está sobrepasando los parámetros permitidos o se evidencian anomalías en el comportamiento de las violaciones.

Profile Optimization	
Name	Value
☒ Alert Occurrences	100
The number of alerts that must occur within the timeframe to generate an optimization issue.	
☒ Alert Timeframe in Hours	24
The period interval during which the number of alerts must occur to generate an optimization issue.	
☒ Size Limit (%)	75
The percentage of the Profile size limit which when reached, will generate an optimization issue.	

Figura 25: Perfil de optimización. Fuente. Imperva (2021)

3.6.10 Validaciones de adecuada protección

El Web Application Firewall (WAF) de Imperva en modo bridge con funciones de Transparent Reverse Proxy (TRP) es una herramienta crucial para la protección de aplicaciones web y la prevención de ataques cibernéticos. Es importante validar que su configuración y mantenimiento sean adecuados para garantizar una protección óptima. En este sentido, se deben realizar validaciones para asegurarse de que el WAF esté funcionando de manera efectiva y que las políticas de seguridad estén correctamente implementadas. Se valida el bloqueo de la herramienta cuando las consultas vienen de IPs maliciosas.

Alert 313159: ThreatRadAr - Malicious IPs

Actions: Immediate Block
To SEM: A message was written to the system log at [REDACTED] (May 6, 2023 6:55:19 PM)

Policy: ThreatRadAr - Malicious IPs (Policy Description)
[Edit Policy](#) [Knowledge Base](#)

Event 7219069164070631803: Custom Rule Violation

Key	Value
Violation Type	http
Severity	High
Policy Name	ThreatRadAr - Malicious IPs (Policy Description)
Alert Number	313159
Violation Description	ThreatRadAr - Malicious IPs
Violated Item	Custom Violation
Immediate Action	Block
Matched Patterns	

Event Details:

Event Time		Gateway
May 6, 2023 6:55:18 PM		GW-IMPERVA

Server Group	Service	Application
LAN-CatalogoBiblioteca	Http	[REDACTED]

Host	Source GeoLocation
[REDACTED]	United States of America

Connection	
[REDACTED]	198.235.24.219 :54909 → [REDACTED]

User	Session
	N/A

Response Code	Response Size	Response Time
	N/A Bytes	N/A msec.

Figura 26: Bloqueo de IPs maliciosas por ThreatRadAr. Fuente. Ingemmet 2021

Alert 307879: Multiple SQL injection from 157.245.134.6

Actions: Immediate Block
Policy: Web Correlation Policy
[Edit Policy](#) [Knowledge Base](#)

Aggregated from: 4/28/23 (2 hour(s), 34 minute(s)), 24 violations (last updated 4/28/23)



Alert aggregated by:

Distinct value for:	Value
Application	ingemmet.gob.pe
Immediate Action	Block
Session	N/A
Source IP	157.245.134.6
User	

Statistical Information:
Based on all violations

Key	Value
Source GeoLocations	1
URLs	20
User Agents	17

Violations:

Host	Method	URL	Input Type	Parameter Name
[REDACTED]	POST	/dfsms/	parameter	username
[REDACTED]	POST	/wp-admin/admin-ajax.php	parameter	order_id
[REDACTED]	POST	/cgi-bin/supportinstaller	parameter	customerTID
[REDACTED]	POST	/classes/login.php	parameter	username
[REDACTED]	POST	/hms/admin/	parameter	password
[REDACTED]	POST	/admin/ajax.php	parameter	username
[REDACTED]	POST	/ajax/api/content_infraction/getindexablecontent	parameter	nodeId[nodeid]
[REDACTED]	POST	/admin/index.php	parameter	username
[REDACTED]	POST	/index.php	parameter	USERNAME
[REDACTED]	POST	/account/index.php	parameter	USERNAME
[REDACTED]	POST	/opensis/index.php	parameter	USERNAME
[REDACTED]	POST	/dfsms/index.php	parameter	username
[REDACTED]	POST	/admin/assign-single-student-subjects.php	parameter	course_code
[REDACTED]	GET	/	parameter	q
[REDACTED]	POST	/scgi-bin/platform.cgi	parameter	USERDBDomains.Domainname
[REDACTED]	POST	/scgi-bin/platform.cgi	parameter	USERDBDomains.Domainname
[REDACTED]	POST	/admin/	parameter	appno
[REDACTED]	POST	/graphql	parameter	query
[REDACTED]	POST	/wp-admin/admin-ajax.php	parameter	id_form
[REDACTED]	POST	/hms/doctor/	parameter	password

