NOMBRE DEL TRABAJO

IMPLEMENTACIÓN DEL ACCESO VÍA WEB AL CORREO ELECTRÓNICO OWA EMPLEANDO BALANCEO DE CARGA Y F5 BIG IP

AUTOR

Kent Yhonny Cueva Rupacho

RECUENTO DE PALABRAS

16776 Words

RECUENTO DE CARACTERES

95597 Characters

RECUENTO DE PÁGINAS

90 Pages

TAMAÑO DEL ARCHIVO

4.4MB

FECHA DE ENTREGA

Mar 26, 2024 8:03 AM GMT-5

FECHA DEL INFORME

Mar 26, 2024 8:06 AM GMT-5

3% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 3% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

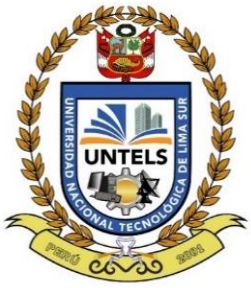
Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES



"IMPLEMENTACIÓN DEL ACCESO VÍA WEB AL CORREO ELECTRÓNICO OWA EMPLEANDO BALANCEO DE CARGA Y F5 BIG IP ASM PARA GARANTIZAR LA CIBERSEGURIDAD EN UNA ENTIDAD BANCARIA"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

Kent Yhonny Cueva Rupacho

ASESOR: Bernardo Castro Pulcha

Villa el Salvador, 2023

DEDICATORIA

A Dios por ser mi fortaleza y quien me sustenta en todo tiempo, en mis luchas, pruebas y dificultades, nunca me desampara. A mis padres, Segundo Dionisio Cueva Sanchez y Maria Consuelo Rupacho Alcántara.

A mis hermanos (as), A mi futura esposa e hijos, A mi tío Julio Cesar Rupacho Alcantara quien inculcó desde mi niñez el estudio, A mis Pastores Hebert y Lidia Torres, Al seminario bíblico y Pastores de estudio Juan Cano y Victor Castañeda, A toda la Iglesia del Salvador.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios a quien le pertenece toda la gloria y la honra, por permitirme la vida y ser partícipe del programa de titulación, así mismo a mis Padres Segundo Dionisio Cueva Sanchez y Maria Consuelo Rupacho Alcántara por todo su apoyo y ayuda incondicional.

Al Ing. Jose Carlos Wong y la Ing. Karina Paco por brindarme la oportunidad de crecer profesionalmente en el área de Ciberseguridad. Al Mg. Brayan Navarrete Curi por su apoyo incondicional y consejos en el área técnica.

Al ing. Bernardo Castro Pulcha, por su orientación durante el desarrollo del presente trabajo.

INDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

El presente trabajo hace referencia a la implementación del acceso vía web al correo electrónico OWA, empleando balanceo de carga y protocolos de ciberseguridad, para una entidad bancaria (cuyo nombre fue censurado por motivos de confidencialidad).

Dicha labor fue realizada durante mi instancia como ingeniero Onsite en la empresa Securesoft Corporation S.A.C, empresa dedicada a brindar soporte, ventas, asesorías y servicios especializados a diferentes clientes en el ámbito de las tecnologías de la información "T.I".

Como resultado de la pandemia gran porcentaje de personas requieren laborar mediante conexión remota o teletrabajo, ya que, por restricciones decretadas por el estado peruano, la concurrencia de trabajadores en toda entidad no debe de ser en su totalidad sino parcialmente. Sumado a esto la problemática se agravó, cuando un trabajador operaba desde una red externa, es decir no conectado en la red de banco, este no podía acceder a su buzón de correo, por tal razón los trabajadores se encontraban en la necesidad de acudir presencialmente a la entidad bancaria para acceder a su correo electrónico.

Bajo este escenario, se planteó brindar el acceso al correo electrónico desde internet, pero con la debida seguridad, ya que involucra gestión de información sensible. Por lo cual, la respuesta ante tal problemática fue realizar la integración de los servidores de correo electrónico con la solución de F5 BIG-IP ASM, y una política de bloqueo con protocolo seguro.

Finalmente se configuro la redundancia del servicio a través de 2 proveedores de internet, realizando un ruteo de tráfico de alta disponibilidad, asegurando así la permanencia del servicio ante algún fallo en la red.

Como resultado del trabajo se logró implementar el acceso vía web al correo electrónico OWA de manera satisfactoria, lográndose ingresar a los buzones de correo desde cualquier ordenador o equipo móvil, conectado a internet.

INTRODUCCIÓN

Debido a la coyuntura que atravesó el País durante el año 2020 hasta fines del año 2022 periodo del Covid19, nació la necesidad de utilizar el teletrabajo, pero el problema se agrava posteriormente al retornar a las oficinas, la concurrencia no era del 100% de los trabajadores, sino parcialmente. Además, como el acceso al correo electrónico outlook web estaba solo disponible en la red privada o mediante conexión con un agente VPN, los trabajadores se vieron afectados para acceder al recurso de correo corporativo, especialmente cuando no estaban en sus equipos corporativos ni conectados a la red de Banco, o no tenían instalado un agente VPN.

En resumen, muchos no tenían un medio para acceder a la red corporativa, ya que a medida que un usuario cambiaba de equipo, esté requería reinstalar su agente VPN y gestionar permisos a nivel de Firewall para que puedan abrir la misma cuenta de correo en diferentes equipos, asegurando así su conexión al buzón de correo, pero en la mayoría de los casos presentados los permisos eran denegados, porque cada sesión de usuario en otra PC implicaba una nueva licencia VPN a utilizar, siendo así que 1 usuario llegaba a utilizar más de 1 licencia en cada equipo en el que operaba, ocasionando perdida de licencias de forma innecesaria.

Por lo cual este proyecto tiene como objetivo realizar la implementación del acceso vía web al correo electrónico OWA desde Internet. Esto se realizó con la intención de utilizar cualquier equipo móvil o PCs “sin tener la necesidad de gastar licencias cada vez que un trabajador utilice diferentes equipos para sus labores cotidianas”.

En síntesis, se eliminó la necesidad de reinstalar agentes VPNs, la gestión de permisos y la necesidad de asistencia presencial para conectarse a la red interna.
Es decir, el propósito final es reducir la congestión de usuarios en las instalaciones físicas, mejorar el rendimiento y la eficiencia de los trabajadores, permitiéndoles realizar sus tareas desde cualquier computadora portátil y disfrutar de la comodidad de trabajar desde sus hogares o sitios trabajo.
Bajo este escenario, la solución fue implementar el acceso vía web correo electrónico OWA en internet de forma segura mediante un firewall de aplicaciones F5 BIG-IP ASM.
Finalmente, se logró la conexión de forma segura, controlada y auditable.

CAPÍTULO I. ASPECTOS GENERALES

1.1. Contexto

Securesoft Corporation S.A.C, empresa en la que laboro, desarrollada en el área de ciberseguridad, ofrece venta de soluciones, servicios especializados, asesorías y cyberSoc, operando 24 x 7 los 365 días del año, tanto en los Países de Perú, Ecuador y Colombia.

Siendo identificada de esta manera con su misión, la cual es respaldar la evolución digital de los clientes mediante la oferta de productos, consultorías y soporte para asegurar la operatividad vigente e ininterrumpida del servicio. Su visión al 2025 es ser líder en el Market share de ciberseguridad en Latinoamérica. (Securesoft, 2023)

1.2. Delimitación del Proyecto

1.2.1. Temporal

Este proyecto tuvo una duración de 4 meses y 23 días, iniciando el lunes 9 de Agosto del año 2021 y finalizando el 2 de Enero del 2022.

1.2.2. Espacial

El trabajo realizado se ejecutó mediante sesiones programadas en el data center de la empresa Securesoft ubicado en, San Isidro.

1.3. Objetivos

1.3.1. Objetivo General

- Implementar el acceso vía web al correo electrónico OWA, empleando balanceo de carga y F5 BIG IP ASM para garantizar la ciberseguridad en una entidad bancaria.

1.3.2. Objetivos Específicos

O1. Implementar un servicio de conexión remota a los trabajadores, seguro, confiable y con flexibilidad de conexión a través de cualquier equipo conectado a internet.

O2. Configurar balanceo de carga para asegurar la permanencia del servicio ante algún fallo en la red LAN (Local Area Network).

O3. Configurar un enlace de contingencia con el ISP (internet Service Provider) para asegurar la redundancia del servicio WAN (Wide Area Network) ante una caída de un enlace de internet.

O4. Validar la operatividad del servicio de correo outlook web mediante pruebas de acceso a las bandejas de correos.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

Presentamos proyectos y tesis realizadas, que guardan relación con el trabajo de suficiencia profesional, todo esto con la finalidad enriquecer, complementar y facilitar la comprensión del trabajo.

2.1.1 Antecedentes Internacionales

Cabezas, N. (2020) en su Tesis de titulación “Configuración del firewall de aplicaciones web modsecurity para prevenir diversos ataques hacia aplicaciones web alojados en servidores open source”, Universidad Católica de Ecuador. Propusieron la configuración de un firewall de aplicaciones WAF, para la protección de los servidores web que publican un servicio en internet.

El aporte de la tesis en relación con el trabajo de suficiencia profesional es la necesidad de configurar un firewall WAF para la protección de los servidores web debido a los constantes ataques desde la red pública.

Perdomo, C., Abril, W. y Castro, L. (2020), en su proyecto de titulación “Planeación de un proyecto de implementación para una solución de balanceo de carga F5 BIG-IP en la universidad latinoamericana de Bogotá basado en el modelo PMI” - Universidad Santo Tomás. Propusieron realizar el diseño y planeación para la implementación de la plataforma ADC (Application Delivery Controller) con F5 BIG-IP, utilizando dos servidores en un sistema de balanceo de carga. Así como se implementó el módulo F5 ASM, permitiendo publicar la aplicación web en internet, de forma segura.

El aporte del proyecto de titulación en relación con el trabajo de suficiencia profesional es en la utilización de un sistema de balanceo de carga. Como también la protección de una aplicación web, mediante la configuración de F5 ASM.

Piedrahita, E. (2016) En su proyecto de titulación “Análisis comparativo de un Firewall de aplicaciones web comerciales y un open source frente al top 10 de OWASP” Universidad Nacional abierta y a distancia (UNAD) - Colombia. Luego de

realizar una comparación de marcas, se observó que F5 BIG IP WAF era la mejor opción. Debido a su robustez frente a ataques maliciosos, su versatilidad y su capacidad de soportar complejos lenguajes de programación.
Además, su interfaz de usuario gráfica “GUI” es fácil de usar y permite identificar rápidamente ataques legítimos como falsos positivos.

El aporte del proyecto de titulación en relación con el trabajo de suficiencia profesional es la demostración de que F5 BIG IP es un equipo robusto y confiable para la protección de aplicaciones webs, proporcionando conexiones seguras.

2.1.2 Antecedentes Nacionales

Torres, M. (2020), en su tesis de titulación “Infraestructura tecnológica virtual con alta disponibilidad basada en la nube para mejorar la continuidad operativa del LMS de la UNCP - Universidad Nacional del Centro del Perú”. Argumentó que la plataforma Web LMS, utilizada para asesorías y clases virtuales, ha experimentado frecuentes caídas de servicios debido a la insuficiente capacidad de recursos en los servidores. Para abordar este problema se planteó implementar una infraestructura en la nube, conformado por 4 nodos en un sistema de balanceo de carga, garantizando así la alta disponibilidad. Además, se planteó configurar un Firewall de aplicaciones, para proteger la aplicación web publicada en internet.

El aporte de la tesis en relación con el trabajo de suficiencia profesional es plantear la configuración de un firewall de aplicaciones para la protección del servicio web, como también un balanceo de carga para asegurar la permanencia del servicio.

Ciriaco, N. (2021), en su proyecto de suficiencia profesional de titulación, “Optimización del servicio de red con el respaldo del enlace a internet WAN y la seguridad perimetral para la empresa Sonepar sede Lima “, Universidad Nacional Tecnológica de Lima Sur. Configuró un enlace de respaldo para la conexión a internet, realizado con otro proveedor ISP (internet Service provider) mediante un balanceador de carga en una configuración activo -Pasivo, buscando garantizar un servicio constante ante alguna falla en el enlace principal de internet, sumado a esto busco proporcionar una navegación segura de usuarios y la protección de los servidores mediante un equipo firewall perimetral.

El aporte del proyecto de titulación en relación con el trabajo de suficiencia profesional es implementar un enlace de internet Backup, que permita asegurar la permanencia activa del servicio. Como también contemplar el uso de un firewall perimetral para la protección del servicio web en internet y permitir una navegación segura de usuarios en la red pública.

Jimenez, S. (2021), en su proyecto de suficiencia profesional de titulación “Diseño e implementación de una arquitectura de red redundante empleando balanceo de carga mediante los protocolos BGP y OSPF para optimizar la red regional de Lima” Universidad Nacional Tecnológica de Lima Sur. Planteó realizar un balanceo de tráfico con diferentes proveedores de internet (ISP), asegurando la redundancia de tráfico, ante alguna caída del enlace de internet en algún proveedor “ISP”, evitando la inoperatividad del servicio.

El aporte del proyecto de titulación en relación con el trabajo de suficiencia profesional es en la utilización de un sistema de redundancia de enlace de internet ante alguna falla en el proveedor de internet principal (ISP). Tal como se ha realizado en el presente trabajo profesional.

2.2 BASES TEÓRICAS

Presentamos temas fundamentales relacionados con el trabajo de suficiencia a fin de facilitar la comprensión del proyecto.

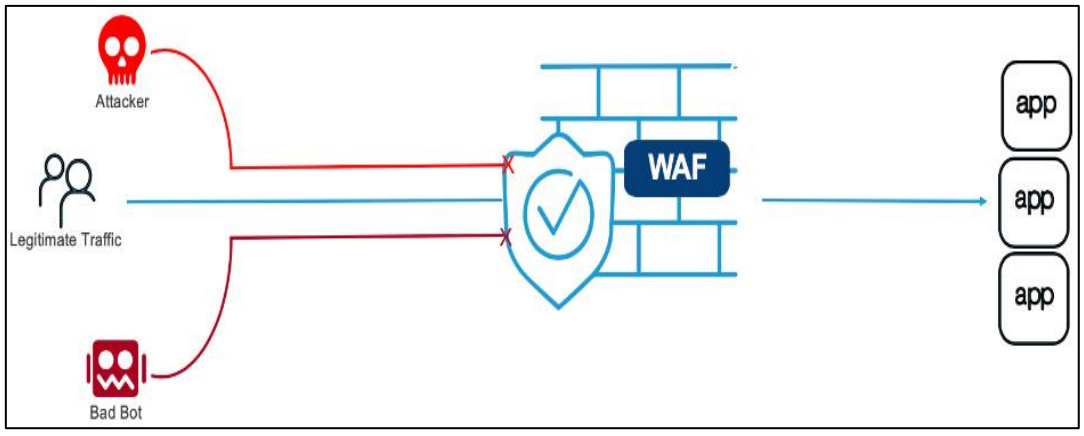
2.2.1 CIBERSEGURIDAD

La ciberseguridad es un conjunto de procesos, reglas y medidas diseñadas para proteger los sistemas (hardware o software) que envían información privada y sensible, como también la información crítica que fluye a través de estos (Como se puede observar en la Figura 1), las conexiones maliciosas son bloqueadas, mientras que las conexiones de usuarios son permitidas y presentan el color celeste.

Buscando de esta manera hacer accesible la información para los usuarios autorizados pero inaccesible para los que no lo están. Salvaguardando la filtración de datos y previniendo que los equipos sean vulnerados ante los constantes ataques de la red pública (Solleiro et al., 2022, p.7).

Figura 1

Ciberseguridad de red, Firewall de aplicaciones



Nota. El gráfico muestra una red protegida por un Firewall de aplicaciones WAF, Adaptado de *Que es WAF* ,F5 Networks, 2020, (https://my.f5.com/manage/s/article/K28426659)

A su vez la ciberseguridad presenta capas de protección para abordar los diferentes tipos de ataques provenientes de la red pública. Por lo cual utiliza las siguientes contramedidas (Solleiro et al., 2022, p.12).

- La Seguridad de la Información
- La Seguridad de Red

2.2.1.1 SEGURIDAD DE RED

La seguridad de la red tiene como responsabilidad fundamental proteger los activos que residen en la topología de una entidad, garantizando una conexión segura y mitigando todo intento de intrusión maliciosa. Este objetivo lo realiza a través diferentes capas de seguridad, lo que conlleva a la necesidad de implementar equipos de seguridad en cada nivel de la red, brindando permisos a los usuarios, y limitando el acceso no autorizado (Romero et al., 2018, p.13).

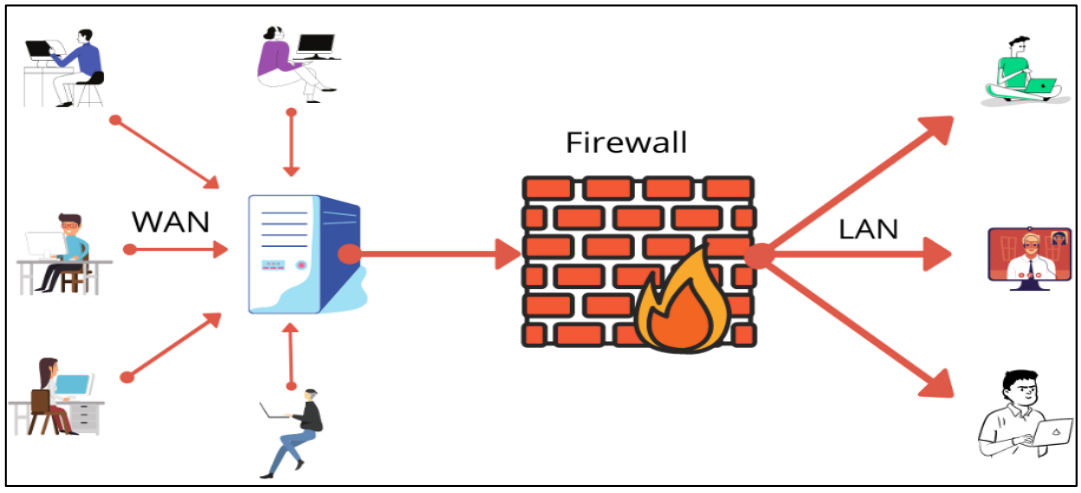
Debido a la escalabilidad de la red y la incompatibilidad de equipos, el pensar en un solo equipo para proteger toda la red, no sería viable como también es inconsistente debido a que no existe un nivel seguridad único, sino que las entidades deben de contar diversas capas de seguridad en todos sus niveles de su información para así identificar en qué punto de la red ocurrió el intento de intrusión.

En síntesis, la seguridad de la red es la actividad diseñada para proteger mediante reglas y protocolos la integridad de los equipos informáticos como también la información que transmiten (Cisco, 2018).

De la Figura 2, se puede observar una topología clásica de seguridad de red, donde usuarios externos establecen una comunicación segura con los trabajadores de una entidad.

Figura 2

Representación básica de seguridad de la red



Nota. El gráfico representa una red basica de seguridad, *Adaptado de Guia de Introduccion Firewall*, por A. Pathak, 2023, (https://geekflare.com/firewall-introduction)

2.2.1.2 NORMATIVAS DE SEGURIDAD DE RED

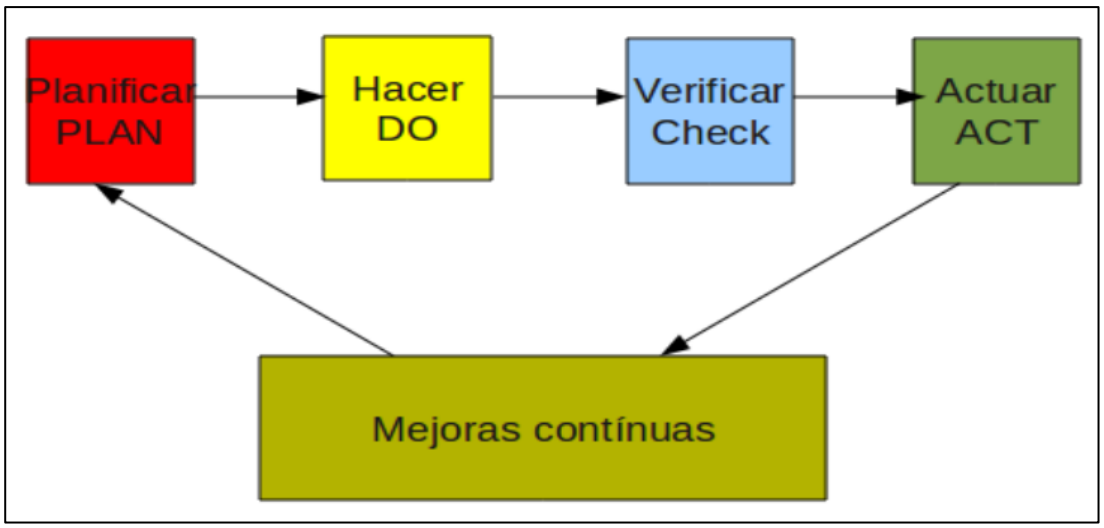
Es importante recabar que todo proceso de seguridad de red deba cumplir con la ISO 27001, código de buenas prácticas para la gestión de información, la cual utiliza el modelo PDCA (Como se puede observar en la Figura 3) cuya la finalidad es obtener mejoras continuas en la productividad de toda entidad (Mesquida, 2003, p.14).

A continuación, se muestra en que consiste el proceso del modelo PDCA (Lorena, 2004, p.2).

- Plan = Consiste en establecer el contexto y análisis de riesgos.
- Do = Consiste en implementar el plan o análisis de riesgos.
- Check = Consiste en realizar auditorías y monitorear las actividades.
- Act = Consiste en ejecutar tareas de Mantenimiento preventivo.

Figura 3

Modelo de mejoras continuas - PDCA



Nota. Adaptado de *Introducción a la seguridad Informatica y Seguridad de la Información* (p.2), por E. Mifsud, 2012, INTEF

ISO 27033; norma dedicada para la seguridad de redes, encargada de asegurar las comunicaciones perimetrales utilizando gateways y configuración de VPNs, para establecer una conexión segura, así mismo regula los problemas relacionados con la operación, monitoreo, implementación y controles de ciberseguridad en la red interna y externa. (ISO/IEC 27033, 2014, p.5).

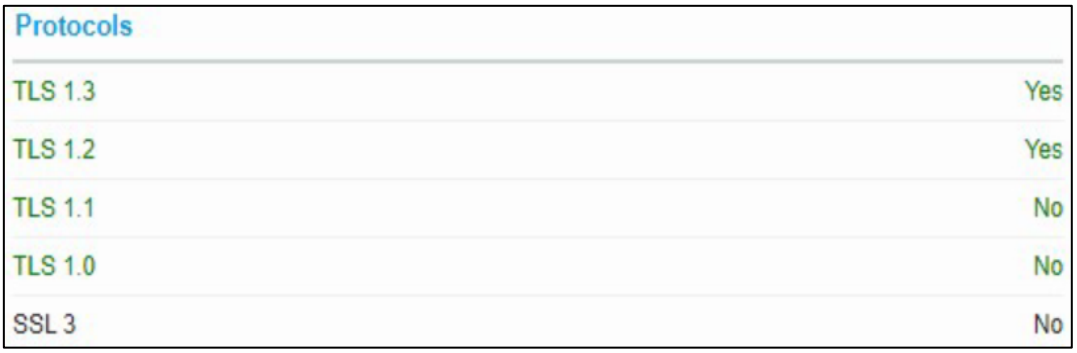
2.2.1.3 PROTOCOLOS DE SEGURIDAD DE RED

Son utilizados en conexiones HTTPS, con la finalidad de permitir una conexión segura, de tráfico encriptado y no vulnerable.

Tener una publicación de aplicación web segura en internet, de acuerdo con la estandarización de protocolos seguros dados por la “ISO 27033”, se debe tener deshabilitado los protocolos vulnerables como TLSv1, TLSv1.1, SSLv2, SSLv3 y solo permitir protocolos seguros como TLSv1.2 y TLSv1.3. Cómo se observa a continuación, en la Figura 4, se puede verificar los resultados de la desactivación de protocolos inseguros, dejando solamente activado los protocolos seguros TLSv1.2 y TLSv1.3 (Varela, 2023).

Figura 4

Versión de TLS seguro 1.2 y 1.3



Nota. Adaptado de *Que versión de TLS utiliza mi página*, INCIBE, 2020, (https://www.incibe.es/empresas/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del-tls)

Luego de lo compartido, se constata que tanto el TLSv1.2 y TLSv.1.3 son permitidos y válidos.

TLSv1.2: Conocido como transport layer Security versión 1.2, es un protocolo de seguridad encargado de cifrar la comunicación HTTPS, brinda una capa de seguridad a la comunicación que existe entre cliente – servidor.

TLSv1.3: Conocido como transport layer Security versión 1.3, es un protocolo que elimina vulnerabilidades del protocolo TLSv1.2, así mismo elimina el cifrado estático y utiliza Ephemeral Diffie-Hellman (DHE) y Elliptic Curve Diffie-Hellman (ECDHE). Esto mejora la seguridad al garantizar que las claves de cifrado cambien en cada sesión.

2.2.2 FIREWALL BALANCEADOR DE CARGA

El firewall de aplicaciones o también conocido como firewall balanceador de carga, es un dispositivo orientado a ofrecer protección a nivel perimetral, protegiendo las aplicaciones en capa 7, adicionalmente realiza el balanceo de carga para evitar la congestión de la red. (F5 Networks , 2023)

2.2.2.1 SEGURIDAD PERIMETRAL

Define la seguridad perimetral como una línea divisoria que separa los equipos que se encuentran en la red interna de la red externa, es decir es el intermediario en la comunicación entre los equipos de una entidad que maneja información sensible con el internet global.

