UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

FIREWALLS INTEGRADOS VS. EXTERNOS EN ARQUITECTURAS DE NUBE: EVALUACIÓN DE EFICACIA MEDIANTE DISEÑO Y COMPARACIÓN

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN .....

AUTOR: DIMITRI EDUARDO CORONEL GOLUBENKO

DIRECTOR: ING. JUAN PABLO CUENCA TAPIA, MSC.

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

FIREWALLS INTEGRADOS VS. EXTERNOS EN ARQUITECTURAS DE NUBE: EVALUACIÓN DE EFICACIA MEDIANTE DISEÑO Y COMPARACIÓN

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR: DIMITRI EDUARDO CORONEL GOLUBENKO

DIRECTOR: ING. JUAN PABLO CUENCA TAPIA, MSC.

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Dimitri Eduardo Coronel Golubenko portador de la cédula de ciudadanía Nº **1104496953**. Declaro ser el autor de la obra: "**Firewalls Integrados vs. Externos en Arquitecturas de Nube: Evaluación de Eficacia mediante Diseño y Comparación"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **11 de septiembre de 2024**

F: .....Firmado electrónicamente por: DIMITRI EDUARDO CORONEL GOLUBENKO.....

Dimitri Eduardo Coronel Golubenko

C.I. **1104496953**

Universidad Católica de Cuenca

Certificación de tutor

Certifico que el presente trabajo de investigación fue desarrollado por DIMITRI EDUARDO CORONEL GOLUBENKO, con el Tema: “Firewalls Integrados vs. Externos en Arquitecturas de Nube: Evaluación de Eficacia mediante Diseño y Comparación”, bajo mi supervisión.

Firmado electrónicamente por: JUAN PABLO CUENCA TAPIA

Ing. Juan Pablo Cuenca, Msc.
DOCENTE - TUTOR

Dedicatoria

Dedico esta tesis a mis padres, Olga y Sergio, quienes siempre han creído en mí y me han brindado su amor incondicional. Su sacrificio, apoyo y confianza me han acompañado en cada paso de este camino. A mis amigos, Camilo y Sofía, por ser un pilar fundamental de apoyo y motivación, y por estar siempre presentes en los momentos más difíciles. Este logro es tanto mío como de ustedes.

Agradecimiento

Quiero expresar mi más profundo agradecimiento a todas las personas que, de diversas maneras, han hecho posible la realización de esta tesis. En primer lugar, agradezco a mi jefe, Juan Pablo Amon, y a todo el equipo de TWS2, por su constante apoyo y comprensión. Su confianza en mis capacidades durante todo este proceso ha sido invaluable.

Mi gratitud también para la Universidad Católica de Cuenca, por brindarme la formación académica y el entorno propicio para el desarrollo de este trabajo. Agradezco a todos los profesores y compañeros que, de alguna manera, contribuyeron a mi crecimiento profesional y personal durante mi tiempo en la universidad.

Al Ing. Juan Pablo Cuenca, mi tutor de tesis, por su guía y asesoramiento a lo largo de todo el desarrollo de este trabajo. Sus consejos y conocimientos fueron cruciales para la finalización exitosa de esta investigación.

Finalmente, agradezco a todos aquellos que, directa o indirectamente, han contribuido a este proyecto. Gracias por estar ahí y ser parte de este camino.

Resumen

En la era de la digitalización, la computación en la nube es clave para desarrollar infraestructuras tecnológicas escalables y eficientes. Sin embargo, esta evolución plantea desafíos significativos en ciberseguridad. Los firewalls, fundamentales para la protección de redes, han evolucionado para abordar las complejidades de las amenazas actuales. Esta investigación evalúa la eficiencia de los firewalls integrados frente a los externos en arquitecturas de nube, proporcionando una comparación que orienta a las organizaciones en su implementación.

Los firewalls integrados, embebidos en la infraestructura de la nube, facilitan la gestión y mejoran la eficiencia operativa, pero pueden carecer del control y personalización necesarios para combatir amenazas complejas. Por otro lado, los firewalls externos ofrecen mayor personalización y control, aunque su integración y gestión pueden ser más complejas y afectar la eficiencia operativa en entornos dinámicos.

El estudio analiza el desempeño, gestión e impacto en el rendimiento de ambos tipos de firewalls mediante simulaciones en un entorno controlado. Los resultados proporcionan una base empírica para decisiones estratégicas en seguridad en la nube. Esta investigación es crucial para los profesionales de TI que buscan soluciones de firewall que no solo protejan sus activos digitales, sino que también se alineen con sus necesidades operativas y estratégicas.

Palabras clave: *Computación en la nube, ciberseguridad, eficiencia operativa, amenazas cibernéticas y firewalls.*

Abstract

In the era of digitalization, cloud computing is crucial for developing scalable and efficient technological infrastructures. However, this evolution poses significant challenges in cybersecurity. Firewalls, essential for network protection, have evolved to address the complexities of current threats. This research evaluates the efficiency of integrated firewalls compared to external ones in cloud architectures, providing a comparison that guides organizations in their implementation.

Integrated firewalls, embedded in cloud infrastructure, facilitate management and improve operational efficiency, but they may lack the control and customization needed to address complex threats. On the other hand, external firewalls offer greater customization and control, although their integration and management can be more complex and may impact operational efficiency in dynamic environments.

The study analyzes the performance, management, and impact on the effectiveness of both types of firewalls through simulations in a controlled environment. The results provide an empirical basis for strategic decisions in cloud security. This research is crucial for IT professionals seeking firewall solutions that not only protect their digital assets but also align with their operational and strategic needs.

Keywords: *Cloud computing, cybersecurity, operational efficiency, cyber threats, firewalls.*

Tabla de contenidos

Lista de figuras

Capítulo 1

Introducción

En la era de la digitalización, la computación en la nube actúa como un pilar fundamental para el desarrollo de infraestructuras tecnológicas eficientes y escalables. Sin embargo, este avance ha traído consigo nuevos desafíos en materia de ciberseguridad. Los firewalls, que históricamente han sido esenciales en la protección de redes, han evolucionado para adaptarse a las complejidades de las amenazas modernas. El presente análisis se enfoca en valorar la eficacia de los firewalls integrados versus los firewalls externos en arquitecturas de nube, ofreciendo una comparación detallada que ayudará a las organizaciones a tomar decisiones informadas sobre su implementación.

El uso de la computación en la nube ha revolucionado la forma en que las compañías gestionan, manejan y almacenan datos, proporcionando flexibilidad, escalabilidad y eficiencia operativa sin precedentes. No obstante, este cambio paradigmático también ha aumentado la superficie de ataque para los ciberdelincuentes, haciendo de la seguridad en la nube una prioridad crítica. En tal sentido, los firewalls desempeñan un rol fundamental en la seguridad de la información y las aplicaciones contra accesos no autorizados y ataques cibernéticos (Friese, Rossmann, & Bröring, 2018).

La disyuntiva entre elegir firewalls integrados, que están embebidos en la infraestructura de servicios en la nube, y firewalls externos, que son soluciones independientes administradas por el usuario, es un tema de gran relevancia. Los firewalls integrados ofrecen ventajas significativas en términos de gestión simplificada y mejor integración con los servicios de la nube, lo cual potencialmente mejora la eficiencia y la escalabilidad operativa (Anisetti, Ardagna, & Damiani,

2020). Sin embargo, pueden no proporcionar el nivel de personalización y control detallado que requieren algunas organizaciones para contrarrestar las amenazas cibernéticas sofisticadas. Por otro lado, los firewalls externos permiten una mayor personalización y control, pero presentan desafíos de integración y una gestión más compleja que pueden afectar la eficiencia operativa en entornos de nube dinámicos (Amazon Web Services, 2020).

Este estudio tiene como propósito analizar el rendimiento operativo mediante la realización de una evaluación comparativa de los firewalls integrados y externos en arquitecturas de nube. Para ello, se establecerán parámetros y métricas clave como la latencia, el throughput, la escalabilidad y la facilidad de gestión. Se simularán escenarios de seguridad en un entorno controlado y se analizarán los resultados para comprender los beneficios y limitaciones de cada tipo de firewall. Esta investigación no solo proporcionará una base empírica sólida que orientará las decisiones estratégicas en la implementación de soluciones de firewall, sino que también contribuirá al conocimiento existente sobre la seguridad en la nube.

El motivo de esta investigación reside en la urgente necesidad de tratar los desafíos de seguridad emergentes en la nube. Con la adopción creciente de estas tecnologías, es imperativo desarrollar soluciones de seguridad que sean tanto eficaces como eficientes. Los profesionales encargados de sistemas y de seguridad en TI se beneficiarán de los conocimientos prácticos derivados de este estudio, permitiéndoles elegir soluciones de firewall que no solo protejan sus activos digitales, sino que también se alineen con sus necesidades operativas y estratégicas (PwC Oriente Medio, 2021).

En conclusión, este estudio busca llenar un vacío en la literatura existente al proporcionar una evaluación comparativa, definiendo parámetros y métricas de la eficacia, la gestión y el rendimiento de los firewalls integrados y externos en arquitecturas de nube. Al hacerlo, ofrecerá

recomendaciones basadas en evidencia que ayudarán a las organizaciones a mejorar su postura de seguridad en un entorno cada vez más digitalizado y complejo.

1.1. Antecedentes

La seguridad informática ha evolucionado significativamente en las últimas décadas, adaptándose a las nuevas tecnologías y a los cambiantes escenarios de amenazas. Con la proliferación de la computación en la nube, los mecanismos tradicionales de seguridad han tenido que transformarse para abordar los desafíos específicos que estos entornos presentan. Dentro de este marco, los firewalls, que tradicionalmente actuaban como barreras entre redes internas y externas, han tenido que adaptarse para proteger datos y aplicaciones en arquitecturas de nube distribuidas.

Firewalls Tradicionales vs. Firewalls en la Nube

Los firewalls tradicionales se diseñaron para entornos de red fijos, protegiendo el perímetro de una red corporativa contra accesos no autorizados y ataques externos. Estos firewalls son altamente efectivos en entornos controlados, donde el tráfico de red puede ser fácilmente monitoreado y gestionado. Sin embargo, presentan limitaciones significativas cuando se aplican a entornos de nube, que se caracterizan por su dinamismo, escalabilidad y la naturaleza descentralizada de sus recursos (Recalde & Veloso, 2022).

Con la adaptación de la computación en la nube, se han desarrollado firewalls específicos para estos entornos, conocidos como firewalls en la nube. Estos se integran directamente con la infraestructura de la nube, brindando capacidades avanzadas como la detección profunda de paquetes (DPI) y la prevención de intrusiones (IPS). Los firewalls en la nube se dividen en varias categorías, incluyendo los firewalls públicos en la nube, los firewalls como servicio (FWaaS) y los firewalls de aplicaciones web (WAF) (Lema, 2023).

Firewalls Integrados vs. Firewalls Externos

Dentro del ámbito de los firewalls en la nube, existe una importante distinción entre los firewalls integrados y los externos. Los firewalls integrados están embebidos en la infraestructura de la nube y ofrecen una gestión simplificada y una integración nativa con los servicios de la nube. Estos firewalls son generalmente fáciles de desplegar y escalar, lo que los hace atractivos para las organizaciones que buscan una solución rápida y eficiente. Sin embargo, su capacidad de personalización puede ser limitada en comparación con las soluciones de firewalls externos (Ramírez, 2024).

Por otro lado, los firewalls externos son soluciones independientes que se administran fuera de la infraestructura de la nube. Estos firewalls ofrecen un mayor grado de personalización y control, permitiendo a las organizaciones adaptar las políticas de seguridad a sus necesidades específicas. No obstante, enfrentan retos en cuanto a integración y gestión, lo que puede afectar la eficiencia operativa (AWS, 2021).

Importancia de la Decryptación TLS

Una característica crítica en la seguridad moderna es la capacidad de los firewalls para realizar decryptación TLS (Transport Layer Security). Esta tecnología permite la inspección del tráfico cifrado, lo cual es esencial dado el creciente uso del cifrado en las comunicaciones en la nube. Sin esta capacidad, los firewalls no podrían detectar y mitigar eficazmente las amenazas ocultas en el tráfico cifrado, dejando a las organizaciones vulnerables a ataques sofisticados (Cisco, 2024).

Evaluaciones Comparativas

Las evaluaciones comparativas entre los diferentes tipos de firewalls son escasas, pero esenciales para entender sus fortalezas y debilidades en distintos contextos. Estudios

recientes han comenzado a explorar estos aspectos, proporcionando una base para decisiones informadas. Por ejemplo, se ha demostrado que los firewalls integrados pueden ofrecer una mejor eficiencia operativa en términos de despliegue y gestión, mientras que los firewalls externos pueden proporcionar una mayor seguridad a través de configuraciones más personalizadas y controladas (Fuentes & Pariajulca, 2023).

1.2. Descripción del problema

Con la adaptación acelerada de la prestación de servicios alojados en la nube, la ciberseguridad ha enfrentado una metamorfosis sin precedentes, impulsando a los firewalls a una posición crítica dentro de las estrategias de protección de infraestructuras digitales. Estos sistemas de seguridad, que históricamente actuaban como simples filtros, ahora desempeñan un papel multifuncional en el control y monitoreo del flujo de datos, un avance necesario frente a la creciente complejidad de las amenazas cibernéticas (Friese et al., 2018). Con el advenimiento de técnicas como la decodificación TLS para inspeccionar tráfico cifrado, los firewalls han tenido que adaptarse para mantener su eficacia en el entorno fluido y abierto de la nube (Cisco, 2024).

La disyuntiva se manifiesta en la elección entre firewalls integrados—embebidos en la infraestructura de servicios en la nube—y firewalls externos, que representan soluciones independientes que el usuario administra. Los primeros ofrecen una gestión simplificada y una integración nativa con la nube, potencialmente mejorando la eficiencia y la escalabilidad operativa (Gómez, 2024). Sin embargo, este tipo de firewalls puede no satisfacer las exigencias de personalización y control minucioso necesarias para contrarrestar las amenazas cibernéticas modernas, caracterizadas por su diversidad y sofisticación.

En contraposición, los firewalls externos proporcionan un nivel de personalización y control detallado sobre las políticas de seguridad, pero plantean desafíos de integración y una gestión más compleja que pueden mermar la eficiencia operativa, un aspecto crítico en los dinámicos entornos de nube actuales (AWS, 2021). La eficacia de cualquier solución de firewall, integrada o externa, requiere de una segmentación de red y políticas de seguridad bien definidas (Echegaray & Julca, 2023).

Esta situación plantea un interrogante crucial sobre cómo las organizaciones pueden equilibrar la necesidad de seguridad robusta, personalización y eficiencia operativa al elegir y desplegar firewalls en arquitecturas de nube. La carencia de estudios comparativos y evaluaciones que consideren tanto aspectos técnicos como operativos profundiza este dilema, dejando a las organizaciones sin una guía clara para tomar decisiones informadas que cumplan con sus requisitos específicos de seguridad y operación (Echegaray & Julca, 2023).

Frente a este escenario, el presente estudio se propone examinar la eficacia, la gestión y la eficiencia operativa de los firewalls integrados frente a los externos en ambientes de nube, con el fin de establecer una base empírica sólida que oriente las decisiones estratégicas en la implementación de soluciones de firewall adecuadas para arquitecturas basadas en la nube.

1.3. Objetivos

1.3.1. Objetivo General

Evaluar la eficiencia operativa, la gestión y el impacto en el rendimiento de firewalls integrados y externos en arquitecturas de nube para guiar las decisiones de implementación y optimización de la seguridad de la infraestructura digital.

1.3.2. Objetivos Específicos

1. Definir parámetros y métricas clave para la evaluación de la eficacia, la gestión y el rendimiento de firewalls integrados y externos en entornos de nube.
2. Establecer un entorno de nube controlado para simular escenarios de seguridad y gestión, facilitando la evaluación comparativa de los firewalls.
3. Analizar resultados para entender las ventajas y limitaciones de firewalls integrados versus externos, incluyendo el costo de implementación, operación y escalabilidad orientando las prácticas y decisiones estratégicas en seguridad de nube.

1.4. Estado del Arte

El creciente uso de la computación en la nube ha cambiado la forma en que las empresas manejan la protección de sus estructuras digitales. La evolución de los firewalls, desde sus versiones tradicionales hasta las adaptadas específicamente para entornos en la nube, refleja esta transformación. La investigación actual se centra en comprender y optimizar la eficacia de estos firewalls en contextos diversos, abordando sus capacidades, limitaciones y las mejores prácticas para su implementación.

Transformación de los Firewalls en la Era de la Nube

Tradicionalmente, los firewalls se diseñaron para proteger el perímetro de redes fijas, regulando el tráfico que entra y sale según políticas de seguridad previamente establecidas. Estos firewalls, aunque efectivos en entornos controlados, presentan limitaciones en escenarios de nube caracterizados por su dinamismo y escalabilidad. TechGenix (s.f.) destaca que los firewalls tradicionales no están equipados para manejar la naturaleza distribuida y el acceso remoto inherente a la nube.

Firewalls Adaptados a la Nube

Con el aumento de los servicios alojados en la nube, han surgido nuevas variantes de firewalls diseñadas para este entorno específico. Los firewalls integrados se destacan por su integración nativa con los servicios de la nube, lo que facilita su gestión y escalabilidad. Echegaray & Julca (2023), señalan que estos firewalls ofrecen una implementación más sencilla y una administración centralizada, lo que puede mejorar significativamente la eficiencia operativa.

Por otro lado, los firewalls externos, aunque requieren una gestión más compleja, proporcionan un nivel superior de personalización y control. Esto permite a las organizaciones adaptar las políticas de seguridad de manera más precisa a sus necesidades específicas, lo cual es crítico en entornos con requerimientos de seguridad rigurosos (AWS, 2021).

Importancia de la Inspección del Tráfico Cifrado

Una de las capacidades más importantes de los firewalls modernos es la inspección del tráfico cifrado, especialmente mediante la decryptación TLS (Transport Layer Security). Cisco (2024), enfatiza que esta capacidad es crucial debido al predominio del tráfico cifrado en las comunicaciones modernas. Sin esta función, los firewalls no podrían detectar amenazas ocultas, lo que aumentaría significativamente el riesgo de ataques cibernéticos

Evaluación Comparativa de Firewalls

Estudios recientes han comparado la eficacia operativa y la seguridad proporcionada por los firewalls integrados y externos en entornos de nube. Echegaray & Julca (2023),encontraron que los firewalls integrados tienden a ofrecer una mejor eficiencia operativa y una implementación más rápida, mientras que los firewalls externos destacan

por su capacidad de personalización y control detallado sobre las políticas de seguridad. Estas evaluaciones son fundamentales para que las entidades puedan tomar decisiones racionales sobre qué tipo de firewall utilizar, dependiendo de sus necesidades específicas de seguridad y operativas.

Desafíos y Beneficios en la Implementación de Firewalls en la Nube

El poner en funcionamiento soluciones de seguridad en la nube, como los firewalls, presenta varios desafíos. Ramos (2024), identifican la visibilidad del tráfico, la complejidad de la integración y la escalabilidad como los principales retos. Sin embargo, los beneficios incluyen una mayor susceptibilidad de adaptación, facilidad de despliegue y la posibilidad de gestionar políticas de seguridad de manera centralizada, lo que puede mejorar la capacidad de seguridad de las organizaciones para detectar, responder y solucionar amenazas.

Innovaciones Tecnológicas

Las innovaciones tecnológicas, como los firewalls de próxima generación (NGFW) y los firewalls como servicio (FWaaS), están redefiniendo las capacidades de los firewalls en la nube. Guanotoa (2024), destacan que estos firewalls avanzados incorporan funciones que ayudan a la identificación de intrusiones y la inspección de contenidos de los paquetes en tiempo real, además de ofrecer la escalabilidad y la gestión simplificada de las soluciones basadas en las plataformas o sistemas de la nube. Estas innovaciones permiten a las organizaciones no solo proteger sus infraestructuras, sino también adaptarse rápidamente a las amenazas emergentes.