Figura 27: Bloqueo de SQL Injection. Fuente. Ingemmet 2021

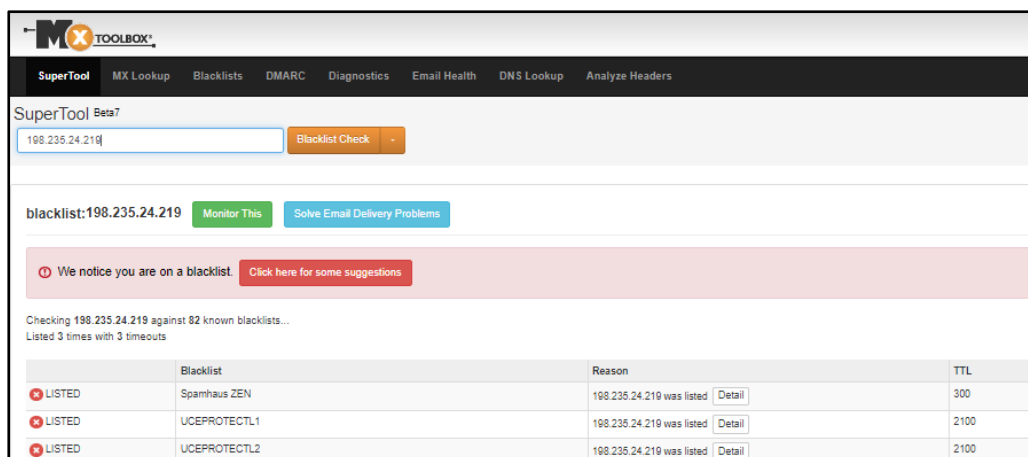


Figura 28: Validación de correcto bloqueo con herramienta de blacklist de MX TOOLBOX. Fuente. Ingemmet 2021

A. Escáner de vulnerabilidades de aplicaciones Web y resultados.

Acunetix es un escáner de vulnerabilidades web; representa una solución completa para evaluar la seguridad de aplicaciones web. Se incorporó la solución de escaneo de vulnerabilidades web con la herramienta Acunetix con el fin de garantizar el fortalecimiento de ciberseguridad y reducción de riesgos después de haberse implementado el WAF en modo Bridge con la opción de TRP habilitado. Las siguientes imágenes muestran un escaneo de vulnerabilidades web antes y después del despliegue del WAF de modo sniffer a modo bridge.

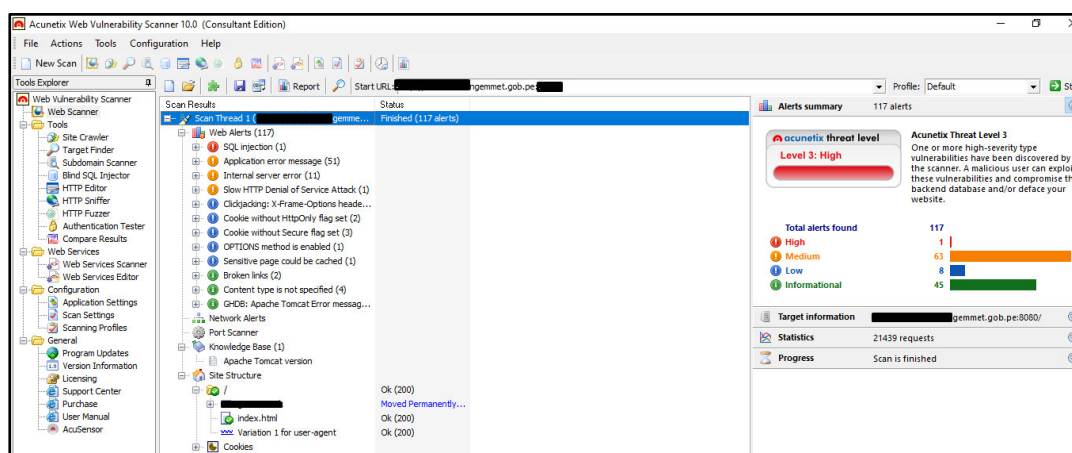


Figura 29: Escaneo de página web de Ingemmet con el WAF en modo Sniffing. Fuente. Acunetix

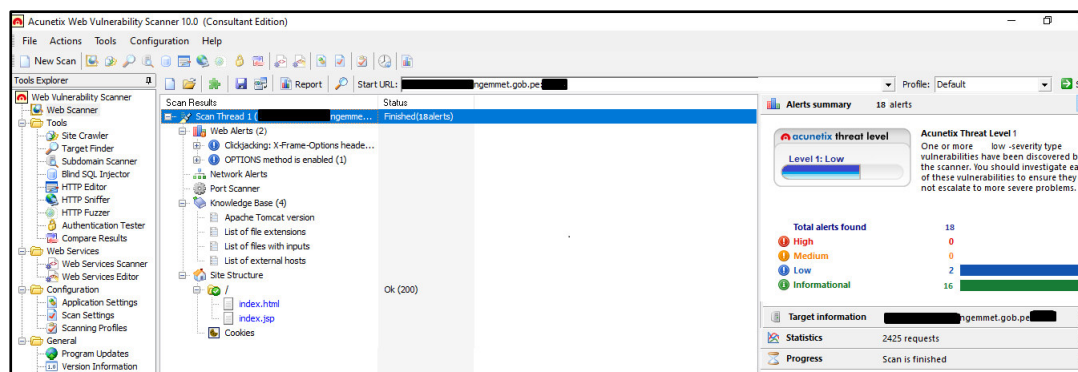


Figura 30: Escaneo de página web de Ingemmet con el WAF en modo Bridge. Fuente. Acunetix