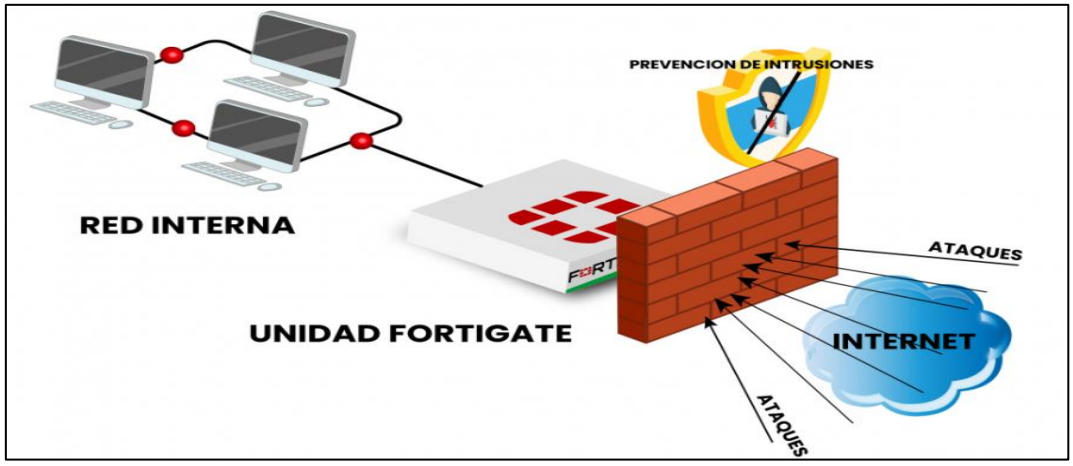
Además, la seguridad perimetral se compone de los equipos conocidos como firewalls, que son los encargados de filtrar intentos de intrusión maliciosa hacía la red interna, para finalmente solo permitir conexión de usuarios autorizados. (González, 2002, p.135)

Como se puede observar en la Figura 5, se presenta una arquitectura de red interna de 3 computadoras que incluye un equipo firewall Fortigate perimetral, el cual presenta la función de proteger la red interna.

En primer lugar, filtra y bloquea intentos de ataques maliciosos que intentan vulnerar la red, como se puede observar los ataques provienen desde internet, por lo cual el firewall Fortigate previene las intrusiones y garantiza la seguridad de la red interna contra los ataques provenientes de internet.

Figura 5

Seguridad perimetral – Firewall línea divisora de red interna y externa



Nota. Adaptado de *Ciberseguridad Firewall Fortinet para empresas*, StemPrinting, 2021, (https://www.stemprinting.com/firewall-para-empresas)

2.2.2.2 FIREWALL PERIMETRAL

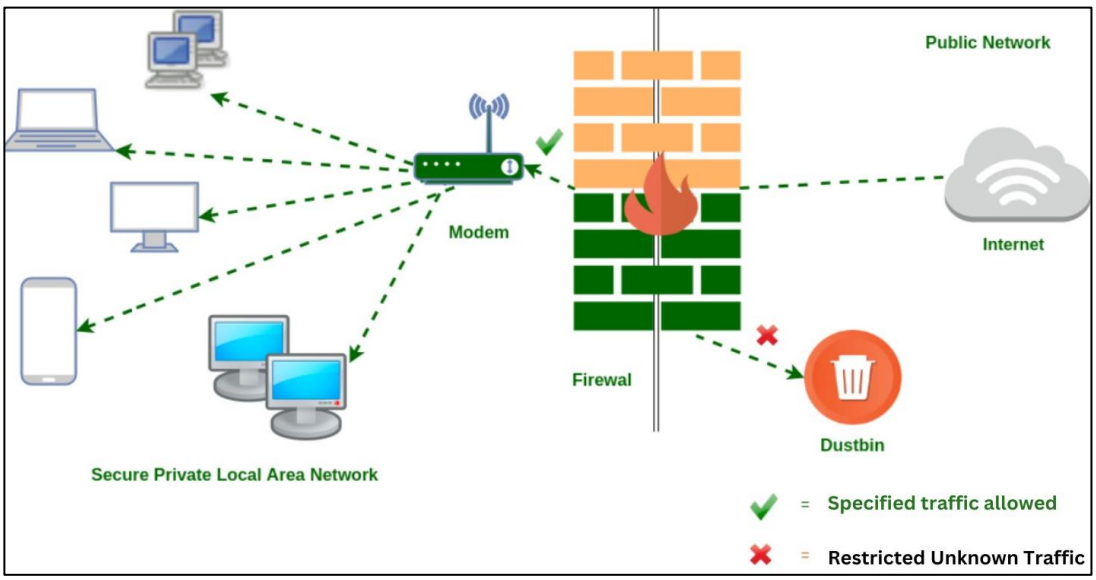
Conocido también como cortafuegos, el cual es un dispositivo de seguridad encargado de realizar el filtrado de paquetes provenientes de la red pública. Los firewalls perimetrales han ido evolucionando en gran manera por lo cual hoy en día se han vuelto un elemento indispensable en toda arquitectura de red, por lo cual es casi costumbre verlo en todas las topologías de red ubicadas entre la red local y la red pública. Como se puede observar en la Figura 6, la importancia de tener un firewall es fundamental, debido a que opera en dos sentidos, filtra tráfico malicioso entrante proveniente de la red, pero a su vez realiza la inspección del tráfico saliente, es decir bloqueo la actividad que puede ser de índole maliciosa proveniente desde un usuario local. (Briceño, 2021, p.80)

Cuáles son los beneficios de un Firewall

- Ofrece el monitoreo de los sitios webs que navegaron los usuarios.
- Protege los servidores de la red interna de vulnerabilidades activas.
- Administra que usuarios pueden acceder a la red privada.
- Realiza el bloqueo manual y automático de los IOCs maliciosos.
- Limita el ancho de banda consumido por los usuarios.

Figura 6

Seguridad perimetral - Red Interna e Externa



Nota. El gráfico muestra tráfico permitido y ataques maliciosos bloqueados por el Firewall perimetral, *Adaptado de Filtrado de paquetes Firewall* , Geeksforgeeks, 2021, (https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks)

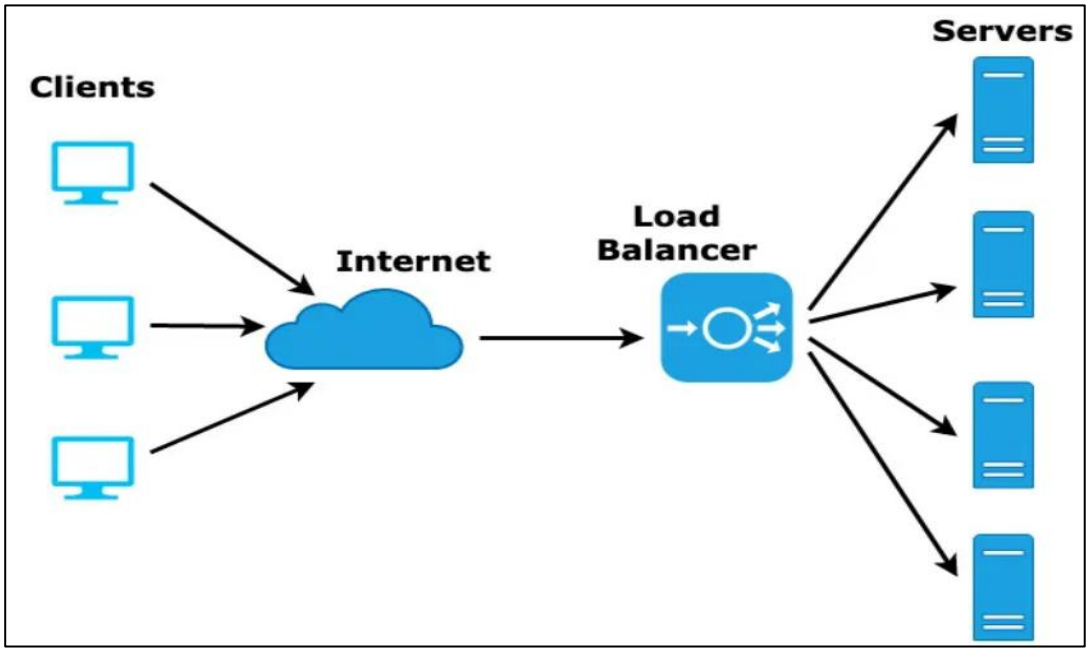
2.2.2.3 BALANCEO DE CARGA

El método de balanceo de carga es utilizado distribuir el tráfico entre los activos de la red y así evitar pérdida del servicio, logrando que los servidores finales reciban el tráfico de manera uniforme y compartan la carga, como también ante algún fallo de la red, los servidores restantes asumirán la carga del servidor impactado. (F5 Networks , 2023)

A continuación, en la Figura 7 se puede observar el proceso de balanceo de carga de tráfico entrante, en relación con los servidores receptores finales.

Figura 7

Distribución de tráfico



Nota. El gráfico representa el equilibrio de carga distribuido en los servidores, Adaptado de *Balanceador de carga*, Codeburst, 2020, (https://codeburst.io/load-balancers-an-analogy-cc64d9430db0)

Es importante mencionar que todo tipo de balanceo de carga puede ser realizado forma automática o manual, esto dependiendo de la necesidad del negocio.

A continuación, se detalla las técnicas de balanceo de carga que existen

A) Balanceo Round Robin**:** Es un tipo de balanceo común que distribuye el tráfico de forma uniforme y sin analizar recursos de cada server, envía el tráfico de una solicitud de forma cíclica, es decir cada servidor presenta aproximadamente la misma cantidad de tráfico, como por ejemplo envía

la primera solicitud al servidor A, segunda solicitud al servidor B, tercera solicitud al servidor C, de no encontrarse servidores adicionales inicia el ciclo de envió de tráfico con el servidor inicial A. (SitMexico, 2016)

B) Ratio**:** Este tipo de balanceo realiza la distribución de tráfico por pesos, distribuyendo el tráfico al servidor que tiene mayor peso designado y menor cantidad de tráfico al servidor de menor peso, este método es útil cuando un servidor tiene mayor cantidad de recursos que otro. (SitMexico, 2016)

C) Least Connection: Este método de balanceo se encarga de distribuir la carga analizando los servidores que presentan menor cantidad de conexiones. Es un método de balanceo eficiente y recomendable. (F5 Networks, 2015)

D) Predictive**:** Es un método de balanceo en la cual se envía el tráfico mediante un algoritmo predictivo con la finalidad de determinar que servidor responderá más rápido a una solicitud. (SitMexico, 2016)

E) Fastest: Es un método de balanceo utilizado para distribuir la carga al servidor que responde más rápido, considerando como parámetro principal para el envío de tráfico la latencia presente en el servidor. (SitMexico, 2016)

F) Dynamic Ratio: Es un método de balanceo inteligente, es decir F5 BIG-IP LTM analiza las capacidades que tiene un servidor en torno a recursos y capacidad de respuesta, asignando un mayor peso al servidor que presenta mayor eficiencia de trabajo. (SitMexico, 2016)

Luego de detallar los tipos de balanceos existentes en servidores, se eligió el balanceo less connection para la realización del proyecto, el cual se detalla en el desarrollo del Capítulo 3.

2.2.2.4 SERVIDORES

Son sistemas físicos o máquinas virtuales las cuales tienen la capacidad de ofrecer servicios de páginas web, siempre y cuando los usuarios naveguen mediante un browser a la página web que expone el servidor, y así el servidor pueda responder, enviando su formulario para que el usuario pueda establecer el inicio de sesión.

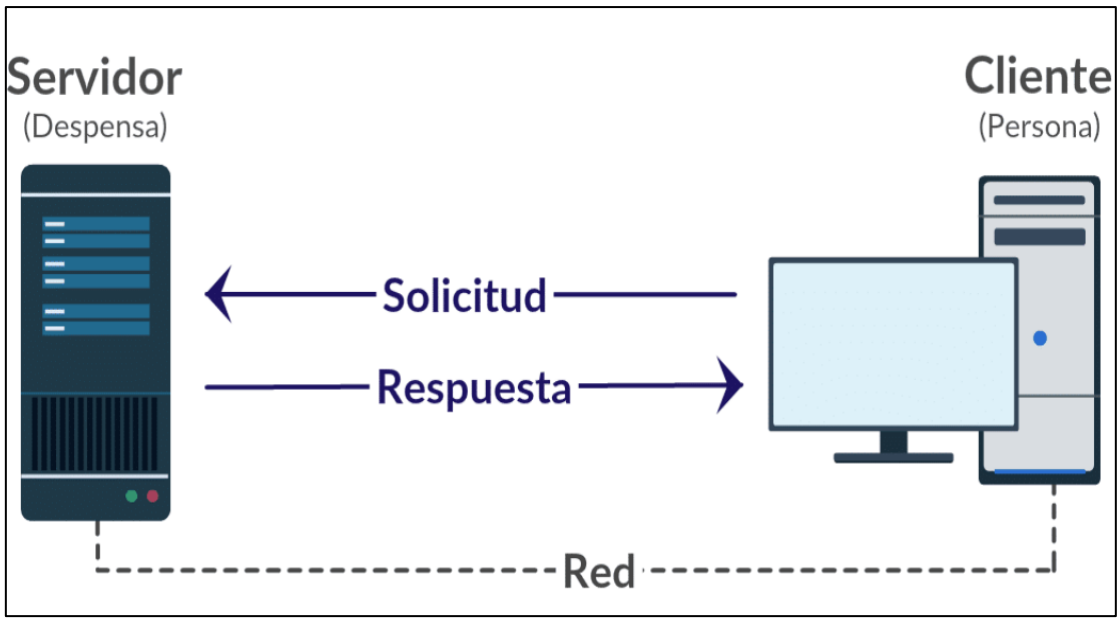
Un tipo de servidor utilizado mayormente es el:

Apache: Debido a su versatilidad para soportar trabajar con diferentes lenguajes de programación. (Carles, 2004, p.29)

A continuación, se muestra la Figura 8, en la cual se puede observar que el cliente inicia la conexión hacía el servidor destino final a lo cual el servidor responde a la solicitud, luego de validar si la web se encuentra en sus ficheros, caso contrario le responderá con un código estatus erróneo. (Bruno Chavarria & Gudiño, 2017, p.44)

Figura 8

Servidor web solicitud y respuesta



Nota. El gráfico representa la conexión entre cliente y servidor, Adaptado de *Arquitectura cliente servidor*, Siaguanta, 2019, (https://siaguanta.com/c-tecnologia/red-cliente-servidor)

2.2.3 ALTA DISPONIBILIDAD DE SERVICIO

La alta disponibilidad se refiere a la permanencia de un servicio constantemente y libre de interrupciones, es decir ante algún fallo en la red los usuarios finales no deben ser afectados. En síntesis, todo problema en la red debe ser transparente para los usuarios. (F5 Networks, 2023)

La alta Disponibilidad consiste en configurar sistemas de redundancia:

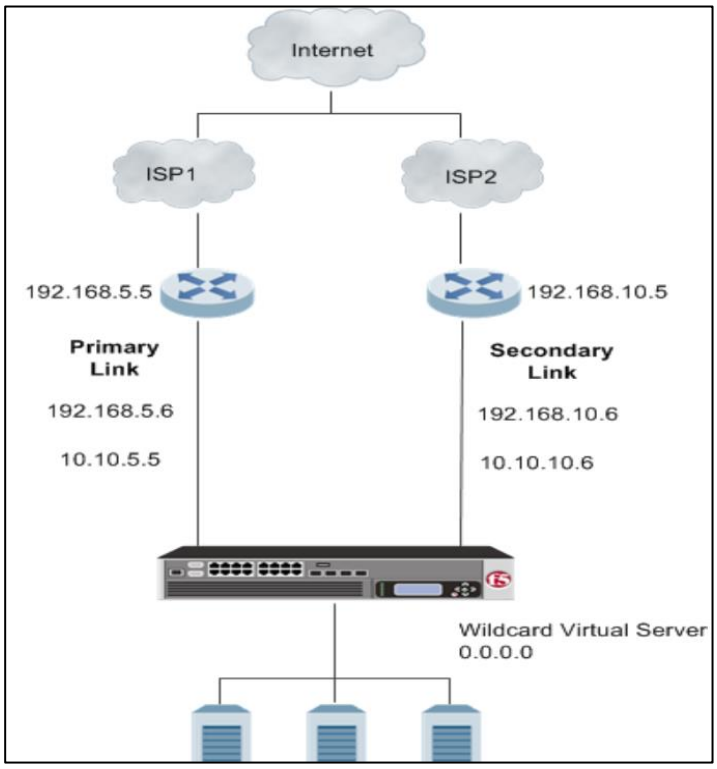
- Redundancia de enlaces de Internet – I.S.P.
- Redundancia de equipos – Cluster

2.2.3.1 REDUNDANCIA DE ENLACE DE INTERNET

Se refiere a la redundancia de los servicios a través de otro ISP (proveedor de servicio de internet), es decir cómo se muestra en la Figura 9, observamos que los servicios operan por 2 enlaces de proveedores de internet, a lo cual, ante alguna caída del enlace principal, el enlace secundario continuaría operando, siendo esto de manera transparente para los usuarios. (F5 Networks, 2023)

Figura 9

Redundancia de ISP



Nota. La gráfica representa la redundancia del enlace del principal, Adaptado de *Enlace de gestión de tráfico*, F5 Networks, 2023, (https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-link-controller-implementations/configuring-link-controller-to-manage-traffic.html)

2.2.3.2 REDUNDANCIA DE EQUIPOS - CLUSTER

Consiste en el establecimiento de una configuración de equipos en estado activo y pasivo, asegurando así la permanencia del servicio, es decir ante alguna falla en el equipo de principal, ocurriría un evento conocido como Failover, asumiendo todo el tráfico el equipo pasivo.

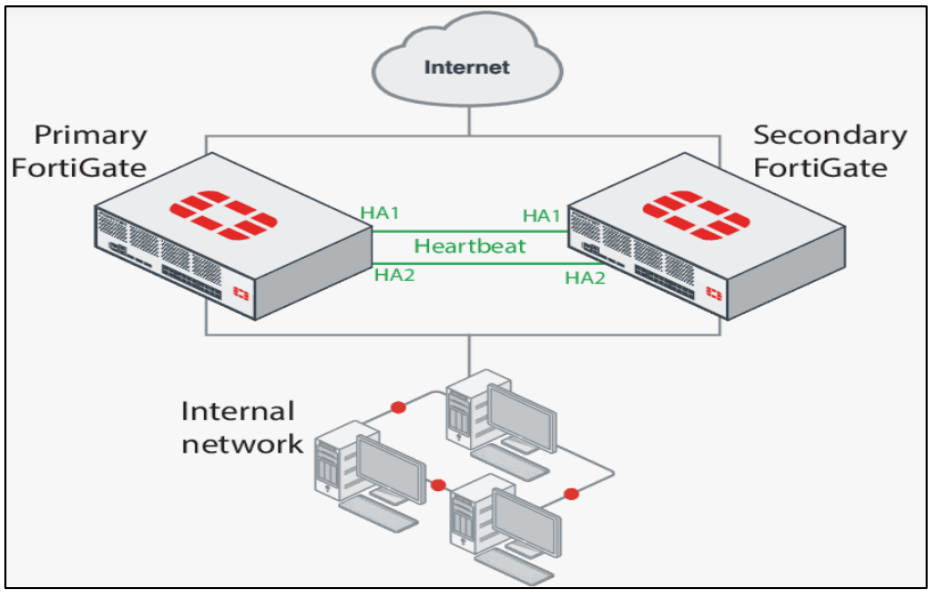
Es importante mencionar que la configuración del H.A alta disponibilidad, se podría configurar solo si ambos equipos se encuentran en una VLAN dedicada. (F5 Networks, 2023)

Funcionamiento: Los sistemas configurados en modo de alta disponibilidad son conocidos como cluster y se caracterizan por tener la capacidad de:

- Conmutación por error - Failover: Significa que, ante el fallo del equipo activo principal, automáticamente se redirecciona el tráfico al equipo redundante.
- Redundancia: Asegura la permanencia del servicio.
- Monitoreo constante: Al ser un cluster, ambos equipos se monitorean uno a otro mediante un heartbeat “el cual es un intercambio de paquetes ICMP”, que sirve de monitoreo para que ambos equipos puedan saber que se encuentran en estado UP.
- Tiempo de recuperación: Ante alguna caída de servicio, el sistema conmuta automáticamente, por lo cual el tiempo de caída de servicio es casi nulo.

Figura 10

Alta disponibilidad de equipos modo activo - pasivo



Nota. El gráfico representa la configuración de un sistema en alta disponibilidad, Adaptado de *Fortigate H.A*, BITS, 2022,(https://bits.com.mx/fortigate-high-availability-ha)

2.2.4 VERIFICACIÓN DE TRANSMISIÓN DE DATOS EN LA RED

La transmisión de datos se refiere a la comunicación entre un conjunto de elementos, ya sean físicos o virtuales, dentro una red. Estos elementos tienen la capacidad de intercambiar información entre sí a través de un medio LAN (red de área local) o WAN (red de área amplia), entablando una comunicación mediante una ruta virtual, durante este proceso de comunicación se intercambian datos que se conocen como paquetes. (Liberatori, 2018, p.34)

Además, en lo que respecta al intercambio de paquetes en la red, es esencial contar con un formato que permita definir las reglas que gobiernen dicho intercambio, a esta estructura se le conoce como protocolo. (Liberatori, 2018, p.35)

2.2.4.1 VERIFICACIÓN DE CONEXIÓN - PROTOCOLO TCP/IP

El protocolo utilizado para la verificar la correcta transmisión de paquetes en la red en internet es denominado como TCP/IP (Protocolo de control de Transmisión / Protocolo de Internet), el cual explica la comunicación que existe desde un equipo cliente hacia un servidor destino. (Liberatori, 2018, p.36)

Como se puede observar en la Figura 11, la comunicación se origina en el equipo cliente, donde paquete enviado se encripta, dicho paquete incluye información esencial como la dirección IP, puerto, etiquetas y el tamaño del paquete. Estos datos son interpretados por el servidor receptor para luego continuar con la respuesta del mensaje recibido.

Figura 11

Transmisión de paquetes Protocolo TCP/IP

Nota. El gráfico representa la comunicación TCP/IP, Adaptado de *Comparando protocolos TCP y UDP*, Nord Security, 2023, (https://nordvpn.com/es/blog/protocolo-tcp-udp/)

2.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Attack Brutte Force:** Se refiere al mecanismo de intento de vulnerar un sistema mediante la combinación de usuario y password, para así lograr descubrir las credenciales correctas. (Networks, 2023)

- **ASM Rule:** Es una política de seguridad de F5 utilizada para filtrar tráfico malicioso intrusivo en las aplicaciones web de capa 7. (F5 Networks, 2021)

- **Balanceo:** Es el encargado de realizar la distribución del tráfico en los servidores que se encuentran operativos. (F5 Networks , 2023)

- **Ciberseguridad:** Se refiere a la protección de las amenazas, de riesgos que se tienen en una organización sobre los equipos informáticos. (Romero et al., 2018, p.25)

- **Exchange server:** Sofware que opera sobre un servidor, ejecutando una aplicación de correo electrónico. (comparitech, 2023)

- **Firewall:** Es un dispositivo encargado de proteger la red interna de los ataques provenientes de la red pública. (Briceño, 2021, p.80)

- **F5 ASM:** Access Security manager, es un firewall de aplicaciones que tiene la funcionalidad de añadir firmas de seguridad para la protección de aplicaciones. (F5 Networks, 2013)

- **F5 LTM:** Local traffic manager, es un software inteligente que gestiona el tráfico de la red, mediante balanceos de carga. (F5 Networks, 2023)

- **H.A:** High availability, es un sistema de redundancia o como también se le conoce como cluster, tiene la función de asegurar la persistencia del

servicio, ante alguna falla en la red, realizando una conmutación de tráfico al servidor que no presenta problemas. (F5 Networks, 2023)

- **Heartbeat:** Son paquetes de icmp enviados en un cluster de equipos activo y pasivo, con la finalidad de conocer que los sistemas se encuentran disponibles, de no recibir paquetes de su equipo par, F5 realizará inmediatamente el failover. (F5 Networks, 2021)

- **HTTP**: Es un protocolo inseguro y la información se puede observar en texto plano. (Editorial Etecé, 2021, p.1)

- **HTTPS:** Es un protocolo seguro utilizado para establecer conexiones seguras mediante tráfico cifrado, es la versión segura de HTTP. (Chavarria & Gudiño, 2017, p.61)

- **IAPPS:** template de Aplicaciones de servicios, es una plantilla utilizada para integrar las aplicaciones Web complejas con F5 WAF, su aplicación se realiza completando datos de un formulario de la aplicación web a integrar (F5 Networks, 2017, p.3)

- **ICMP:** Es utilizado para diagnosticar problemas de red, se utiliza de una manera fácil y sencilla, es para validar si existe comunicación con el destino. (Cloudflare, 2023)

- **ISP:** Proveedor de servicio de internet. Utilizado para asegurar la redundancia del servicio a través de otro proveedor. (Ariganello, 2014, P.343)

- **LAN:** Local Area Network, Se refiere a un ambiente relativamente pequeño donde se encuentran equipos informáticos interconectados. (Ariganello, 2014, p.341)

- **OWA:** Microsoft Exchange Outlook web access, Es utilizado para el acceso al correo electrónico desde la red pública, desde cualquier equipo conectado a la red, mediante la configuración de un template de integración con F5 Big IP. (F5 Networks , 2017, p.5)

- **TLS:** Transport layer Security, Son utilizados para establecer una conexión segura a través de internet. (Varela, 2023).