1.5. Contribuciones

A través del presente trabajo de titulación, se aportan nuevas perspectivas y medidas en la seguridad de la información o ciberseguridad en infraestructuras de nube. Este estudio proporciona una evaluación comparativa entre firewalls integrados y externos, ofreciendo valiosa información y herramientas prácticas que pueden ser aplicadas tanto por académicos como por profesionales en el campo del procesamiento, transmisión y almacenamiento de la información. Los aportes fundamentales de esta investigación se detallan a continuación:

- Innovación en Seguridad en la Nube: El estudio introduce una comparación detallada y empírica entre firewalls integrados y externos, permitiendo a las organizaciones comprender mejor las fortalezas y debilidades de cada enfoque y ayudándoles a seleccionar la solución que mejor se ajusta a sus exigencias de seguridad y operativas.
- Optimización de la Gestión de Firewalls: Se proporcionan recomendaciones prácticas para la implementación y gestión de firewalls en entornos de nube, destacando las mejores prácticas para maximizar la eficiencia operativa y minimizar los riesgos de seguridad.
- Evaluación de Eficiencia Operativa: A través de simulaciones en un entorno controlado, se establecen parámetros y métricas clave para evaluar la eficiencia operativa de los firewalls. Estos resultados proporcionan una base firme para investigaciones futuras y desarrollos para mantener los datos e información privados seguros en las plataformas de la nube.
- Fomento de la Flexibilidad y Escalabilidad: La investigación demuestra cómo los firewalls integrados pueden mejorar la flexibilidad y escalabilidad de las infraestructuras de nube, proporcionando soluciones adaptativas que responden a las demandas cambiantes del entorno tecnológico.

- Guía para la Personalización y Control de Seguridad: Se exploran las capacidades de personalización y control detallado que los firewalls externos pueden ofrecer, permitiendo a las organizaciones adaptar sus políticas de seguridad de manera más precisa y efectiva.
- Contribución al Conocimiento Académico: Este trabajo llena un vacío en la literatura existente sobre la comparación de firewalls en la nube, aportando datos empíricos y análisis que pueden ser utilizados como referencia en estudios futuros. Las conclusiones y hallazgos proporcionan una guía clara para la realización de nuevas investigaciones en esta área.
- Impacto en la Toma de Decisiones Estratégicas: Los resultados de esta investigación ayudan a los responsables de la supervisión y administración de sistemas, como a los profesionales de TI a tomar decisiones informadas sobre la implementación de soluciones de firewall, optimizando la seguridad y eficiencia operativa de sus infraestructuras digitales.

1.6. Conclusiones

El presente estudio ha demostrado que tanto los firewalls integrados como los externos tienen roles cruciales y complementarios en la protección de las arquitecturas de nube. Los firewalls integrados se destacan por su facilidad de implementación y gestión, ofreciendo una integración perfecta con los servicios nativos de la nube. Esto beneficios son una alternativa atractiva para corporaciones y organizaciones que buscan una solución de seguridad rápida y eficiente sin la necesidad de una gestión compleja. Por otro lado, los firewalls externos, aunque requieren una configuración y administración más compleja, proporcionan un mayor nivel de personalización y control sobre las políticas de seguridad,

lo cual es fundamental para organizaciones con requisitos de seguridad específicos y rigurosos.

La capacidad de desencriptación TLS ha sido identificada como una característica esencial en la lucha contra las amenazas ocultas en el tráfico cifrado, y debe ser una consideración clave tanto para los firewalls integrados como para los externos. Los resultados de las simulaciones y evaluaciones realizadas en un entorno controlado han revelado que los firewalls integrados ofrecen ventajas significativas en términos de eficiencia operativa y simplicidad de gestión, mientras que los firewalls externos destacan en su capacidad de adaptación y personalización.

Las organizaciones deben identificar y precisar sus necesidades específicas de seguridad y operativas para determinar la mejor solución de firewall. En muchos casos, una combinación de ambos tipos de firewalls puede ofrecer una protección más robusta y completa. Este estudio no solo proporciona una base empírica sólida para futuras investigaciones, sino que también ofrece recomendaciones prácticas para los profesionales de TI y los encargados de administrar la implementación y operación de soluciones de seguridad en la nube.

El estudio resalta la relevancia de una estrategia de seguridad adaptable y escalable que pueda evolucionar con las amenazas emergentes y las necesidades cambiantes de las infraestructuras digitales. A medida que las tecnologías de la nube continúan avanzando, es fundamental que las soluciones de seguridad también progresen para asegurar la integridad, privacidad y disponibilidad constante y eficiente de la información y aplicaciones.

Capítulo 2

Marco teórico

Al abordar la innovación y seguridad en arquitecturas de nube, es fundamental comprender cómo las tecnologías evolucionan para enfrentar las amenazas modernas. Este capítulo presenta una exploración exhaustiva del uso de firewalls, tanto integrados como externos, dentro de entornos de nube, ofreciendo un marco teórico que guiará el análisis y la comprensión del tema.

En un paisaje digital donde la seguridad es más crítica que nunca, las arquitecturas de nube proporcionan el escenario perfecto para el despliegue de soluciones de seguridad avanzadas. La información fluye continuamente a través de redes corporativas, haciendo esencial la implementación de firewalls eficaces para resguardar los datos y garantizar la integridad de los sistemas.

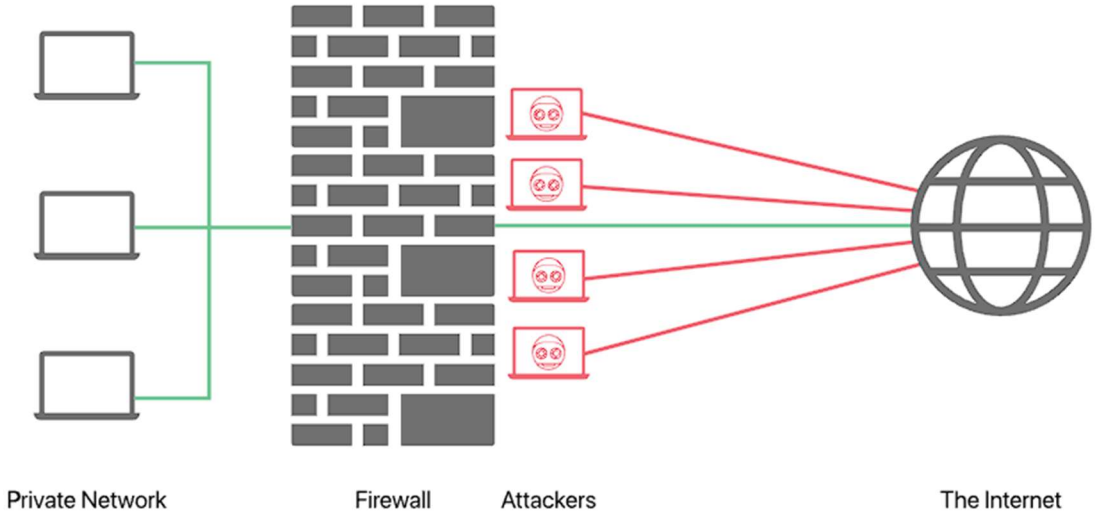
El objetivo de este marco teórico es establecer las bases sobre la relevancia de los firewalls en la protección de infraestructuras en la nube. Se explorarán los principios de funcionamiento, ventajas, desafíos y comparativas entre las opciones de firewalls integrados y externos, proporcionando una visión clara de cómo pueden coexistir y complementarse para mejorar la seguridad de las redes corporativas.

2.1. Definición y Clasificación de Firewalls

Un firewall funciona como una primera línea de defensa en la seguridad de redes, operando como un sistema clave en la protección de datos. Su tarea principal es monitorizar y gestionar el tráfico de red entrante y saliente, aplicando normas de seguridad predeterminadas. Su rol fundamental es establecer una separación entre una red interna, que es segura y fiable, y una red externa, como Internet, que se considera potencialmente riesgosa. Los cortafuegos pueden ser dispositivos físicos, programas de software o una combinación de ambos. Son esenciales para

proteger la información, defendiendo contra ataques externos, bloqueando accesos no autorizados desde redes externas y filtrando el tráfico de red. Así, aseguran que solo el tráfico legítimo y seguro sea permitido, mientras que el tráfico malicioso queda bloqueado (Salinas, 2023).

Figura 1. *Esquema del Firewall*



Fuente: (Cloudflare, 2024)

Además, los firewalls ayudan a prevenir la fuga de datos sensibles fuera de la red sin autorización y regular el acceso a diversos recursos de la red, garantizando que únicamente individuos autorizados puedan. y dispositivos autorizados tengan acceso a ellos. Los firewalls también mantienen registros de los eventos y del tráfico de red, lo cual es crucial para monitorizar, localizar y responder a incidentes de seguridad. Estos registros permiten que los administradores de red monitoreen y auditen el uso de la red, proporcionando una capa adicional de seguridad (Enciso et al., 2023).

2.1.1. Clasificación de los Diferentes Tipos de Firewalls

Los firewalls se pueden clasificar de varias maneras según su implementación, funcionalidad y ubicación. En cuanto a su implementación, pueden clasificarse en dos grupos de hardware o de software. Los firewalls de hardware se encuentran instalados en dispositivos físicos dedicados que se colocan entre la red interna y externa, proporcionando un alto rendimiento y siendo adecuados para redes empresariales. Ejemplos de estos dispositivos incluyen los de Cisco, Palo Alto Networks y Fortinet. Por otro lado, los firewalls de software son aplicaciones instaladas en servidores o dispositivos individuales. Estos son más flexibles y fáciles de actualizar, pero dependen del sistema operativo subyacente, como Windows Defender Firewall y ZoneAlarm (Enciso et al., 2023).

Según los métodos de filtración, los tipos de cortafuegos incluyen los de filtrado de paquetes, los de inspección con estado, los de aplicación (o proxies) y los de nueva generación (NGFW). Los cortafuegos de filtrado de paquetes monitorean los datos transmitidos y autorizan o impiden su paso, centrándose en aspectos como la dirección IP, el puerto y el protocolo, ofreciendo una solución simple y rápida, aunque sin análisis profundo del contenido de los paquetes. Los firewalls de inspección con estado mantienen un registro de las conexiones activas y deciden si un paquete puede pasar basado en el estado de la conexión, aportando mayor protección que los firewalls de filtro de paquetes. Los firewalls de aplicación funcionan como intermediarios entre los usuarios y los recursos externos, inspeccionando el tráfico de aplicaciones específicas, como HTTP y FTP, y ofreciendo un nivel de seguridad más granular. Los firewalls de próxima generación incorporan las funcionalidades de los firewalls comúnmente utilizados con propiedades avanzadas como revisión profunda de paquetes (DPI), supervisión de posibles amenazas (IPS) y control de aplicaciones (Pineda & Quiceno, 2023).

En cuanto a su ubicación, los firewalls pueden ser perimetrales, internos o de nube. Los firewalls perimetrales están situados en el perímetro de la red y protegen la red interna de accesos no autorizados desde el exterior, actuando como la primera protección en una arquitectura de red. Los firewalls internos se utilizan dentro de la red para segmentar subredes y proteger diferentes áreas de la red entre sí, ayudando a contener incidencias de seguridad dentro de la red interna. Los firewalls de nube son herramientas de seguridad que están alojados en la nube que protegen recursos en la nube, y pueden ser integrados (ofrecidos por el proveedor de nube) o externos (soluciones de terceros que se integran con la nube). Ejemplos de firewalls de nube incluyen AWS WAF (Web Application Firewall) y Azure Firewall (AWS, 2021).

Finalmente, los firewalls se pueden clasificar en integrados y externos. Los firewalls integrados son soluciones de firewall que están integradas dentro de otros sistemas o servicios, como los firewalls de aplicaciones web (WAF) ofrecidos por prestadores de servicios en la nube como AWS, Azure y Google Cloud. Estos suelen ser más fáciles de configurar y mantener, y están optimizados para el entorno específico en el que se utilizan. Por otro lado, los firewalls externos son soluciones independientes que se implementan fuera del entorno principal, como dispositivos de hardware o software que se instalan y configuran por separado. Estos ofrecen mayor flexibilidad y control, y normalmente tienen competencias más avanzadas y personalizables, como las soluciones de Fortinet, Palo Alto Networks y Check Point (Pineda & Quiceno, 2023).

2.2. Arquitecturas de Red en la Nube

En los sitios donde se ejecutan las aplicaciones, entorno de nube, las arquitecturas de red se diseñan para ofrecer alta disponibilidad, escalabilidad y seguridad. Un ejemplo destacado de estas arquitecturas es la VPC (Virtual Private Cloud) en AWS. Una VPC facilita a los usuarios

apartar aisladamente una sección de la infraestructura en la nube de AWS permite desplegar recursos de AWS en una red virtual configurada por el usuario.

Dentro de una VPC, se pueden definir subredes, que son segmentos de la red que permiten organizar y asegurar los recursos. Las subredes pueden ser públicas o privadas, dependiendo de si necesitan acceso directo a Internet. Las subredes públicas están asociadas a una tabla de ruta que facilita el acceso a Internet por medio de una Gateway de Internet, mientras que las subredes privadas no tienen acceso directo a Internet, lo que las hace ideales para recursos que no necesitan ser accesibles desde fuera, como los bancos o bases de datos y servidores de aplicaciones internos (AWS, 2021).

Una nube virtual privada (VPC) también permite configurar otras características de red como tablas de enrutamiento, gateways NAT (para proporcionar acceso a Internet a instancias en subredes privadas), y endpoints de VPC (para conectar servicios de AWS directamente a su VPC sin usar una Gateway de Internet). Además, las VPC pueden interconectarse a través de Peering de VPC, lo que permite el tráfico entre VPCs diferentes dentro de la misma región o en regiones diferentes sin pasar por Internet (AWS, 2021).

2.2.1. Integración de Firewalls en las Arquitecturas de Red en la Nube

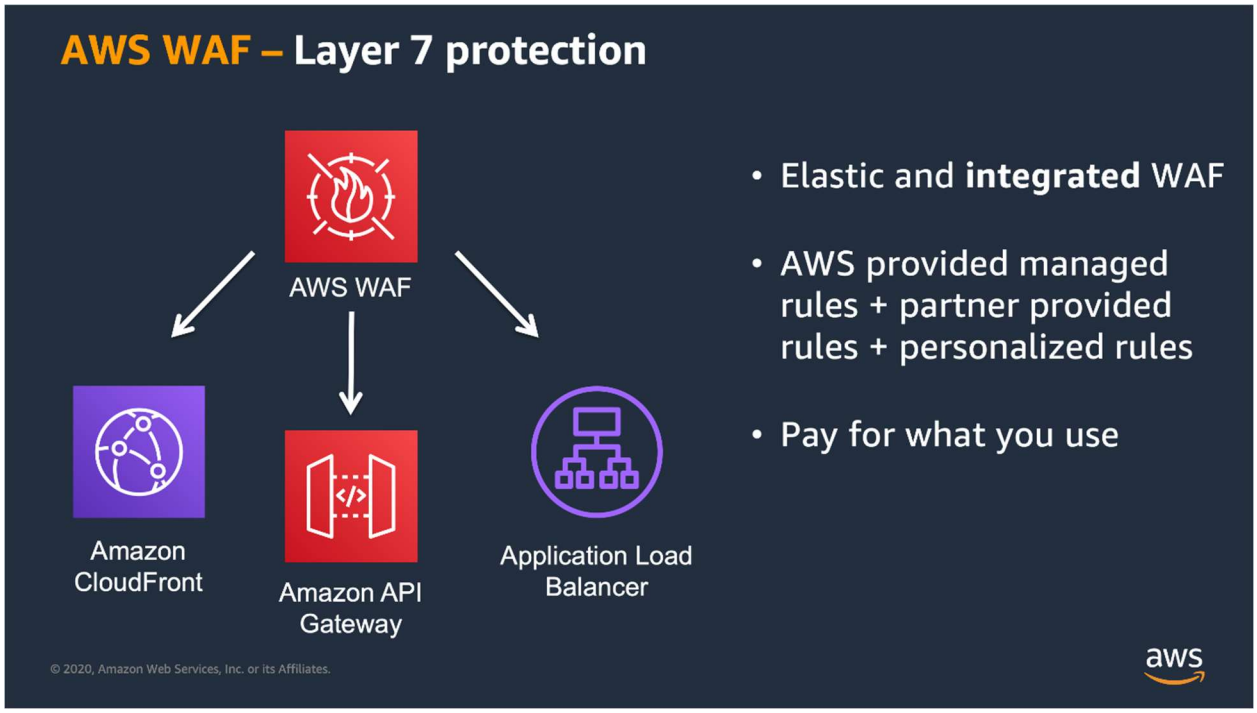
Los firewalls son componentes cruciales en las arquitecturas de red en la nube, proporcionando una forma eficaz para prevenir posibles ciberataques, una capa adicional de protección para salvaguardar los recursos en la nube. En AWS, los firewalls se integran de varias maneras dentro de una VPC. Un componente esencial es el Security Group, que funciona como un firewall virtual para instancias EC2, verificando el tráfico entrante y saliente a nivel de instancia.

Los Security Groups permiten definir reglas de tráfico basadas en direcciones IP y puertos, asegurando que solo el tráfico legítimo pueda llegar a las instancias (AWS, 2021).

Otra herramienta importante es el Network ACL (Access Control List), que actúa como un firewall a nivel de subred. A diferencia de los Security Groups, los Network ACLs son reglas de firewall asociadas a subredes enteras y permiten o deniegan tráfico basado en reglas explícitas. Esto proporciona una capa adicional de control y seguridad cuando entra el tráfico de red y sale de las subredes (AWS, 2021).

Para proteger aplicaciones web, AWS presenta el AWS WAF (Web Application Firewall), que se puede vincular a servicios como Amazon CloudFront, Application Load Balancer, y API Gateway. AWS WAF ayuda a resguardar las aplicaciones web frente a ataques habituales como inyecciones SQL y Cross-Site Scripting (XSS), añadiendo una capa adicional de protección específica para el tráfico de aplicaciones web (AWS, 2021).

Figura 2. *Protección de capa 7*



Fuente: (AWS, 2024)

Respecto a la seguridad avanzada, los firewalls de próxima generación (NGFW) también se pueden aplicar en entornos de nube. Estos NGFWs, como los ofrecidos por Palo Alto Networks y Fortinet, proporcionan funcionalidades modernas de supervisión profunda de paquetes (DPI), prevención de intrusiones (IPS), y verificación de aplicaciones. Estos dispositivos se pueden implementar como instancias virtuales dentro de la VPC y se configuran para inspeccionar y filtrar el tráfico de red de manera granular (Pineda & Quiceno, 2023).

Además de estas herramientas, los entornos de nube también permiten la integración con soluciones de seguridad externas. Por ejemplo, las empresas pueden implementar firewalls de terceros, tanto hardware como software, dentro de su arquitectura de red en la nube para complementar y reforzar las medidas de seguridad proporcionadas por el proveedor de nube. Esto incluye configuraciones híbridas donde los firewalls físicos en las instalaciones de la empresa se integran con las soluciones de firewall en la nube para una protección coherente y robusta (Cisco, 2024)

2.3.Seguridad en la Nube

El cambio hacia el uso de plataformas en la nube para servicios ha revolucionado la forma en que las empresas administran sus recursos tecnológicos, ofreciendo flexibilidad, escalabilidad y ahorro de costos. Sin embargo, esta transición también presenta una serie de retos específicos de seguridad que deben ser gestionados correctamente para salvaguardar la información y aplicaciones sensibles. Los firewalls juegan un papel esencial en mitigar estos desafíos al proporcionar control y protección sobre el tráfico de red en entornos de nube.