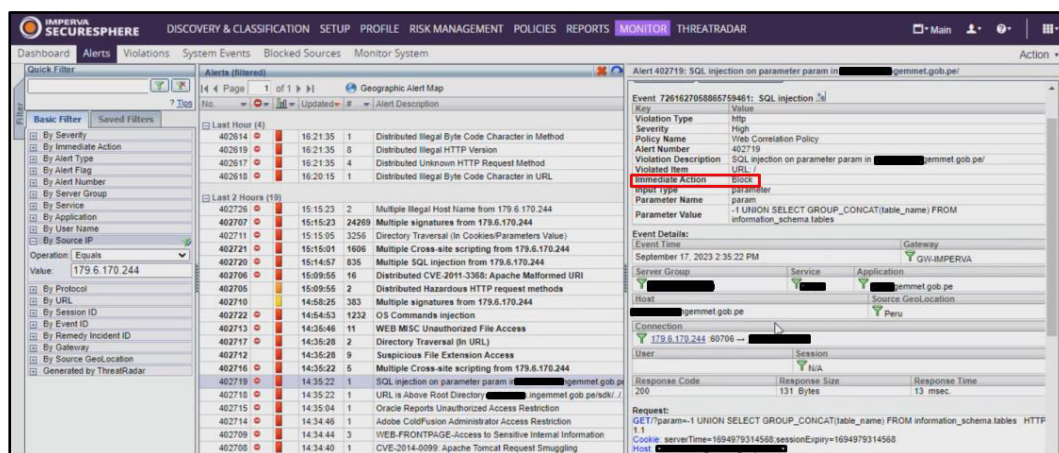


Figura 31: Respuesta del WAF en modo Bridge. Fuente. Imperva Ingemmet.

Como resultado de los escaneos con los dos modos de despliegue del WAF Imperva, aplicados en modo sniffer (antes de la implementación) y en modo bridge (después de la implementación), se evidencia que la herramienta no detecta vulnerabilidades críticas, altas ni medias con el WAF en modo Bridge – TRP.

3.6.11 Organigrama de responsabilidad de administración del WAF

El organigrama presentado destaca la importancia de contar con el personal capacitado en monitoreo y atención de incidentes según la severidad, así

como la implementación de procesos de mejora continua en la seguridad de las páginas webs. El organigrama de la entidad muestra la estructura del área de sistemas después de implementar la herramienta WAF, liderada por el jefe del área de Oficina de sistemas de la Información (OSI) y seguido de la oficial de seguridad (La CISO). Ella gestiona la mejora continua de la seguridad, se encarga de dirigir, coordinar y supervisar que la solución implementada cumpla con las necesidades de seguridad de la entidad. El coordinador del OSI también supervisa la herramienta en busca de incidentes críticos. El proveedor brinda soporte, capacitación y actualizaciones para mantener la solución robusta. El grupo de seguridad de la información del Ingemmet, el Onsite y el SOC de Imperia monitorean la herramienta y gestionan los reportes y alarmas generadas por el WAF. Los reportes críticos son enviados al Centro Nacional de Seguridad Digital.

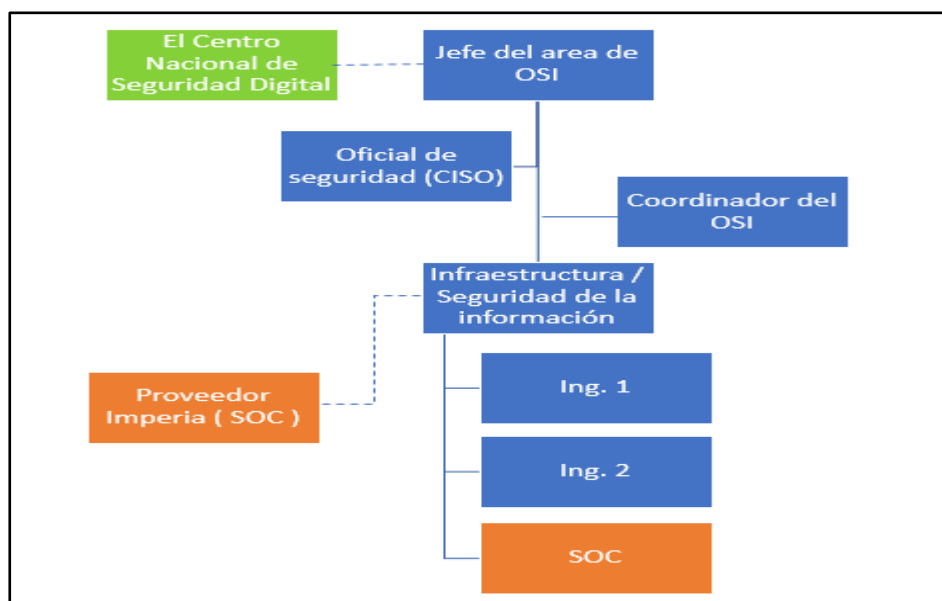


Figura 32: Organigrama de la OSI- Administradores del WAF. Fuente: Propia

A. Capacitación a personal del OSI del Ingemmet

Con el fin de obtener una mejora continua en la seguridad de los sites del Ingemmet, se llevó a cabo la capacitación y evaluación de la implementación

del Web Application Firewall (WAF) y la norma ISO 27001. Se estableció un plan de capacitación que fue compartido con el personal a cargo del OSI y se coordinó un plan de divulgación con el departamento de recursos humanos. Se realizaron capacitaciones programadas y se finalizó con una retroalimentación positiva del personal, quienes sugieren que se realicen capacitaciones continuas sobre ciberseguridad y gestión de vulnerabilidades. Las evidencias de dichas capacitaciones reposan en los anexos de este proyecto: Anexo 11 y 12.