- **TCP/ IP:** Protocol control transmissión / Protocol Internet, Es utilizado para definir en conjunto de reglas de comunicación entre dos equipos o más dentro de la red.

- **WAN:** Wide Area Networks, Se refiere a un ambiente geográficamente grande, que interconecta varias LAN. (Ariganello, 2014, p.341)

- **WEB:** Se refiere a un espacio lógico que opera en un ambiente virtual. (Universidad de Chile, 2008, p.9)

CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL

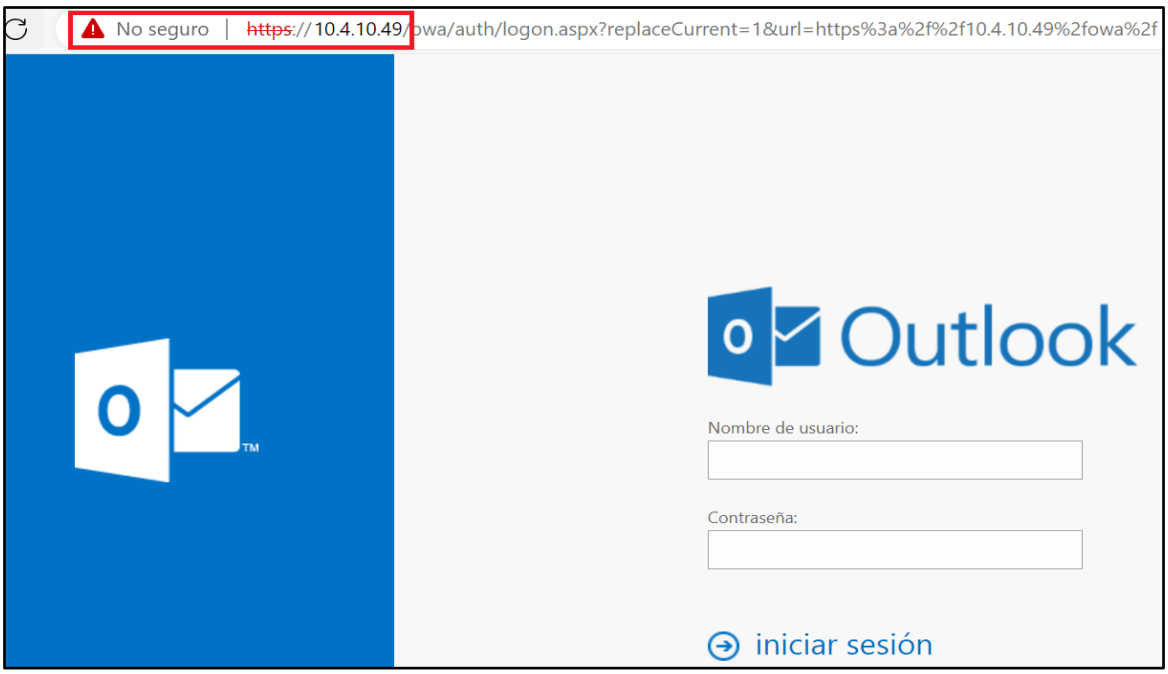
3.1 DETERMINACIÓN Y ANÁLISIS DEL PROBLEMA

Securesoft Corporation S.A.C, Durante una verificación de los servicios brindados identificó que; uno de los clientes del sector Bancario, no tenían acceso vía web al correo electrónico OWA desde la red pública (internet), solo tenían acceso desde la red interna; por lo cual acceder a sus buzones de correo era posible asistiendo presencialmente a la entidad bancaria y conectándose a la red interna mediante un cable de red, wifi o mediante una conexión VPN (lo cual implica gestión de permisos en distintas áreas).

Sumado a esto, la arquitectura del acceso al correo electrónico interno no era segura, los usuarios se conectaban ingresando en el navegador o browser la IP del servidor "10.4.10.49", para así acceder al buzón de correo, como se puede observar en la Figura 12.

Figura 12

Acceso al Correo Electrónico



Nota. El gráfico representa el acceso no seguro al correo electrónico Interno

Conforme a lo mostrado en la Figura 12, esto es una mala práctica debido a que; ante alguna intrusión en la red interna o algún trabajador con conocimientos básicos de hacking, podría explotar alguna vulnerabilidad del servidor de correo, y

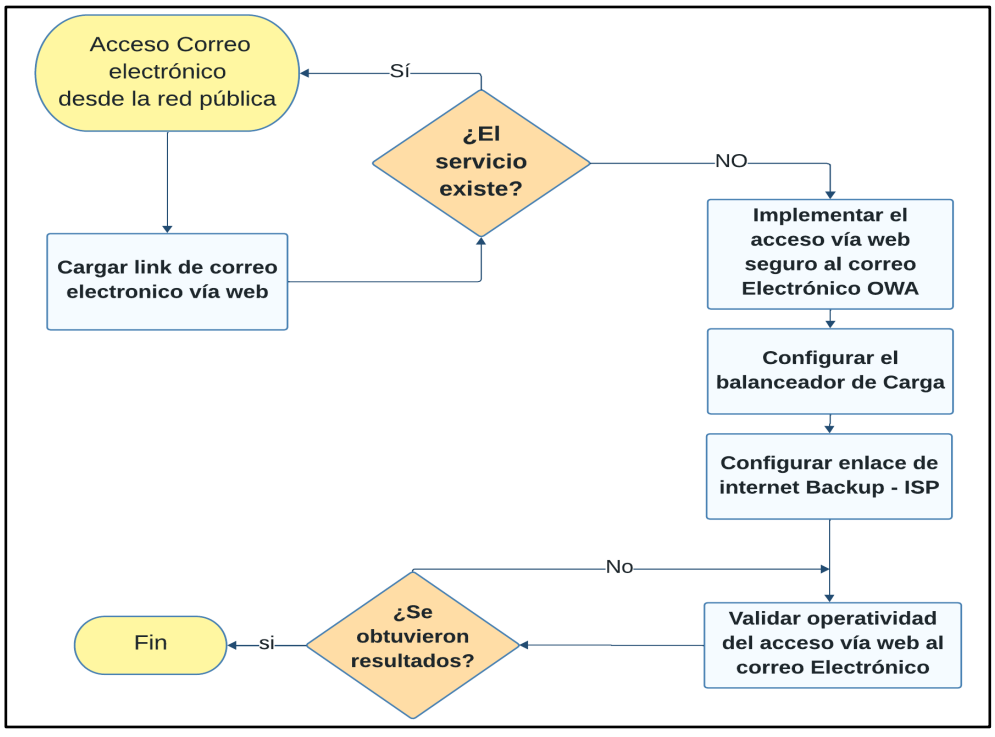
filtrar todo tipo de información del servidor, la cual al ser un Banco maneja información sensible. Sumado a esto, se observó que no había medidas de permanencia de servicio, lo que significa que no había redundancia ante algún fallo en la red. Por lo tanto, si el servidor falla, todos los usuarios perderían el acceso al buzón de correo.

Considerando todos los problemas descritos, la gerencia de Ingeniería – Soporte Onsite, Comunicó la urgencia de realizar la implementación del acceso vía web al correo electrónico Owa de forma segura, tanto accesible desde la red interna y externa (internet), con balanceo de carga y alta disponibilidad de enlace ISP mediante un equipo firewall de aplicaciones F5 BIG IP ASM, equipo físico que presentaba otras aplicaciones en ejecución, pero no el servicio del acceso vía web al correo electrónico.

La planificación y ejecución del trabajo se llevó a cabo bajo la supervisión del supervisor de ingenieros Onsite asignado a la entidad bancaria, quien procedió a asignarme la tarea como ingeniero a cargo del proyecto - implementación del acceso vía web al correo Electrónico OWA mediante el F5 BIG-IP modelo 4000s. Como se detalla en la Figura 13.

Figura 13

Implementación del acceso vía web al correo Electrónico OWA



3.2 MODELO DE SOLUCIÓN PROPUESTO

3.2.1 CONTRIBUCIÓN PARA EL DESARROLLO DEL TRABAJO

Durante mi experiencia profesional, aprendí que las competencias y habilidades claves no solo están conformadas por conocimiento técnico, sino que, las habilidades blandas son esenciales para expresar, aplicar y enseñar lo que sabemos. Por lo tanto, las asignaturas como Liderazgo, Emprendedores I y II, me ayudaron a identificar mis fortalezas y debilidades y ganar la confianza para liderar proyectos o proponer soluciones de problemas de manera proactiva.

Este punto es significativo ya que me permitió tener la confianza de liderar como ingeniero asignado del Proyecto a un cliente importante como es el caso una entidad bancaria.

Para la realización del trabajo, las asignaturas que forman una base esencial en el aspecto técnico del campo de ingeniería fueron; Administración de Redes y Arquitectura de redes de Protocolos, debido a que establecieron las bases teóricas para comprender el flujo de conexión entre equipos dentro de una red digital.

Así mismo para los cursos especialización es fundamental presentar conocimientos básicos de redes, de esta manera los conocimientos adquiridos me permitieron entender y estar al día con información actualizada y necesario para adquirir certificaciones de los Fabricantes de las soluciones de ciberseguridad, lo cual brindó la confianza y credibilidad para ser asignado como ingeniero a cargo del proyecto de acceso vía web al correo electrónico OWA.

Cursos internacionales que contribuyeron a la implementación del proyecto

- NS3 Firewall Fortinet: **W7oMg0Neqf** (código de validación de certificado)
  La contribución que brindo el curso para la realización del proyecto fue el aprender a configurar reglas de protección de tráfico malicioso de la red.
- IU_Database Security and Compliance Course: **hrq7ud4hszcu**
  La contribución que permitió el curso de base de datos fue aprender a configurar servidores de aplicación que son protegidos por el equipo firewall.
- IU_Administering Imperva Security Infrastructure: **yxy77acqq6px**
  Su contribución fue permitirme conocer todos los equipos que conforman una red y cómo realizar la integración de equipos de diferentes fabricantes.

3.2.2 IMPLEMENTACIÓN DEL ACCESO VÍA WEB AL CORREO ELECTRÓNICO

Como etapa inicial del proyecto, la arquitectura de red para la implementación del acceso vía web al correo electrónico OWA, fue definida por el área de Ingeniería Securesoft bajo la supervisión del supervisor Ingenieros Onsite en colaboración con el Gestor de proyectos de la entidad bancaria.

Por tanto, como ingeniero asignado a cargo del proyecto, procedí con la implementación del presente trabajo, tal como se puede observar en la Figura 14, se realizó la integración de 3 servidores de correo mediante dos firewalls de aplicaciones F5 WAF ASM, uno en modo activo (Firewall primario) y el segundo equipo en modo pasivo (Equipo Backup o secundario), así mismo se configuró los equipos F5 WAF ASM para realizar balanceo de carga hacía los 3 servidores Exchange de correo electrónico, distribuyendo así el tráfico de conexiones y asegurando la permanencia del servicio ante algún fallo de la red.

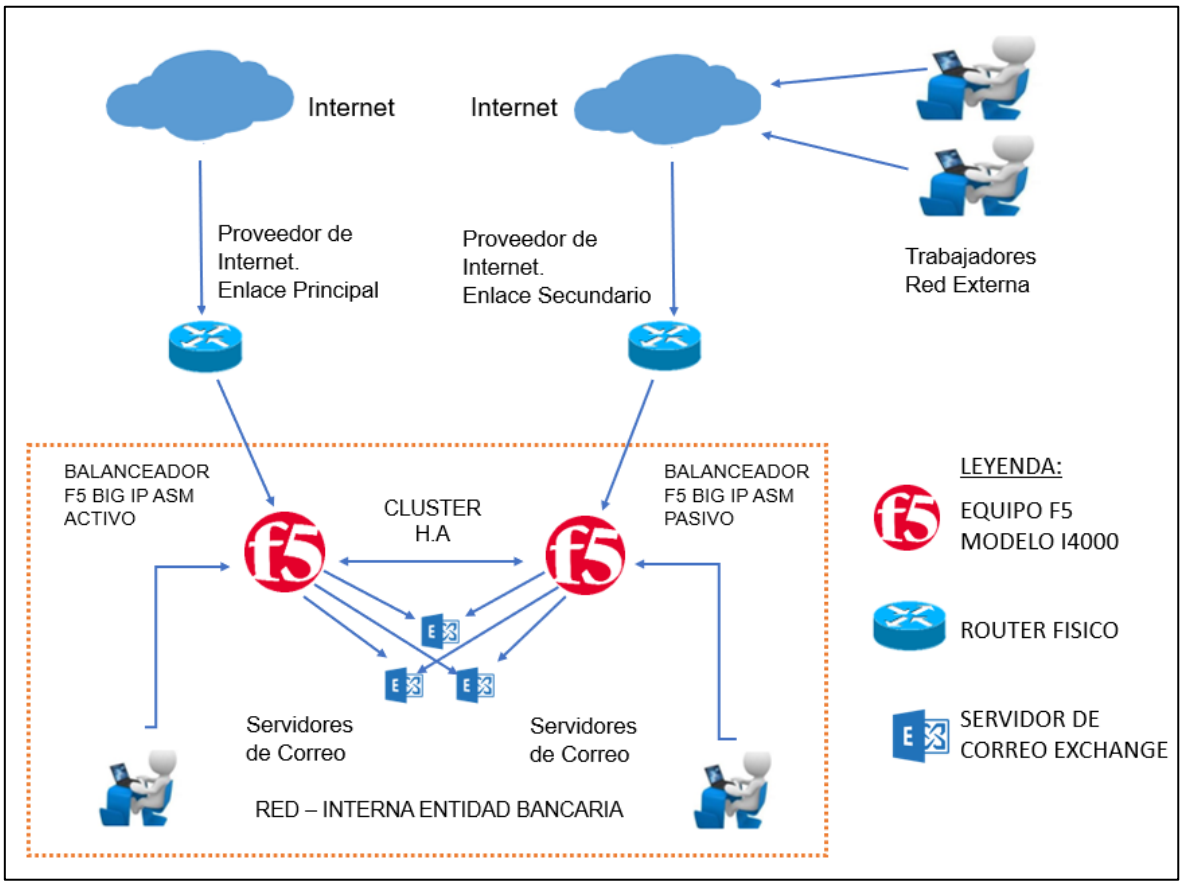
Posteriormente, luego de validar la configuración del cluster H.A (Activo - Pasivo) y balanceo de carga, se configuró reglas de ciberseguridad (ASM), protegiendo así el acceso vía web al correo electrónico OWA ante los diversos ataques de la red pública.

Finalmente se configuró la redundancia de enlace con diferentes proveedores de internet (ISP), para así evitar pérdidas del servicio ante alguna caída del enlace principal.

La Figura 14, nos brinda un panorama de las conexiones externas por parte de usuarios que navegan a través de internet y las conexiones internas referente a usuarios que acceden al correo electrónico mediante la red corporativa. Todo el tráfico es procesado por el equipo F5 BIG IP ASM, quien realiza el balanceo del tráfico hacía los 3 servidores de correo, y así mismo brinda la protección ante ataques de índole malicioso.

Figura 14

Implementación del acceso vía web correo electrónico – Solución Propuesta



Nota. El gráfico representa la arquitectura propuesta para el Acceso a correo electrónico

Para la implementación del proyecto es necesario dar a conocer si el modelo del equipo seleccionado (F5 BIG IP modelo 4000s), la cual soporta la integración con la aplicación de correo electrónico OWA, como también se validó si presenta recursos libres, tales como memoria, CPU y Disco.

En el apartado 3.2.2.1 se detalla las especificaciones del equipo F5 BIG IP ASM utilizados, en el apartado 3.2.2.2 la factibilidad de la integración del equipo F5 BIG IP con la aplicación de correo, como también en el apartado 3.2.2.3 se sustenta la validación de los recursos disponibles en el equipo, en el apartado 3.2.3 se detalla la implementación del balanceo de carga y en el apartado 3.2.4 la configuración de un enlace de redundancia con el proveedor de internet secundario, finalmente la validación de los resultados se detallaron en el apartado 3.3.

3.2.2.1 ESPECIFICACIONES DEL EQUIPO F5 BIG IP ASM

F5 BIG IP ASM conocido también como firewall de aplicaciones, presenta la funcionalidad de balanceador de carga, brindado por el módulo LTM y de seguridad ante ataques desde la red pública brindado por el módulo ASM.

El modelo utilizado en el presente trabajo es el 4000s como se puede observar en el Anexo 2 y versión de software 15.1.6.1 build 0.0.10.

A continuación, en la Tabla 1 se muestran las especificaciones de los equipos F5 BIG IP ASM.

Tabla 1

Parámetros de configuración

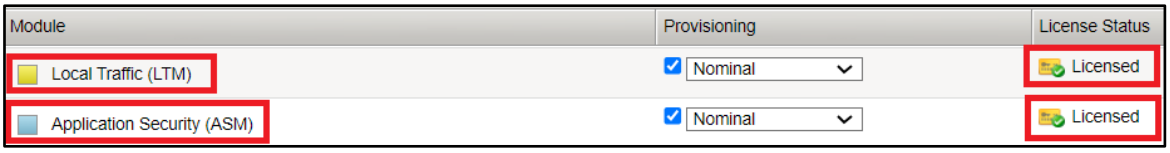
Balanceador	ítems	Especificaciones
F5 BIG IP	Módulos	LTM – ASM
	Versión	15.1.6.1 Build 0.0.10
	Modelo	4000s
	IP Gestión – F5 Activo	10.1.17.10
	IP Gestión – F5 Pasivo	10.1.17.11
	F5 Activo – Nombre	BIGIP.F5.COM.PE
	F5 Pasivo – Nombre	BIGIP2.F5.COM.PE
	IP Gateway	10.1.17.1

Nota. La tabla 1 representa los Parámetros de configuración F5 BIG IP ASM

Conforme a lo descrito, se observa en la Figura 15, los módulos LTM (Local Traffic) y ASM (Application Security) los cuales se encuentran licenciados, con lo cual podemos sustentar que es posible realizar la funcionalidad de balanceo de carga y protección de ataques maliciosos.

Figura 15

Módulo LTM Y ASM activos en F5 WAF ASM



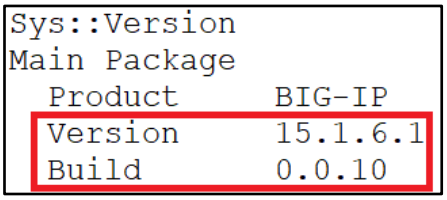
Nota. El gráfico representa los módulos licenciados F5 BIG IP

3.2.2.2 COMPATIBILIDAD DE CORREO ELECTRÓNICO Y F5 BIG IP ASM

Para la validar la factibilidad de la integración de F5 BIG IP con el correo electrónico Outlook web, en primer lugar, se verificó en la documentación publicada por F5 Networks, donde se logró validar que es posible realizar la implementación del acceso vía web al correo electrónico OWA mediante F5 BIG IP, solo si la versión de Software es mayor a la versión 11.x, a lo cual se verificó que el equipo seleccionado para la implementación cumple con el requisito de una versión superior a lo establecido, como se puede observar en la Figura 16, el F5 BIG IP presenta la versión 15.1.6.1 Build 0.0.10.

Figura 16

Versión equipo F5 BIG IP

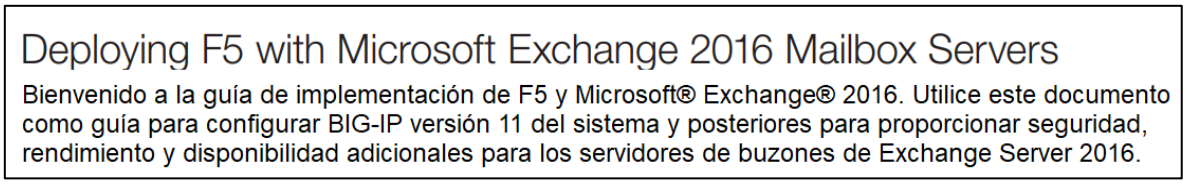


Nota. El gráfico representa la versión de Software instalado F5 BIG IP ASM

Adicional a lo sustentado la documentación KB11163, publicado por F5 Networks brinda veracidad que la integración entre F5 BIG IP ASM y los servidores de correo es posible desde la versión 11.x y posteriores (Como se puede observar en la Figura 17).

Figura 17

Integración F5 BIG IP con servidores de correo electrónico



Nota. Compatibilidad F5 BIG-IP y Servidores Correo, Adaptado de *Implementacion de F5 con servidores de correo exchange 2016*, F5 Networks, 2019, (https://www.f5.com/pdf/deployment-guides/microsoft-exchange-2016-dg.pdf)

Es importante mencionar este punto que F5 presentó la última versión de IAPP la cual es exchange 2016 (Como se observó en la Figura 17), pero a su vez está

misma IAPP es utilizada para exchange 2019, lo mencionado se consultó en el portal comunity F5 Networks, (Conforme a lo mostrado en la Figura 18).

Figura 18

Validación de Template IAPP exchange server 2016 y 2019

Descripción

Hola, por favor,
Tenemos una pregunta. ¿La plantilla F5 para exchange 2016 es la misma para exchange 2019?
En realidad, tenemos IAPP Exchange 2016 pero el cliente implementará Exchange 2019, por este motivo queremos saber si necesitaremos configurar una nueva plantilla.
Sé que el soporte de la plantilla AIPP finalizó, pero tenemos preguntas sobre si podemos usar la plantilla IAPP 2016 a 2019 o si es necesaria una configuración diferente para trabajar con Exchange 2019.
Busqué información al respecto, pero entendí que los IAPP para exchange 2016 son los mismos para exchange 2019, ¿Pueden confirmar mi pregunta?
por favor, ¿puedes agregar mi correo electrónico: kcueva@securesoftcorp.com?
atentamente
Kent Cueva

Nota. Validación de compatibilidad de template Exchange 2016 y 2019, Adaptado de *F5 IAPP para exchange 2019* ,F5 Networks, 2023, (https://community.f5.com/t5/technical-forum/iapp-for-mail-exchange-2019/td-p/296125)

Como se observa en la Figura 19, nos compartieron documentación respecto a la veracidad de que Exchange 2019 opera con la versión de Exchange 2016 a nivel de F5 BIG IP.

Figura 19

Respuesta portal Comunidad F5 – IAPP Exchange 2016 y 2019

Enviado el: martes, 31 de Agosto de 2022 02:54
Asunto: F5 PREGUNTA ACERCA IAPP F5 EXCHANGE 2016 AND 2019

Hola **Kent**,

Buenos días,

Basado en los casos revisados internamente, Si el IAPP Exchange 2016 es utilizado con el deploy Exchange 2019.

https://community.f5.com/t5/technical-forum/iapp-for-mail-exchange-2019/td-p/296125

Saludos

Nota. Respuesta de consulta de compatibilidad Exchange 2016 y 2019, Adaptado de *Dev central Comunity IAPP exchange 2019*,F5 Networks, 2023, (https://community.f5.com/t5/technical-forum/iapp-for-mail-exchange-2019/td-p/296125)

La última plantilla publicada por F5 Networks para aplicaciones de correo electrónico web presenta en el nombre de servicio el año 2016 (microsoft_Exchange_2016 v1.0.2), esto hace referencia a la versión del producto publicado, por lo cual la versión del producto es independiente del año publicado, como se puede observar en la Figura 20, se muestra las ultimas 3 versiones disponibles publicadas por Microsoft, siendo Exchange 2019 la última.