Uno de los principales desafíos de seguridad en la nube es la superficie de ataque ampliada. El proceso de transferencia de datos a la nube implica que todos los servicios y recursos ahora son

accesibles desde múltiples ubicaciones y dispositivos, lo que aumenta significativamente las posibles vías de ataque. Los firewalls, como los Security Groups y Network ACLs en AWS, ayudan a limitar esta superficie de ataque al restringir el acceso a los recursos solo a direcciones IP y puertos específicos. Esto asegura que solo el tráfico legítimo pueda alcanzar las aplicaciones y datos críticos (AWS, 2021).

Otro desafío importante es la segmentación de red. En un entorno de nube, es crucial segmentar adecuadamente la red para limitar el movimiento lateral de posibles atacantes que hayan comprometido un recurso. Los firewalls internos, como los Network ACLs y las políticas de seguridad de subredes, permiten crear zonas aisladas dentro de la nube, asegurando que diferentes partes de la red no puedan comunicarse libremente a menos que esté explícitamente permitido. Esto reduce el riesgo de que un ataque en una parte de la red se propague a otras partes (AWS, 2021).

El aislamiento de tráfico es otro aspecto crítico de la seguridad en la nube. En una nube pública, los recursos de múltiples clientes a menudo comparten la misma infraestructura subyacente. Es vital garantizar que el tráfico de un cliente esté completamente aislado del tráfico de otros clientes para evitar filtraciones de datos y otros problemas de seguridad. Los firewalls de próxima generación (NGFW) y las soluciones de firewall virtual proporcionan capacidades avanzadas de inspección de tráfico, asegurando que solo el tráfico autorizado y seguro pueda entrar y salir de las VPCs y otras redes virtuales (Pineda & Quiceno, 2023).

Además de estos desafíos, la complejidad de la gestión de seguridad en la nube requiere soluciones que puedan integrarse y escalar fácilmente. Los firewalls en la nube constituirá con la capacidad de ajustarse a modificaciones dinámicas en la infraestructura, como la creación y eliminación de instancias, y deben integrarse con herramientas de gestión y monitoreo para

proporcionar una visión coherente y centralizada de la seguridad de la red. Soluciones como AWS WAF y Azure Firewall están diseñadas para integrarse estrechamente con otros servicios de la nube, proporcionando una protección robusta sin agregar complejidad innecesaria a la gestión de la red (Angulo et al., 2023).

En resumen, los firewalls en la nube están diseñados para mitigar varios desafíos de seguridad específicos, incluyendo la ampliada superficie de ataque, la necesidad de segmentación de red, el aislamiento de tráfico y la complejidad de la gestión de seguridad. Al proporcionar control granular sobre el tráfico de red y asegurar que solo el tráfico autorizado pueda acceder a los recursos, los firewalls son instrumentos imprescindibles para proteger los entornos de nube.

2.4.Firewalls Integrados vs. Externos

En la protección de entornos de nube, las organizaciones pueden optar por utilizar firewalls integrados ofrecidos por los proveedores de nube, como AWS Network Firewall, o soluciones externas, que pueden ser dispositivos físicos o virtuales independientes. Cada opción presenta ventajas y desventajas en términos de costos, escalabilidad, mantenimiento y rendimiento.

Los firewalls integrados usualmente son más económicos en términos de costos iniciales, ya que no requieren hardware complementario ni licencias de software separadas, y sus costos están incluidos en el sistema de cobro según el consumo del proveedor de la nube (AWS, 2021). Además, están diseñados para escalar automáticamente con los recursos de la nube, lo que permite manejar aumentos repentinos en el tráfico sin necesidad de intervención manual o reconfiguración (AWS, 2021). La administración y el mantenimiento de estos firewalls son gestionados en gran medida por el proveedor de la nube, incluyendo actualizaciones de software, parches de seguridad y ajustes de configuración necesarios para mantener el rendimiento y la seguridad óptimos (Angulo

et al., 2023). Otro beneficio importante es la integración perfecta con otros servicios y herramientas del proveedor de la nube, facilitando la gestión, monitoreo y regulación de la protección de la red desde una sola interfaz, lo que mejora de una manera eficiente el funcionamiento y la consistencia de la seguridad (AWS, 2024).

Los firewalls integrados pueden ser menos flexibles en términos de personalización y funcionalidades avanzadas comparados con soluciones externas. Están programados para cubrir la mayoría de los casos de uso comunes, pero pueden carecer de características específicas requeridas por algunas organizaciones (Pineda & Quiceno, 2023). Además, el uso de firewalls integrados implica una mayor dependencia del proveedor de la nube, lo cual puede ser una desventaja si la organización necesita cambiar de proveedor o si surgen problemas de confianza con el proveedor actual.

Por otro lado, los firewalls externos, tanto físicos como virtuales, ofrecen una mayor flexibilidad en términos de personalización y funcionalidades avanzadas. Las organizaciones pueden seleccionar y configurar soluciones que se adapten específicamente a sus necesidades de seguridad y políticas de red (Pineda & Quiceno, 2023).Utilizar firewalls externos permite a las organizaciones mantener una mayor independencia de su proveedor de nube, facilitando la migración entre proveedores y reduciendo la dependencia de un único proveedor para todas las necesidades de seguridad (Cisco, 2024). Además, estos firewalls a menudo proporcionan capacidades avanzadas de inspección y control del tráfico, como la revisión exhaustiva de paquete (DPI), prevención de intrusiones (IPS), y monitoreo de aplicaciones, facilitando una protección más granular y sofisticada.

Los firewalls externos pueden implicar costos iniciales más altos debido a la necesidad de hardware adicional, licencias de software y posiblemente personal especializado para su

configuración y mantenimiento. Además, los costos operativos pueden aumentar con la necesidad de gestionar y actualizar estos dispositivos de forma independiente (Cisco, 2024). La administración y el mantenimiento de firewalls externos requieren recursos adicionales dentro de la organización, incluyendo la implementación de actualizaciones de software, parches de seguridad y ajustes de configuración necesarios para mantener el rendimiento y la seguridad óptimos (Cisco, 2024). Además, escalar soluciones de firewall externas puede ser más complicado y menos ágil en comparación con las soluciones integradas, ya que puede ser necesario adquirir y configurar hardware adicional a medida que aumenta el tráfico, lo que puede retrasar la capacidad de respuesta a picos repentinos en la demanda de tráfico (Pineda & Quiceno, 2023).

2.5.Casos de Uso y Escenarios de Aplicación

En la práctica, la elección entre firewalls integrados y externos puede variar significativamente según factores como el tamaño de la organización, los requisitos regulatorios y el nivel de riesgo. A continuación, se presentan algunos estudios de caso y ejemplos específicos que ilustran cómo estos factores influyen en la preferencia por firewalls integrados o externos.

Firewalls Integrados

2.5.1. Caso 1: Pequeñas y Medianas Empresas (PYMEs)

Una pequeña empresa de desarrollo de software con menos de 50 empleados decide trasladar sus aplicaciones, su infraestructura y datos a la nube utilizando Amazon Web Services (AWS). La empresa no tiene un equipo de TI dedicado y necesita una solución de seguridad que sea fácil de implementar y gestionar. Optan por usar AWS Network Firewall debido a su integración perfecta con otros servicios de AWS y la facilidad de configuración con la ayuda de la consola de AWS. La capacidad de avanzar automáticamente con la infraestructura de AWS y el

costo basado en la utilización son beneficios adicionales que se ajustan con el presupuesto y las exigencias operativas de la empresa (AWS, 2021).

2.5.2. Caso 2: Startups en Crecimiento

Un startup en rápido crecimiento en el sector de fintech utiliza Google Cloud Platform (GCP) para alojar sus aplicaciones. Debido a la rápida expansión y la necesidad de mantener el enfoque en el desarrollo de productos, la empresa elige Google Cloud Armor para la protección de aplicaciones web y Cloud Firewall para la seguridad de la red. Estas soluciones integradas proporcionan la escalabilidad y el mantenimiento automatizado necesarios para soportar su crecimiento acelerado sin requerir un equipo de seguridad especializado (Suárez et al., 2024).

Firewalls Externos

2.5.3. Caso 3: Grandes Corporaciones

Una gran corporación multinacional en el sector de servicios financieros tiene una infraestructura híbrida que combina centros de datos locales y múltiples proveedores de nube. Debido a los estrictos requisitos regulatorios y la necesidad de personalización avanzada de seguridad, la corporación elige implementar firewalls externos de Palo Alto Networks en sus centros de datos y en sus entornos de nube. Estos firewalls proporcionan una revisión a fondo de paquetes (DPI), prevención de intrusiones (IPS) y vigilancia granular de aplicaciones, lo que permite a la corporación cumplir con las normas de seguridad y directrices internacionales, mientras mantiene una supervisión consistente en toda su infraestructura global (Pineda & Quiceno, 2023).

2.5.4. Caso 4: Instituciones de Salud

Un hospital universitario que maneja datos sensibles de pacientes y debe cumplir con regulaciones estrictas como HIPAA decide utilizar firewalls externos para asegurar sus sistemas de TI. El hospital implementa dispositivos de firewall Cisco ASA en su red local y firewalls virtuales en su infraestructura de nube para garantizar la seguridad de información sensible y satisfacer las demandas normativas. La capacidad de particularizar las políticas de seguridad y la conexión con varios sistemas de gestión de eventos de seguridad (SIEM) posibilitan al hospital mantener un alto nivel de seguridad y monitoreo (Cisco, 2024).

2.5.5. Caso 5: Organizaciones con Alta Exposición al Riesgo

Una empresa de comercio electrónico de gran tamaño con operaciones globales enfrenta un alto nivel de exposición al riesgo debido al volumen y la esencia de las operaciones y transacciones financieras que gestiona. Para protegerse contra amenazas avanzadas y ataques dirigidos, la empresa decide implementar firewalls de próxima generación (NGFW) de Fortinet. Estos firewalls externos proporcionan capacidades avanzadas de inspección de tráfico, análisis de amenazas y segmentación de red, lo que permite a la empresa mitigar el riesgo de manera efectiva y asegurar su infraestructura en la nube y local (Vera, 2024).

2.6.Tendencias y Futuro de los Firewalls en la Nube

La tecnología de firewalls está en constante evolución para hacer frente a las crecientes y cambiantes amenazas a la seguridad de la red. En la actualidad y en el futuro próximo, la tendencia tecnológica principal es la integración de inteligencia artificial (IA) y aprendizaje automático (ML) en la protección de redes. Estas tecnologías están transformando la manera en que los cortafuegos identifican, examinan y reaccionan ante las amenazas.

2.6.1. Inteligencia Artificial y Aprendizaje Automático

La incorporación de IA y ML en los firewalls facilita una detección y respuesta más acelerada y precisa ante peligros y amenazas. Los algoritmos de ML pueden analizar una gran cantidad de datos de tráfico de red para reconocer patrones y anomalías que podrían indicar acciones maliciosas. Esto permite a los firewalls adaptarse y mejorar continuamente su capacidad de detección sin intervención manual. Además, la IA puede automatizar la respuesta a amenazas en tiempo real, mitigando ataques antes de que puedan causar daños significativos (Villacís et al., 2024).

Automatización y Orquestación: La automatización de tareas de seguridad es otra tendencia clave. Los firewalls modernos están integrando capacidades de automatización para gestionar configuraciones, aplicar políticas de seguridad y responder a incidentes de manera eficiente. La orquestación de seguridad, que implica la coordinación de múltiples herramientas y sistemas de seguridad, permite una gestión más coherente y eficiente de la seguridad en entornos híbridos y multicloud (Stocovaz, 2023).

2.6.2. Seguridad Zero Trust

El modelo de seguridad Zero Trust, que asume que ninguna entidad dentro o fuera de la red es de confianza por defecto, está ganando popularidad. Los firewalls están evolucionando para soportar este modelo mediante la implementación de controles granulares de acceso y la verificación continua de usuarios y dispositivos. Esto incluye la segmentación de red y la microsegmentación para limitar el movimiento lateral de atacantes dentro de la red (ESET, 2024).

2.6.3. Integración con Plataformas de Seguridad en la Nube

Las empresas que proporciona los servicios de seguridad en la nube están mejorando para integrarse mejor con firewalls y otras soluciones de seguridad. Esto incluye la oferta de servicios

de firewall nativos que están profundamente integrados con la infraestructura de nube, permitiendo una gestión unificada y simplificada de la seguridad (AWS, 2021).

2.6.4. Firewalls de Próxima Generación (NGFW)

Los NGFW continúan progresando con capacidades avanzadas como la inspección a fondo de los paquetes (DPI), prevención de intrusiones (IPS), y el control de aplicaciones. Estas funcionalidades avanzadas permiten una protección más detallada y efectiva contra amenazas complejas (Pineda & Quiceno, 2023).

2.6.5. Influencia de estas Tendencias en la Elección entre Firewalls Integrados y Externos

La adopción de IA y ML en la tecnología de firewalls está afectando la elección entre firewalls integrados y externos. Los firewalls integrados, ofrecidos por proveedores de nube como AWS y Azure, están aprovechando estas tecnologías para mejorar la detección y respuesta a amenazas. La integración nativa con otros servicios de nube permite una implementación más sencilla y una gestión centralizada, lo cual es beneficioso para organizaciones que buscan simplicidad y eficiencia en sus operaciones de seguridad (AWS, 2021).

Por otro lado, los firewalls externos, tanto físicos como virtuales, también están incorporando IA y ML para ofrecer capacidades avanzadas de seguridad. Las soluciones externas suelen proporcionar una mayor flexibilidad y personalización, lo cual es crucial para organizaciones con requisitos de seguridad específicos o que operan en entornos híbridos y multicloud. Estas organizaciones pueden preferir firewalls externos para mantener un control más granular y una capacidad de respuesta más adaptativa a las amenazas avanzadas (Pineda & Quiceno, 2023).

La automatización y la orquestación están facilitando la gestión de la seguridad en entornos complejos. Los firewalls integrados se benefician de la integración estrecha con los servicios de nube, permitiendo una orquestación fluida y una respuesta coordinada a incidentes de seguridad. Sin embargo, los firewalls externos pueden ofrecer soluciones de automatización más avanzadas y personalizables, lo que es ideal para organizaciones que necesitan adaptarse rápidamente a cambios en la infraestructura y las amenazas (ESET, 2024).

El modelo de seguridad Zero Trust está potenciando la adopción tanto de firewalls integrados como externos, de acuerdo con los requerimientos particulares de cada empresa. Los firewalls integrados pueden proporcionar una implementación más rápida y sencilla de políticas Zero Trust, especialmente en entornos de nube nativos. Sin embargo, los firewalls externos pueden ofrecer un mayor nivel de control y personalización, lo que es esencial para implementar un modelo Zero Trust en entornos híbridos y multicloud (ESET, 2024).

2.7.Normativas y Cumplimiento

El empleo de firewalls en entornos de nube está sujeto a diversas normativas, reglamentos y requisitos de cumplimiento que varían según la jurisdicción. Estas normalizaciones son fundamentales para asegurar la seguridad y privacidad de la información, y su cumplimiento es fundamental para evitar sanciones legales y daños en la reputación. A continuación, se examinan algunas de las principales normativas y sus implicaciones en el uso de firewalls, incluyendo un enfoque en las leyes relevantes en Ecuador.

2.7.1. Reglamento General de Protección de Datos (GDPR)

La GDPR, aplicable en la Unión Europea (UE), es una de las normativas de protección de datos más estrictas y severas a nivel mundial. Esta normativa exige que las organizaciones adopten

medidas adecuadas de protección y seguridad para salvaguardar la información personal de los residentes de la UE. Los firewalls proporcionan una barrera contra accesos no autorizados y ataques cibernéticos. Las organizaciones deben asegurarse de que sus firewalls sean capaces de señalar y monitorear el tráfico de datos para localizar y responder a posibles incidentes de seguridad (PowerData, 2024).

Además, la GDPR requiere que las organizaciones realicen evaluaciones de impacto sobre la protección de datos (DPIA) al implementar tecnologías que puedan influir de manera significativa en la privacidad de la información personal. La aplicación de firewalls y otras medidas de seguridad deben estar documentadas y formar parte de estas evaluaciones para evidenciar el acatamiento de la normativa.

2.7.2. Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA)

En Estados Unidos, la HIPAA establece criterios para la protección de la información de salud de los pacientes. Las entidades en el sector salud deben implementar medidas de seguridad físicas, administrativas y tecnológicas para salvaguardar la privacidad, integridad y disponibilidad de la información electrónica de salud protegida (ePHI). Como elemento informático, los firewalls son una parte fundamental de estas medidas técnicas, ya que vigilan el acceso a los sistemas que manejan la información médica protegida electrónica (ePHI) y protegen contra amenazas externas e internas (Merck & Co, 2024).

Las organizaciones para dar cumplimiento a lo que exige la HIPAA, deben asegurarse de que sus firewalls estén configurados para limitar el acceso a los datos de salud solo al personal y usuarios autorizados y además registrar las actividades de acceso para auditar el uso de la

información. Además, deben implementar políticas de gestión de incidentes para responder rápidamente a cualquier violación de seguridad.

2.7.3. Ley de Privacidad del Consumidor de California (CCPA)

Esta ley de privacidad es una normativa de protección de datos que regula a las organizaciones que operan y residen en California y gestionan información personal de los residentes del estado. Similar a la GDPR, la CCPA exige que las organizaciones implementen medidas de protección apropiadas para asegurar la defensa de la información personal frente a infracciones de seguridad y ciberataques. Los firewalls son una herramienta fundamental para cumplir con esta obligación al dotar una primera línea de defensa contra los peligros y riesgos (Google Cloud, 2024).

Además de proteger los datos, la CCPA exige que las empresas informen a los consumidores sobre sus prácticas de recopilación de datos y les garanticen ejecutar sus derechos de acceso, eliminación y portabilidad de datos. Los firewalls deben estar configurados para asegurar y delimitar que solo el tráfico permitido pueda acceder a los datos sensibles, y las organizaciones deben de demostrar que han aplicado medidas de seguridad adecuadas.

2.7.4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

La LFPDPPP es una normativa mexicana que establece los requisitos para la gestión de datos personales y la privacidad. Las organizaciones deben implementar medidas de seguridad administrativas, tecnológicas y físicas para asegurar la integridad de la información y así impedir el deterioro, pérdida, modificaciones o el uso no permitido. Los firewalls son piezas importantes

de las medidas técnicas que las organizaciones deben implementar para cumplir con esta ley (Instituto Nacional de Transparencia, 2021).

La LFPDPPP también requiere que las organizaciones realicen procesos de verificación de seguridad periódicos para determinar la eficacia y cumplimiento de las medidas implementadas. Los firewalls deben estar configurados para dar seguimiento y registrar el tráfico de red, posibilitando la localización y respuesta a incidentes de seguridad, y las organizaciones deben mantener registros de estas actividades para fines de auditoría.

2.7.5. Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP)

En Ecuador, la (LOPDP) define los principios, derechos, deberes y procedimientos para asegurar el derecho a la protección de la información personal. Esta ley exige que las entidades adopten medidas adecuadas de seguridad y protección, tanto técnicas como organizativas, para salvaguardar los datos personales frente a accesos no autorizados, pérdida o destrucción. Aunque la normativa no especifica claramente el uso de cortafuegos, se recomienda su implementación, así como la adherencia a los principios de seguridad establecidos por la ley (CONAFIPS, 2021).

La LOPDP también establece que las organizaciones deben realizar evaluaciones periódicas de riesgos y auditorías de seguridad para garantizar la efectividad de las medidas implementadas. Los firewalls, como parte de las medidas de seguridad técnicas, deben configurarse para monitorear el tráfico de red, registrar actividades sospechosas y permitir una respuesta rápida a incidentes de seguridad. Además, la ley requiere que las organizaciones comuniquen a las autoridades y a las personas perjudicadas si llega a darse el caso de incidente de seguridad que dé lugar a la infracción de la privacidad de la información personal.