3.7 Resultado de la actividad

Este capítulo tiene como fin corroborar y verificar los resultados de la eficiencia de seguridad de los sites del INGEMMET mediante una tabla comparativa de la cantidad de incidencias reportadas al Centro nacional de seguridad digital en los últimos 3 meses donde se tenía aplicado el WAF en modo Sniffing y en modo Bridge, también se puede demostrar la eficiencia de las buenas prácticas de seguridad con los reportes generados por la herramienta de Acunetix.

Tabla 3: Reporte de los últimos 3 meses al Centro nacional de seguridad digital con el WAF en modo Sniffing

Reporte de los últimos 3 meses al Centro nacional de seguridad digital			
# de incidencias reportadas x día	# de sites afectados	Tipo de ataque empleado	Tiempo de afectación de los servicios
1	3	Cross-Site Scripting (Reflected XSS)	45 minutos
1	1	DDoS attack	20 minutos
1	1	Broken Access Control	120 minutos
1	1	SQL Injection	56 minutos
1	2	DDoS attack	24 minutos
1	2	SQL Injection	150 minutos
1	1	DDoS attack	15 minutos

Fuente: propia

Tabla 4: Reporte de los últimos 3 meses al Centro nacional de seguridad digital con el WAF en modo Bridge

Reporte de los últimos 3 meses al Centro nacional de seguridad digital			
# de incidencias reportadas x día	# de sites afectados	Tipo de ataque empleado	Tiempo de afectación de los servicios
2	1	DDoS attack	15 minutos
1	1	DDoS attack	12 minutos

Fuente: propia (2023)

Realizando una comparativa de las dos tablas identificadas se puede observar que la cantidad de ataques mitigados han mejorado en un 71.42 por ciento.

Tabla 5: Comparativa de resultados de escaneo de páginas Web del Ingemmet.

Comparativa de escaneo de vulnerabilidades antes y después del despliegue del WAF.		
Criticidad	Antes del despliegue (Modo Sniffer)	Después del despliegue (Modo Bridge -TRP)
High	1	0
Medium	63	0
Low	8	2
Informational	45	16

Fuente: Acunetix – Web Vulnerability Scanner

Realizando una comparativa de los resultados mostrados en la tabla 5, se puede observar que la cantidad de vulnerabilidades web mitigadas han mejorado exponencialmente en un 93.5%, teniendo como resultado solo la identificación de 2 vulnerabilidades bajas y 16 vulnerabilidades informativas en el modo de despliegue Bridge - TRP.

CAPÍTULO IV: CONCLUSIONES

4.1 Justificación

Existe un incremento acelerado de ataques cibernéticos por la creciente cantidad de vulnerabilidades en materia de seguridad adquiridas por empresas pequeñas y grandes, los ciberatacantes aprovechan estas vulnerabilidades con fines maliciosos. Es por ello, que se busca con el desarrollo de las actividades descritas en el presente TSP implementar un WAF con las mejores prácticas de seguridad para brindar protección robusta a los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.

4.2 Evaluación económica

Para analizar la proyección de costos y beneficios de este proyecto, se tomó en consideración el costo inicial del producto y servicios, la implementación, el mantenimiento del hardware, el soporte del área del SOC y el ingeniero residente a lo largo de los 3 años de contrato. Los costos iniciales incluyeron la adquisición del equipo, la garantía y los gastos de implementación. Los costos recurrentes involucraron soporte, mantenimiento preventivo y correctivo, capacitación y mano de obra. Se estimaron los beneficios en términos de reducción de riesgos de ataques cibernéticos y pérdida de datos. El retorno de inversión (ROI) calculado fue del 21.389%, lo que indica que la inversión fue rentable. Además, se consideró la tasa interna de retorno (TIR) con un equivalente de 22%, que se determinó en 36 meses por contrato y el

valor actual neto (VAN) resultó en S/ 29,245.07, mostrando que el proyecto es financieramente favorable. La evaluación mostró que la implementación del firewall no solo mejoró la seguridad, sino que también generó beneficios económicos significativos para el INGEMMET. A continuación, se muestran la lista de costos de ingreso y egresos utilizados para calcular el ROI, VAN y TIR.