Figura 20

Versiones disponibles para Microsoft Exchange

Ciclo de vida del servidor Microsoft Exchange

Una vez que Exchange Server 2013 finalice su vida útil, quedarán **2 versiones compatibles: 2016 y 2019.**

Versión	Fin de la vida
Servidor Exchange 2013	11 de abril de 2023
Servidor Exchange 2016	14 de octubre de 2025
Servidor Exchange 2019	14 de octubre de 2025

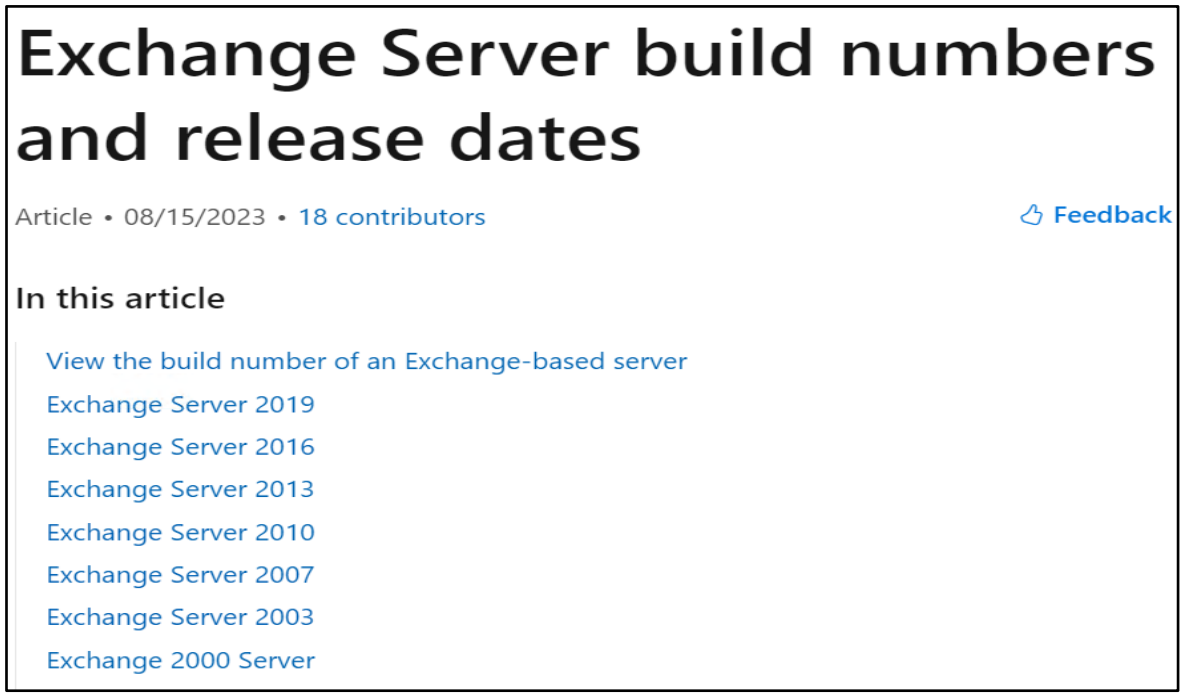
Nota. Tiempo de vida de versiones de soportadas por Microsoft, Adaptado de *Microsoft ciclo de vida*, Lansweeper, 2023, (https://www.lansweeper.com/eol/microsoft-exchange-server-end-of-life)

Así mismo, se precisó que a nivel de F5 BIG IP; si el cliente utilizó la versión de correo electrónico OWA 2016, y desea implementar la versión de Microsoft exchange 2019, a nivel de F5 BIG IP no sé realiza cambios. El témplate IAPP exchange 2016 es el mismo utilizado para OWA 2019, conforme a lo compartido previamente en la Figura 19.

A continuación, se detalla las versiones disponibles brindadas por Microsoft, y así verificar que no hay versiones disponibles de correo después de Exchange 2019, como se puede observar en la Figura 21, se verifica que existen versiones inferiores iniciando el año 2000 hasta la versión 2019, la cual es la última disponible por parte de Microsoft.

Figura 21

Versiones disponibles Servidores de correo Exchange



Nota. El gráfico representa las versiones disponibles para servidores de correo, Adaptado de *Microsoft versiones publicadas*, Microsoft, 2023, (https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019)

Finalmente, luego de validar la factibilidad de la implementación en la integración de los servidores de correo mediante F5 BIG IP ASM, utilizando IAPP 2016 exchange server.

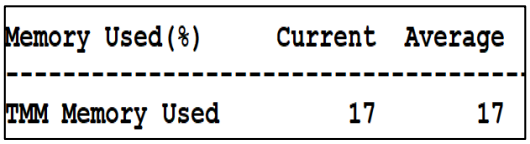
Se realizó la validación de recursos disponibles, donde se verificó que F5 BIG IP ASM presenta los recursos necesarios tales como, Memoria y CPU disponibles para soportar la implementación de una nueva aplicación web a proteger y realizar el balanceo de tráfico.

3.2.2.3 VERIFICACIÓN DE RECURSOS DEL EQUIPO - F5 BIG IP ASM

Luego de verificar que F5 BIG IP ASM es compatible la aplicación de correo electrónico web, para continuar con la implementación del servicio mediante F5 BIG IP ASM, es necesario evaluar los recursos del módulo LTM (local traffic manager) que utiliza la TMM memory, módulo encargado de ejecutar los procesos de balanceo de carga y configuración de la integración de la aplicación de correo electrónico OWA, Por lo tanto es indispensable contar con memoria libre para la implementación, a lo cual como se puede observar en la Figura 22, la memoria utilizada en el equipo es un 17% de un total de 100%.

Figura 22

Memoria módulos LTM, ASM y Other Memory

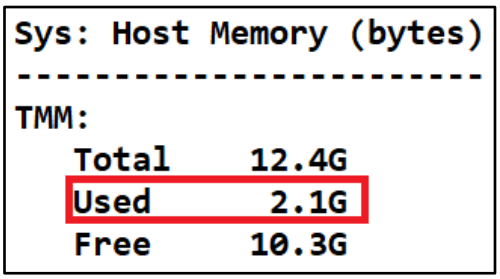


Nota. El gráfico representa la Memoria TMM utilizada en F5 BIG IP

Y en términos numéricos el 17% representa el 2.1G de un total de 12.4G, conforme a lo mostrado en la Figura 23.

Figura 23

Memoria TMM - F5 LTM



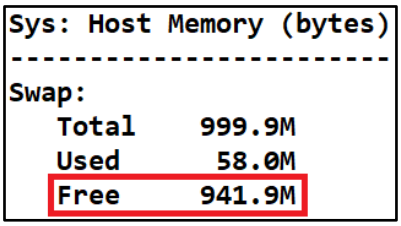
Nota. El gráfico representa la Memoria TMM del Módulo LTM

Memoria SWAP, memoria utilizada para la protección de aplicaciones web configuradas, este tipo de memoria hace referencia al módulo ASM, la cual se validó que el equipo F5 BIG IP tiene libre un 94.19% (941.9M) de su capacidad total (como se puede observar en la Figura 24), es decir el equipo solo utiliza alrededor del 0.58% de memoria (58M), por lo tanto, podemos concluir que, a nivel de memoria swap, se tiene libre un 94.19% (941.9 M), lo cual fue óptimo para la

implementación de la aplicación de correo electrónico para el acceso vía web desde la red pública.

Figura 24

Memoria SWAP - Módulo F5 ASM



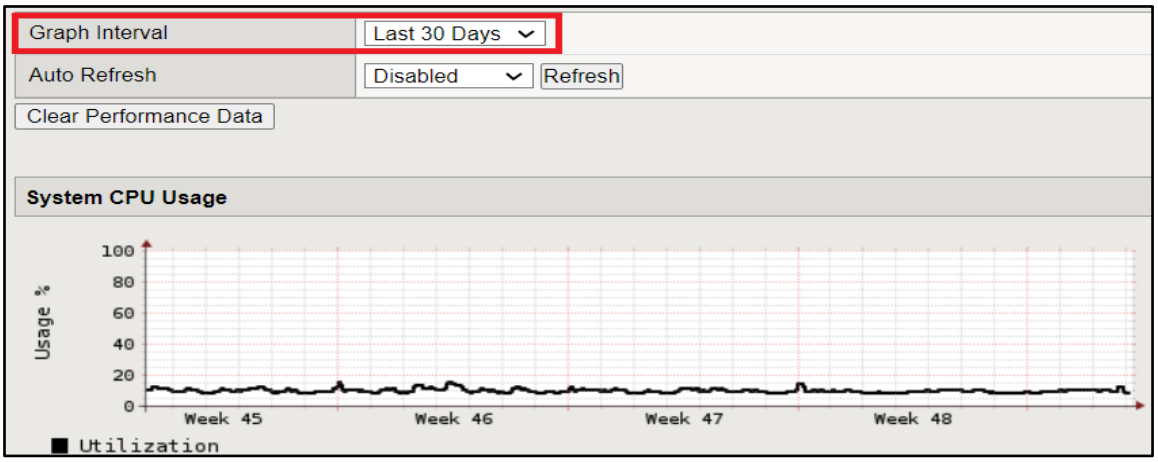
Nota. El gráfico representa la Memoria Swap utilizada y libre en el módulo ASM

Bajo este escenario se validó que los recursos a nivel de memoria en el equipo F5 BIG IP ASM son óptimos para realizar la configuración del balanceo de los servidores de correo electrónico y así implementar el acceso vía web para el servicio de correo electrónico OWA.

Finalmente se realizó la validación de recursos – CPU, Conforme a lo mostrado en la Figura 25, se extrajo una captura en un rango de 30 días, para verificar el comportamiento del CPU del equipo F5 BIG IP, de esta manera se validó si el equipo tenía algún exceso de consumo de CPU que pueda causar problemas en la integración de F5 BIG IP ASM con la aplicación de correo electrónico, de lo cual se observa que oscila entre el 0-20% de utilización, verificando de esta manera que el equipo no presenta problemas de CPU y puede trabajar de manera óptima.

Figura 25

CPU equipo F5 BIG IP ASM



Nota. El gráfico representa el comportamiento de CPU del F5 BIG IP ASM

3.2.3 CONFIGURACIÓN DE BALANCEO DE CARGA

El primer paso para la configuración de la integración del balanceo de los servidores de correo exchange y F5 BIG IP ASM, es ingresar vía web al balanceador F5 WAF ASM, mediante un navegador web y colocar la IP de gestión del equipo (IP address - 10.1.17.10), como se muestra a continuación en la Figura 26.

Figura 26

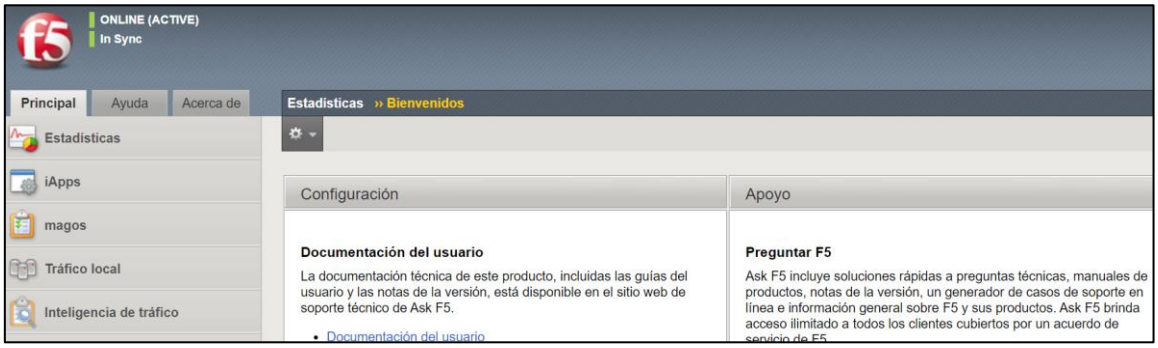
Login F5 WAF

Nota. El gráfico representa el acceso al equipo F5 BIG IP ASM vía web

Luego de ingresar en el equipo se observará una vista conocida como interfaz gráfica de usuario (Como se muestra a continuación en la Figura 27).

Figura 27

Interfaz de Gráfica de Usuario



Nota. Interfaz de configuraciones F5 BIG IP ASM

Posteriormente nos dirigimos al apartado IApps→ Applications Services, donde se debe de rellenar un formulario para la configuración de la integración de F5 BIG IP y los servidores de correo, estos datos son referentes a la Aplicación a integrar.

3.2.3.1 PARÁMETROS DE CONFIGURACIÓN DE BALANCEO DE CARGA

La información de los parámetros a configurar es proporcionada por la entidad bancaria, como se muestra en la Tabla 2, son datos únicos que dependen de la aplicación del cliente.

Tabla 2

Formulario de aplicación de Correo a integrar con F5 BIG IP

Formulario	Configurar	Datos
Configurar balanceo de carga de servidores de correo	Si	------
¿Desean utilizar el módulo APM?	NO	------
¿Desean implementar el módulo AFM?	NO	------
¿Desean tráfico encriptado?	SI	------
¿Se desea encriptar el tráfico en la comunicación F5 y servidores de correo?	SI	------
¿Se desea utilizar certificado SSL seguro?	SI	------
¿Se desea limitar el número máximo de conexiones de usuarios menor a 6000?	SI	------
¿Cuál es la IP pública a utilizar?	-----	20.6.25.154
¿Se desea deploying Microsoft Outook, including EWS y OAB?	SI	------
¿Qué protocolo se desea habilitar?	-----	HTTPS
¿Se desea habilitar ActiveSync?	SI	------
¿Se desea habilitar Autodiscover?	SI	------
¿Se desea habilitar POP3 y IMAP4?	NO	------
¿Cuáles son las IPs de los servidores de correo?	-----	10.20.100.108 10.20.100.109 10.20.100.110
¿Cuál es el FQDN para las conexiones de los usuarios mediante los navegadores de internet?	-----	BancoTI.Peru.com.pe

Nota. La Tabla 2 representa los parámetros de configuración de plantilla de Correo Electrónico

Para acceder al formulario a configurar se debe de hacer click en:

IApps→ Applications Services→ New Application Service

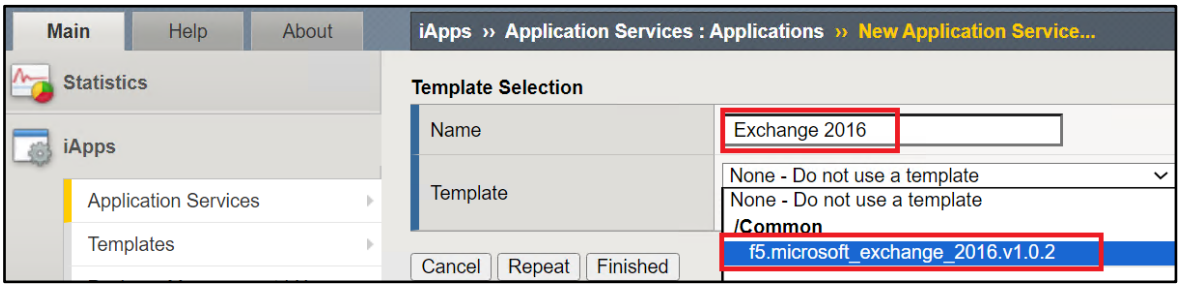
Se puede observar en la Figura 28, la aplicación de correo disponible tiene el nombre de F5 Microsoft_exchange_2016 v1.0.2 (última versión disponible

publicado por F5 el 24-10-2019, para integrar correo electrónico OWA 2016 o 2019, con F5 BIG IP ASM, la documentación que sustenta lo mencionado fue mostrada en la Figura 17.

Así mismo luego de seleccionar la aplicación a integrar conforme a lo mostrado en la Figura 28 y configurar el nombre de la Aplicación de correo con la etiqueta de Exchange_2016, se procede a iniciar la configuración de la integración de los servidores de exchange 2016 y el balanceo de carga.

Figura 28

Configuración IAPP aplicación de Correo Electrónico Exchange 2016



Nota. El gráfico representa la Implementación de la plantilla de correo *electrónico*

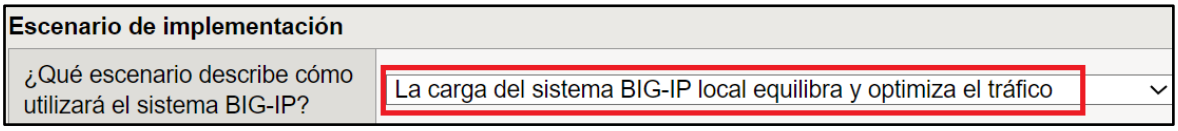
Con los datos compartidos por la entidad bancaria (conforme a lo compartido en la Tabla 2), se procedió a configurar el formulario de integración de la aplicación de correo electrónico en el equipo F5 BIG IP ASM.

3.2.3.2 CONFIGURACIÓN DE PLANTILLA DE BALANCEO DE CARGA

El proceso de configuración del IAAP- plantilla de correo electrónico OWA 2016 se completó con los datos compartidos por el cliente. El paso número uno es elegir el sistema de operación, como se muestra en la Figura 29, la configuración elegida es el balanceo de tráfico de servidores.

Figura 29

Paso 1 - Configuración de Balanceo de tráfico

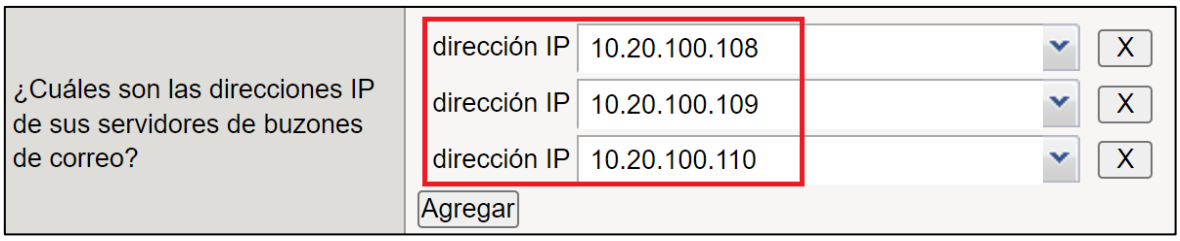


Nota. Plantilla de Selección del método de Balanceo de carga

Luego de configurar el balanceo de carga, el formulario nos solicita que servidores serán balanceados, por lo cual en la Figura 30 detalla las IPs (10.20.100.108, 10.20.100.109,10.20.100.110) pertenecientes a los servidores de correo exchange.

Figura 30

Paso 2 - Servidores de Correo Electrónico a balancear



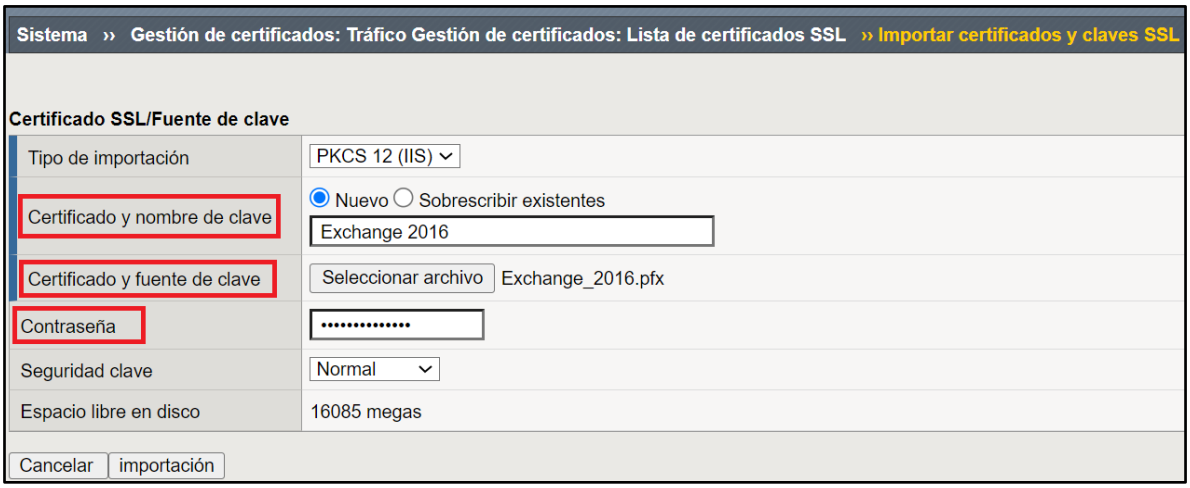
Nota. Configuración de las direcciones IPs de los servidores de correo

Tras la configuración del balanceo de carga de los servidores de correo exchange, es esencial establecer un protocolo seguro que garantice una comunicación encriptada entre el equipo F5 BIG IP ASM con los servidores de correo. Para ello se requiere importar un certificado de correo electrónico en el equipo F5 BIG IP ASM, por lo cual resultó esta tarea imprescindible previo a continuar con la configuración del formulario de correo electrónico.

Para configurar el certificado SSL en el equipo F5 BIG IP se realizó los siguientes pasos: **System→ Certificate Management→ Uploaded**

Figura 31

Paso 3 - Importar certificado SSL a utilizar



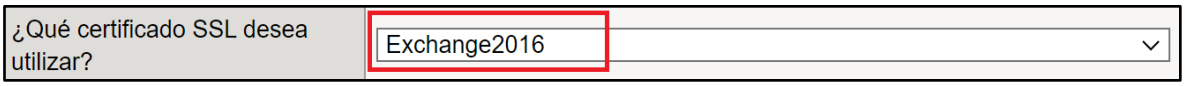
Nota. El gráfico representa el SSL Certificado importado en el equipo F5 BIG IP

Luego de importar el certificado en el F5 BIG IP ASM, se continúa con la configuración de la plantilla, se asocia el certificado importado previamente en la Figura 31.

Como se muestra a continuación, en la Figura 32 se configuró el certificado previamente importado de nombre “Exchange 2016”.

Figura 32

Paso 4 - Certificado SSL Exchange 2016

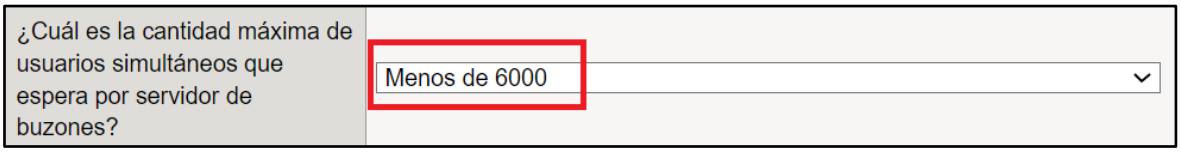


Nota. El gráfico representa la Configuración del certificado SSL asociada a la plantilla Exchange

Tras configurar el Certificado para obtener una comunicación segura e encriptada. En el template del OWA exchange 2016, se configuró la cantidad de conexiones máxima que puede procesar cada servidor, las cuales son 6000.

Figura 33

Paso 5 - F5 BIG IP ASM Distribución de tráfico

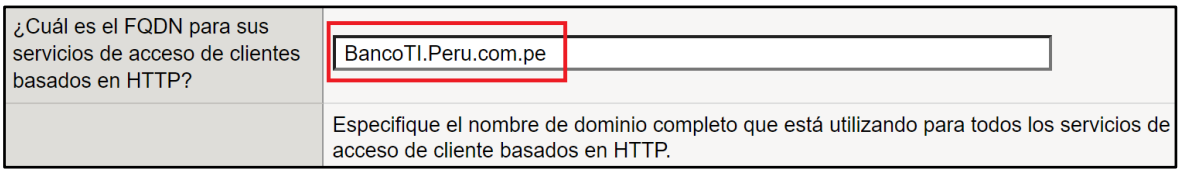


Nota. El gráfico representa la cantidad máxima de conexiones permitidas por servidor de correo

Finalmente se procedió a configurar el nombre de resolución de dominio (DNS) para acceder al correo electrónico mediante un enlace web desde la red pública e interna y no mediante una IP pública, el nombre de dominio configurado es BancoTI.Peru.com.pe, conforme a lo mostrado en la Figura 34.

Figura 34

Paso 6 - Configuración de dominio de acceso al correo electrónica vía web

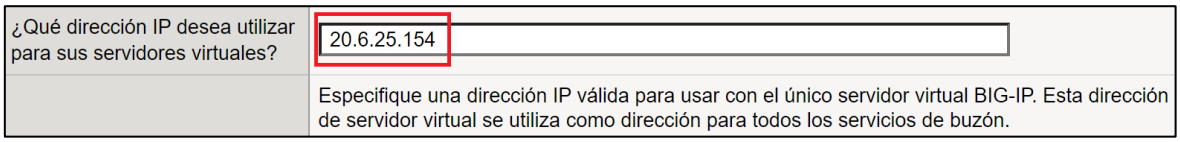


Nota. El gráfico representa la configuración del FQDN para el acceso al correo electrónico vía web

Es importante precisar que la IP pública 20.6.25.154, está asociada al Nombre de resolución de Dominio, por lo cual cuando un usuario escribe en el navegador web la IP Pública del servicio de correo electrónico, el Balanceador de Carga F5 BIG IP ASM realiza la traducción al enlace web “BancoTI.Perú.com.pe”.

Figura 35

Paso 7 – Configuración de IP pública



Nota. El gráfico muestra la IP pública para el acceso vía web al Correo electrónico OWA

Luego de completar el formulario para la integración de la aplicación de correo electrónico web con F5 BIG IP, se debe validar la generación automática del servidor virtual con la IP pública y los servidores de correo.

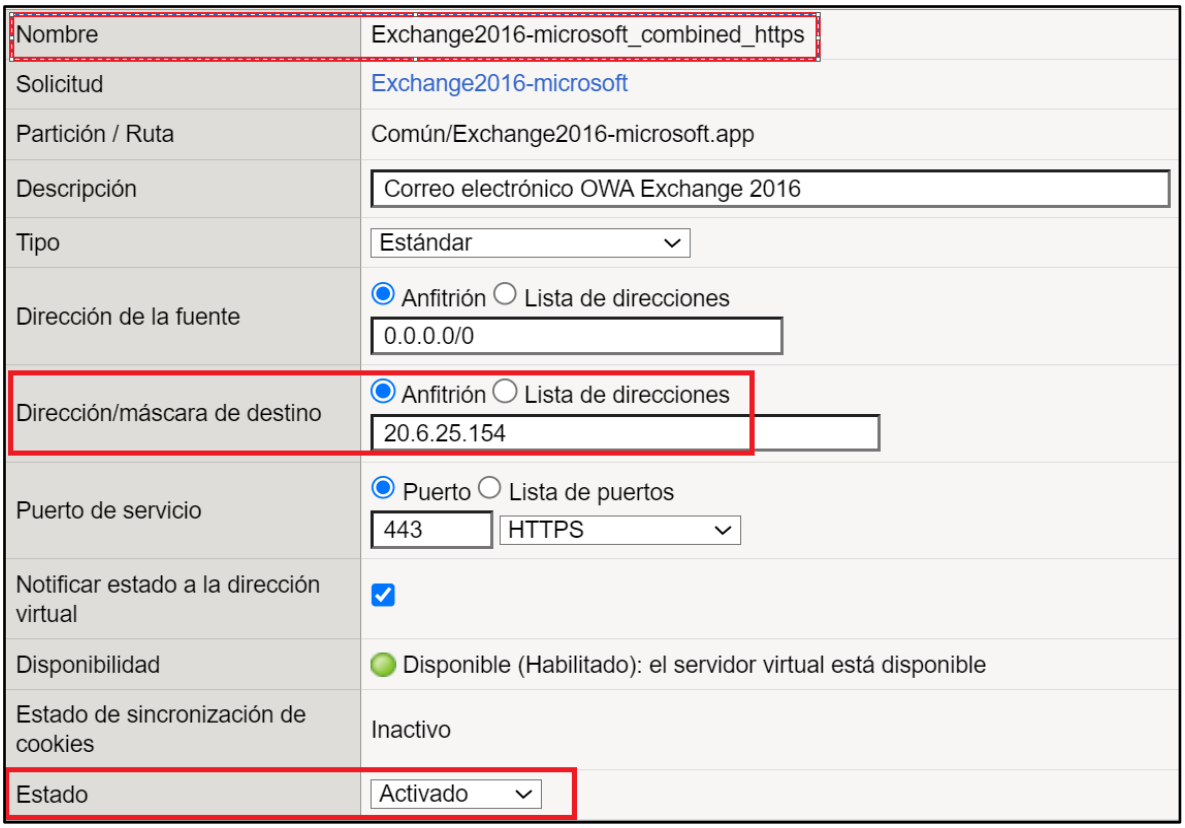
Es importante precisar que al completar los datos del formulario de integración (como se muestra desde la Figura 29), ya no es necesario configurar manualmente el balanceador, sino que al finalizar el formulario en la Figura 35, F5 BIG IP ASM genera automáticamente la configuración de balanceo de carga y la protección del servicio por medio de una política de seguridad ASM.