2.8.Evaluación de Eficiencia

2.8.1. Marco para Evaluar la Efectividad de los Firewalls

Realizar un proceso de prueba de la efectividad de los firewalls en un entorno de nube es determinante para asegurar que las organizaciones logren el mayor retorno posible de sus inversiones en protección. Este marco proporciona una metodología para evaluar la eficiencia de los firewalls en términos de costos, complejidad operativa y eficacia en la protección contra amenazas.

2.8.1.1. Costos

La evaluación de costos debe considerar tanto los costos directos como los indirectos asociados con la implementación y operación de los firewalls.

2.8.1.2. Costos Directos

Costo de Adquisición: Incluye la inversión que las organizaciones realizan para la adquisición del hardware o las licencias de software necesarias para implementar los firewalls. Los firewalls integrados en la nube a menudo tienen costos basados en el uso, lo que puede ser más flexible y escalable (AWS, 2021).

2.8.1.3.Costo de Implementación

Considera los gastos iniciales relacionados con la configuración e instalación de los firewalls. Esto puede incluir gastos de personal, servicios de consultoría y cualquier infraestructura adicional necesaria.

2.8.1.4. Costo de Mantenimiento

Incluye las actualizaciones de software, parches de seguridad, y el soporte técnico. Los firewalls integrados pueden tener menores costos de mantenimiento debido a la gestión proporcionada por el proveedor de la nube (ESET, 2024).

2.8.1.5. Costos Indirectos

Costo de Operación: Evalúa los recursos necesarios para operar los firewalls, incluyendo el tiempo y esfuerzo del personal de TI para gestionar las configuraciones, monitorear el tráfico de red y responder a incidentes de seguridad.

Costo de Capacitación: Considera como objetivo la mejora en conocimientos del personal encargado del uso y gestión de los firewalls, especialmente si se implementan nuevas tecnologías o actualizaciones importantes.

2.8.1.6. Complejidad Operativa

La complejidad operativa se refiere a la facilidad o dificultad con la que los firewalls pueden ser gestionados y operados dentro de una organización.

Facilidad de Implementación: Evalúa cuán fácil es implementar y configurar los firewalls. Los firewalls integrados suelen ser más sencillos de desplegar debido a su integración con los servicios de nube existentes (AWS, 2021).

Gestión y Monitoreo: Considera la facilidad con la que se pueden gestionar y monitorear los firewalls. Las soluciones con interfaces intuitivas y capacidades de automatización pueden reducir la complejidad operativa (Pineda & Quiceno, 2023).

Integración con Otros Sistemas: Evalúa la capacidad de los firewalls para poderse integrar con otras herramientas y sistemas de seguridad, como sistemas de ejecución y evaluación

de eventos e información de seguridad (SIEM). La integración fluida puede simplificar la gestión y mejorar la visibilidad de la seguridad.

Escalabilidad: Considera la capacidad de los firewalls para escalar con las necesidades de la organización. Los firewalls integrados en la nube suelen ofrecer escalabilidad automática, mientras que las soluciones externas pueden requerir configuraciones adicionales (Delgado, 2023).

2.8.2. Eficacia de los firewalls en la Protección frente a Amenazas

La eficacia en las actividades dirigidas a garantizar la protección contra amenazas evalúa la capacidad de los firewalls para descubrir, prevenir y garantizar respuestas a las amenazas de seguridad.

Capacidades de Inspección de Tráfico: Evalúa la capacidad de los firewalls para reconocer y filtrar el tráfico de red. Los firewalls avanzados, así como los de próxima generación (NGFW), brindan capacidades de análisis y monitoreo profundo de paquetes (DPI) y prevención de tráfico malicioso (IPS) (Pineda & Quiceno, 2023).

Indicador de Detección y Respuesta a Incidentes: Contempla la eficacia de los firewalls para descubrir y responder de una manera rápida a los incidentes de seguridad. Los firewalls con capacidades de inteligencia artificial y aprendizaje automático pueden mejorar la detección y respuesta (Delgado, 2023).

Prevención de Acceso No Autorizado: Evalúa la capacidad de los firewalls para prevenir accesos no autorizados y proteger los datos sensibles. Esto incluye la implementación de políticas de seguridad sólidas y la habilidad para diseñar modelos arquitectónicos para la segmentación de redes.

Registro y Monitoreo de Actividades: Considera la capacidad de los firewalls para registrar y monitorear las actividades de la red, proporcionando visibilidad y capacidad de auditoría para detectar comportamientos anómalos y realizar análisis forenses.

2.8.3. Implementación del Marco

Para implementar este marco, las organizaciones deben realizar una evaluación periódica de sus firewalls utilizando los criterios mencionados. Esto abarca la recolección de información sobre gastos, el análisis de los procedimientos operativos y la valoración de la eficacia en la protección contra amenazas. Además, es importante realizar auditorías regulares y ajustar las configuraciones de seguridad según sea necesario para adaptarse a las nuevas amenazas y cambios en la infraestructura de la organización.

2.9.Metodología

2.9.1. Introducción a la Metodología de la Plataforma Scrum

Scrum es un entorno de trabajo ágil dirigido a la ejecución y desarrollo de proyectos complejos. Originalmente concebido para el desarrollo de software, ha sido adaptado a diversos contextos, incluyendo proyectos de desarrollo e implementación en la nube. Scrum se fundamenta en la colaboración, la autoorganización y el enfoque en la entrega incremental de productos funcionales (Merchán et al., 2024). Esta metodología es particularmente adecuada para proyectos en la nube debido a su naturaleza iterativa, que permite la entrega continua y rápida de funcionalidades. Los ciclos cortos de desarrollo, denominados sprints, facilitan la retroalimentación constante y permiten realizar ajustes oportunos. Además, Scrum promueve la transparencia y una comunicación efectiva, elementos esenciales en proyectos de nube donde la colaboración y la adaptación rápida son cruciales (Maita, 2024).

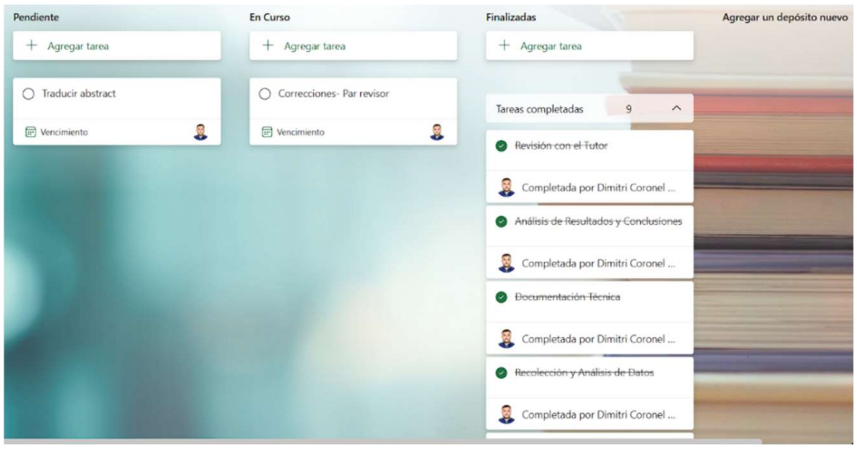
Las ventajas de Scrum incluyen su flexibilidad, permitiendo ajustar prioridades y enfoques en cada sprint para responder a cambios rápidos en el entorno de nube. Esta adaptabilidad se fomenta a través de la retroalimentación y la mejora continua, mientras que la eficiencia en la gestión del proyecto se logra mediante roles y ceremonias específicas que facilitan la planificación, el seguimiento y la entrega de productos (AWS, 2021).

Monitorización y Control del Proyecto

Microsoft Planner se utilizó para monitorear el progreso del proyecto y realizar ajustes necesarios. Este software facilitó la visibilidad del avance del proyecto a todas las partes interesadas, proporcionando un seguimiento detallado de las tareas y el estado de los sprints.

Gestión de Iteraciones: Microsoft Planner permitió la gestión efectiva de las iteraciones, facilitando la planificación de los sprints, asignación de tareas y rastrear el progreso. Las vistas de tablero Kanban y diagramas de Gantt proporcionaron una representación visual del progreso del proyecto, posibilitando la identificación de puntos críticos y la realización de elecciones fundamentadas.

Visibilidad del Proyecto: Las herramientas de reporte y análisis de Microsoft Planner permitieron generar informes detallados sobre el progreso del proyecto, que fueron compartidos regularmente con mi tutor para mantenerlo informado y comprometido con el proyecto.



Fuente: Elaboración propia.

Capítulo 3

Experimento

3.1.Introducción

En este capítulo se abordarán los objetivos específicos de la evaluación de firewalls en ambientes de nube. La infraestructura basada en la nube plantea retos singulares en cuanto a seguridad, y los firewalls son una pieza clave para mitigar estos riesgos. Este capítulo se enfoca en describir detalladamente cómo se implementan y comparan diferentes soluciones de firewall, específicamente Web Application Firewall (WAF) y FortiWeb, dentro de un entorno de Amazon Web Services (AWS).

La importancia de este capítulo se basa en la necesidad de entender las diferencias en términos de eficacia, costos y facilidad de uso entre estas soluciones. La evaluación detallada de estos aspectos permitirá tomar decisiones informadas sobre qué solución es más adecuada para proteger aplicaciones web en la nube. Además, se presentará una arquitectura general de la infraestructura utilizada, así como los procedimientos de despliegue y configuración específicos para cada tipo de firewall.

Entender cómo se implementan y comparan los firewalls en la nube no solo ayuda a mejorar la seguridad, sino que también optimiza los recursos y reduce los costos operativos. Este conocimiento es esencial para cualquier entidad que busque salvaguardar sus aplicaciones y datos en la nube de forma eficiente y eficaz.

3.2.Metodología del Experimento

La metodología del experimento se diseñó meticulosamente para evaluar la eficacia, facilidad de instalación, uso y costos operativos de dos soluciones de firewall: Web Application Firewall (WAF) y FortiWeb. A continuación, se detallan los métodos de prueba definidos para garantizar la precisión y consistencia de los resultados.

3.2.1. Aplicación de Scrum en el Proyecto

Para gestionar y desarrollar la arquitectura en AWS, he configurado y utilizado Microsoft Projects para implementar Scrum, con el apoyo y guía de mi tutor de tesis. Aunque soy principalmente responsable de la ejecución del proyecto, he asumido múltiples roles dentro de Scrum para asegurar una gestión eficiente y la obtención de los objetivos del proyecto.

Roles Asumidos:

Scrum Master: Facilitador de las ceremonias de Scrum, eliminador de obstáculos y garante del seguimiento de los principios de Scrum. Coordiné las reuniones y apoyé en la resolución de problemas.

Product Owner: Definí y prioricé el Product Backlog, asegurando que se trabajara en las tareas más valiosas para el proyecto. Mantuvé una comunicación constante con mi tutor para alinear los objetivos del proyecto con sus expectativas.

Team Member: Ejecuté las tareas planificadas para cada sprint, colaborando estrechamente con mi tutor para alcanzar los objetivos del proyecto.

3.2.2. Sprints y Ceremonias

Sprints: Cada sprint duró dos semanas, durante las cuales trabajé en tareas específicas seleccionadas del Product Backlog.

Reuniones de Planificación del Sprint: Estas reuniones se efectuaron al inicio de cada sprint para determinar las tareas a realizar y establecer los objetivos del sprint, en consulta con mi tutor.

Revisiones del Sprint: Al final de cada sprint, se realizaron revisiones para presentar el incremento del producto y recibir retroalimentación de mi tutor.

Retrospectivas: Después de cada sprint, se llevó a cabo una retrospectiva para examinar y analizar lo que funcionó bien, lo que podría mejorar y cómo aplicar mejoras en el próximo sprint, siempre con la orientación de mi tutor.

Artefactos de Scrum Utilizados

Product Backlog: Lista de niveles de prioridad de todas las funcionalidades y tareas indispensables para el proyecto. Gestioné el Product Backlog como la fuente principal de trabajo.

Sprint Backlog: Lista de tareas escogidas del Product Backlog para ser completadas en el marco de un sprint, ayudando a organizar y enfocar el trabajo en objetivos específicos y alcanzables.

Incremento: Suma de todos los elementos completados durante un sprint, representando una versión funcional y potencialmente entregable del producto. Los incrementos se presentaron durante las revisiones de sprint para obtener retroalimentación y asegurar el avance correcto del proyecto.

Estos artefactos fueron esenciales para organizar y priorizar el trabajo, proporcionando claridad y enfoque, asegurando alineación con los objetivos del proyecto.

3.2.3. Objetivos del Experimento

Eficacia en la detección y prevención de amenazas.

Facilidad y rapidez de instalación y configuración.

Usabilidad y gestión en un entorno operativo.

Costos iniciales y operativos.

Procedimientos de Prueba

3.2.4. Preparación del Entorno de Prueba

Para garantizar un entorno controlado y repetible, se estableció una infraestructura de prueba en Amazon Web Services (AWS), utilizando instancias dedicadas para cada firewall. La infraestructura incluye:

Instancias EC2: Se configuraron instancias t2. micro para la mayoría de los componentes, con una instancia t3.medium dedicada para FortiWeb debido a sus mayores requisitos de recursos.

Configuraciones de Red: Incluyendo VPC, subredes, tablas de enrutamiento y grupos de seguridad para aislar y proteger las instancias.

Balanceadores de Carga: Para simular tráfico real hacia las aplicaciones protegidas por los firewalls.

3.2.5. Instalación y Configuración de los Firewalls

Web Application Firewall (WAF)

Selección de Instancias: Se eligieron instancias t2.micro en AWS por su balance entre costo y rendimiento.

Configuración Inicial: Se desplegó AWS WAF utilizando CloudFormation para automatizar la configuración inicial, estableciendo reglas básicas de protección contra amenazas comunes.

Establecimiento de Políticas de Seguridad: Configuración de reglas específicas para SQL Injection y Command Injection, basadas en patrones conocidos y utilizando Managed Rules de AWS.

FortiWeb

Selección de Instancias: Se utilizó una instancia t3. medium para FortiWeb, configurada a través de FortiManager.

Configuración Inicial: Instalación del software FortiWeb en la instancia EC2, seguida de la configuración inicial a través de la interfaz de gestión web.

Establecimiento de Políticas de Seguridad: Definición de reglas personalizadas para SQL Injection y Command Injection, configurando perfiles de seguridad detallados para una protección granular.

3.2.6. Ejecución de Pruebas de Seguridad

Las pruebas de seguridad se centraron en evaluar la capacidad de los firewalls para detectar y mitigar ataques comunes. Se utilizaron herramientas automatizadas para generar y simular ataques, garantizando la consistencia de las pruebas.

- Configuración de Páginas de Prueba en Nginx
- Página de Bienvenida: Una página simple que confirme que el servidor está funcionando correctamente.
- Prueba de SQL Injection: Un formulario básico que simula intentos de inyección SQL.
- Prueba de Command Injection: Un formulario básico que permite la entrada de comandos para simular intentos de inyección de comandos.

Pruebas de SQL Injection

Preparación del Ataque: Envío de comandos SQL simples como SELECT * FROM users WHERE id='1' OR '1'='1'; para probar la capacidad de detección y bloqueo de los firewalls.

Ejecución del Ataque: Utilización de herramientas como curl y siege para enviar las solicitudes, verificando que el WAF o FortiWeb bloqueen estas solicitudes y registren el intento.

Pruebas de Command Injection

Preparación del Ataque: Envío de comandos básicos como; ls o && echo vulnerable para evaluar la efectividad de los firewalls en bloquear estos intentos.

Ejecución del Ataque: Uso de curl y siege para enviar las solicitudes, verificando que el WAF o FortiWeb bloqueen estas solicitudes y registren el intento.

Se aseguró que los ataques fueran lo más sencillos posible, sin técnicas avanzadas, para evaluar la eficacia básica de cada solución de firewall.

3.2.7. Recolección y Registro de Datos

Durante las pruebas, se recopilaron datos exhaustivos sobre la performance de cada firewall. Esto incluyó:

- Logs de Detección y Bloqueo: Captura de todas las incidencias de detección y bloqueo reportadas por los firewalls.
- Tiempo de Respuesta: Medición del tiempo que cada firewall tardó en identificar y bloquear los ataques.
- Impacto en el Rendimiento: Monitoreo del impacto en el rendimiento de las aplicaciones protegidas, incluyendo latencia y throughput.

3.2.8. Análisis de Costos

Se realizó un análisis detallado de los costos asociados con la implementación y operación de cada firewall, considerando:

- Costos Iniciales: Incluyendo licencias, configuración inicial y despliegue.
- Costos Operativos: Gastos recurrentes relacionados con la gestión y mantenimiento, incluyendo costos de instancias en AWS y soporte técnico.

3.2.9. Validación de los Resultados

Para garantizar la precisión de los resultados, se siguieron las mejores prácticas de pruebas de seguridad, incluyendo:

- Repetición de Pruebas: Cada prueba se repitió múltiples veces para asegurar la consistencia y reproducibilidad de los resultados.
- Condiciones Controladas: Mantener las mismas condiciones de red y carga para cada prueba, asegurando que los resultados no fueran influenciados por variables externas.
- Auditoría Independiente: Revisión de los procedimientos y resultados por un tercero independiente para validar la objetividad y precisión de las conclusiones.

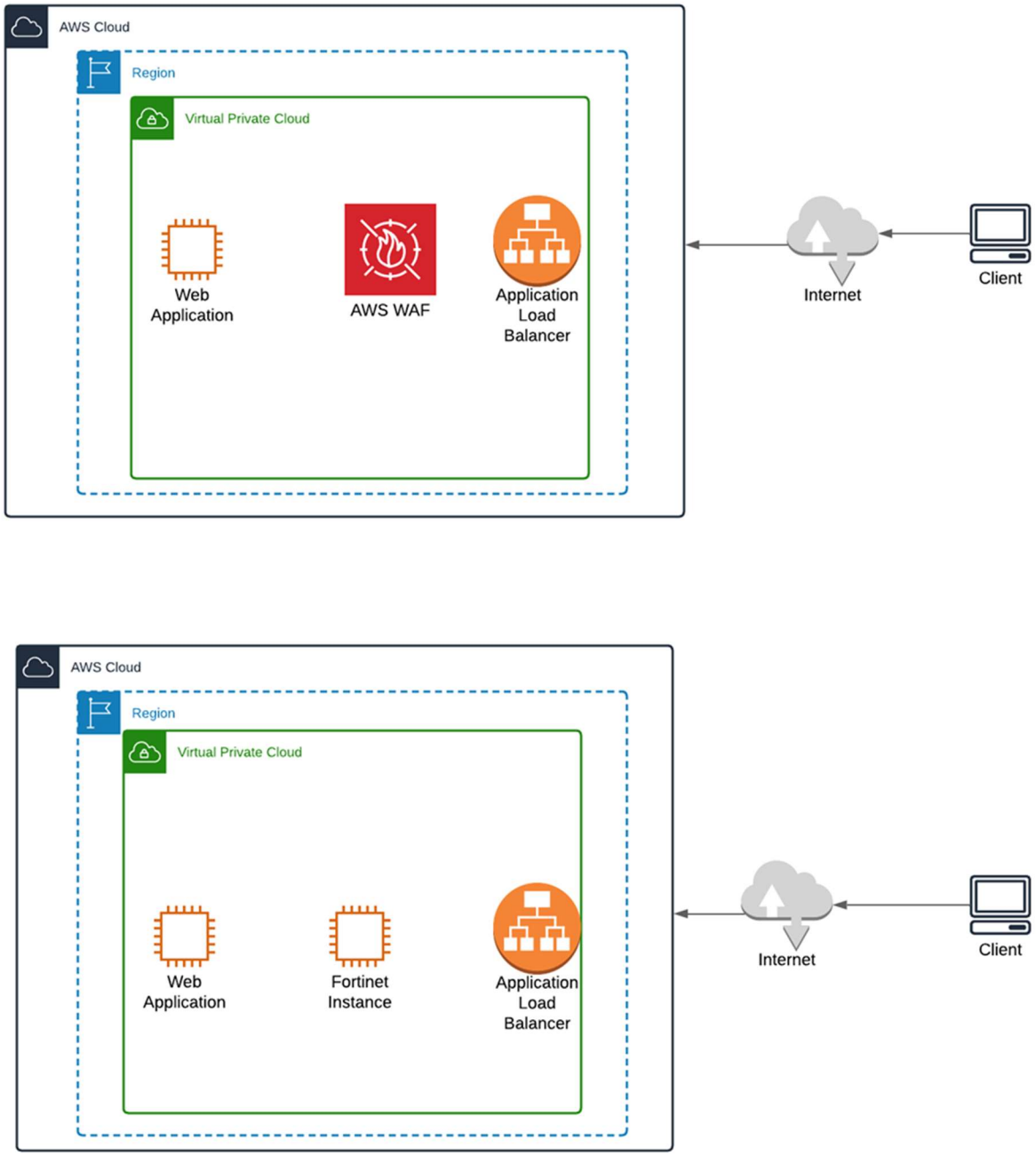
3.2.10. Justificación de la Metodología y Herramientas Utilizadas

La elección de las metodologías y herramientas utilizadas en este experimento se basó en criterios de relevancia, precisión y reproducibilidad. AWS fue seleccionado por su robustez y escalabilidad, permitiendo una configuración flexible y controlada del entorno de pruebas. Herramientas como SQLMap fueron elegidas por su capacidad para simular ataques de manera realista y consistente, lo que es crucial para evaluar la eficacia de las soluciones de firewall en situaciones de ataque reales.