Tabla 6: Lista de costos de Egresos

ITEM	DESCRIPCION	COSTO
1	Costo del GATEWAY + MX + COMPONENTES	\$ 56,435.30
2	Costo de Licencias + Garantía	\$ 28,225.66
3	Costo de Implementación + Capacitación	\$ 1,500.00
4	Ingeniero Residente	\$ 23,571.42
5	Servicio de soporte gestionado 24x7 - SOC + Mantenimiento Preventivo	\$ 27,000.00
	TOTAL	\$ 136,732.38

Fuente: propia

Tabla 7: Lista de costos de ingresos

ITEM	DESCRIPCION	COSTO
1	Costo del GATEWAY + MX + COMPONENTES	\$ 78,616.44
2	Costo de Licencias + Garantía	\$ 33,692.89
3	Costo de Implementación + Capacitación	\$ 1,500.00
4	Ingeniero Residente	\$ 30,343.04
5	Servicio de soporte gestionado 24x7 - SOC + Mantenimiento Preventivo	\$ 56,073.60
	TOTAL	\$ 200,225.97

Fuente: propia

4.3 Conclusiones

En el presente trabajo de suficiencia profesional se ha obtenido los resultados esperados con respecto a la rigurosa recaudación de información, tomando como principios una planificación cuidadosa, la incorporación de fuentes secundarias como estudios previos y certificaciones, la colaboración de expertos en el área y la experiencia de profesionales en el campo de Ethical Hacking. Tomando como pilar a la información recaudado se ha proporcionado una comprensión profunda de las necesidades de seguridad que requiere los sites del Ingemmet.

Los resultados obtenidos después de una correcta configuración de políticas de seguridad del WAF evidencian la importancia de identificar los parámetros adecuados para reducir la superficie de ataque y mejorar la seguridad al establecer una postura rígida en la protección de los sites del Ingemmet, esto se ve reflejado en la disminución del número de incidentes de seguridad que provocaron pérdidas de servicio por ataques a las páginas y aplicativos WEB del Ingemmet.

La adopción de las mejores prácticas en el diseño e implementación de un WAF resultó en una mejora exponencial en la seguridad de los sites del INGEMMET, esto se ve reflejado en el análisis de vulnerabilidades web tomadas por la herramienta de Acunetix, observándose la eliminación de las vulnerabilidades críticas y medias anteriormente identificadas.

Posterior a la etapa del afinamiento de políticas se ha logrado optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.

4.4 Recomendaciones

Se debe de contar con un estricto plan de recolección de información y recursos de ciberseguridad para obtener el mejor plan de implementación y diseño de una solución WAF, como se ha mostrado en el presente trabajo de suficiencia profesional, puesto que esta información es la base que se utilizará para obtener los resultados esperados.

Se recomienda identificar vulnerabilidades y amenazas a las que un SITE se ve expuesto mediante una etapa de simulación previa a la de producción para poder identificar de forma adecuada los parámetros y el nivel de seguridad que debe recibir un activo protegido por el WAF.

Se recomienda trabajar con datos 100% reales, es por ello que al inicio de la implementación se ejecutó una etapa de simulación, para estudiar el comportamiento de las políticas con respecto al tráfico que se desarrolla en una aplicación, esto debe aplicarse siempre al agregar un nuevo site.

Es importante enfocarse en aplicar las configuraciones en un WAF utilizando las mejores prácticas recomendadas por el fabricante de la solución y en base a la experiencia desarrollada en otros trabajos de implementación para poder obtener los mejores resultados.

Agregar una solución de WAF en la nube brinda mayores beneficios a nivel de ataques volumétricos, por lo que se recomienda a futuro poder migrarse a esta solución.

CAPÍTULO V: BIBLIOGRAFÍA

- Bonilla, J. (2018). Identificación y diseño de las reglas de detección de amenazas de INEGI para un web application firewall. *Tesis de Maestría*. Universidad Autónoma de Aguascalientes, Aguascalientes.
- Cabeza, N. (2020). Configuración del Firewall de Aplicaciones Web Modsecurity para prevenir diversos ataques hacia aplicaciones web alojados en servidores open source. (*Tesis de Grado*). PUCESE - Escuela de Sistemas y Computación, Esmeraldas.
- Cano, Á. (2018). Implementación y medida del rendimiento de un Firewall para aplicaciones Web (WAF) en un balanceador de carga. *Tesis de Grado*. Escuela Técnica Superior de Ingeniería Universidad de Sevilla, Sevilla.
- Evangelista, E. O. (2018). Web Application Firewall - WAF. *Web Application Firewall - WAF*. Universidad Piloto de Colombia, Bogotá D.C. – Colombia. Obtenido de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2917/Trabajo%20de%20grado1884.pdf?sequence=1&isAllowed=y>
- Flament, G. V. (2018). Implementación de un web application firewall basado en mod_security. *Artículo Tesis Grado*. Escuela Superior Politécnica del Litoral, Guayaquil-Ecuador.
- Hernández, M. (21 de Marzo de 2022). *¿Cuál son la 5 Fases del Pentesting?* Obtenido de Cybersecurity & Intelligence: <https://ciberseguridadbidaidea.com/fases-del-pentesting/>
- Hernández, M. (4 de Marzo de 2022). *¿Qué es el Pentesting?* Obtenido de Cybersecurity & Intelligence: <https://ciberseguridadbidaidea.com/que-es-el-pentesting/>
- Imperva. (2023). Management Server Manager User Guide. Obtenido de Docs Imperva: <https://docs.imperva.com/bundle/v13.6-management-server-manager-user-guide/page/10969.htm>