A continuación, se valida la creación automática del balanceo de carga y posteriormente la regla ASM para la protección del servicio.

Se verificó en la ruta Trafico Local → Servidores Virtuales → seleccionar el balanceador auto configurado por el template IAPP exchange 2016, de nombre Exchange2016-microsoft-combined_https, que hace referencia al servicio configurado en la Figura 36, donde la dirección de la IP fuente “0.0.0.0/0” indica que el acceso es permitido para cualquier dirección IP origen, adicionalmente observamos que la plantilla autoconfiguró el balanceador con la IP pública 20.6.25.154, puerto seguro “HTTPS” y en estado activo.

Figura 36

Creación Balanceador Exchange 2016



Nota. El gráfico representa el Balanceador de carga Exchange 2016 en estado activo

Luego de verificar que el balanceador está creado, el siguiente paso es validar que los servidores estén recibiendo el tráfico de manera distribuida, esto de acuerdo con el tipo de balanceo asignado. Este punto se valida mediante el código de colores, debido a que el balanceador auto generado presenta el icono color ver (como se observó en la Figura 36).

La Tabla número 3, indica que el color verde se refiere a la correcta operatividad del balanceo de carga con los servidores.

Tabla 3

Código de colores status Balanceador de carga

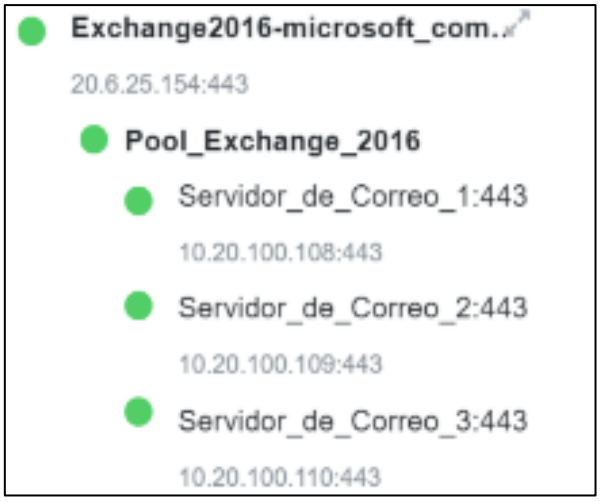
Indicador de estado	Descripción
circulo verde	El objeto está disponible. Este icono indica que el sistema BIG-IP da servicio al tráfico destinado a este objeto. Para sesiones BIG-IP APM, este icono indica que la sesión está establecida.
Cuadrado azul	Se desconoce la disponibilidad del objeto. Por ejemplo, este estado puede ocurrir cuando el objeto no está configurado para la verificación del servicio, la dirección IP del objeto está mal configurada o el objeto está desconectado de la red. Para sesiones de BIG-IP APM, este icono indica que la sesión está pendiente y aún no establecida. ***Nota** : Los miembros del grupo y los nodos con estado desconocido son elegibles para recibir solicitudes de clientes.*
triangulo amarillo	El objeto no está disponible actualmente, pero podría estarlo más adelante sin intervención del usuario. Por ejemplo, un objeto que ha alcanzado su límite de conexiones configurado puede mostrar un estado amarillo y luego cambiar a un estado verde cuando el número de conexiones cae por debajo del límite configurado.
Diamante rojo	El objeto no está disponible. Este icono indica que el sistema BIG-IP no puede atender el tráfico destinado a este objeto. Por ejemplo, este estado puede ocurrir cuando un nodo falla en la verificación del servicio porque ya no está disponible. Este estado requiere la intervención del usuario para restaurar el estado del objeto a verde.

Nota. La tabla 3 indica el estado operativo de un balanceador, Adaptado de *Codigos de colores* ,F5 Networks, 2023, (https://my.f5.com/manage/s/article/K12213214)

Para la verificación del balanceo se debe ingresar a Locall trafic → network map Como se evidencia en la Figura 37, se puede observar que el color verde indica que las conexiones son establecidas con los servidores de correo balanceados por F5 BIG IP, donde se tiene 3 servidores que brindan el servicio de correo electrónico mediante cada sesión https de usuarios, se establece una sesión la cual es balanceada para evitar saturar un solo servidor con múltiples conexiones.

Figura 37

Balanceo de Carga - servidores de correo

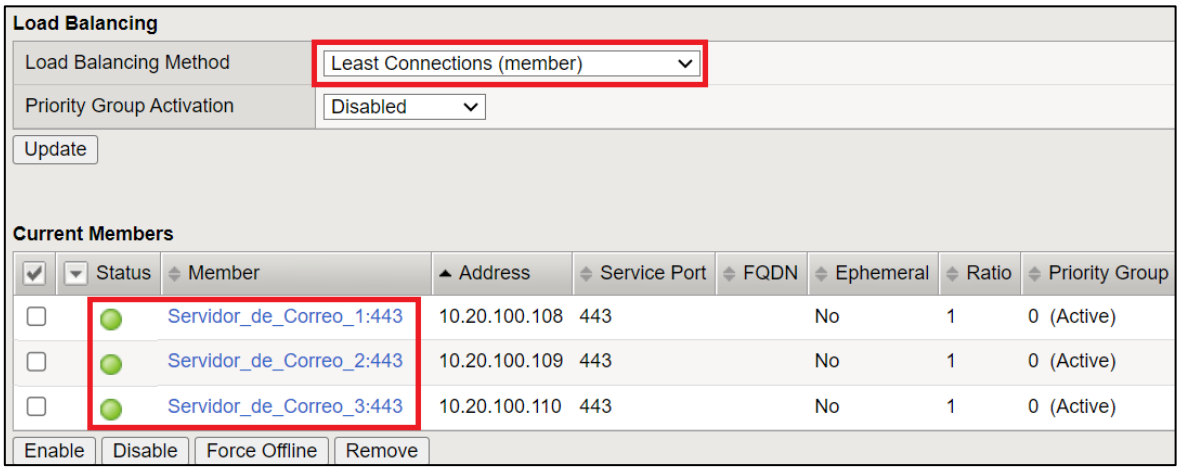


Nota. El gráfico representa la operatividad del Balanceador de carga

Finalmente cuando un trabajador en su browser o navegador si dirige a la IP publica https://20.6.25.154 o al nombre de dominio “https://BancoTI.Peru.com.pe”, se establece una sesión y el balanceador de carga establece una conexión con uno de los tres servidores que brinda el servicio de correo, de esta manera el servicio es publicado a través de una IP publica o nombre de dominio de forma segura (es decir no sé expone la IP de los servidores a internet), como también ante una falla en un servidor, el balanceador reenvía automáticamente todo el tráfico a los servidores que no presenten problemas, así mismo F5 BIG IP tiene la capacidad de evaluar si un servidor final presenta menor cantidad de recursos (memoria, cpu, tiempo de respuesta alta o baja a una conexión) que los servidores restantes balanceados realizando de esta manera un equilibrio de carga, esté tipo de balanceo es posible gracias a la configuración del balanceo en modo least connections (lo mencionado se puede observar en la Figura 38 y fue precisado en el capítulo II del presente trabajo de suficiencia profesional).

Figura 38

Método de balanceo less connections



Nota. El gráfico representa el Método de balanceo Least Connections

3.2.3.3 CONFIGURACIÓN DE POLÍTICA DE SEGURIDAD ASM

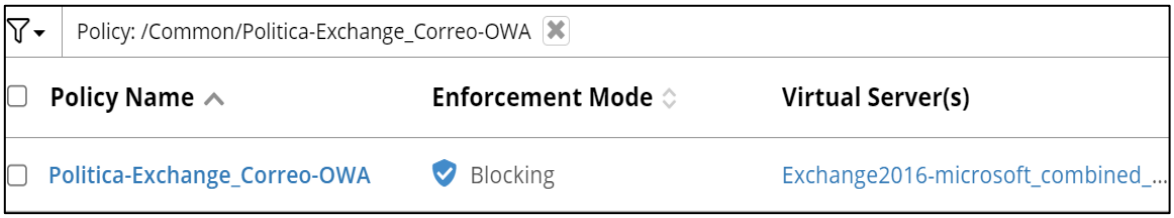
En este punto se validó la creación de un control que asegure la protección de la aplicación de correo electrónico Web publicado en internet (el cual fue implementado a lo largo del capítulo 3.2.3.2 mediante la configuración del IAPP exchange 2016), el proteger los activos informáticos como es el caso de un servidor de correo que gestiona información sensible es de suma importancia, por lo cual es una necesidad está implementación.

Conocemos que existen distintos intentos de intrusiones que buscan vulnerar aplicaciones que se encuentran en la red pública, como se puede ver en la Figura 39 se tiene configurada la política de seguridad ASM en modo Bloqueo.

Dicha política ASM es la encargada de realizar el filtro de los intentos maliciosos, como se puede observar la política, se encuentra aplicada al balanceador generado luego de configurar el formulario de exchange 2016 “cuyo nombre es Exchange2016-microsfot_combined_https”, y su funcionamiento es aplicar filtros de seguridad a todo usuario que intente conectarse al acceso vía web desde la red pública o interna.

Figura 39

Política ASM WAF

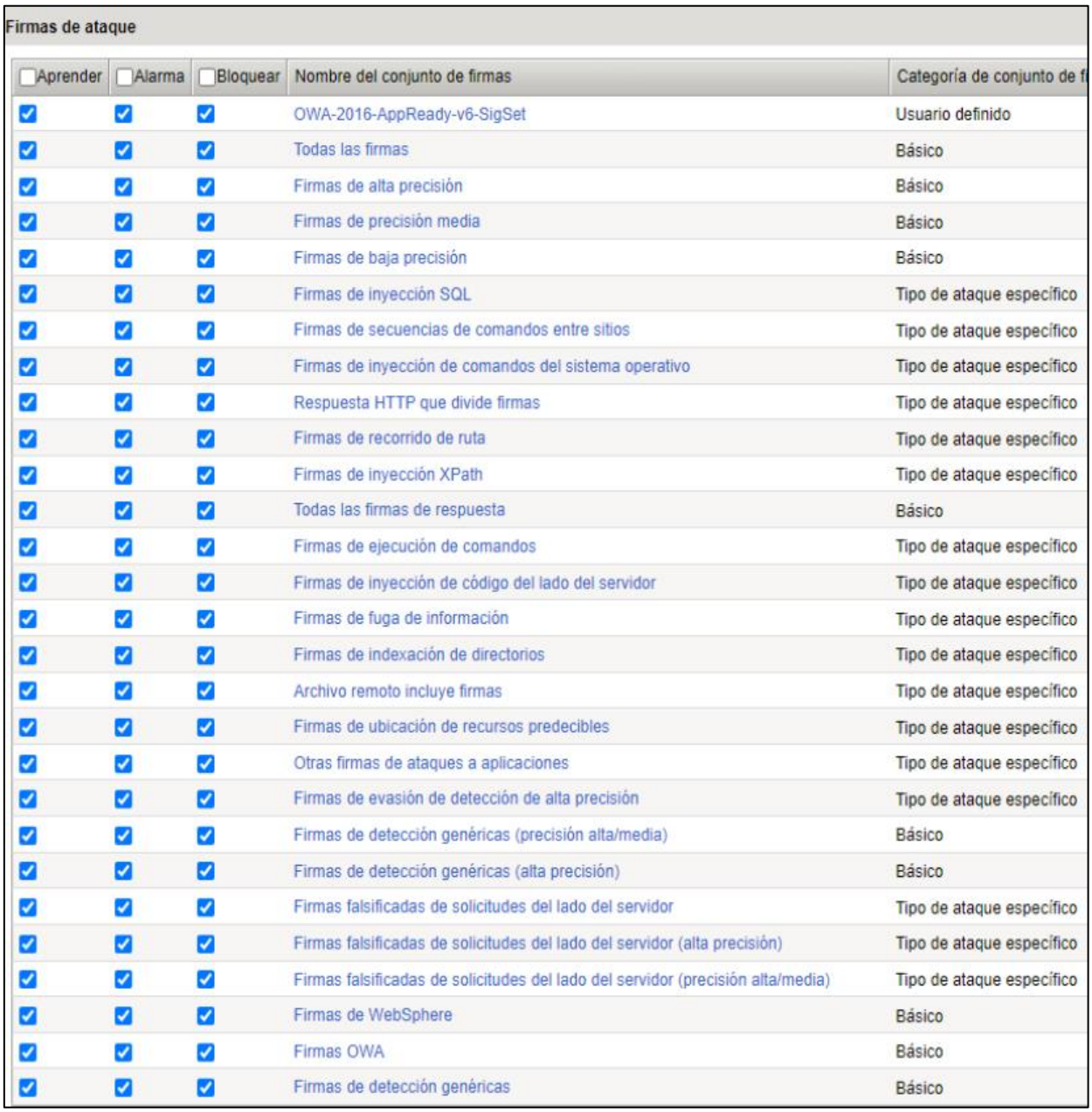


Nota. El siguiente gráfico representa la configuración de política de seguridad

A continuación, se da a conocer el paquete de firmas de seguridad que opera como mecanismo de seguridad a través de la política ASM (como se puede ver en la Figura 40) frente a intentos de ataques maliciosos.

Figura 40

F5 ASM - Attack Signatures maliciosos



Firmas de ataque

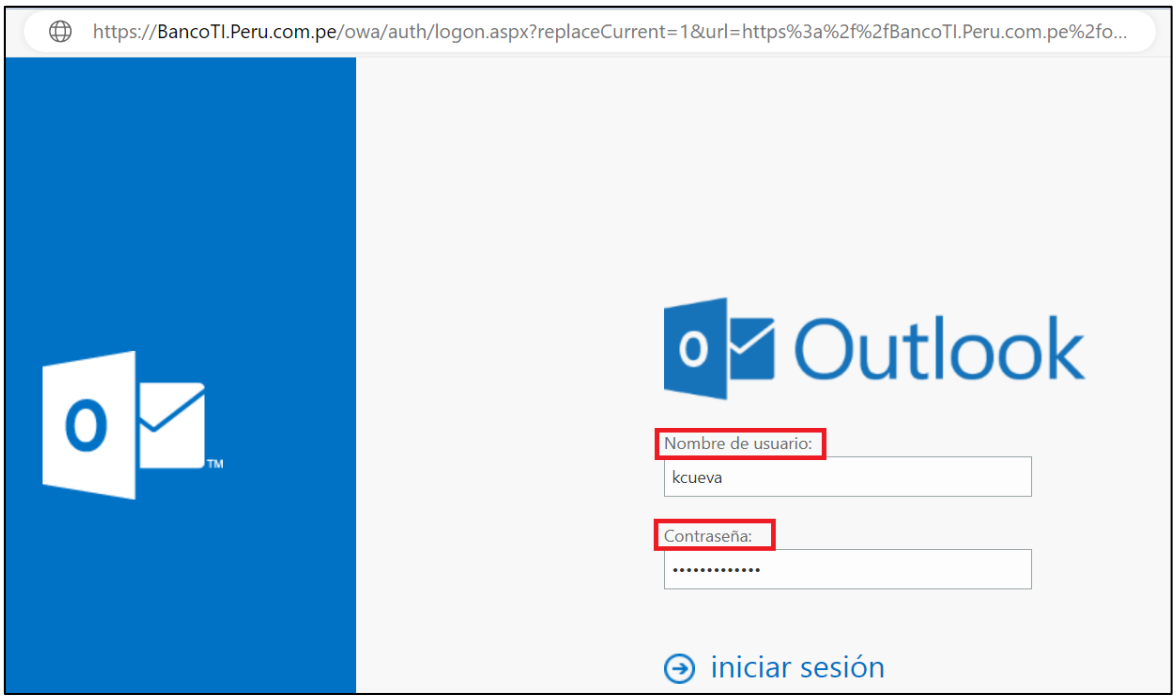
Aprender	Alarma	Bloquear	Nombre del conjunto de firmas	Categoría de conjunto de f
☑	☑	☑	OWA-2016-AppReady-v6-SigSet	Usuario definido
☑	☑	☑	Todas las firmas	Básico
☑	☑	☑	Firmas de alta precisión	Básico
☑	☑	☑	Firmas de precisión media	Básico
☑	☑	☑	Firmas de baja precisión	Básico
☑	☑	☑	Firmas de inyección SQL	Tipo de ataque específico
☑	☑	☑	Firmas de secuencias de comandos entre sitios	Tipo de ataque específico
☑	☑	☑	Firmas de inyección de comandos del sistema operativo	Tipo de ataque específico
☑	☑	☑	Respuesta HTTP que divide firmas	Tipo de ataque específico
☑	☑	☑	Firmas de recorrido de ruta	Tipo de ataque específico
☑	☑	☑	Firmas de inyección XPath	Tipo de ataque específico
☑	☑	☑	Todas las firmas de respuesta	Básico
☑	☑	☑	Firmas de ejecución de comandos	Tipo de ataque específico
☑	☑	☑	Firmas de inyección de código del lado del servidor	Tipo de ataque específico
☑	☑	☑	Firmas de fuga de información	Tipo de ataque específico
☑	☑	☑	Firmas de indexación de directorios	Tipo de ataque específico
☑	☑	☑	Archivo remoto incluye firmas	Tipo de ataque específico
☑	☑	☑	Firmas de ubicación de recursos predecibles	Tipo de ataque específico
☑	☑	☑	Otras firmas de ataques a aplicaciones	Tipo de ataque específico
☑	☑	☑	Firmas de evasión de detección de alta precisión	Tipo de ataque específico
☑	☑	☑	Firmas de detección genéricas (precisión alta/media)	Básico
☑	☑	☑	Firmas de detección genéricas (alta precisión)	Básico
☑	☑	☑	Firmas falsificadas de solicitudes del lado del servidor	Tipo de ataque específico
☑	☑	☑	Firmas falsificadas de solicitudes del lado del servidor (alta precisión)	Tipo de ataque específico
☑	☑	☑	Firmas falsificadas de solicitudes del lado del servidor (precisión alta/media)	Tipo de ataque específico
☑	☑	☑	Firmas de WebSphere	Básico
☑	☑	☑	Firmas OWA	Básico
☑	☑	☑	Firmas de detección genéricas	Básico

Nota. El gráfico representa Firmas de protección de ataques de maliciosos conocidos

Como un punto adicional para reforzar la seguridad, se verificó que la página de correo Outlook web del banco, presenta 2 parámetros de inicios de sesión renombrados como “nombre de usuario y contraseña” los cuales se utilizarán para configurar la prevención contra ataques de fuerza bruta (como se muestra en la Figura 41).

Figura 41

Inicio de Sesión - Usuario y Password

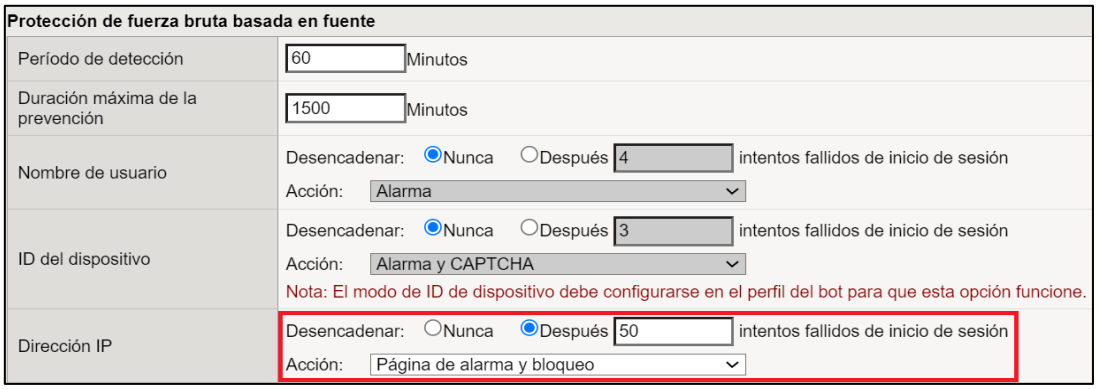


Nota. El siguiente gráfico muestra los parámetros de inicio de sesión usuario y contraseña

Los parámetros por ingresar son usuario y contraseña, siendo este punto clave y vulnerable ante algún ataque desde la red pública. Este ataque consiste en realizar logins fallidos consecutivos al servicio de correo electrónico con la finalidad de descubrir las credenciales del usuario, por lo cual se valida un punto fundamental e importante, es la configuración de la regla ASM contra ataques de fuerza bruta mostrado a continuación en la Figura 42, la cual es limitada a 50 intentos fallidos.

Figura 42

Configuración Política ASM Fuerza Bruta



Nota. Regla Fuerza Bruta – bloqueo luego de 50 intentos fallidos en robo de credenciales

3.2.4 CONFIGURACIÓN DE ENLACE DE CONTINGENCIA

Previo a la configuración del enlace de contingencia con el proveedor de internet secundario, como primer requisito es configurar el clúster del equipo F5 BIG IP ASM pasivo y activo, debido a que cada router se comunicará con ambos equipos F5, por lo cual es necesario la configuración del clúster de equipos F5 BIG IP ASM.

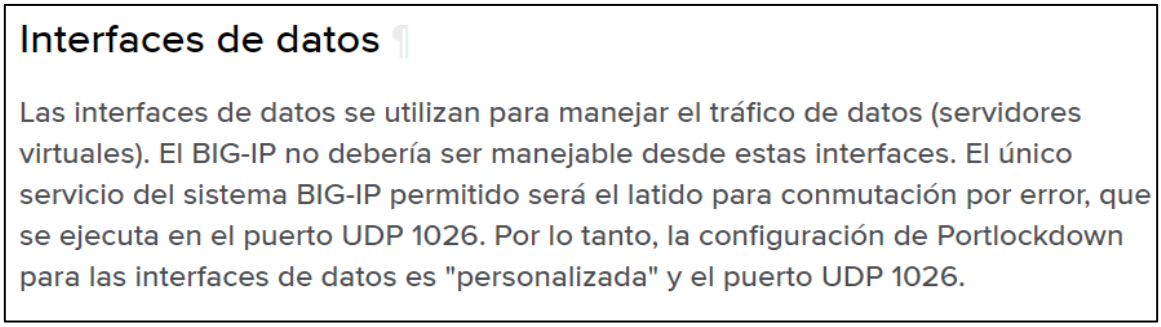
3.2.4.1 F5 BIG IP ASM CLUSTER - ACTIVO Y PASIVO

Uno de los puntos principales de la implementación realizada es la configuración de un equipo de redundancia, esto con la finalidad de obtener un site de contingencia que pueda recibir todo el tráfico de equipo F5 BIG IP ASM primario, para lo cual todos los cambios se replicaron mediante la configuración de sincronización con otro equipo F5 BIG IP ASM secundario en modo pasivo.

En la Figura 43, se evidencia que para la configuración del H.A “alta disponibilidad”, se requiere configurar el puerto 1026, específicamente dicho puerto es utilizado en configuraciones en H.A, permitiendo la comunicación de heartbeats entre equipo F5 activo y F5 pasivo.