3.3.Arquitectura General

La infraestructura utilizada para este experimento está desplegada en Amazon Web Services (AWS), aprovechando sus servicios de Virtual Private Cloud (VPC) para crear un entorno seguro y escalable. La arquitectura se divide en dos configuracion:es principales: una para el Web Application.

Figura 3. *Arquitectura General*



Fuente: Elaboración propia.

Firewall (WAF) y otra para FortiWeb. A continuación, se describe detalladamente la configuración general de la arquitectura ilustrada en el diagrama.

3.3.1. Configuración del Web Application Firewall (WAF)

En la parte superior del diagrama, se observa la configuración del WAF. Esta configuración incluye los siguientes componentes:

Web Application: Representada por la instancia de servidor web que ejecuta Nginx, configurada para servir páginas de prueba de seguridad.

AWS WAF: El firewall de aplicación web de AWS, configurado para proteger la aplicación web de ataques comunes.

Application Load Balancer: Un equilibrador de carga de aplicaciones que distribuye el tráfico de entrada entre las instancias de la aplicación web, garantizando alta disponibilidad y escalabilidad.

El tráfico de internet entra a través del Application Load Balancer, que está configurado para enviar las solicitudes a través de AWS WAF. AWS WAF inspecciona y filtra el tráfico antes de dirigirlo a la aplicación web. Esta configuración permite una protección avanzada contra amenazas como SQL Injection y Command Injection, garantizando que solo el tráfico legítimo llegue a la aplicación web.

3.3.2. Configuración de FortiWeb

En la parte inferior del diagrama, se observa la configuración de FortiWeb. Esta configuración incluye:

- Web Application: Similar a la configuración del WAF, con una instancia de servidor web ejecutando Nginx.
- FortiWeb Instance: El firewall de aplicaciones web de Fortinet, configurado para proteger la aplicación web.
- Application Load Balancer: Un distribuidor de carga de aplicaciones que reparte el tráfico de entrada entre las instancias de la aplicación web.

El tráfico de internet también entra a través del Application Load Balancer en esta configuración. Sin embargo, en este caso, el tráfico es dirigido primero a través de la instancia de FortiWeb antes de llegar a la aplicación web. FortiWeb está configurado con reglas de seguridad personalizadas para detectar y bloquear amenazas como SQL Injection y Command Injection. Esta configuración proporciona una capa adicional de protección y permite una inspección detallada del tráfico.

3.3.3. Descripción de la Integración y Funcionamiento

Ambas configuraciones aprovechan la flexibilidad y escalabilidad de AWS para establecer un entorno seguro y eficiente. En la configuración del WAF, el tráfico entrante es primero inspeccionado por el AWS WAF, que aplica reglas de seguridad para identificar y prevenir amenazas antes de que lleguen al Application Load Balancer. Por lo que, distribuye el tráfico a las instancias de Nginx, asegurando que la aplicación web se mantenga disponible y responda eficientemente a las solicitudes de los usuarios.

En la configuración de FortiWeb, el tráfico HTTP/HTTPS es dirigido a través de FortiWeb, donde se inspecciona utilizando reglas de seguridad personalizadas para detectar y bloquear intentos de SQL Injection y Command Injection. Una vez inspeccionado, el tráfico es gestionado

por el Application Load Balancer y dirigido a las instancias de Nginx. Esta configuración permite una protección adicional y más detallada de la aplicación web, aunque a un costo potencialmente mayor debido a los recursos adicionales necesarios para ejecutar FortiWeb.

3.4.Implementación de Infraestructura para Evaluación de AWS WAF

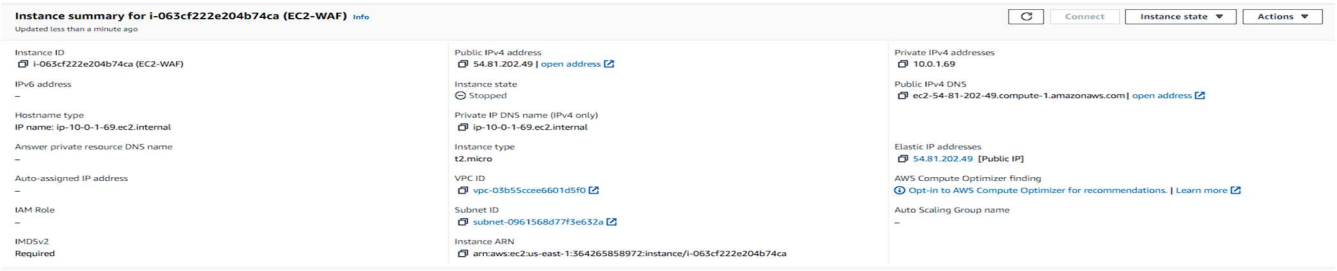
En esta sección se detalla el procedimiento para configurar la infraestructura de AWS para el Web Application Firewall (WAF). El despliegue incluyó el despliegue de las instancias EC2, la configuración inicial de la VPC, las tablas de enrutamiento, los CIDR, los grupos objetivos y otros componentes necesarios para implementar un WAF efectivo en un entorno seguro y escalable. Además, se implementó una aplicación web simple utilizando Nginx para realizar pruebas de seguridad.

3.4.1. Despliegue de Instancias EC2

Para implementar la aplicación web destinada a probar el Web Application Firewall (WAF) en AWS, se configuró una instancia EC2 con las siguientes especificaciones:

- **Nombre de la Instancia:** EC2-WAF
- **ID de la Instancia:** i-063cf222e204b74ca
- **Tipo de Instancia:** t2.micro
- **Sistema Operativo:** Amazon Linux

Figura 4. *Despliegue de Instancias EC2*



Fuente: Elaboración propia.

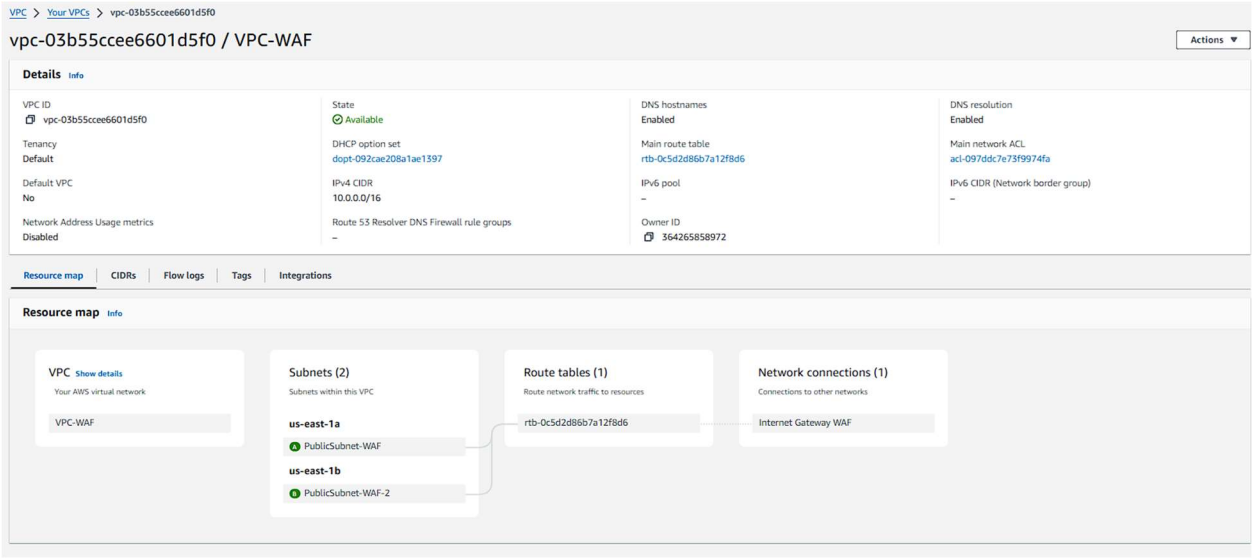
La instancia EC2-WAF se utiliza para alojar una aplicación web simple con Nginx, que incluye una página de inicio básica, una página de prueba de inyección SQL y una página de prueba de inyección de comandos. Estas páginas están diseñadas para evaluar la efectividad del WAF en la protección de aplicaciones web. El tipo de instancia t2.micro se seleccionó por su costo eficiente y suficiente capacidad para alojar una aplicación web básica.

3.4.2. Configuración de la VPC

Creación de la VPC

Para comenzar, se creó una VPC (Virtual Private Cloud) llamada VPC-WAF. Una VPC es una red virtual que se encuentra dentro de AWS que permite el aprovisionamiento de un entorno de red aislado donde se pueden lanzar recursos de AWS de forma segura. La VPC se configuró con el siguiente bloque CIDR: 10.0.0.0/16, lo que proporciona una amplia gama de direcciones IP para subnets y otros recursos.

Figura 5. *Creación de la VPC*



Fuente: Elaboración propia.

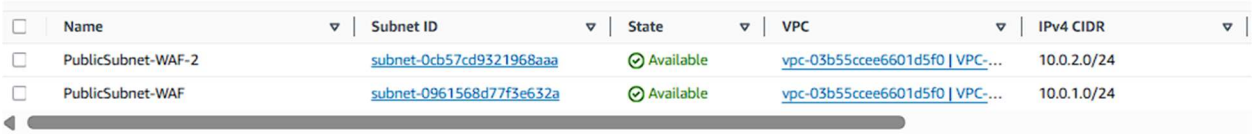
Configuración de Subnets

Se configuraron dos subnets públicas dentro de la VPC, cada una en diferentes zonas de disponibilidad (us-east-1a y us-east-1b). Las subnets públicas permiten que los recursos dentro de ellas puedan comunicarse con internet a través de un Internet Gateway:

PublicSubnet-WAF: 10.0.1.0/24 en us-east-1a

PublicSubnet-WAF-2: 10.0.2.0/24 en us-east-1b

Figura 6. *Configuración de Subnets*

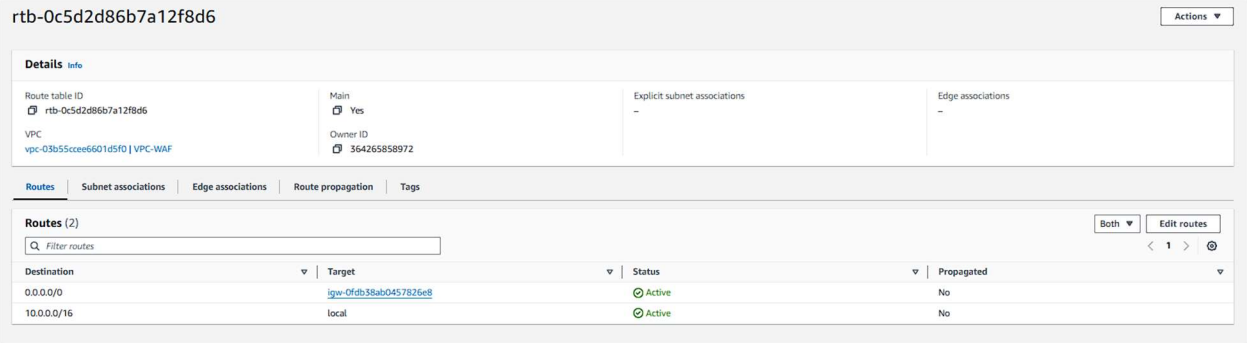


Fuente: Elaboración propia.

Configuración de la Tabla de Enrutamiento

Se creó una tabla de enrutamiento asociada a las subnets, permitiendo el tráfico hacia internet mediante un Internet Gateway. La ruta 0.0.0.0/0 se añadió a la tabla de enrutamiento, lo que permite que todo el tráfico de salida se dirija a internet.

Figura 7. *Configuración de la Tabla de Enrutamiento*



Fuente: Elaboración propia.

3.4.3. Configuración del Application Load Balancer (ALB)

Creación del ALB

Se implementó un Application Load Balancer (ALB) denominado ALB-WAF. Un ALB distribuye el tráfico de aplicación entrante a múltiples instancias EC2, proporcionando alta disponibilidad y escalabilidad. El ALB se configuró para estar orientado a internet (internet-facing), permitiendo recibir tráfico externo.

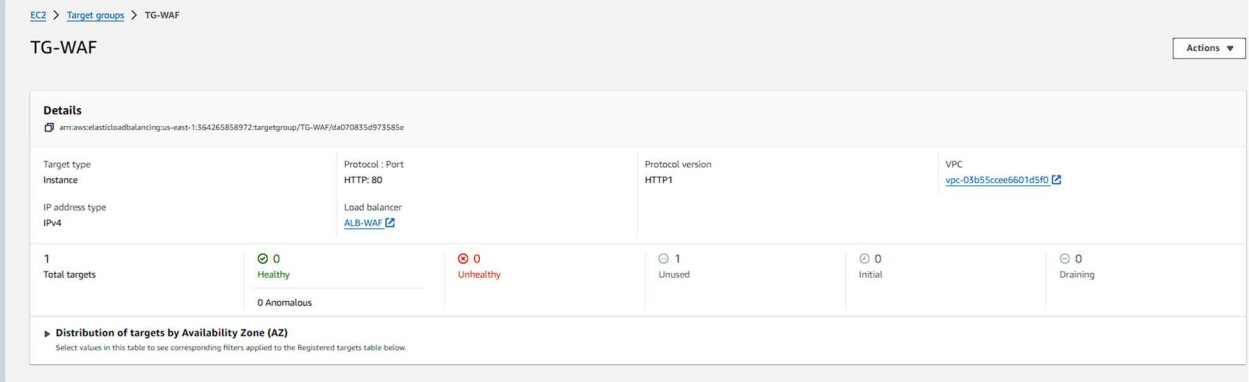
Figura 8. *Creación del ALB*

Fuente: Elaboración propia.

Configuración del Grupo Objetivo

Se creó un grupo objetivo (Target Group) llamado TG-WAF, al que se añadió la instancia EC2 configurada anteriormente. Los grupos objetivo son utilizados por los balanceadores de carga para dirigir el tráfico a las instancias registradas.

Figura 9. *Configuración del Grupo Objetivo*



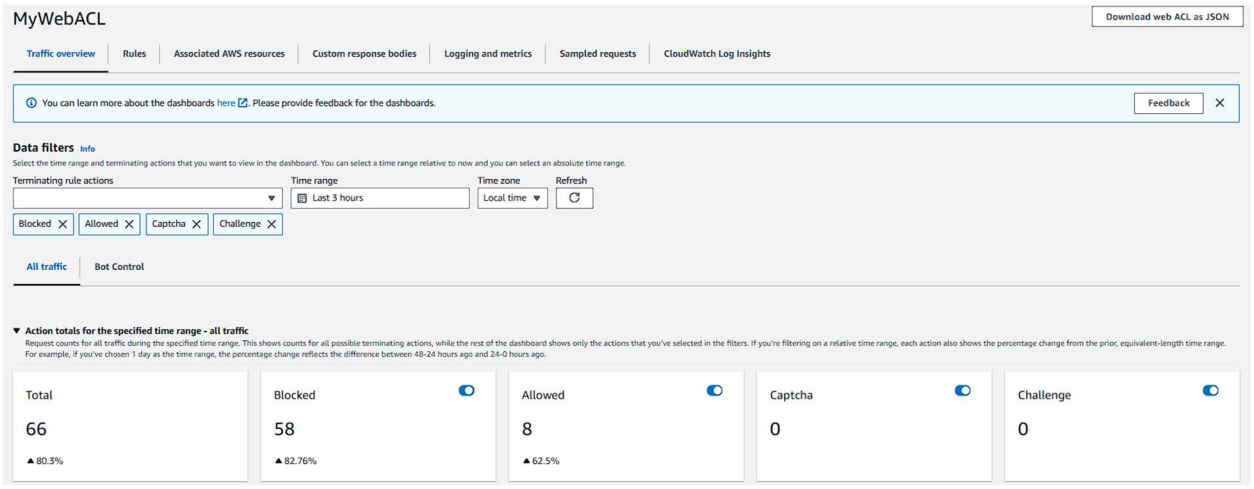
Fuente: Elaboración propia.

3.4.4. Configuración del AWS WAF

Creación de un Web ACL

Un Web ACL (Access Control List) denominado MyWebACL se creó para asociarse con el ALB. Un Web ACL contiene una lista de reglas que inspeccionan y filtran el tráfico web, aplicando acciones como permitir, bloquear o contar solicitudes basadas en condiciones específicas.

Figura 10. *Creación de un Web ACL*

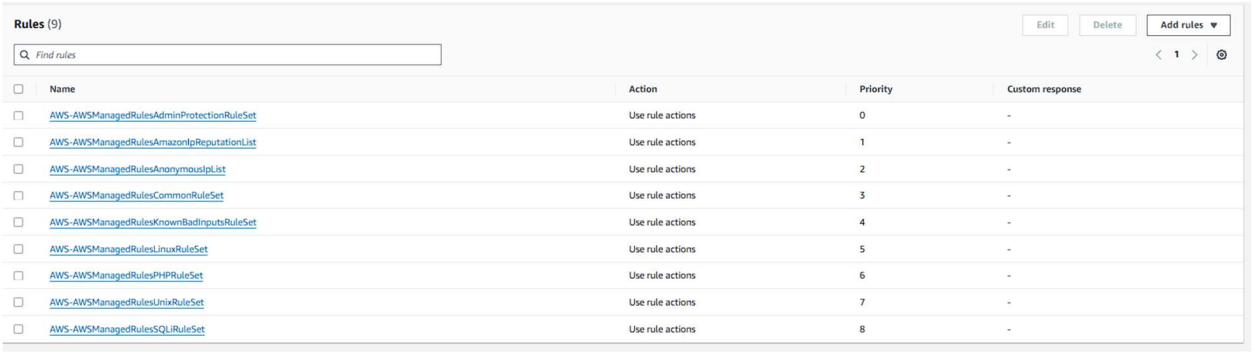


Fuente: Elaboración propia.

Configuración de Reglas del Web ACL

Se configuraron varias reglas administradas por AWS en el Web ACL para proporcionar protección contra una variedad de amenazas comunes. Las reglas configuradas incluyen:

Figura 11. *Configuración de Reglas del Web ACL*



Fuente: Elaboración propia.

AWS-AWSManagedRulesAdminProtectionRuleSet: Protege contra accesos no autorizados a interfaces de administración.