- Luque, A. y. (2021). Diseño e implementación de un sistema de protección contra el ataque de inyección SQL, en un servidor vulnerable utilizando herramientas Open Access. *Tesis de Grado*. Universidad distrital Francisco José de Caldas, Bogotá D.C.
- Morocho, V. (2019). Implementación de seguridad perimetral en la red de datos del Hospital Nacional Daniel Alcides Carrión. *Tesis de Grado*. Universidad Tecnológica del Perú, Lima.
- Palacios Gallardo, M. L. (2021). Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo. *Tesis de Bachiller*. Universidad Continental, Huancayo.
- Palacios, M. (2021). Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo. *Tesis de Bachiller*. Universidad Continental, Huancayo.
- Ramirez, J. (2022). Análisis, desarrollo e implementación de un sistema de seguridad para el fortalecimiento de vulnerabilidades e integridad de aplicaciones web académicas. *Tesis de Grado*. Escuela Superior Politécnica de Chimborazo, Riobamba.
- Rodriguez, J. (2022). Proyecto de implementación de un modelo Machine Learning para la evaluación de riesgo de operaciones sospechosas a los clientes de una entidad bancaria. *Tesis de Grado*. Universidad Nacional Mayor de San Marcos, Lima.
- Taipe, D. (2020). La auditoría de seguridad informática y su relación en la ciberseguridad en el sector público año 2018. *Tesis de Maestría*. Universidad Nacional de Piura, Piura.
- Toribio, M. (2021). Optimización de la infraestructura de red LAN y y WAN, para las empresas del grupo Inversiones Educa S.A. basado en la metodología PPDIOO Cisco. *Tesis de Grado*. Universidad Nacional Mayor de San Marcos, Lima.
- Valverde, J. (2017). Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana. *Tesis de Grado*. Universidad Nacional Mayor San Marcos, Lima.

CAPÍTULO VI: ANEXOS

Anexo 1: Matriz de consistencia

Matriz de Consistencia					
Título: "Diseño e Implementación de un Firewall de Aplicaciones Web que permita optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú en la ciudad de Lima en el año 2021"					
PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	INDICADORES	MÉTODO Y DISEÑO
Problema General: ¿De qué manera el diseño e implementación de un Firewall de Aplicaciones Web, permite optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú ante un continuo incremento de ataques cibernéticos?	Objetivo General: Diseñar e implementar un Firewall de Aplicaciones Web que permita optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.	Hipótesis General: El diseño e implementación de un Firewall de Aplicaciones Web permitirá optimizar la seguridad de los sites de un organismo adscrito al Ministerio de Energía y Minas del Perú.	Variable Independiente 1 Vulneraciones de seguridad en sites 1.1 Vulneraciones críticas 1.2 Vulneraciones leves 2 Optimización de la seguridad en sites	a) Incremento de los Sites b) Mayor número de ataques no detectados c) Mejorar la seguridad de los sites d) Aprendizaje y protección	Método Temporal. El estudio es del tipo transversal, su ejecución se inició en agosto del año 2021 y su término en diciembre del 2021.
Problemas Específicos:	Objetivos Específicos:	Hipótesis Específicas	Variable Dependiente		Especial.
•Problema específico 1: ¿Cómo obtener los parámetros necesarios para realizar el diseño de un WAF? •Problema específico 2 ¿Qué consideraciones se deben de tomar para configurar las políticas de seguridad de los aplicativos webs? •Problema específico 3 ¿Cómo realizar las mejores prácticas en el diseño e implementación de un WAF?	•Objetivo Específico 1: Recolectar información previa para el diseño del WAF. •Objetivo Específico 2: Implementar las políticas de seguridad de cada aplicativo web •Objetivo Específico 3: Evaluar las mejores prácticas en el diseño e implementación de un WAF.	•Hipótesis Específico 1: La recolección de información previa será el soporte principal para el diseño del WAF. •Hipótesis Específico 2: La correcta configuración de políticas de seguridad de un WAF será de vital importancia en la seguridad de los sites de un organismo adscrito al ministerio de energías y minas de Perú. •Hipótesis Específico 3: La aplicación de las mejores prácticas en el diseño e implementación de un WAF influye directamente en la optimización de seguridad de INGENMET.	1 Diseño e implementación de un WAF 1.1 Modo de operación 1.1.1 Modo de aprendizaje		El proyecto se circunscribe a la ciudad de Lima en el año 2021.

Anexo 2: Características de cada modo de despliegue del Gateway- Parte 1

Features Available in Each Deployment Mode

The table below lists some of the SecureSphere features for which the deployment mode affects the feature's availability. Note that sniffing deployments do not support proxies.

Some SecureSphere Features for which the Deployment Mode Affects the Feature's Availability

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes	
			Transparent RP	Kernel RP (Non- Transparent)
Inspect TCP handshake	√	√	√	√
Normalize traffic (decode encoded content, such as URL-encoded or UTF-encoded content)	√	√	√	√
Decrypt and inspect SSL (either interface to a FIPS-compliant HSM or store an encrypted copy of the SSL key)	√	√	√	√
HTTP / SQL protocol conformance	√	√	√	√
Session / cookie protection	√	√	√	√
Input validation (white list)	√	√	√	√