Figura 43

F5 Recomendación Configuración de Puerto



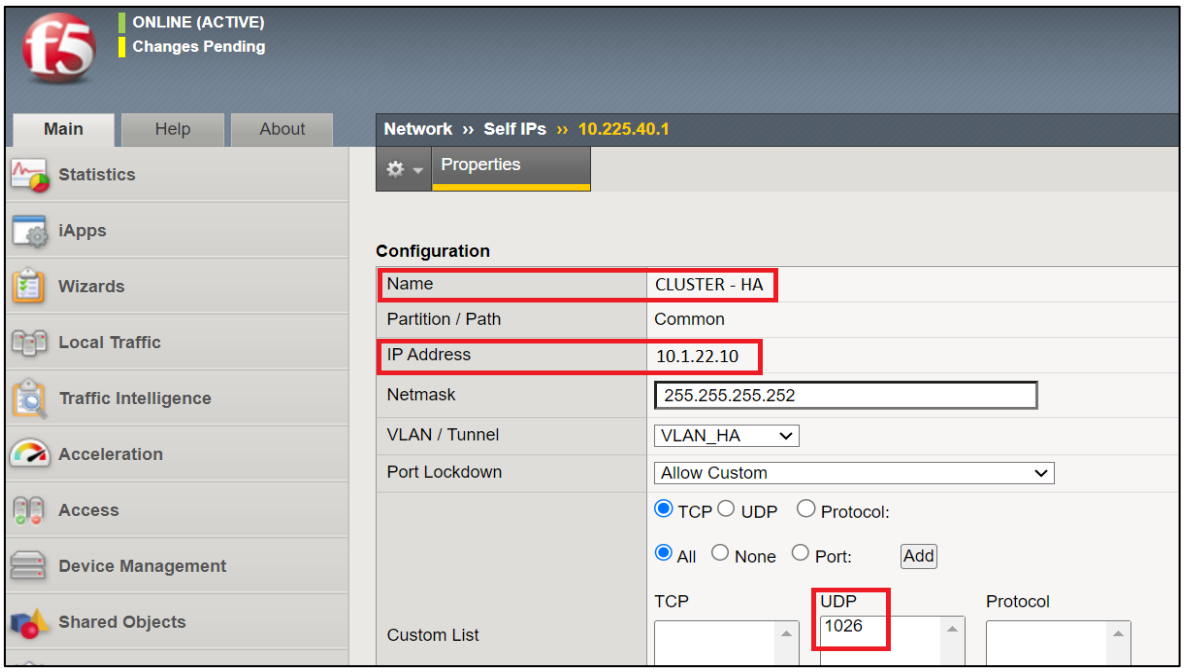
Nota. El gráfico representa a el puerto UDP a habilitar en la configuración del HA, Adaptado de F5 Alta disponibildiad de cluster, F5 Networks, 2023,(https://clouddocs.f5.com/training/community/adc/html/class6/intro.html)

Posterior a ello, para iniciar las configuraciones del H.A o alta disponibilidad del cluster, nos dirigimos hacía el apartado: Self IPs → Create new self IP

Se inicia configurando en el equipo F5 Activo el self IP con las IP 10.1.22.10 y máscara 255.255.255.252, proporcionadas por el cliente para la configuración del H.A.

Figura 44

Configuración Cluster H.A F5 BIG IP ACTIVO

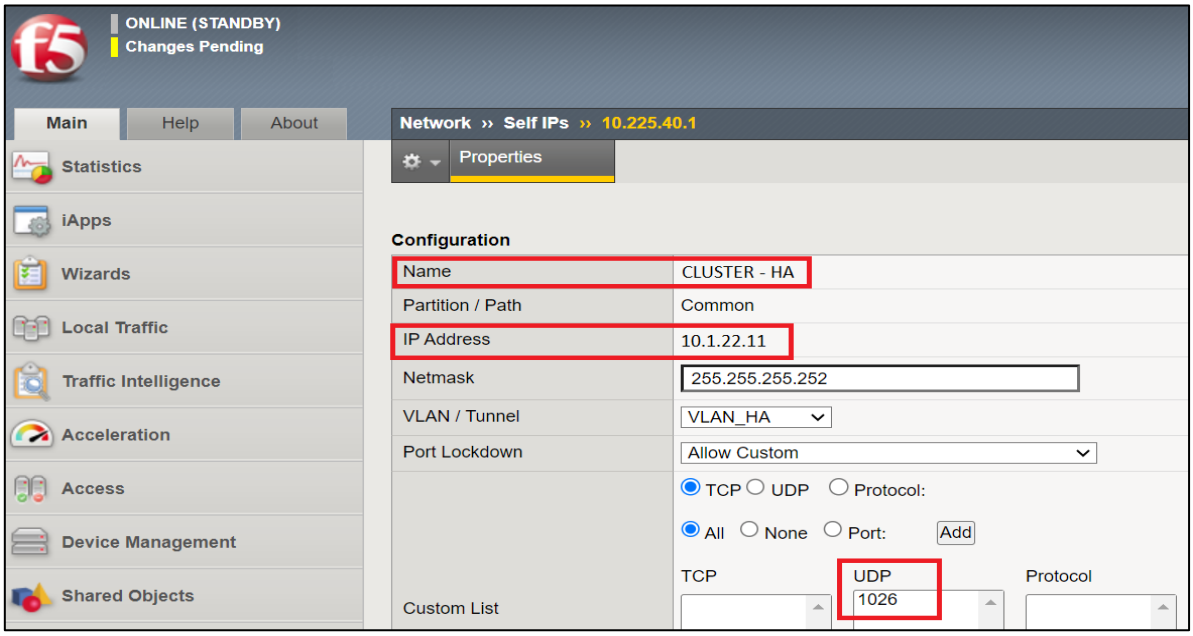


Nota. El gráfico representa la Configuración H.A en el F5 Activo

Luego de configurar el Self IP en el F5 Activo, se procede a replicar la configuración en el equipo F5 BIG IP Secundario, la IP proporcionada por el cliente es 10.1.22.11 y máscara 255.255.255.252, lo presente se puede observar en la Figura 45.

Figura 45

Configuración Cluster H.A F5 BIG IP secundario



Nota. El gráfico representa la configuración del H.A del F5 Pasivo

Finalmente se realizó la sincronización de los equipos F5 pasivo y activo para que el equipo F5 Pasivo presente la configuración del equipo F5 activo, lo mencionado se puede observar en la Figura 46.

Figura 46

Sincronización de equipos - Configuración Homologada F5

Nota. El gráfico representa la configuración Homologada – F5 sincronizados

Finalmente se validó que la configuración de política ASM y el Balanceo de los servidores de correo Exchange2016-microsoft fue replicado en ambos equipos (como se puede observar en la Figura 46) tanto F5 activo y pasivo fueron sincronizados de manera correcta, por lo cual el último paso es configurar la redundancia de enlace entre el F5 BIG IP Activo y pasivo con los proveedores de internet.

3.2.4.2 CONFIGURACIÓN DE ENLACE DE CONTINGENCIA F5 BIG IP Y ISP

En el presente apartado se realizó la configuración de los enlaces de internet entre el F5 Activo y Pasivo con los routers de los proveedores de Internet (ISP).

Iniciándose la configuración en el F5 activo, se configuró el self IP (el cual es una IP de una interfaz del equipo F5 BIG IP que se utilizó para entablar comunicación con el router principal del proveedor de Internet_1).

Para la configuración de la IP del router del principal proveedor de internet y F5 BIG IP ASM activo, se utilizó la información de la Tabla 4:

Tabla 4

Especificaciones del router Proveedor Internet principal

Datos	Especificaciones
Nombre de Router	Router_Proveedor_Internet_1
IP de Router	168.200.127.10
Máscara	255.255.255.128
Túnel	Eth1.3
Nombre del equipo	F5 BIG IP ASM ACTIVO

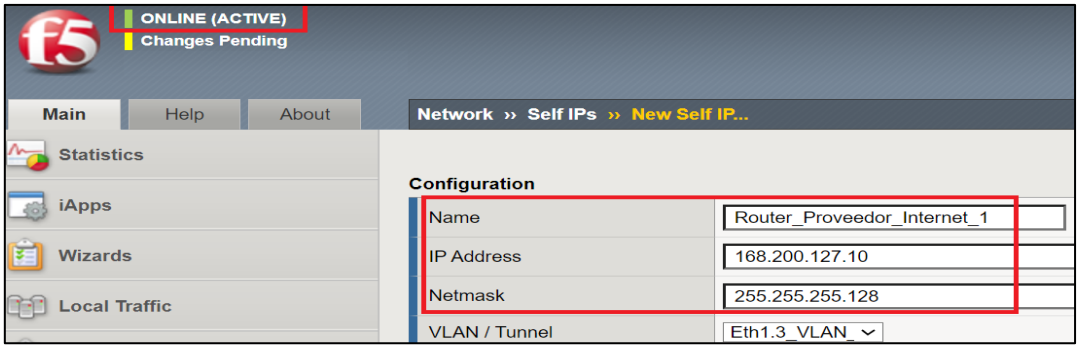
Nota. La tabla 4 representa las especificaciones del enlace Principal ISP

Es importante precisar que el túnel Eth1.3 está configurado para la comunicación entre Router y F5 BIG IP Activo.

La configuración se realizó a nivel de gráfica de interfaz de usuario (GUI) conforme a lo mostrado en la Figura 47, se configuró los parámetros compartidos por el cliente en la Tabla 4, IP address 168.200.127.10 y la máscara 255.255.255.128.

Figura 47

Configuración IP, Mask, Vlan - Router de proveedor Internet principal (ISP)



Nota. *El presente gráfico representa la configuración de enlace de principal - ISP*

Luego de realizar las configuraciones a nivel de F5 Activo con el proveedor de internet principal, se realizó de forma homóloga la configuración del F5 pasivo con el proveedor de internet_2, los datos proporcionados por la entidad bancaria se muestran en la Tabla 5.

Tabla 5

Datos router Proveedor Internet secundario

Datos	Especificaciones
Nombre de Router	Router_Proveedor_Internet_2
IP de Router	162.150.100.15
Máscara	255.255.255.128
Túnel	Eth1.4
Nombre del equipo	F5 BIG IP ASM PASIVO

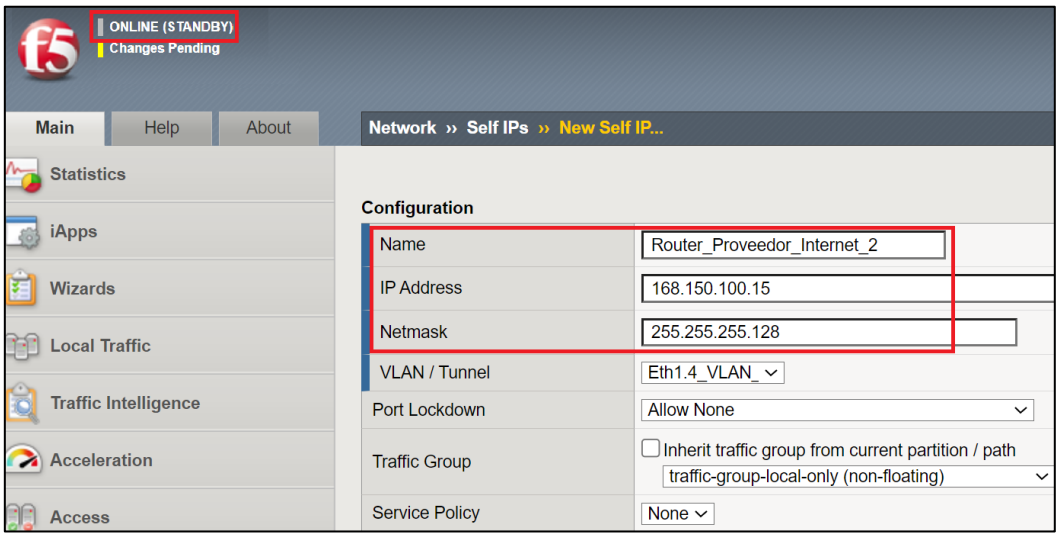
Nota. La tabla 5 representa las especificaciones del enlace secundario ISP

El túnel Eth1.4 está configurado para la comunicación entre Router y F5 BIG IP Pasivo.

Así mismo, la configuración se realizó a nivel de gráfica de interfaz de usuario (GUI) como se muestra en la Figura 48, donde se configuró los parámetros compartidos por el cliente en la Tabla 5, IP address 168.150.100.15 y mascara 255.255.255.128.

Figura 48

Configuración IP, Mask, Vlan - Router de proveedor Internet secundario



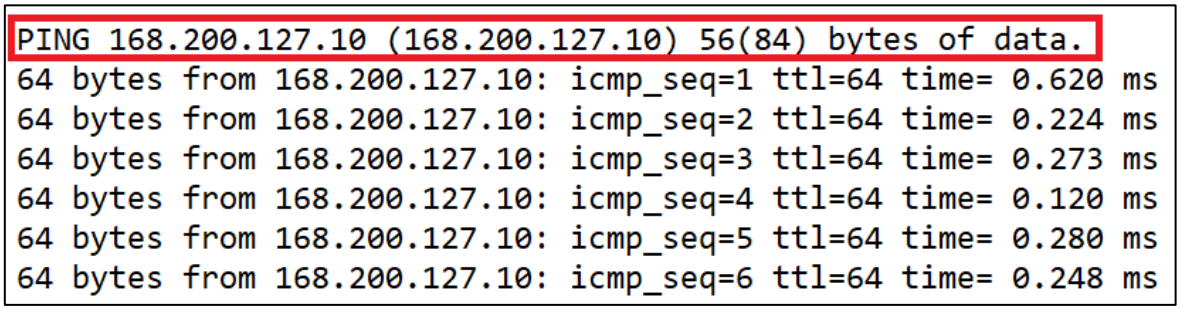
Nota. El presente gráfico representa la configuración de enlace de secundario ISP

Finalmente se validó la configuración de los enlaces de internet obteniendo conexión satisfactoria desde los equipos F5 Activo y pasivo hacía los Routers que brindan el servicio de Internet.

Conforme a lo mostrado en la Figura 49, se valida conexión mediante el comando “ping” hacía el default Gateway del router principal “IP 168.200.127.10”, observándose conexión satisfactoria hacia el router principal.

Figura 49

Conexión Router Principal - Proveedor de Internet_1.

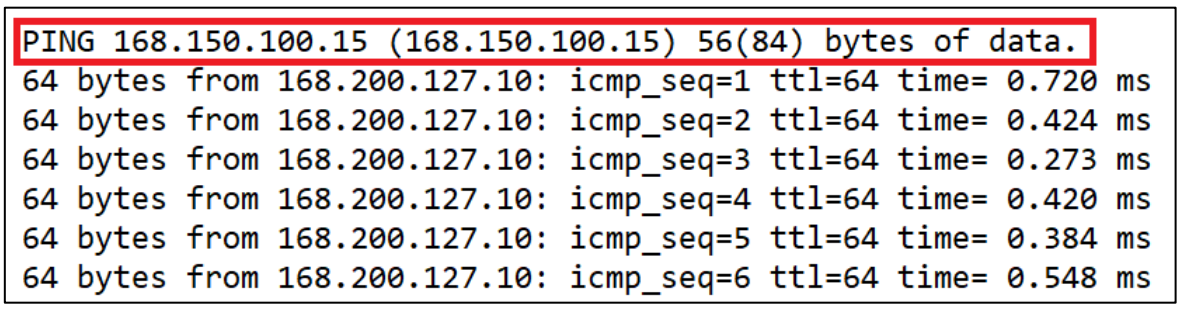


Nota. El presente gráfico representa la conexión ICMP con el Router primario

De igual manera se puede observar en la Figura 50, se valida conexión mediante el comando “ping” hacía el default Gateway del router secundario “IP 168.150.100.15”.

Figura 50

Conexión Router Secundario - Proveedor de Internet_2



Nota. El presente gráfico representa la conexión ICMP con el Router pasivo

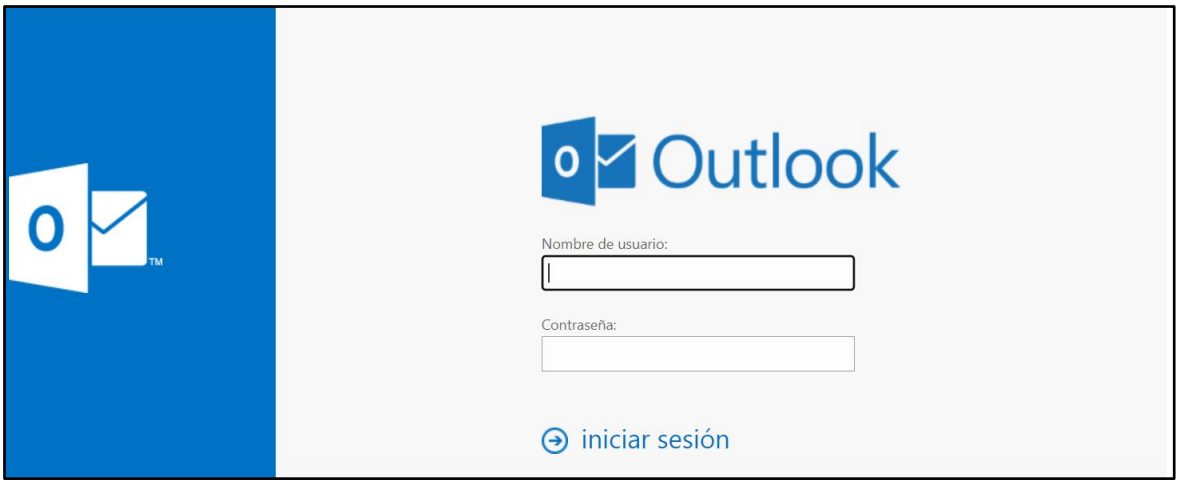
Lográndose así la configuración del enlace de contingencia y configuración de respaldo ante alguna falla en la red o enlace de internet.

3.2.5 VALIDACIÓN DE OPERATIVIDAD DEL SERVICIO DE CORREO OWA

Luego de realizar la implementación de la plantilla de integración F5 BIG IP ASM con exchange 2016 y la política de seguridad como también la implementación del ISP (enlace de redundancia), en este punto se constata que el servicio web para el acceso al correo electrónico se encuentra operativo, es decir como servicio la página web de acceso al correo OWA se encuentra operativa y carga el inicio de sesión de usuario, como se puede observar en la Figura 51.

Figura 51

Validación de operatividad del acceso web al correo electrónico

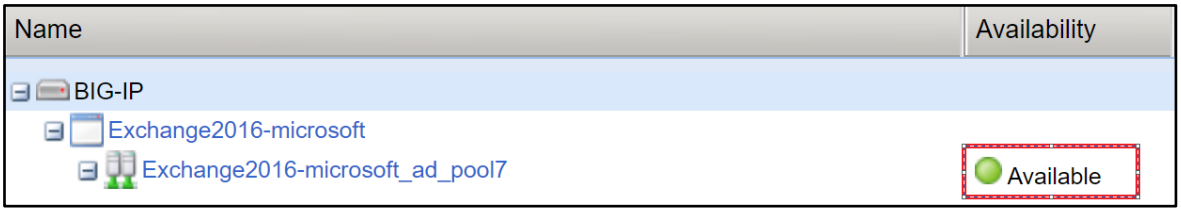


Nota. El siguiente gráfico representa el acceso al correo web OWA

Otra forma de validar que el servicio para el acceso vía web al correo electrónico se encuentra operativo, es verificando el estado de la aplicación, como se puede observar en la Figura 52, presenta el color verde, lo que indica de acuerdo con la Tabla 3, del código de colores que el servicio se encuentra operativo.

Figura 52

Verificación del estado del servicio web de Correo



Nota. El siguiente gráfico representa el servicio de correo web

Debido a que se valida que el servicio se encuentra operativo en el apartado 3.3.4 se realizará pruebas a nivel de usuario.

3.3 RESULTADOS

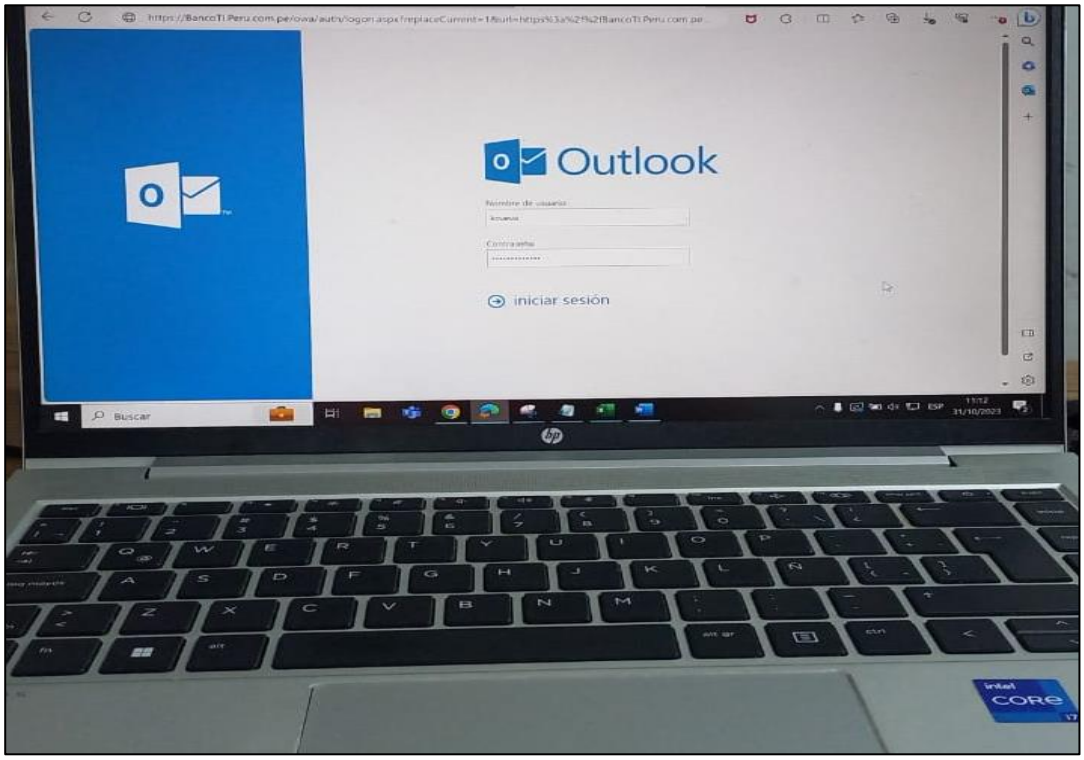
3.3.1 VERIFICACIÓN DE CONEXIÓN SEGURA VÍA WEB AL CORREO OWA

Verificación a través de Laptop, PC, Celular:

1- Como se puede observar en la Figura 53, se verifica la conexión remota a través de una laptop modelo HP, donde el servicio implementado del acceso vía web al correo electrónico está operando correctamente, la conexión mediante el protocolo seguro https al nombre de dominio "BancoTI.Peru.com.pe/owa" estableciéndose conexión a la interfaz web de acceso al correo electrónico OWA.

Figura 53

Prueba de acceso al correo electrónico en Laptop HP

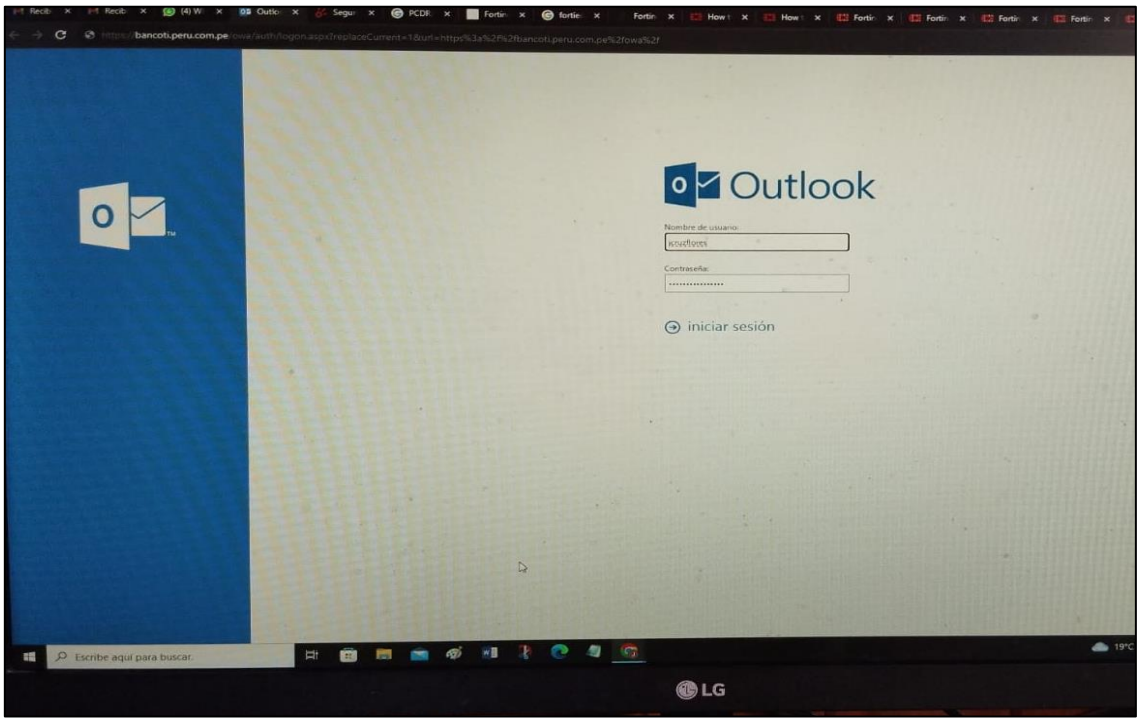


Nota. El gráfico representa la prueba de conexión al correo electrónico OWA vía web desde una laptop de prueba HP

2- Como se puede observar en la Figura 54, se verifica la conexión remota a través de una PC de escritorio.

Figura 54

Prueba de acceso al correo electrónico en Computadora de escritorio



Nota. El gráfico representa la prueba de conexión al correo electrónico Owa vía web desde una PC de escritorio

3- La verificación del acceso a través de teléfono celular, se puede observar en la Figura 55, el establecimiento de la conexión con el servicio de correo electrónico.