Descripción: Esta regla bloquea intentos de acceso a páginas de administración como /admin o /login.

AWS-AWSManagedRulesAmazonIpReputationList: Bloquea solicitudes de direcciones IP conocidas por actividad maliciosa.

Descripción: Utiliza una lista de direcciones IP que AWS ha identificado como fuentes de tráfico malicioso.

AWS-AWSManagedRulesAnonymousIpList: Bloquea solicitudes de direcciones IP anónimas, como las de proxies o VPNs.

Descripción: Filtra tráfico proveniente de IPs que suelen ser utilizadas para ocultar la identidad del usuario.

AWS-AWSManagedRulesCommonRuleSet: Proporciona protección general contra vulnerabilidades web comunes.

Descripción: Incluye reglas para proteger contra ataques como Cross-Site Scripting (XSS) y Local File Inclusion (LFI).

AWS-AWSManagedRulesKnownBadInputsRuleSet: Bloquea entradas conocidas por ser maliciosas.

Descripción: Identifica y bloquea patrones de entrada que son comúnmente utilizados en ataques.

AWS-AWSManagedRulesLinuxRuleSet: Protege contra ataques específicos a sistemas basados en Linux.

Descripción: Incluye reglas para proteger contra técnicas de explotación específicas de sistemas Linux.

AWS-AWSManagedRulesPHPRuleSet: Protege contra vulnerabilidades específicas de aplicaciones PHP.

Descripción: Bloquea ataques dirigidos a aplicaciones PHP, como la ejecución remota de código.

AWS-AWSManagedRulesSQLiRuleSet: Protege contra inyecciones SQL, un tipo común de ataque de inyección.

Descripción: Detecta y bloquea patrones de inyección SQL en las solicitudes.

AWS-AWSManagedRulesUnixRuleSet: Protege contra ataques específicos a sistemas basados en Unix.

Descripción: Incluye reglas que bloquean técnicas de explotación comúnmente usadas en sistemas Unix.

3.4.5. Implementación de la Aplicación Web para Pruebas

En la instancia EC2 configurada (EC2-WAF), se instaló y configuró Nginx para servir una aplicación web simple con las siguientes páginas:

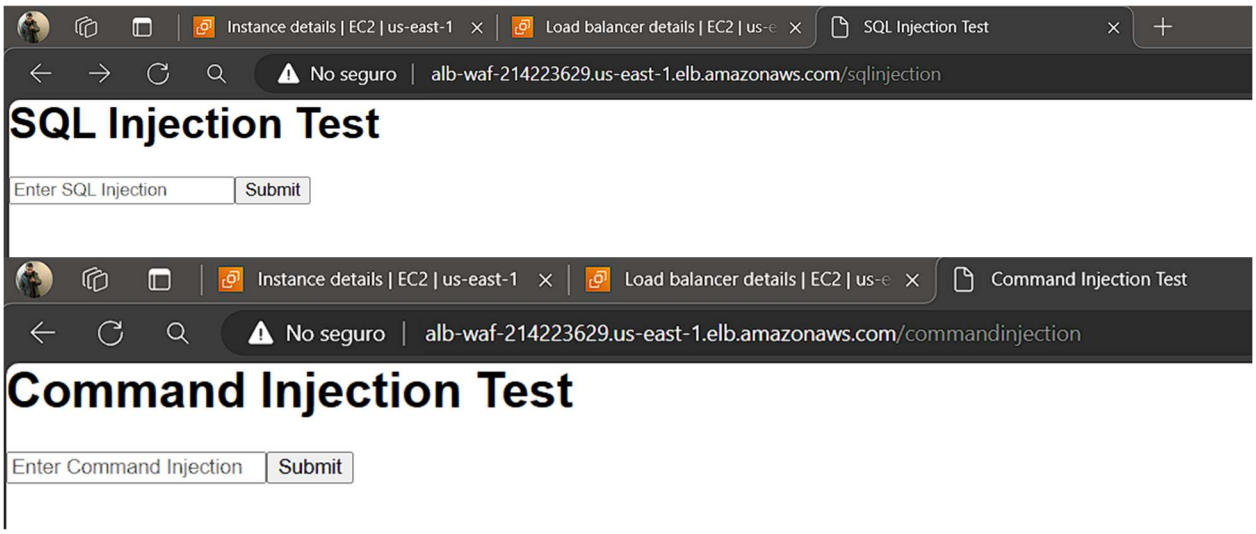
Página de Inicio: Una página básica para confirmar que el servidor está funcionando correctamente.

Prueba de SQL Injection: Un formulario simple diseñado para probar la capacidad del WAF para detectar y bloquear inyecciones SQL.

Prueba de Command Injection: Un formulario básico que permite la entrada de comandos para simular intentos de inyección de comandos.

Estas páginas fueron diseñadas para ser simples y no contienen lógica de backend ni bases de datos, facilitando así la evaluación del WAF en un entorno controlado.

Figura 12. *Implementación de la Aplicación Web para Pruebas*



Fuente: Elaboración propia.

3.4.6. Verificación de la Configuración

Se verificó que el ALB estuviera correctamente asociado con el Web ACL MyWebACL y que todo el tráfico estuviera siendo procesado correctamente a través del puerto 80. La URL del ALB (ALB-WAF-214223629.us-east-1.elb.amazonaws.com) se utilizó para realizar estas verificaciones.

3.5.Implementación de Infraestructura para Evaluación de FortiWeb

En esta sección se detalla los pasos de configuración de las instancias de AWS para FortiWeb. Este despliegue incluye la configuración inicial de la VPC, las subnets, las tablas de

enrutamiento y otros componentes necesarios para implementar un WAF (Web Application Firewall) efectivo en un entorno seguro y escalable.

3.5.1. Despliegue de Instancias EC2

Para implementar FortiWeb en AWS, se configuraron las siguientes instancias EC2

Instancia FortiWeb:

Nombre de la Instancia: EC2-Fortinet-Instance

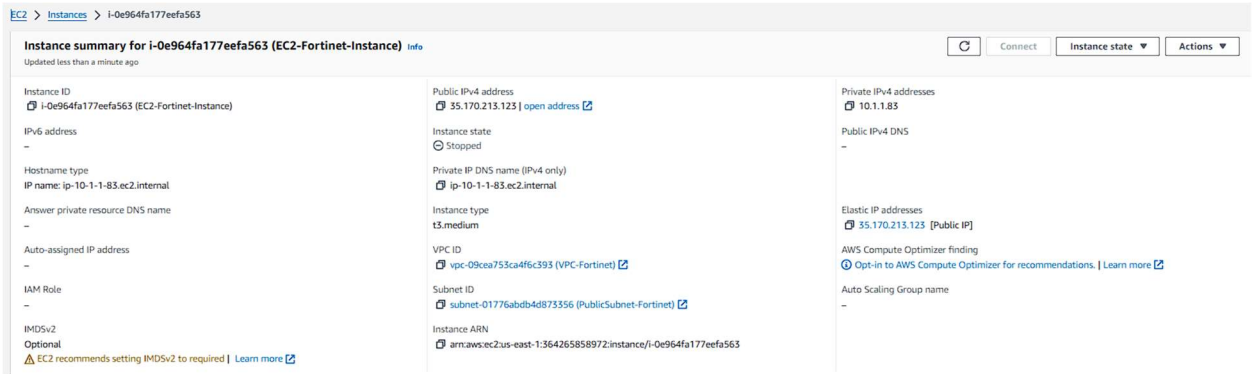
ID de la Instancia: i-0e964fa177eefa563

Tipo de Instancia: t3.medium

Sistema Operativo: Fortinet FortiGate Next-Generation Firewall

La instancia EC2-Fortinet-Instance se utiliza para alojar FortiWeb, un firewall avanzado que proporciona protección de aplicaciones web mediante la mitigación de puntos ciegos y la adherencia a políticas esenciales de protección. El tipo de instancia t3.medium se seleccionó debido a sus mayores requisitos de recursos, necesarios para ejecutar FortiWeb eficientemente. Se utilizó la AMI de Fortinet FortiGate Next-Generation Firewall para esta instancia.

Figura 13. *Despliegue de Instancias EC2*



Fuente: Elaboración propia.

Instancia de Aplicación Web:

Nombre de la Instancia: Fortinet-Web-App

ID de la Instancia: i-016e99da99cb06dab

Tipo de Instancia: t2.micro

Sistema Operativo: Amazon Linux =

La instancia Fortinet-Web-App se utiliza para alojar una aplicación web simple con Nginx, que incluye una página de inicio básica, una página de prueba de inyección SQL y una página de prueba de inyección de comandos. Estas páginas están diseñadas para evaluar la efectividad de FortiWeb en la protección de aplicaciones web. El tipo de instancia t2.micro se seleccionó por su costo eficiente y suficiente capacidad para alojar una aplicación web básica.

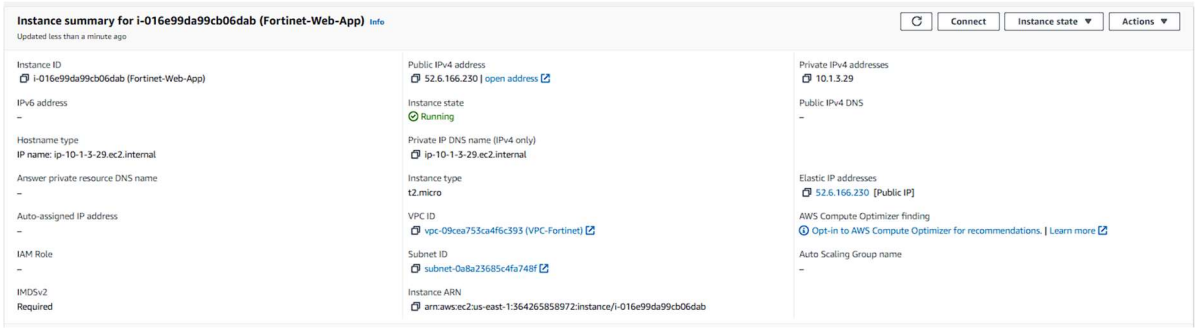
Figura 14. *Instancia Fortinet-Web-App*

Fuente: Elaboración propia.

3.5.2. Configuración de la VPC

Creación de la VPC

Se creó una VPC llamada VPC-Fortinet. Esta VPC tiene el bloque CIDR 10.1.0.0/16, lo que proporciona un rango de direcciones IP amplio para subnets y otros recursos. La VPC está



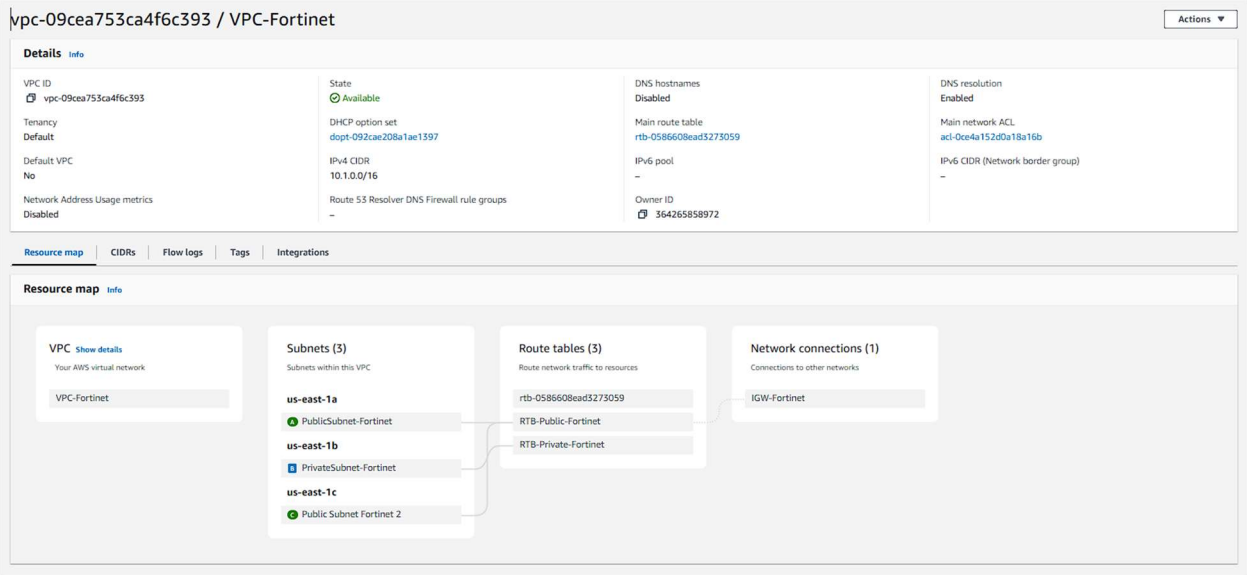
configurada para estar en estado "Available" y tiene habilitada la resolución DNS, pero los nombres de host DNS están deshabilitados.

Figura 15. *Creación de la VPC*

Fuente: Elaboración propia.

Configuración de Subnets

Dentro de la VPC, se configuraron tres subnets distribuidas en diferentes zonas de disponibilidad. La primera subnet, denominada PublicSubnet-Fortinet, está ubicada en la zona de disponibilidad us-east-1a y es una subnet pública que permite la comunicación con internet a través



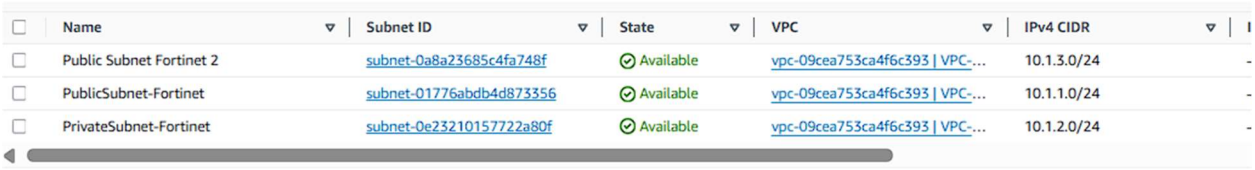
de un Internet Gateway. La segunda subnet, PrivateSubnet-Fortinet, se encuentra en la zona de disponibilidad us-east-1b y es una subnet privada destinada a recursos internos que no requieren acceso directo a internet. La tercera subnet, llamada Public Subnet Fortinet 2, está ubicada en la zona de disponibilidad us-east-1c y es una segunda subnet pública, proporcionando redundancia y alta disponibilidad para los recursos expuestos a internet.

Figura 16. *Configuración de Subnets*

Fuente: Elaboración propia.

Configuración de la Tabla de Enrutamiento

Se configuraron tres tablas de enrutamiento para gestionar el tráfico de red dentro de la VPC. La tabla de enrutamiento principal, identificada como rtb-0586608ead3273059, está asociada a las subnets públicas y privadas. La tabla de enrutamiento RTB-Public-Fortinet está



Name	Subnet ID	State	VPC	IPv4 CIDR
Public Subnet Fortinet 2	subnet-0a8a23685c4fa748f	Available	vpc-09cea753ca4f6c393 | VPC-...	10.1.3.0/24
PublicSubnet-Fortinet	subnet-01776abdb4d873356	Available	vpc-09cea753ca4f6c393 | VPC-...	10.1.1.0/24
PrivateSubnet-Fortinet	subnet-0e23210157722a80f	Available	vpc-09cea753ca4f6c393 | VPC-...	10.1.2.0/24

asociada a las subnets públicas y permite el tráfico hacia internet a través de un Internet Gateway. Por último, la tabla de enrutamiento RTB-Private-Fortinet está asociada a la subnet privada y gestiona el tráfico interno de la red.

3.5.3. Configuración del Application Load Balancer (ALB)

Figura 17. *Configuración del Application Load Balancer (ALB)*

Fuente: Elaboración propia.

Creación del ALB

Se implementó un Application Load Balancer (ALB) denominado ALB-Fortinet. Un ALB distribuye el tráfico de aplicación entrante, proporcionando alta disponibilidad y escalabilidad. El ALB se configuró para estar orientado a internet (internet-facing), permitiendo recibir tráfico

RTB-Public-Fortinet	rtb-0f4f442f8f18c532b	2 subnets	-	No	vpc-09cea753ca4f6c393 | VPC-...	364265858972
RTB-Private-Fortinet	rtb-0ffeb88e500383fcd	subnet-0e23210157722a...	-	No	vpc-09cea753ca4f6c393 | VPC-...	364265858972

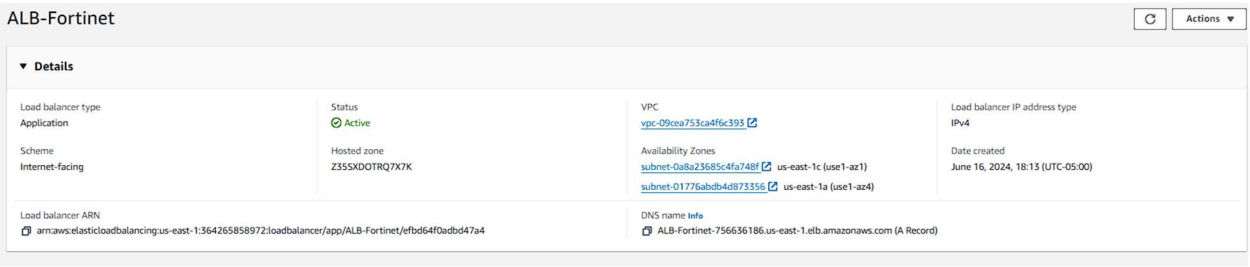
externo.

Figura 18. *Creación del ALB*

Fuente: Elaboración propia.

Configuración del Grupo Objetivo

Se creó un grupo objetivo (Target Group) llamado TG-Fortinet. Los grupos objetivo son utilizados por los balanceadores de carga para dirigir el tráfico a las instancias registradas en este



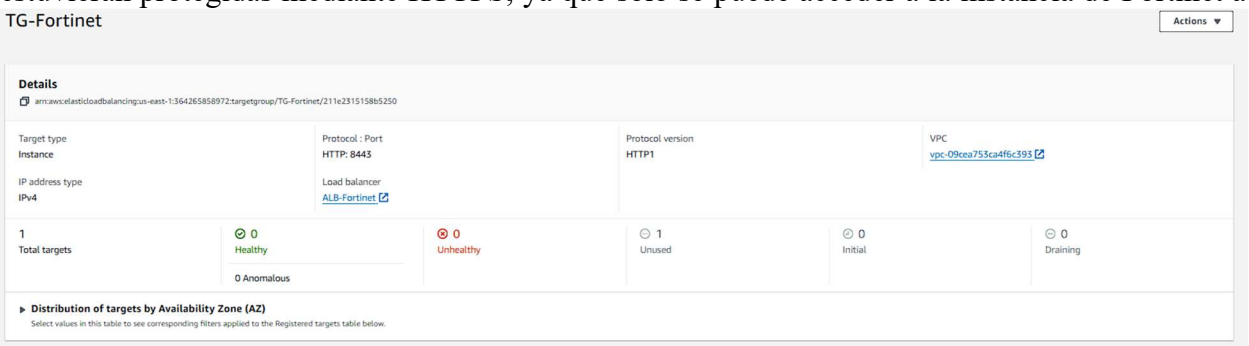
caso al puerto 3443 donde se ejecuta el servicio de Fortinet.

Figura 19. *Configuración del Grupo Objetivo*

Fuente: Elaboración propia.