Anexo 3: Características de cada modo de despliegue del Gateway- Parte 2

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes	
			Transparent RP	Kernel RP (Non- Transparent)
Attack detection (black list, including application, network, Web server and OS attacks)	√	√	√	√
Correlated attack validation	√	√	√	√
Block attacks	√	√*	√	√
Block data leaks (inspect outgoing traffic for sensitive data such as SSN, credit card numbers, CVV numbers and data matching custom signatures)	√	-*	√	√
Rewrite content	-	-	√	√
Application level auditing (record complete HTTP request and server response code)	√	√	√	√
Ignore IP Group (Server Groups)	√		√	√
Application user tracking	√	√	√	√
Firewall and Network Protocol Violation Policies enforced	√	-	-	-

Anexo 4: Características de cada modo de despliegue del Gateway- Parte 3

SecureSphere feature	Transparent Bridge	Sniffing	Reverse Proxy Modes	
			Transparent RP	Kernel RP (Non- Transparent)
Redirect client to an error page	√	-*	√	√

*A SecureSphere Gateway in sniffing mode cannot send an error page or block a connection. Instead, it sends a TCP reset to the server. The client sees a timeout message.

Anexo 5: Security Policy Types parte 1

Server Group Level Network Policy Types

TYPE	DESCRIPTION
Firewall Policy	Defines the services is used to access the protected servers, see Firewall Policy .
Network Protocol Validation	Validates a proper use of the TCP/IP protocol according to the RFC standard, preventing attacks that are based on TCP/IP protocol vulnerabilities, see Network Protocol Validation .
Stream Signature	Identifies well known attacks for generic services, see Stream Signature .

Anexo 6: Security Policy Types parte 2

Web Service Policy Types

TYPE	DESCRIPTION
HTTP Protocol Validation	Validates a proper use of the HTTP protocol according to the RFC standard, see HTTP Protocol Validation Policy .
Web Service Correlated Validation	Protects against multi-stage web application attacks, see Web Service Correlated Validation Policy .
HTTP Protocol Signatures	Protects against known protocol attacks using signatures, see HTTP Protocol Signature Policies .
Web Service Custom	Enables creating user-defined web service level policies based on various combinations of the match criteria, see Web Service Custom Policies .
Cookie Signing Validation	When SecureSphere operates in the Kernel Reverse Proxy mode, this policy enables cookie signing and verification, see Cookie Signing Validation Policy .

Anexo 7: Security Policy Types parte 3

Web Application Policy Types

TYPE	DESCRIPTION
Anti Scraping	Identifies scraping events in which someone is attempting to "scrape" data from web pages. For more information, see Anti Scraping Policy .
Bot Mitigation	Identifies bot attacks meant to cause Denial of Service and other automated attacks. For more information see Bot Mitigation Policy .
ThreatRadar Bot Protection	Works together with third party vendors to determine if devices connecting to the network are compromised. Then determine policies for handling problematic traffic. For more information see ThreatRadar Fraud Prevention Services.
Web Profile	Alerts on and prevents the application user behavior that deviates from the Application Profile, as defined in SecureSphere, see Web Profile Policy .
Web Worm	Provides protection for zero day web worms based on Imperva unique technology, see Web Worm Policy .
Web Application Signatures	Protects against known application attacks using signatures, see Web Application Signatures Policy .
Web Application Custom	Enables creating of user-defined web application level policies based on various combinations of the match criteria, see Web Application Custom Policies .
OCSP Protocol Validation	Verifies the revocation status of X.509 digital certificates. This assists web infrastructure including servers and Internet browsers in determining if a web site certificate is valid, has been revoked, or if its status is unknown. For more information, see OCSP Protocol Validation Policies .

Anexo 8: Security Policy Types parte 4

CAPTCHA Policy Types

TYPE	DESCRIPTION
Event Based	Defines the events that trigger a CAPTCHA challenge that is then presented to the end user. The policy also prevents access to the protected resources until the challenge is passed. The challenge is presented only when the current page is changed (via page reload or navigation action). When suspicious activity is detected, the configured action and followed action is applied and an alert is issued.

Anexo 9: Security Policy Types parte 5

Account Take Over Policy Types

TYPE	DESCRIPTION
Device Intelligence	Configuration Policies: ■ ATO - Device Intelligence Profiling Marks the location where the device fingerprinting process is to take place. ■ ATO - Device Intelligence for failed logins Informs the cloud about a login failure. This information is used when assessing the risk of the devices. ■ ATO - Device Intelligence for successful logins Gets the risk of a device when a login attempt succeeds. Enforcement Policies: ■ ATO - Device Intelligence with multiple occurrences Enforcement Triggered when there are multiple occurrences of a source IP being reported with high or medium risk. ■ ATO - Device Intelligence High Risk Login Enforcement Triggered when a high risk is reported for a device. ■ ATO - Device Intelligence + Anonymous Proxy Enforcement Triggered when a high or medium risk is reported for a device and the request is originated from an Anonymous Proxy. ■ ATO - Device Intelligence + TOR IP Enforcement Triggered when a high or medium risk is reported for a device and the request is originated from TOR.