Figura 55

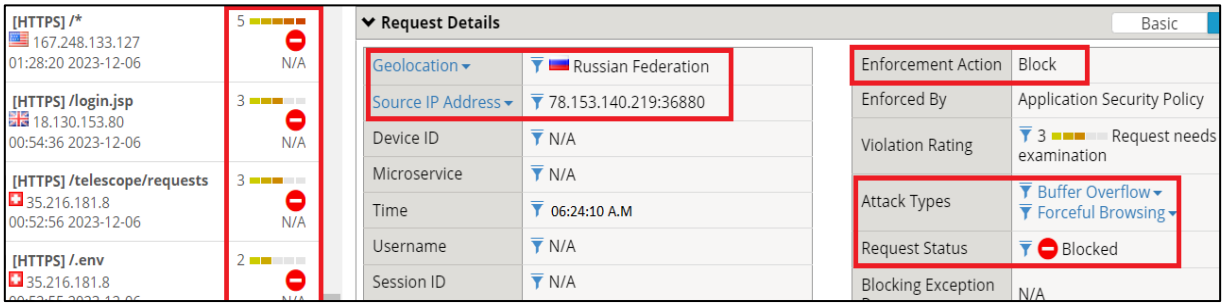
Prueba de acceso al correo electrónico desde teléfono celular

Por otra parte, si bien las conexiones de los usuarios fueron establecidas de manera satisfactoria, pero también se observan conexiones maliciosas, por lo cual la Figura 56 brindó fiabilidad de la operatividad de la política ASM que protege el acceso al correo electrónico vía web, donde se observa que IPs públicas del extranjero intentan explotar alguna vulnerabilidad del servicio de correo, siendo esto bloqueado por la regla ASM aplicado al servicio de correo Exchange 2016.

En la Figura 56, se muestra los ataques buffer overflow y forceful browsing los cuales fueron bloqueados inmediatamente, dando como resultado el bloqueo de la IP 78.153.140.219 proveniente de Rusia, sumado a esto otras IPs públicas “167.248.133.127, 18.130.153.80, 35.216.181.8, 25.216.181.8” fueron bloqueadas por intentos maliciosos sobre el servicio de acceso vía web al correo electrónico.

Figura 56

Validación de operatividad de la política de seguridad ASM

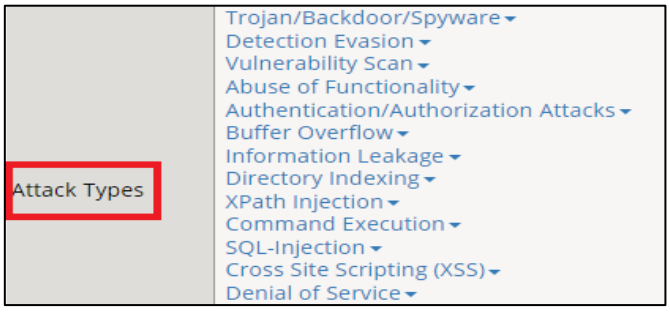


Nota. El gráfico representa la validación de mitigación de tráfico malicioso política ASM,

En la Figura 57 se comparte el detalle de los tipos de ataques como Trojan, Detection evasión, abuse functionality, command excution) ejecutados por usuarios externos hacia la red interna, los cuales fueron bloqueados por la regla ASM.

Figura 57

Verificación de Bloqueo de ataques maliciosos

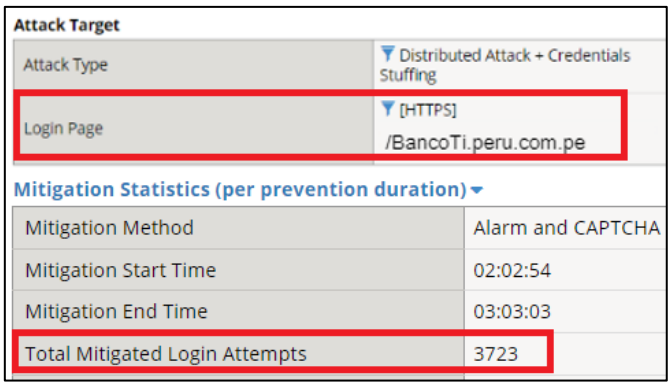


Nota. El gráfico representa la validación de tipos de ataques maliciosos

Adicionalmente, se evidencia en la Figura 58, múltiples bloqueos ante los ataques de fuerza bruta, se intentó realizar un ataque distribuido de robo de credenciales con un total de 3723 login fallidos para intentar lograr obtener las credenciales correctas a través de pruebas de inserción de credenciales erróneas hasta obtener la correcta, donde validamos que la política ASM de fuerza bruta opera correctamente y protegió el inicio de sesión del correo electrónico OWA con nombre de dominio " https://BancoTI.Peru.com.pe.

Figura 58

Bloqueo de ataques de fuerza bruta



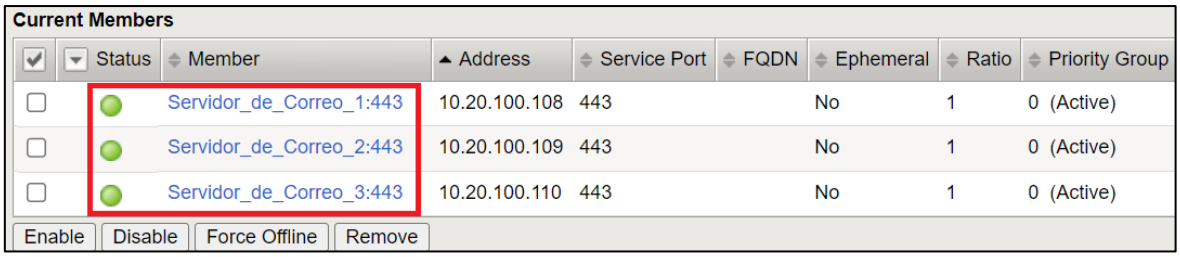
Nota. El gráfico representa la validación de mitigación del intento de robo de credenciales

3.3.2 VERIFICACIÓN DE BALANCEO DE CARGA

A continuación, se comparte la evidencia del balanceo de carga el cual distribuye el tráfico uniforme a los servidores de correo (10.20.100.108, 10.20.100.109, 10.20.100.110) los cuales se pueden observar en la Figura 59, los datos compartidos en la Tabla 2.

Figura 59

Balanceo de carga - Servidores de correo exchange

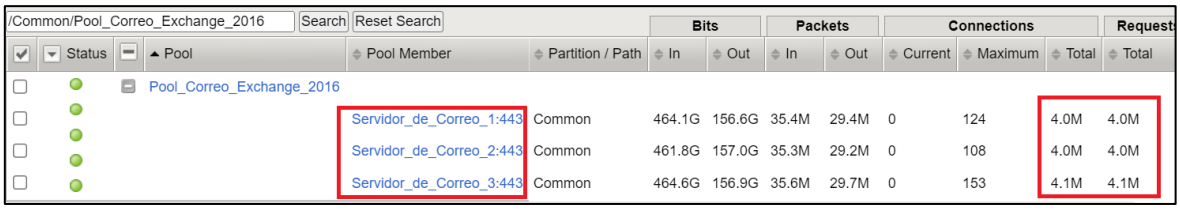


Nota. El gráfico representa los servidores de correo electrónico balanceados

De la Figura 60, se verifica que las conexiones son distribuidas entre los 3 servidores, como se puede observar en la columna connections " Total" se observa que la cantidad de conexiones es distribuida de forma equitativa entre el Servidor de correo_1 con "4.0 M" de conexiones, el servidor de correo_2 con "4.0 M" de conexiones y el servidor de correo_3 con "4.0M" de conexiones evitando de esta manera causar saturación cuando se realizan múltiples conexiones de usuarios, es importante precisar que el límite de cantidad de conexiones dependerá de la capacidad de recursos servidor y no de F5 BIG IP. Sin embargo, si algún servidor presenta problema de saturación, F5 BIG IP realizará el redireccionamiento de tráfico entre los servidores operativos que no presenten problemas de operatividad.

Figura 60

Estadísticas de Balanceo de carga



Nota. El gráfico representa las estadísticas de los servidores de correo

Posteriormente se observa que el servicio del acceso vía web al correo electrónico es utilizado por múltiples usuarios, como se observa en la Figura 60, verificamos

las conexiones establecidas y balanceadas correctamente de forma distribuida hacía los servidores de correo electrónico.

Otra manera de evidenciar el funcionamiento del servicio, se evidencia en la Figura 61 y Anexo 5, donde el tráfico inicia desde la columna de IP pública (la IP 107.154.67.3 pertenece al usuario que realiza la conexión) y se conecta a la IP Server (IP pública del acceso al correo electrónico vía web, la cual es 20.6.25.154), en este punto ya inició una conexión para posteriormente F5 BIG IP ASM, Realice la conexión a través de su interfaz (Llamada Self IP con IP 168.200.127.10) para enviar el tráfico a los servidores de correo (expresados en la columna como servers mails, que presentan la IP 10.20.100.108-10.20.100.110), luego de lo cual se establece la sesión y recibe el nombre de conexión tcp (como se puede observar en la columna type), es importante acotar que el número 5 hace referencia al tiempo de inactividad luego de establecerse la sesión y no se ejecuten operaciones por parte del usuario.

Figura 61

Conexiones establecidas y Balanceadas

```
show sys connection cs-server-addr 20.6.25.154 | grep Exchange 2016-microsoft
Sys::Connections
IP Public            IP Server        Selft IP              Server mails        Type
107.154.67.3:4252    20.6.25.154:443  168.200.127.10:49762  10.20.100.108:443   tcp  5
192.230.87.3:28468   20.6.25.154:443  168.200.127.10:29461  10.20.100.109:443   tcp  2
198.143.41.21:44362  20.6.25.154:443  168.200.127.10:31763  10.20.100.110:443   tcp  89
107.154.67.7:25660   20.6.25.154:443  168.200.127.10:49661  10.20.100.108:443   tcp  115
192.230.87.3:28474   20.6.25.154:443  168.200.127.10:29111  10.20.100.109:443   tcp  2
107.154.67.7:25674   20.6.25.154:443  168.200.127.10:59662  10.20.100.109:443   tcp  115
193.143.41.40:22338  20.6.25.154:443  168.200.127.10:39760  10.20.100.108:443   tcp  73
107.154.67.12:8914   20.6.25.154:443  168.200.127.10:19461  10.20.100.110:443   tcp  118
198.143.41.17:36850  20.6.25.154:443  168.200.127.10:34750  10.20.100.108:443   tcp  17
199.230.87.21:63516  20.6.25.154:443  168.200.127.10:41711  10.20.100.110:443   tcp  4
194.143.41.18:46822  20.6.25.154:443  168.200.127.10:32751  10.20.100.109:443   tcp  79
199.230.87.9:58716   20.6.25.154:443  168.200.127.10:71260  10.20.100.108:443   tcp  6
198.143.41.29:36608  20.6.25.154:443  168.200.127.10:49761  10.20.100.110:443   tcp  64
107.154.67.7:25696   20.6.25.154:443  168.200.127.10:33745  10.20.100.109:443   tcp  115
197.230.87.3:28566   20.6.25.154:443  168.200.127.10:49766  10.20.100.109:443   tcp  2
194.230.87.19:22890  20.6.25.154:443  168.200.127.10:19765  10.20.100.108:443   tcp  102
131.230.87.2:52504   20.6.25.154:443  168.200.127.10:49767  10.20.100.110:443   tcp  64
160.143.41.17:36948  20.6.25.154:443  168.200.127.10:29760  10.20.100.110:443   tcp  16
128.143.41.12:52226  20.6.25.154:443  168.200.127.10:49769  10.20.100.109:443   tcp  114
152.230.87.21:63506  20.6.25.154:443  168.200.127.10:69762  10.20.100.108:443   tcp  17
172.230.87.3:28518   20.6.25.154:443  168.200.127.10:79761  10.20.100.108:443   tcp  2
148.143.41.11:39902  20.6.25.154:443  168.200.127.10:69762  10.20.100.110:443   tcp  121
212.230.87.2:52490   20.6.25.154:443  168.200.127.10:89761  10.20.100.109:443   tcp  64
```

Nota. Conexión establecida a nivel TCP/IP y Balanceo de carga

3.3.3 VERIFICACIÓN DE ENLACE DE CONTINGENCIA - ISP

Para la validación del enlace de contingencia se deshabilito el selft IP de IP 168.200.127.10 del enlace del router principal, conforme a lo mostrado en la Figura 62, por lo cual al no operar el router principal todo el tráfico se redirecciona sobre el enlace secundario que presenta la IP 162.150.100.15.

Figura 62

Enlace de internet principal ISP deshabilitado

Nota. Enlace principal deshabilitado con proveedor de internet – ISP

Se realizó pruebas de conexión con el router principal y secundario y en efecto se tiene conexión con el router secundario de IP 162.150.100.15, pero con el router principal la comunicación fue deshabilitada, como se observa en la Figura 63, se presenta pérdida de paquetes a la IP 168.200.127.10 del router principal en un 100%.

Figura 63

Verificación de enlace secundario de internet

```
# PING 168.150.100.15 (168.150.100.15) 56(84) bytes of data.
64 bytes from 168.200.127.10: icmp_seq=1 ttl=64 time= 0.720 ms
64 bytes from 168.200.127.10: icmp_seq=2 ttl=64 time= 0.424 ms
64 bytes from 168.200.127.10: icmp_seq=3 ttl=64 time= 0.273 ms
64 bytes from 168.200.127.10: icmp_seq=4 ttl=64 time= 0.420 ms
64 bytes from 168.200.127.10: icmp_seq=5 ttl=64 time= 0.384 ms
64 bytes from 168.200.127.10: icmp_seq=6 ttl=64 time= 0.548 ms´
^C
--- 162.150.100.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms

# PING 168.200.127.10 (168.200.127.10) 56(84) bytes of data.
^C
--- 168.200.127.10 ping statistics
48 packets transmitted, 0 received, 100% packet loss, time 57026ms
```

Nota. Validación de operatividad de enlace secundario de internet – ISP

Así mismo validamos que el servicio no presentó impacto, por lo cual en la nueva captura de tráfico se observa en la columna “selft IP”, la IP 162.150.100.15 perteneciente al router secundario, la cual F5 BIG IP ASM utiliza al no presentar conexión con el enlace principal de internet “IP 168.200.127.10” estableciendo así la conexión con el enlace secundario, lo mencionado se puede verificar a continuación en la Figura 64.

Figura 64

Conexión TCP con enlace de internet Secundario

```
show sys connection cs-server-addr 20.6.25.154 | grep Exchange 2016-microsoft
Sys::Connections
IP Public            IP Server        Selft IP                Server mails         Type
177.154.67.3:4252    20.6.25.154:443  162.150.100.15:49762    10.20.100.108:443    tcp  5
152.230.87.3:28468   20.6.25.154:443  162.150.100.15:29461    10.20.100.109:443    tcp  2
195.143.41.21:44362  20.6.25.154:443  162.150.100.15:31763    10.20.100.110:443    tcp  89
167.154.67.7:25660   20.6.25.154:443  162.150.100.15:49661    10.20.100.108:443    tcp  115
142.230.87.3:28474   20.6.25.154:443  162.150.100.15:29111    10.20.100.109:443    tcp  2
107.154.67.7:25674   20.6.25.154:443  162.150.100.15:59662    10.20.100.109:443    tcp  115
183.143.41.40:22338  20.6.25.154:443  162.150.100.15:39760    10.20.100.108:443    tcp  73
157.154.67.12:8914   20.6.25.154:443  162.150.100.15:19461    10.20.100.110:443    tcp  118
194.143.41.17:36850  20.6.25.154:443  162.150.100.15:34750    10.20.100.108:443    tcp  17
199.230.87.21:63516  20.6.25.154:443  162.150.100.15:41711    10.20.100.110:443    tcp  4
149.143.41.18:46822  20.6.25.154:443  162.150.100.15:32751    10.20.100.109:443    tcp  79
199.230.87.9:58716   20.6.25.154:443  162.150.100.15:71260    10.20.100.108:443    tcp  6
198.143.41.29:36608  20.6.25.154:443  162.150.100.15:49761    10.20.100.110:443    tcp  64
197.154.67.7:25696   20.6.25.154:443  162.150.100.15:33745    10.20.100.109:443    tcp  115
157.230.87.3:28566   20.6.25.154:443  162.150.100.15:49766    10.20.100.109:443    tcp  2
194.230.87.19:22890  20.6.25.154:443  162.150.100.15:19765    10.20.100.108:443    tcp  102
131.230.87.2:52504   20.6.25.154:443  162.150.100.15:49767    10.20.100.110:443    tcp  64
199.143.41.17:36948  20.6.25.154:443  162.150.100.15:29760    10.20.100.110:443    tcp  16
128.143.41.12:52226  20.6.25.154:443  162.150.100.15:49769    10.20.100.109:443    tcp  114
152.230.87.21:63506  20.6.25.154:443  162.150.100.15:69762    10.20.100.108:443    tcp  17
172.230.87.3:28518   20.6.25.154:443  162.150.100.15:79761    10.20.100.108:443    tcp  2
188.143.41.11:39902  20.6.25.154:443  162.150.100.15:69762    10.20.100.110:443    tcp  121
212.230.87.2:52490   20.6.25.154:443  162.150.100.15:89761    10.20.100.109:443    tcp  64
```

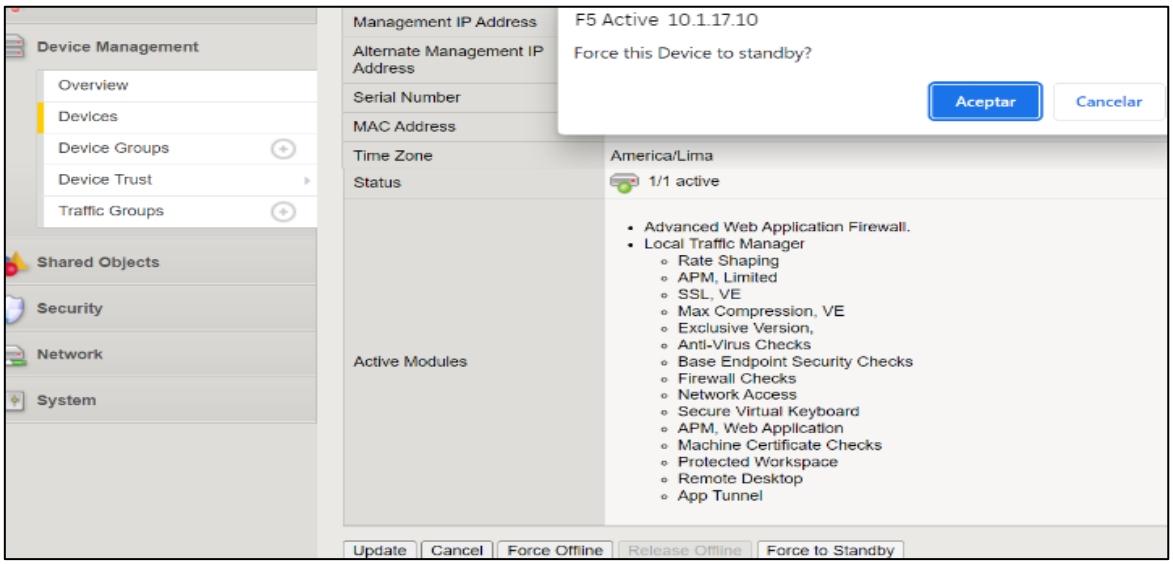
Nota. Conexión operativa con router de contingencia – ISP

De esta manera se observa que el servicio permanece sin interrupción, finalmente se verificó el estado del clúster F5 BIG IP ASM, es decir ante alguna falla del equipo principal todo el tráfico funciona a través del equipo F5 BIG IP ASM secundario.

Como se observa en la Figura 65, se puede observar que el equipo activo de IP 10.1.17.10 fue forzado a standby.

Figura 65

F5 BIG IP ASM principal conmutación de tráfico a F5 BIG IP ASM Pasivo



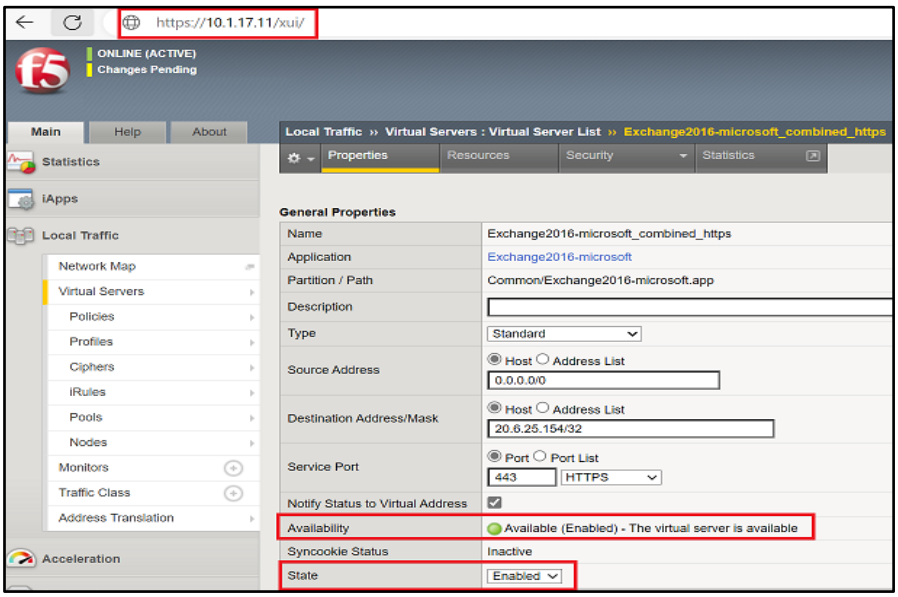
Nota. El gráfico representa la conmutación del tráfico desde el F5 Activo hacía el balanceador pasivo

Y el equipo de IP de gestión 10.1.17.11 como se mostró en la Tabla 1 previamente compartida, referente al equipo F5 secundario, asume todo el tráfico debido a que toda la configuración fue replicada mediante la sincronización de equipos F5 activo y pasivo, conforme a lo anteriormente mostrada en la Figura 46.

En la Figura 66 se puede observar el F5 secundario asumió el rol de F5 activo luego de la conmutación realizada en la Figura 65.

Figura 66

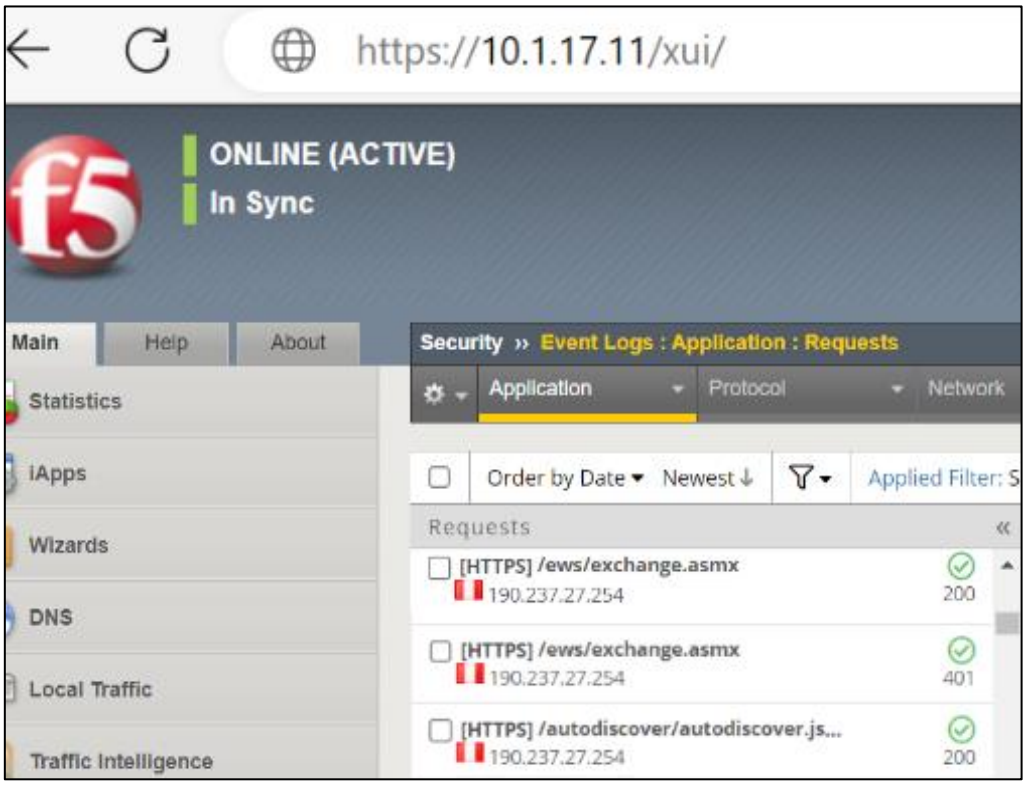
Balanceador secundario en modo Activo



De las pruebas observamos que el servicio del acceso vía web al correo electrónico OWA opera correctamente, como se observa a continuación en la Figura 67, se puede verificar las conexiones a través del equipo F5 BIG IP ASM secundario de IP 10.1.17.11 que asumió el rol de activo, presenta conexiones de distintas IPs públicas externas.