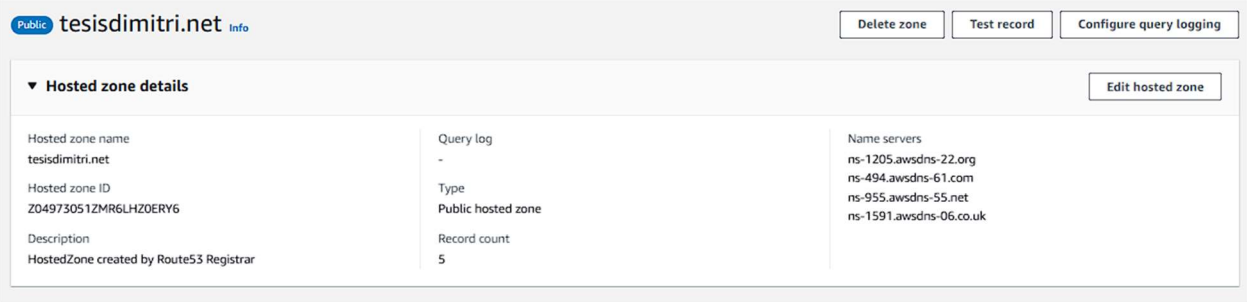
Compra y Configuración del Dominio

Durante la configuración del ALB, fue necesario asegurar que las comunicaciones estuvieran protegidas mediante HTTPS, ya que solo se puede acceder a la instancia de Fortinet a



través de este protocolo. Para esto, se compró el dominio "tesisdimtri.net" a través de AWS Route 53. Este dominio fue registrado y se configuró una zona alojada en Route 53 para gestionar el DNS del dominio.

Figura 20. *Compra y Configuración del Dominio*



Fuente: Elaboración propia.

Emisión del Certificado SSL

A continuación, se utilizó AWS Certificate Manager para emitir un certificado SSL para el dominio, permitiendo que el ALB maneje el tráfico HTTPS de manera segura. El certificado SSL asegura que todas las comunicaciones entre los clientes y el ALB estén encriptadas, proporcionando una capa adicional de seguridad para las aplicaciones web protegidas por FortiWeb.

Figura 21. *Emisión del Certificado SSL*

Fuente: Elaboración propia.

3.5.4. Implementación de la Aplicación Web para Pruebas

De igual manera que en la instancia donde se evaluará el WAF, se ha creado una pagina con los mismos criterios. Se realizó una página web donde se evaluará el SQL injection y el Command Injection.

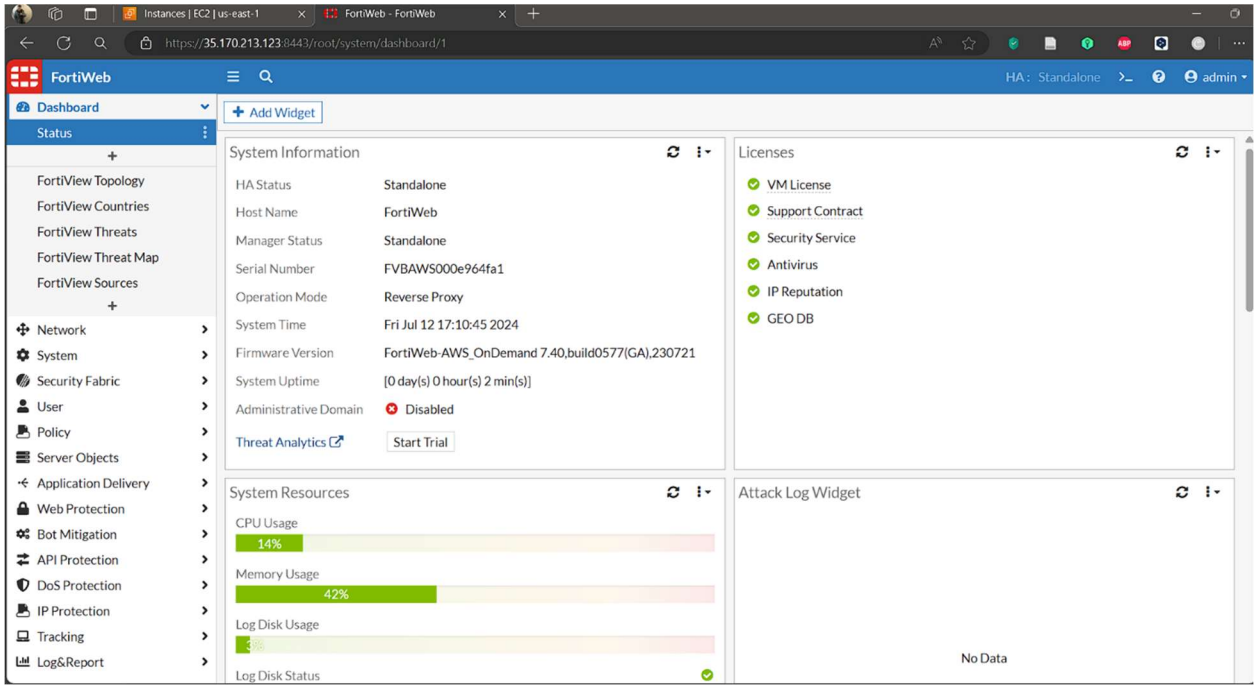
Figura 22. *Implementación de la Aplicación Web para Pruebas*

Fuente: Elaboración propia.

3.5.5. Configuración del WAF FortiWeb

La configuración del FortiWeb se realizó para proteger un servidor Nginx que hospeda aplicaciones web vulnerables a pruebas de inyección SQL y de comandos. A continuación, se detallan los pasos completos de configuración, desde la creación de objetos de servidor hasta la aplicación de políticas de seguridad.

Figura 23. *Configuración del WAF FortiWeb*



Fuente: Elaboración propia.

Configuración del Server Pool

Para comenzar, se creó un Server Pool denominado BackendPool1, configurado como Reverse Proxy con balanceo de carga. En este pool, se añadió el servidor Nginx con la IP privada 10.1.3.29 y el puerto 80. Esta configuración permite distribuir el tráfico entrante de manera equilibrada entre los servidores backend.

Creación de la Virtual Server

Se configuró una Virtual Server llamada MyVirtualServer, especificando la interfaz y la IP virtual previamente configurada para FortiWeb. Esta Virtual Server actúa como el punto de entrada para el tráfico HTTP/HTTPS destinado a las aplicaciones web protegidas.

Creación de la Server Policy

En la Server Policy, se definió una nueva política denominada WebServerPolicy, configurada en modo de despliegue Single Server/Server Balance. Esta política se asoció con la Virtual Server MyVirtualServer y el Server Pool BackendPool1. Los nombres de host protegidos incluyeron tesisdimitri.net y www.tesisdimitri.net. Además, se habilitó la opción de Client Real IP para mantener la IP real del cliente en los registros. Si se poseen certificados SSL locales, estos se configuraron en esta sección junto con otras opciones de seguridad necesarias.

Configuración del Perfil de Protección Web

Se creó un perfil de protección web llamado Default_WPP. En este perfil, se habilitaron y configuraron reglas para proteger contra inyecciones SQL, inyecciones de comandos, ataques XSS

e intentos de trasversal de directorios. Estas reglas aseguran que las aplicaciones web estén protegidas contra una amplia gama de amenazas comunes.

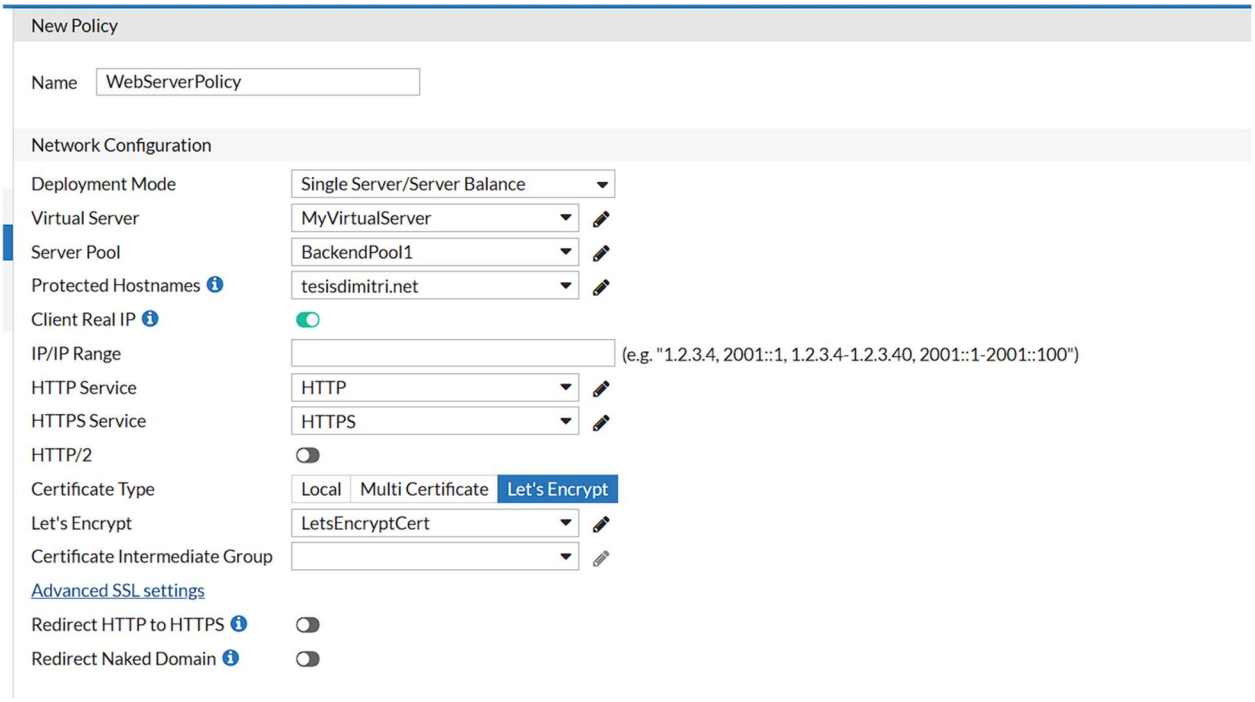
Aplicación del Perfil de Protección Web

El perfil de protección Default_WPP se aplicó a la Server Policy WebServerPolicy en la sección de Security Configuration. Esta aplicación garantiza que todas las solicitudes que pasen por la política de servidor sean evaluadas y filtradas según las reglas de seguridad definidas en el perfil de protección.

Verificación y Monitoreo

Para garantizar la correcta configuración, se verificó que tanto el Server Pool como la Server Policy estuvieran en estado habilitado. Se realizaron pruebas de acceso al dominio tesisdimitri.net para confirmar la funcionalidad de la configuración. Adicionalmente, se llevaron a cabo pruebas de vulnerabilidad utilizando herramientas de seguridad para confirmar que FortiWeb está protegiendo adecuadamente el servidor. Finalmente, se habilitó el logging en FortiWeb para monitorear cualquier intento de ataque, revisando los logs periódicamente para asegurar la seguridad continua del servidor.

Figura 24. *Aplicación del Perfil de Protección Web*



Fuente: Elaboración propia.

Capítulo 4

Análisis de resultados

4. Introducción

En este capítulo, se exponen y examinan los resultados obtenidos de la implementación y evaluación de firewalls integrados y externos en arquitecturas de nube. La evaluación se centra en dos aspectos cruciales: el análisis de costos y la facilidad de operación, seguidos por los resultados de las pruebas de seguridad. A través de un enfoque meticuloso y basado en datos, se busca ofrecer una comprensión integral de las diferencias y ventajas entre el AWS Web Application Firewall (WAF) y FortiWeb. Este estudio ofrece a las organizaciones los datos requeridos para hacer elecciones fundamentadas sobre la selección y implementación de soluciones de cortafuegos en ambientes de nube.

4.1.Análisis de Costos

4.1.1. Costos Iniciales

Los costos iniciales incluyen la adquisición de licencias, la configuración inicial y el despliegue de los firewalls. Aquí se comparan los costos de implementación del AWS Web Application Firewall (WAF) y FortiWeb.

AWS WAF:

AWS WAF se basa en un modelo de pago por uso, lo que proporciona flexibilidad y escalabilidad. Los costos se calculan según el número de reglas activas y las solicitudes web procesadas, permitiendo a las empresas ajustar sus gastos según la demanda real. Este enfoque es especialmente beneficioso para empresas con patrones de tráfico fluctuantes o aquellas que anticipan un crecimiento continuo.

La implementación de AWS WAF es relativamente sencilla, utilizando herramientas como AWS Management Console, CloudFormation o Elastic Load Balancer. Dado que es un servicio completamente gestionado por AWS, no se requieren costos adicionales significativos para hardware o software. AWS también ofrece documentación extensa y guías paso a paso, facilitando la implementación y reduciendo los costos asociados al tiempo y personal necesario.

En cuanto a la configuración inicial, AWS WAF ofrece reglas administradas disponibles para protección inmediata. Las empresas pueden utilizar una variedad de plantillas y configuraciones predeterminadas para establecer rápidamente políticas de seguridad. Esto incluye reglas comunes para proteger contra amenazas como inyecciones SQL, ataques de cross-site scripting (XSS) y denegación de servicio (DoS).

FortiWeb:

FortiWeb requiere la adquisición de licencias, que pueden ser costosas, especialmente para empresas que necesitan características avanzadas y soporte premium. A diferencia del modelo de pago por uso de AWS WAF, FortiWeb utiliza un esquema de licenciamiento tradicional, lo que implica un gasto inicial considerable. Además, es posible que se necesiten licencias adicionales para módulos específicos o funcionalidades avanzadas.

La implementación de FortiWeb en AWS implica la creación de instancias dedicadas, como la instancia t3.medium, cuyo costo es aproximadamente $0.0416 por hora, lo que equivale a aproximadamente $30 por mes si se ejecuta continuamente. Este costo se suma a los costos de licenciamiento de FortiWeb que tiene un costo de $0.96 por hora o $700.1 al mes, incrementando significativamente los costos iniciales.

La configuración inicial de FortiWeb es más compleja en comparación con AWS WAF y puede requerir asistencia técnica especializada. Este proceso incluye la personalización de reglas de seguridad y la configuración detallada de políticas de protección. La necesidad de un conocimiento técnico avanzado y la posible asistencia de consultores externos pueden incrementar tanto los costos iniciales como el tiempo de despliegue.

4.1.2. Costos Operacionales

Los costos operacionales incluyen el mantenimiento continuo, las actualizaciones y la gestión diaria de los firewalls.

AWS WAF:

AWS se encarga del mantenimiento y las actualizaciones del WAF, minimizando el esfuerzo necesario por parte del equipo de TI. Las actualizaciones de seguridad se aplican automáticamente, asegurando que el firewall esté siempre actualizado. Este enfoque gestionado reduce los costos asociados al mantenimiento manual y la necesidad de personal especializado para aplicar parches y actualizaciones.

La gestión diaria de AWS WAF se facilita mediante la inclusión con otros servicios de AWS, como CloudWatch para monitoreo y SNS para alertas. Las reglas administradas simplifican la operación continua, reduciendo la necesidad de ajustes frecuentes y permitiendo que el equipo de TI se concentre en tareas estratégicas en lugar de operativas.

FortiWeb:

El mantenimiento de FortiWeb puede ser más laborioso, ya que requiere intervenciones manuales para aplicar actualizaciones y parches. Esto implica un mayor costo en términos de

tiempo y recursos humanos, ya que se necesita personal especializado para realizar estas tareas de manera eficiente. Además, la posibilidad de errores humanos durante el proceso de actualización puede causar períodos de inactividad inesperados.

La gestión diaria de FortiWeb puede ser más compleja y demandante, requiriendo supervisión constante y ajustes regulares. La necesidad de un equipo especializado para gestionar el firewall puede incrementar los costos operacionales, ya que se deben asignar recursos para el monitoreo continuo, la configuración de políticas y la respuesta a incidentes de seguridad.

4.1.3. Costos de Escalabilidad

Los costos de escalabilidad son los gastos asociados con el aumento de la capacidad de los firewalls para manejar mayores volúmenes de tráfico y amenazas.

AWS WAF:

AWS WAF ofrece escalabilidad automática, ajustando los recursos según la demanda sin intervención manual. Por lo que, facilita a las organizaciones controlar aumentos en el flujo de tráfico sin incurrir en gastos extras considerables. La capacidad de AWS para escalar automáticamente en respuesta a la demanda asegura que las aplicaciones permanezcan protegidas incluso durante eventos de tráfico elevado.

El modelo de pago por uso asegura que los costos de escalabilidad estén alineados con el uso real, evitando gastos excesivos en infraestructura subutilizada. Las empresas pueden aumentar su capacidad de protección sin necesidad de realizar inversiones significativas en hardware adicional o licencias.

FortiWeb:

FortiWeb requiere una planificación más cuidadosa para la escalabilidad, con la necesidad de adquirir y configurar instancias adicionales. Este enfoque manual puede resultar en costos adicionales y tiempo de inactividad durante la ampliación de la capacidad. Así también, se deben tomar en cuenta los gastos vinculados con el ajuste de la infraestructura de red para soportar las nuevas instancias.

Los costos de licenciamiento pueden aumentar significativamente con la escalabilidad, ya que las licencias adicionales pueden ser necesarias para manejar el tráfico incrementado y las funcionalidades avanzadas. Este enfoque escalonado puede resultar en gastos considerables conforme las necesidades de la organización se expanden, y la gestión de estas licencias puede añadir una capa adicional de complejidad administrativa.

4.1.4. Comparación de Costos Mensuales

Durante el mes de junio de 2024 se dejó encendidas todas las instancias por 42 horas, los costos asociados con AWS WAF y FortiWeb fueron los siguientes:

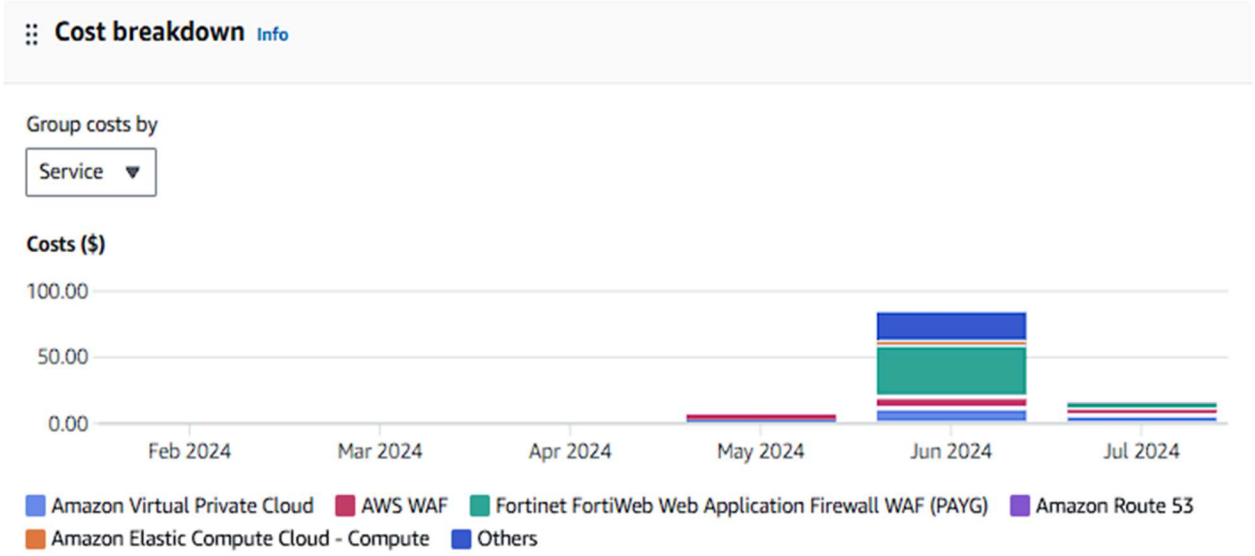


Figura 25. *Comparación de Costos Mensuales*

Fuente: Elaboración propia.

AWS WAF: $8.46

FortiWeb: $39.52

Amazon Virtual Private Cloud (VPC): $11.57

Amazon Route 53: $0.51

Amazon Elastic Compute Cloud (EC2): $1.54

Otros: $24.12

4.2.Facilidad de Operación

4.2.1. Implementación y Configuración

AWS WAF:

La implementación y configuración de AWS WAF son directas y se integran fácilmente con otros servicios de AWS. Las reglas administradas facilitan la configuración inicial, proporcionando protección inmediata sin necesidad de configuraciones complejas. La interfaz de usuario es intuitiva y accesible, permitiendo a los administradores realizar ajustes rápidamente.