Privileged Account	Enforcement Policies: ■ ATO - Privileged Account Brute Force + Bot Enforcement Triggered when a Privileged Users Brute Force attack is detected and the client type is identified as non-human. ■ ATO - Privileged Account Brute Force Enforcement Triggered when a Privileged Users Brute Force attack is detected.
Credential Stuffing	Configuration Policies: ■ ATO - Credential Stuffing - Low Risk API Sends the user name information to the cloud when a login fails and the source IP is set with low risk. ■ ATO - Credential Stuffing - Medium Risk API Sends the user name and hashed password information to the cloud when a login fails and a Credential Stuffing attack from the source IP is suspected. Enforcement Policies: ■ ATO - Credential Stuffing + Bot Enforcement Triggered when a Credential Stuffing Brute Force attack is detected and the client type is identified as non-human. ■ ATO - Credential Stuffing - Enforcement Triggered when a Credential Stuffing Brute Force attack is detected.
Dictionary Attack	Enforcement Policies: ■ ATO - Dictionary Attack + Bot Enforcement Triggered when a Dictionary Attack (Weak Password) Brute Force attack is detected and the client type is identified as non-human. ■ ATO - Dictionary Attack Enforcement Triggered when a Dictionary Attack (Weak Password) Brute Force attack is detected.

Anexo 10: Cifrados TLS

TLS Ciphers

SecureSphere supports a number of ciphers to enable the decryption and inspection encrypted packets in your network. The following table lists the ciphers supported by SecureSphere and if they are enabled by default.

Supported TLS1.2 Ciphers

TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_RSA_WITH_AES_256_GCM_SHA384	Yes	All
TLS_RSA_WITH_AES_256_CBC_SHA256	Yes	All
TLS_RSA_WITH_AES_128_GCM_SHA256	Yes	All
TLS_RSA_WITH_AES_128_CBC_SHA256	Yes	All
TLS_RSA_WITH_AES_256_CBC_SHA	Yes	All
TLS_RSA_WITH_AES_128_CBC_SHA	Yes	All
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes	Reverse Proxy, ABR

TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_AES_256_GCM_SHA384	Yes	Reverse Proxy, ABR
TLS_CHACHA20_POLY1305_SHA256	Yes	Reverse Proxy, ABR
TLS_AES_128_GCM_SHA256	Yes	Reverse Proxy, ABR
TLS_AES_128_CCM_SHA256	Yes	Reverse Proxy, ABR
TLS_AES_128_CCM_8_SHA256	Yes	Reverse Proxy, ABR

Supported TLS1.2 Ciphers - Diffie-Hellman

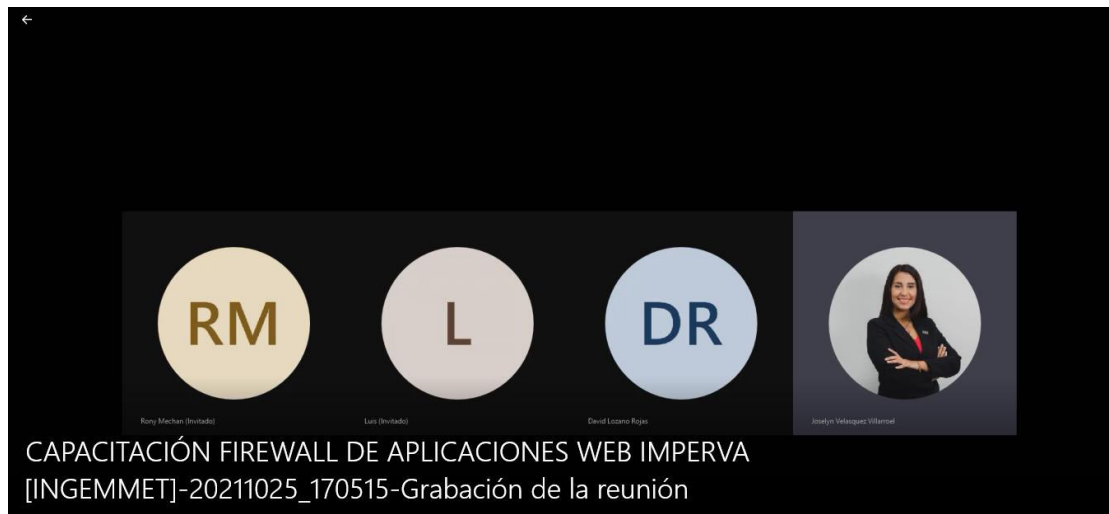
TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Yes	Reverse Proxy, ABR, TRP
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Yes	Reverse Proxy, ABR, TRP
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Yes	Reverse Proxy, ABR, TRP
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Yes	Reverse Proxy, ABR, TRP

TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Yes	Reverse Proxy, ABR, TRP
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Yes	Reverse Proxy, ABR, TRP
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Yes	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	Yes	Reverse Proxy, ABR

TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Yes	Reverse Proxy, ABR
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	Yes	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Yes	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Yes	Reverse Proxy, ABR, TRP
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Yes	Reverse Proxy, ABR, TRP
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Yes	Reverse Proxy, ABR, TRP
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Yes	Reverse Proxy, ABR, TRP

TLS Cipher	Enabled By Default	Supported Gateway Mode
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_RSA_WITH_SEED_CBC_SHA	No	Reverse Proxy, ABR
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	No	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Yes	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_SEED_CBC_SHA	No	Reverse Proxy, ABR
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	No	Reverse Proxy, ABR

Anexo 11: Capacitación del Firewall de Aplicaciones Web para el OSI



Anexo 12: Capacitación sobre el rendimiento del WAF Imperva