FortiWeb:

FortiWeb requiere una configuración más detallada y especializada. La interfaz de gestión proporciona una variedad extensa de alternativas que pueden ser abrumadoras para usuarios no técnicos. La personalización de políticas de seguridad es más avanzada, pero también más compleja de implementar. Esta complejidad permite un alto grado de personalización, lo que puede ser ventajoso para organizaciones que ya utilizan productos de Fortinet, facilitando la integración y gestión coherente de la seguridad.

4.2.2. Gestión y Monitoreo

AWS WAF:

La gestión y el monitoreo de AWS WAF se realizan a través de la consola de AWS, que ofrece una interfaz sencilla y fácil de manejar. La integración con AWS CloudWatch para monitoreo y alertas en tiempo real facilita la supervisión continua. CloudWatch permite rastrear métricas clave y detectar anomalías en tiempo real, proporcionando una visibilidad completa del rendimiento y la seguridad de la aplicación.

FortiWeb:

La gestión de FortiWeb se realiza a través de FortiManager, que ofrece herramientas avanzadas de monitoreo y gestión. FortiManager proporciona un conjunto completo de funcionalidades para la configuración detallada y la administración centralizada de múltiples instancias de FortiWeb. Sin embargo, requiere mayor conocimiento técnico para aprovechar completamente sus capacidades de monitoreo y configuración avanzada. La complejidad de las herramientas y las funcionalidades disponibles implica una curva de aprendizaje más pronunciada y puede requerir formación especializada para los administradores.

4.3.Resultados de las Pruebas de Seguridad

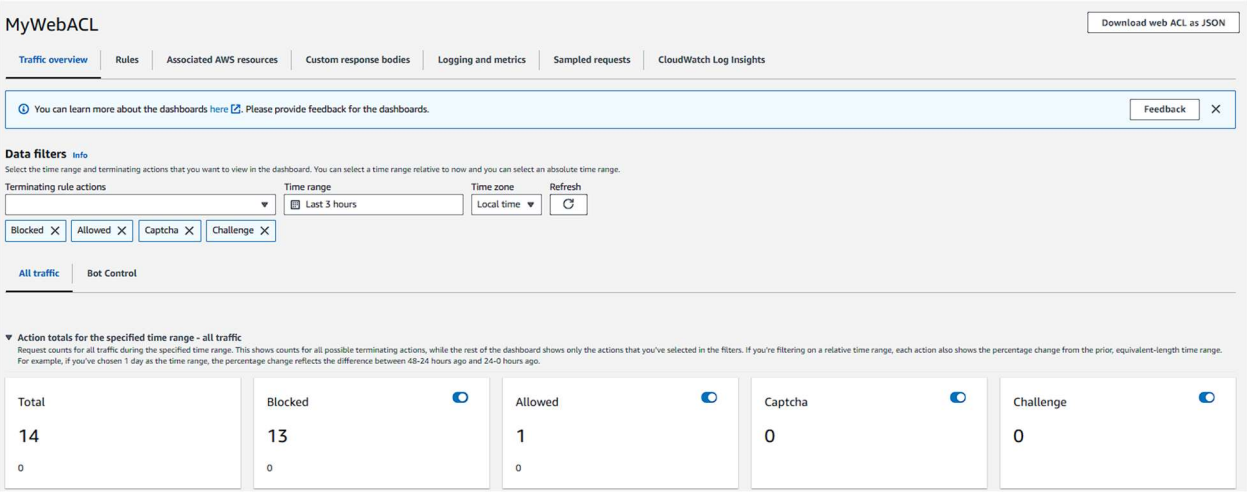
4.3.1. Detección y Bloqueo de Amenazas

Durante las pruebas, se evaluó la capacidad de los firewalls para detectar y bloquear ataques comunes como SQL Injection y Command Injection.

AWS WAF:

SQL Injection: AWS WAF detectó y bloqueó todos los intentos de SQL Injection utilizando las reglas administradas. La protección automatizada y la rápida actualización de las reglas permiten una defensa eficaz contra estas amenazas.

Command Injection: La protección contra Command Injection fue efectiva, bloqueando



todos los intentos basados en patrones conocidos. La capacidad de AWS WAF para adaptarse rápidamente a nuevas amenazas asegura una defensa robusta.

Figura 26. *Detección y Bloqueo de Amenazas*

Fuente: Elaboración propia.

FortiWeb:

SQL Injection: FortiWeb también detectó y bloqueó todos los intentos de SQL Injection, con una capacidad adicional para personalizar las reglas de detección. La personalización avanzada permite ajustar las políticas de protección para ajustarse a los requerimientos particulares de la entidad.

Command Injection: FortiWeb mostró una eficacia similar en la detección y bloqueo de intentos de Command Injection, con opciones avanzadas para ajustar la sensibilidad de las

reglas. Esto proporciona una capa adicional de seguridad, permitiendo una detección más precisa y adaptativa.

4.3.2. Impacto en el Rendimiento

Se evaluó el efecto en el desempeño de las aplicaciones protegidas por cada firewall, considerando la latencia y el throughput.

AWS WAF:

Latencia: La latencia adicional introducida por AWS WAF fue mínima, asegurando una experiencia de usuario fluida. La infraestructura de AWS está optimizada para minimizar el impacto en el rendimiento.

Throughput: El throughput se mantuvo constante, sin afectaciones significativas en el rendimiento de la aplicación. La capacidad de manejar grandes volúmenes de tráfico sin degradación del servicio es una ventaja clave.

FortiWeb:

Latencia: La latencia fue ligeramente mayor en comparación con AWS WAF debido a la complejidad de las reglas personalizadas y la profundidad de inspección. Aunque este aumento en la latencia es pequeño, puede ser notable en aplicaciones altamente sensibles al tiempo de respuesta.

Throughput: Aunque hubo un ligero impacto en el throughput, FortiWeb proporcionó una inspección más granular. Esta capacidad de análisis profundo es útil para entornos con altos requisitos de seguridad, aunque puede afectar marginalmente el rendimiento general.

Capítulo 5

Conclusiones

5. Resumen de los Resultados

En este estudio se ha comparado la eficiencia, costos, facilidad de operación y la capacidad de detección y bloqueo de amenazas entre AWS Web Application Firewall (WAF) y FortiWeb. A través de una serie de pruebas controladas y análisis detallados, se han detectado las fortalezas y debilidades de cada solución de firewall en el contexto de arquitecturas de nube.

5.1. Principales Hallazgos

Eficacia en la Detección y Bloqueo de Amenazas

Se definió parámetros y métricas clave que permitieron evaluar de manera precisa la eficacia de AWS WAF y FortiWeb en la detección y bloqueo de amenazas comunes como SQL Injection y Command Injection. Ambos firewalls demostraron ser altamente efectivos en estas áreas. AWS WAF, con sus reglas administradas, proporciona una protección sólida y actualizaciones rápidas ante nuevas amenazas, facilitando una respuesta inmediata y eficaz. Por otro lado, FortiWeb ofrece opciones avanzadas de personalización, permitiendo ajustes específicos que son cruciales en entornos de alta seguridad. Esta capacidad de personalización adicional hace que FortiWeb sea una opción recomendada para organizaciones que enfrentan amenazas más sofisticadas y que requieren una respuesta adaptativa y detallada.

Impacto en el Rendimiento

Para establecer un entorno de nube controlado y realizar simulaciones que faciliten la evaluación comparativa de AWS WAF y FortiWeb, se configuró múltiples escenarios de seguridad

y gestión. En términos de rendimiento, AWS WAF tuvo un impacto menor, asegurando una experiencia de usuario fluida con latencia mínima y un throughput constante. Esto lo hace ideal para aplicaciones donde la velocidad y la eficiencia son críticas. FortiWeb, por otro lado, proporcionó una inspección más detallada y granular, lo que, aunque incrementó ligeramente la latencia y afectó marginalmente el throughput, ofreció un nivel de seguridad más profundo. Este trade-off puede ser aceptable en entornos donde la seguridad detallada es prioritaria sobre la velocidad absoluta.

Facilidad de Operación, Personalización y Costos

Al realizar el análisis de AWS WAF se destaca su facilidad de operación y rápida implementación, lo cual es especialmente ventajoso para organizaciones con menos recursos técnicos que buscan una solución escalable. La facilidad de uso y la integración nativa con otros servicios de AWS simplifican su gestión, lo que a su vez reduce los costos operacionales a lo largo del tiempo. FortiWeb mostró una eficacia similar, requiriendo una configuración más detallada y especializada, proporcionando una capa adicional de seguridad y permitiendo ajustes específicos que son cruciales en entornos de alta seguridad. La personalización de políticas de seguridad es más avanzada, pero también más compleja de implementar, lo que se puede aplicar para organizaciones que ya utilizan productos de Fortinet, facilitando la integración y gestión coherente de la seguridad.

Comparando los costos iniciales y operacionales de los AWS WEB y FortiWeb se puede concluir, que en el primero se paga por uso, lo que le proporciona la flexibilidad y escalabilidad y no se requieren gastos adicionales, por lo que es un servicio completamente gestionado por AWS. FortiWeb tiene el costo más alto debido a la adquisición de licencias iniciales y requiere gastos adicionales de tiempo y recursos por las intervenciones manuales. Aunque su costo operativo y de

implementación es más alto, esta solución es adecuada para organizaciones con mayores requisitos de seguridad y recursos técnicos que pueden aprovechar sus capacidades avanzadas de configuración y monitoreo.

Se observó que FortiWeb se posiciona como una solución más completa y personalizable, beneficiando especialmente a las organizaciones que ya utilizan productos de Fortinet. Su capacidad para personalizar detalladamente las políticas de seguridad y su integración con otros productos de Fortinet lo hacen ideal para entornos que requieren una protección integral y coordinada. Aunque AWS WAF ofrece una alternativa más económica y fácil de operar, FortiWeb proporciona las herramientas necesarias para una gestión de seguridad avanzada y personalizada, adaptándose mejor a las necesidades de organizaciones con requisitos de seguridad más sofisticados.

5.2. Recomendaciones

Para Organizaciones con Recursos Limitados y Necesidades de Implementación Rápida

Para organizaciones que buscan una solución rápida, costo-efectiva y fácil de gestionar, AWS WAF es la opción más adecuada. Su integración con la infraestructura de AWS y la simplicidad de gestión permiten una protección eficaz con mínima inversión en recursos técnicos.

Para Organizaciones con Requisitos de Seguridad Avanzados y Recursos Técnicos

FortiWeb es la elección óptima para aquellas organizaciones que requieren un alto grado de personalización y control sobre sus políticas de seguridad. Su integración con otros productos de Fortinet y sus capacidades avanzadas de configuración y monitoreo ofrecen una protección más detallada y ajustada a las necesidades específicas de seguridad.

Para los estudiantes y profesionales de TI se recomienda incluir en futuros trabajos investigativos la implementación de inteligencia artificial (IA) en la gestión avanzada de firewalls en arquitecturas de nube, siendo una línea de investigación prometedora del desarrollo de sistemas basados en IA para la detección y respuesta automatizada a amenazas cibernéticas. La IA puede analizar grandes volúmenes de datos de tráfico en tiempo real, utilizando técnicas de aprendizaje automático para identificar patrones de comportamiento y anomalías que podrían indicar ataques, mejorando la efectividad de los firewalls, reduciendo la carga operativa asociada con la gestión manual de la seguridad.

5.3. Conclusión Final

En el presente trabajo se analizó la eficacia, la gestión y la eficiencia operativa de los firewalls integrados frente a los externos en la nube, con el fin de establecer una base empírica

sólida que oriente las decisiones estratégicas en la implementación de soluciones de firewall adecuadas para arquitecturas basadas en la nube. La información recopilada y los conocimientos prácticos derivados de este estudio benefician a los profesionales de TI y de seguridad y les permitirán elegir soluciones de firewall que no solo protejan sus activos digitales, sino que también se alineen con sus necesidades operativas y estratégicas.

En conclusión, la elección entre AWS WAF y FortiWeb debe basarse en las necesidades específicas de seguridad, recursos técnicos y presupuestos de la organización. AWS WAF proporciona una solución fácil de gestionar y económica, ideal para una rápida implementación y escalabilidad. Por otro lado, FortiWeb, con su alto grado de personalización y capacidades avanzadas, es más adecuado para entornos que requieren una protección detallada y controlada, siendo una inversión valiosa para organizaciones con mayores demandas de seguridad.

La comprensión de estas diferencias y la evaluación cuidadosa de las necesidades específicas permitirán a las organizaciones tomar decisiones informadas sobre la implementación de soluciones de firewall en sus arquitecturas de nube, optimizando así tanto la seguridad como la eficiencia operativa.

Bibliografía

Angulo, F., Ramírez, L., & Villegas, P. (2023). *Plan de Marketing para Ibux Cloud, dirigido al sector público, durante el periodo: Setiembre 2023 a marzo del 2024* [Universidad Nacional de Costa Rica]. https://repositorio.una.ac.cr/handle/11056/26119

AWS. (2021). *Integrating Third-Party Firewall Appliances with VMware Cloud on AWS Using VMware Transit Connect | AWS Partner Network (APN) Blog*. https://aws.amazon.com/blogs/apn/integrating-third-party-firewall-appliances-with-vmware-cloud-on-aws-using-vmware-transit-connect/

AWS. (2024). *AWS WAF with managed rules: AWS Security Maturity Model*. https://maturitymodel.security.aws.dev/en/1.-quickwins/waf/

Cisco. (2024). *Valtix Is Now Part of Cisco—Cisco*. https://www.cisco.com/c/en/us/products/security/valtix-is-part-of-cisco.html

Cloudflare. (2024). *¿Qué es un firewall? | Firewall de red*. https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/

CONAFIPS. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Delgado, K. (2023). *Propuesta de una solución tecnológica para el agendamiento medico a través de tecnología inteligente Chatbot a pacientes de consulta externa del Hospital de Especialidades Eugenio Espejo* [masterThesis, Universidad de las Américas]. http://dspace.udla.edu.ec/handle/33000/14990

Echegaray, E., & Julca, G. (2023). *Sistema de mantenimiento y eficiencia energética (BMS) a través de un gemelo digital para instalaciones aeroportuarias* [Universidad Peruana de Ciencias Aplicadas (UPC)]. https://repositorioacademico.upc.edu.pe/handle/10757/670222

Enciso, J., Portilla, J., & Mendoza, A. (2023). *Análisis integral de los sistemas de detección de intrusos y sus algoritmos asociados en la seguridad de la información | INGENIERÍA INVESTIGA*. *5*, 1-22.

ESET. (2024). *Qué es el modelo de seguridad Zero Trust y por qué creció su adopción*. https://www.welivesecurity.com/la-es/2020/09/14/zero-trust-que-es-modelo-seguridad-crecio-adopcion/

Fuentes, W., & Pariajulca, L. (2023). *Implementación de un sistema ERP SAP para la gestión financiera y presupuestal de un canal de televisión* [Universidad Peruana de Ciencias Aplicadas (UPC)]. https://repositorioacademico.upc.edu.pe/handle/10757/671816

Gómez, J. (2024). *Evaluación de la viabilidad de la implementación de escritorios virtuales en una pequeña empresa* [Universitat Oberta de Catalunya]. https://openaccess.uoc.edu/handle/10609/150624

Google Cloud. (2024). *Ley de Privacidad del Consumidor de California (CCPA) | Google Cloud*. https://cloud.google.com/security/compliance/ccpa?hl=es

Guanotoa, A. (2024). *Implementación de un firewall de siguiente generación que minimice el riesgo que corren los niños al navegar por internet en una red doméstica* [bachelorThesis, Universidad Técnica del Norte]. https://repositorio.utn.edu.ec/handle/123456789/15568

Instituto Nacional de Transparencia. (2021). *Normativa y legislación en PDP – Marco Internacional de Competencias de Protección de Datos Personales para Estudiantes*. https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

Lema, D. (2023). *Control de amenazas e instrucciones informáticas en una red domestica basadas en Open Source.* [bachelorThesis, Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/handle/49000/14188

Maita, F. (2024). *Implementación de metodología agile para mejorar la calidad del software en una entidad financiera* [Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/handle/20.500.11818/8300

Merchán, N., Palma, E., & Poma, D. (2024). Comparación de metodologías ágiles para el desarrollo de software. *MQRInvestigar*, *8*(1), Article 1. https://doi.org/10.56048/MQR20225.8.1.2024.5052-5074

Merck & Co. (2024). *La confidencialidad y la HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud en Estados Unidos)—Fundamentos*. Manual MSD versión para público general. https://www.msdmanuals.com/es-ec/hogar/fundamentos/asuntos-legales-y-éticos/la-confidencialidad-y-la-hipaa-ley-de-portabilidad-y-responsabilidad-de-seguros-de-salud-en-estados-unidos

Morris, & Opazo. (2024). *Portafolio de Soluciones en AWS - Morris & Opazo*. https://www.facebook.com/MorrisOpazo

Pineda, M., & Quiceno, A. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia. *Revista CIES Escolme*, *14*(2), Article 2.

PowerData. (2024). *GDPR: Lo que debes saber sobre el reglamento general de protección de datos*. https://www.powerdata.es/gdpr-proteccion-datos

Ramírez, L. (2024). Tecnologías de defensa frente a inteligencia de amenazas y ciberataques. *InnDev*, *3*(1), Article 1. https://doi.org/10.69583/inndev.v3n1.2024.94

Ramos, M. (2024). *Implementación de la tecnología Secure SD-WAN para optimizar el tráfico de la red corporativa de una empresa del sector retail* [Universidad Tecnológica del Perú]. http://repositorio.utp.edu.pe/handle/20.500.12867/8353

Recalde, P., & Veloso, E. (2022). *Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.* [masterThesis, UISRAEL]. http://repositorio.uisrael.edu.ec/handle/47000/3369

Salinas, Á. (2023). *GUÍA DE BUENAS PRÁCTICAS PARA PREVENIR Y REACCIONAR ANTE UN ATAQUE DE RANSOMWARE* [PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR]. https://repositorio.puce.edu.ec/server/api/core/bitstreams/4b8e0dfe-cac0-455a-8102-005254ec0020/content

Stocovaz, M. (2023). *ITSpend: El verdadero costeo de proyectos digitales* [Universidad de San Andrés]. http://repositorio.udesa.edu.ar/jspui/handle/10908/23619

Suárez, Lady, Suárez, C., & Triviño, L. (2024). *Análisis de viabilidad para el desarrollo de una empresa prestadora de servicios y soluciones de control y automatización* [Master Thesis, Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos Virtual]. https://repository.universidadean.edu.co/handle/10882/13548

Vera, E. (2024). *Estudio del proceso de migración en sistemas locales en entornos en la nube, análisis de beneficios, desafíos y lecciones aprendidas en la transición con ISP en la Empresa Jatnet de la ciudad de Babahoyo.* [bachelorThesis, Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/handle/49000/15704

Villacís, B., Toasa, R., & Urdaneta, M. (2024). *Análisis de Vulnerabilidades basado en Técnicas de Inteligencia Artificial para la Seguridad Informática en Redes de Área Local.* [masterThesis, Universidad Tecnológica Israel]. http://repositorio.uisrael.edu.ec/handle/47000/4140

ANEXOS

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Dimitri Eduardo Coronel Golubenko portador(a) de la cédula de ciudadanía Nº **1104496953**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación "**Firewalls Integrados vs. Externos en Arquitecturas de Nube: Evaluación de Eficiencia mediante Diseño y Comparación"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca**,** para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **11 de septiembre de 2024**

F: .....Firmado electrónicamente por: DIMITRI EDUARDO CORONEL GOLUBENKO.....

Dimitri Eduardo Coronel Golubenko

C.I. **1104496953**