Figura 67

Conexiones a nivel de interfaz gráfica de usuario en F5 BIG IP ASM Secundario



Nota. Conexiones al servicio de correo electrónico en F5 BIG IP Secundario

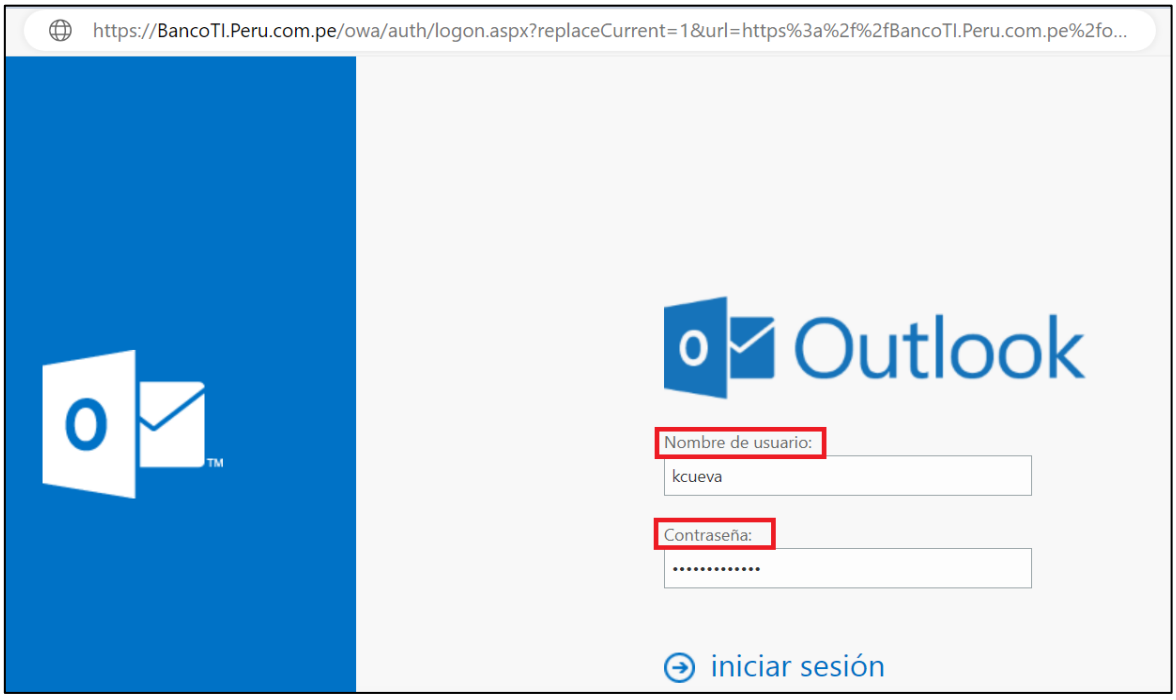
Con lo cual se verifica el funcionamiento del cluster F5 y el enlace con el ISP (proveedor de Internet).

3.3.4 VALIDACIÓN DEL ACCESO VÍA WEB A BANDEJA DE CORREO

Luego de compartir que el servicio se encuentra operativo y seguro, en la Figura 68 se da a conocer el proceso de validación del acceso al buzón de correo electrónico, para ello se introducen las credenciales, el usuario de prueba es “User: kcueva”, validándose así la comprobación de manera satisfactoria del acceso vía web al correo electrónico y su operatividad.

Figura 68

Prueba de operatividad del acceso vía web a bandeja de correo electrónico



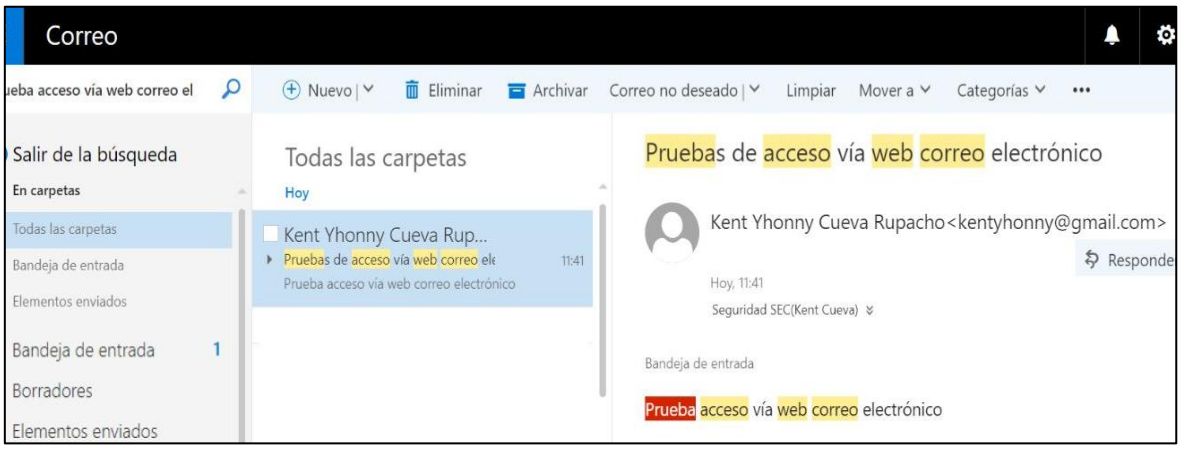
Nota. El gráfico representa la validación de credenciales del usuario de prueba

En la Figura 69, se validó el acceso satisfactorio al buzón de correo electrónico de enlace web “https://BancoTI.Peru.com.pe”, donde se realizaron pruebas de recepción de correo desde el correo kentyhonny@gmail.com hacía el buzón del usuario de prueba de la entidad bancaria “kcueva” siendo los resultados de recepción satisfactorios como se puede ver a continuación.

Es importante acotar que solo personal de banco puede acceder al buzón de correo electrónico web desde internet, mientras que otras cuentas de correo como (Hotmail.com, Gmail.com, yahoo.com, etc) al no pertenecer al dominio del banco no pueden ingresar y su tráfico de intento de inicio de sesión es bloqueado.

Figura 69

Prueba de recepción de correo



Nota. verificación de recepción de correo en buzón de usuario

De igual manera en la Figura 70, se pudo observar que se realizaron pruebas de conexión a nivel de un dispositivo móvil, donde se ingresó el usuario de pruebas “kcueva” de lo cual se verificó que el acceso y recepción de correo fueron satisfactorios, como se muestra a continuación:

Figura 70

Acceso al correo electrónico vía mediante dispositivo móvil

Nota. Pruebas de recepción de correo electrónico

Las pruebas fueron realizadas de manera satisfactoria, de lo cual la IP pública de la conexión remota de la laptop HP proveniente de la Figura 71, utilizó la IP “38.25.25.76”.

Figura 71

IP Pública utilizada para el acceso vía web al correo electrónico OWA

Nota. El gráfico mostrado hace referencia a la IP publica del usuario de prueba en la laptop HP para el acceso vía web al correo electrónico OWA, Adaptado de adslzone.net, 2023, (https://www.cual-es-mi-ip.net/)

Y la IP pública del celular de la Figura 72 mediante el cual se ejecutó las pruebas del acceso vía web al correo electrónico fue “132.191.1.117”, como se puede observar en la Figura 72.

Figura 72

IP Pública utilizada para el acceso vía web al correo electrónico OWA

Nota. El gráfico mostrado hace referencia a la IP publica del usuario de prueba mediante un teléfono celular para el acceso vía web al correo electrónico OWA, Adaptado de adslzone.net, 2023, (https://www.cual-es-mi-ip.net)

El detalle de la verificación de la conexión establecida inicia en la IP publica 38.25.25.76 “ IP de la Laptop HP, que establece la conexión remota” y se conecta a la IP pública 20.6.25.154 “IP pública configurada para el acceso vía web al correo electrónico, dicha IP fue compartida en la Tabla 2”.

Del mismo modo ocurre con la conexión del acceso al correo electrónico vía web desde el celular, cuya IP publica es “132.191.1.117” conforme a lo mostrado en la Figura 72 previamente compartida.

Se observa que las IPs establecen una conexión al balanceador de IP publica “20.6.25.154” quien establece la sesión con los servidores de correo electrónico de IPs “10.20.100.108, 10.20.100.109, 10.20.100.110” IPs compartidas en la Tabla 2, demostrando así que el balanceador de carga F5 BIG IP balancea el tráfico entrante entre los servidores, repartiendo el tráfico de manera uniforme, ver Figura 73.

Figura 73

Verificación de conexión satisfactoria de IPs publicas

```
show sys connection cs-server-addr 20.6.25.154
Sys::Connections
IP Public             IP Server         Selft IP          Server mails         Type
38.25.25.76:6756      20.6.25.154:443   168.200.127.10    10.20.100.108:443    tcp  12
132.191.1.117:1258    20.6.25.154:443   168.200.127.10    10.20.100.109:443    tcp  10
181.176.41.247:4651   20.6.25.154:443   168.200.127.10    10.20.100.110:443    tcp  14
```

Nota. El gráfico representa a la verificación de conexiones establecidas del usuario de prueba mediante teléfono celular y laptop HP

CONCLUSIONES

- Se implementó el acceso vía web al correo electrónico OWA, de forma segura, flexible y remota, permitiendo a los trabajadores acceder de manera efectiva a sus buzones de correo desde cualquier equipo conectado a la red pública, lográndose así cumplir con las expectativas del proyecto y beneficiando a la entidad bancaria con un sistema de conexión estable.

- Se configuró el balanceo de carga, lográndose verificar la correcta distribución del tráfico ante alguna caída del servidor de correo, así mismo F5 BIG IP ASM redirecciona el tráfico solo a los servidores operativos, evitando así la pérdida del servicio y se garantizando una conexión con mínima tolerancia a fallos.

- Se configuró un enlace de contingencia con el ISP (proveedor de internet) lográndose asegurar la redundancia del servicio en caso de una caída del enlace de internet principal. Además, se configuró el clúster de tipo activo y pasivo para el equipo F5 BIG IP ASM, de modo que ante cualquier fallo en este dispositivo no afecte negativamente la operatividad del servicio, asegurando así la alta disponibilidad y minimizando el impacto de posibles incidencias garantizando así la continuidad y confiabilidad del servicio.

- Verificamos la operatividad del acceso vía web al correo electrónico mediante pruebas de acceso a las bandejas de los trabajadores así mismo se realizó pruebas de recepción de correo, todas con resultados satisfactorios.

- Se concluye que el trabajo es replicable al cumplir todos los objetivos específicos, siendo aplicable a múltiples entidades que requieran una conexión remota, flexible, eficiente, segura y confiable.

RECOMENDACIONES

- Se recomienda la implementación de un captcha en la interfaz de acceso de credenciales para el acceso vía web al correo electrónico OWA, esta medida fortalecerá la seguridad de las cuentas de correo y ayudará a prevenir accesos no autorizados, garantizando un desafío adicional de protección ante ataques frecuentes de la red pública para el robo de credenciales, previo a esta nueva implementación se debe de adquirir el licenciamiento del módulo APM.

- Recomendamos implementar un repositorio de recepción de eventos integrado al equipo F5 BIG IP ASM, para almacenar registros y eventos antiguos que exceden su capacidad de almacenamiento, permitiendo así solventar los procesos de auditorías y generación de respaldo de información, este servidor puede ser virtual, físico o en la nube, pero en todos los casos involucra costos monetarios.

- Se recomienda configurar la periodicidad semanal de backups del equipo F5 BIG IP ante alguna avería del equipo.

- Se recomienda realizar la actualización periódica de la base de firmas maliciosas del equipo F5 BIG IP ASM utilizada para la protección de aplicaciones web y apps.

- Se recomienda implementar el servicio de DDOS para la protección de ataques de denegación de servicio, su implementación involucra costo monetario para acceder a los recursos de F5 en la nube, y utilizar el licenciamiento de mitigación de ataques DDos.

BIBLIOGRAFÍA

Adslzone.net. (2023). Cual es mi IP pública. Obtenido de Cual es mi IP: https://www.cual-es-mi-ip.net/

Ariganello, E. (2014). Guía de estudio para la certificación CCNA Routing y Switching. En E. Ariganello, *Guía de estudio para la certificación CCNA Routing y Switching.* Mexico: RA-MA. Obtenido de https://www.academia.edu/44609332/Redes_Cisco_Gu%C3%ADa_de_estudio_para_la_certificaci%C3%B3n_CCNA_Routing_y_Switching_S%C3%B3lo_fines_educativos_LibrosVirtual

Benavides Guayacán, E. A., & Olaya Toledo, D. (2018). Diseño de un plan de contingencia para un enlace crítico del banco Financorp. Universidad Piloto de Colombia. Facultad de Ingeniería especialización en Telecomunicaciones, Bogotá. Obtenido de http://repository.unipiloto .edu. co/handle/ 20.500.122 77/10139

BITS. (2022). *FortiGate High Availability HA [Figura 10]*. Obtenido de: https://bits.com.mx/fortigate-high-availability-ha/

Briceño, E. v. (2021). *Seguridad de la Información.* Editorial Área de Innovación y Desarrollo,S.L. doi. Obtenido de: https://doi.org/10.17993/tics.2021.4

Bruno Chavarria, N., & Gudiño, E. (2017). *Implementación de un servidor web y un diseño de una pagina utilizando herramientas de sofware libre, para el dispensario "Sagrada Familia" De la ciudad de Guayaquil.* Obtenido de https://dspace.ups. edu.ec/bitstream/123456789/14162/1/GT001840.pdf

Cabezas Cedeño , N. (2020). *Configuración del Firewall de aplicaciones web Modsecurity para prevenir diversos ataques hacia aplicaciones web alojados en servidores Open Source.* Universidad Católica del Ecuador sede Esmeraldas. Obtenido de https://repositorio.pucese.edu.ec/bitstream/123456789/2232/1/cabezas%20cede%c3%91O%20natalie%20karine.pdf

Carles, M. (2004). *Desarrollo de aplicaciones Web.* Barcelona: GNU free documentation License. Obtenido de https://libros.metabiblioteca.org/server/api/core/ bitstreams/a37985ce-f55b-49a6-9ac4-bff7d082cdbf/content

Ciriaco Susanibar, N. A. (2021). *Optimización del servicio de red con el respaldo del enlace a internet Wan y la seguridad perimetral para la empresa Sonepar sede Lima.* Universidad Nacional Tecnológica de Lima Sur, Lima.

Cisco. (2018). *Conceptos básicos de seguridad de red para pymes.* Cisco. Obtenido de https://www.cisco.com/c/dam/global/es_es/solutions/small-business/pdf/smb_network-security_checklist.pdf

Cloudflare. (2023). *¿Qué es el protocolo de control de mensajes de Internet (ICMP)?*. Obtenido de: https://www.cloudflare.com/eses/learning/ddos/ glossary/ internet-control-message-protocol-icmp/

codeburst. (2020). *Load Balancers, An Analogy [Figura 6]*.Obtenido de codeburst: https://codeburst.io/load-balancers-an-analogy-cc64d9430db0

comparitech. (2023). *Guía del servidor Microsoft Exchange*. Obtenido de Guía: https://www.comparitech.com/net-admin/ microsoft-exchange-server-guide/

Editorial Etecé. (2021). *HTTP*. (E. Etecé, Editor). Obtenido de: https://concepto.de/ http/

F5 Networks . (2023). *Equilibrador de carga*. Obtenido de Equilibrador de carga: https://www.f5.com/es_es/glossary/load-balancer

F5 Networks . (2023). *What is a Web Application Firewall (WAF)?*. Obtenido de: https://www.f5.com/glossary/web-application-firewall-waf

F5 Networks. (2013). *BIG-IP Application Security Manager.* Obtenido de: https://www.f5.com/pdf/products/big-ip-application-security-manager-overview.pdf

F5 Networks. (2015). *Overview of Least Connections, Fastest, Observed, and Predictive pool member load balancing*. Obtenido de: https://my.f5.com/manage/s/article/K6406

F5 Networks. (2017). *Deploying F5 with Microsoft Exchange 2016 Mailbox Servers.* Obtenido de: https://www.f5.com/pdf/deployment-guides/microsoft-exchange-2016-dg.pdf

F5 Networks. (2019). *Deploying F5 with microsoft exchange 2016 mailbox servers* Obtenido de: https://www.f5.com/pdf/deployment-guides/microsoft-exchange-2016-dg.pdf

F5 Networks. (2020). *K28426659: What is a WAF [Figura 2]*. Obtenido de: https://my.f5.com/manage/s/article/K28426659

F5 Networks. (2021). *K40456534: Descripción general de la detección de amenazas BIG-IP ASM*. Obtenido de: https://my.f5.com/manage/s/article/K40456534

F5 Networks. (2021). *K9231: Overview of BIG-IP daemon heartbeat failsafe*. Obtenido de K9231: https://my.f5.com/manage/s/article/K9231

F5 Networks. (2023). *BIG-IP HA - Do it the Proper Way*. https://clouddocs.f5.com/training/community/adc/html/class6/ intro.html

F5 Networks. (2023). *Configuring Bandwidth Load Balancing [Figura 9]*. Obtenido de: https://techdocs.f5.com/kb/en-us/products/lc_9_x/manuals/product/lc-implementations-12-1-0/3.html

F5 NETWORKS. (2023). *Configuring the Link Controller System to Manage Traffic*. Obtenido de: https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-link-controller-implementations/configuring-link-controller-to-manage-traffic.html

F5 NETWORKS. (2023). *F5 SUPPORT*. Obtenido de: https://www.f5.com/support

F5 Networks. (2023). *Intelligent application traffic management*. https://www.f5.com/products/big-ip-services/local-traffic-manager

F5 Networks. (2023). *Intro to: BIG-IP HA - Do it the Proper Way*. https://clouddocs.f5.com/training/community/adc/html/class6/intro.html

F5 Networks. (2023). *Overview of colored status icons in the Configuration utility.* Obtenido de: https://my.f5.com/manage/s/article/K12213214

F5 Networks. (2023). *Question about IAPP F5 exchange 2016 and 2019*. Obtenido de: https://my.f5.com/manage/s/case/500Hs00001wzymUIAQ/question-about-iapp-f5-exchange-2016-and-2019

F5 Networks. (2023). *Set up BIG-IP High Availability mode*. https://clouddocs.f5.com/products/openstack/agent/v9.8/ha-mode.html

F5 Networks. (2023). *Set up BIG-IP High Availability mode*. https://clouddocs.f5.com/products/openstack/agent/v9.8/ha-mode.html

geeksforgeeks. (2021). *Packet Filter Firewall and Application Level Gateway [Figura 5]*. Obtenido de: https://www.geeksforgeeks.org/ types-of-firewall-and-possible-attacks/

González Sánchez,]. L. (2002). La seguridad en la Red. *La seguridad en la Red.* Obtenido de: https://dialnet.unirioja.es

INCIBE. (2020). *versión de TLS tiene mi web*. Obtenido de INCIBE: https://www.incibe.es/empresas/blog/si-tu-web-cuent-certificado-seguridad-comprueba-utilizas-version-segura-del-tls

ISO/IEC, 2.-4. (2014). *Information technology — Security techniques — Network security .* Switzerland: ISO/IEC. Obtenido de https://www.amnafzar.net/ files/1/ISO%2027000/ISO%20IEC%2027033-4-2014.pdf

Jimenez Donayre, S. D. (2021). *Diseño e Implementación de una arquitectura de red redundante empleando balanceo de carga mediante los protocolos BGP y OSPF para optimizar la red Regional de Lima.*Universidad Nacional Tecnológica de Lima Sur, Lima. Obtenido de https://repositorio.untels. edu.pe/jspui/bitstream/123456789/918/1/T088A_48457179_T.pdf

Lansweeper. (2023). *Fin de vida útil del servidor Microsoft Exchange*. Obtenido de https://www.lansweeper.com/eol/microsoft-exchange-server-end-of-life/

Liberatori, M. C. (2018). *Redes de Datos y sus protocolos.* (J. M. Finochietto, Ed.) Argentina: EUDEM. Obtenido de http://www2.mdp.edu.ar/images/eudem/ pdf/redes%20de%20datos.pdf

Lorena, C. A. (2004). *Seguridad informática y seguridad de la información [Figura 1]*. Obtenido de Universidad Piloto de Colombia. Calderón: http://polux.unipiloto.edu.co:8080/00002658.pdf

Mesquida, C. L. (2003). *Guía de Iniciación a Actividad profesional Implantación de Sistemas de gestión de la seguridad de la Información (SGSI) según la norma ISO 27001 .* Obtenido de: https://www.coit.es/sites/default/files /informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_ la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Microsoft. (2023). *Exchange Server build numbers and release dates*. Obtenido de: https://learn.microsoft.com/en-us/exchange/new-features/ build-numbers-and-release-dates?view=exchserver-2019

Mifsud, E. (26 de Marzo de 2012). *Introducción a la seguridad informática - Seguridad de la información / Seguridad informática.* (INTEFP, Ed.) Obtenido de: http://recursostic.educacion.es/observatorio/web/en/software/ software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Networks, F. (2023). *Mitigating Brute Force Attacks - MyF5 | Support*. Obtenido de: https://techdocs.f5.com/kb/en-us/products/big-ip_asm/ manuals/product/ asm-implementations-11-5-0/3.html

Nord Security. (2023). *TCP vs. UDP, comparamos los dos protocolos*. Obtenido de: https://nordvpn.com/es/blog/protocolo-tcp-udp/

Pathak, A. (2023). *What is Firewall? – An Introduction Guide*. Obtenido de: https://geekflare.com/firewall-introduction/

Perdomo Salazar, C. A., Abril Avella, W. F., & Castro Avedaño, L. C. (2020). *Planeación de un proyecto de implementación para una solución de balanceo de carga BIG-IP F5 en la universidad Latinoamericana de Bogotá basado en el modelo PMI.* Universidad Santo Tomás especialización en Gestión de Redes de datos. Obtenido de https://repository.usta. /edu.co/ bit stream/handle/11634/30410/2020luiscastro.pdf?sequence=1&isAllowed=y

Piedrahita Villarraga, E. M. (2016).*Análisis comparativo de un Firewall de aplicaciones web comercial y un open source frente al TOP 10 de OWASP.* Universidad Nacional Abierta y a distancia (UNAD) Escuela de Ciencias Básicas, Tecnología e Ingeniería especialización en seguridad Informática -

Bogotá, Bogotá. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/9161/1022324147.pdf?sequence=1&isAllowed=y

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la Seguridad Informática y el análisis de Vulnerabilidades.* Manabi, Ecuador: Área de Innovación y Desarrollo, S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Securesoft. (2023). *Securesoft Corporation*. Obtenido de: https://www.securesoft corp.com/vision-y-mision

siaguanta. (2019). *Red cliente servidor [Figura 7]*. Obtenido de: https://siaguanta.com/c-tecnologia/red-cliente-servidor/

SitMexico. (2016). *Balanceadores de Carga*. Obtenido de: https://www.sitmexico.com/balanceadores-de-carga.php

Solleiro Rebolledo, J. L., Castañón Ibarra, R., Guillén Valencia, Á. D., Hernández Molina, T. Y., & Solís Mérida, N. (2022). *Vigilancia Tecnológica en ciberseguridad.* Obtenido de: https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia _Tecnologica_en_Ciberseguridad_Boletin.pdf

StemPrinting . (2021). *Ciberseguridad firewalls para empresas [Figura 4]*. Obtenido de: https://www.stemprinting.com /firewall-para-empresas/

Torres Almonacid, M. R. (2020). *Infraestructura Tecnológica virtual con alta disponibilidad basada en la nube para mejorar la continuidad operativa del LMS de la UNCP.* Universidad Nacional del centro del Perú Huancayo. Obtenido de: https://repositorio.uncp.edu.pe/bitstream/handle/ 20.500.12894/6416/T010_71868711_T.pdf?sequence=1

Universidad de Chile. (2008). *Como funciona la web.* (C. G. Gallardo, Ed.) Santiago de Chile. Obtenido de https://repositorio.uchile.cl/bitstream/handle/2250/120326/libroWeb-NV.pdf?sequence=1

Varela, V. (2023). *Qué es TLS*. Obtenido de prodigia: https://www.prodigia.com.mx/blog/espacio-prodigio-1/que-es-tls-111

ANEXOS

ANEXO 1. *VALIDACIÓN DEL ROL DE INGENIERO ONSITE*

SECURE SOFT CORPORATION

Protegemos tu información

Lima, 15 de agosto del 2023

CONSTANCIA DE TRABAJO

El Sr. Jorge Bernardo Castañeda Sanchez, Identificado con DNI N° 10121110, Gerente General de Securesoft Corporation S.A.C., con RUC N.º 20601317461.

CERTIFICA:

Que el(la) Sr(ta). **CUEVA RUPACHO KENT YHONNY**, identificado(a) con DNI - 77251552, labora en nuestra empresa desde el **09 de setiembre del 2019** hasta la actualidad, desempeñándose a la fecha como **INGENIERO ONSITE**.

Se expide la presente constancia a solicitud del interesado para los fines que estime conveniente.

Atentamente,

Jorge Bernardo Castañeda Sánchez
Gerente General

EL EMPLEADOR

SECURESOFT CORPORATION S.A.C.
Av. Manuel Olguin N° 325, Santiago de Surco – Lima Perú Central Telefónica (511) 711-2900
www.securesoftcorp.com

ANEXO 2. BALANCEADOR F5 BIG IP ASM 4000s

Especificaciones	4000s
Procesamiento de tráfico inteligente :	Solicitudes L7 por segundo: 425 000 conexiones L4 por segundo: 150 000 solicitudes HTTP L4 por segundo: 1,25 M Máximo de conexiones simultáneas L4: 10 M Rendimiento: 10 Gbps L4/L7
SSL de hardware:	Incluido: 4500 TPS (claves 2K) Máximo: 4500 TPS (claves 2K) Cifrado masivo de 8 Gbps*
SSL FIPS:	N / A
Protección DDoS de hardware:	N / A
Compresión de hardware:	N / A
Compresión de software:	Incluido: 4 Gbps Máximo: 4 Gbps
Arquitectura de software:	TMOS de 64 bits
Actualizable bajo demanda:	Sí
Procesador:	1 procesador Intel Xeon de cuatro núcleos (8 núcleos de procesamiento lógico hiperproceso en total)
Memoria:	16 GB
Disco duro:	500 GB
Puertos CU Gigabit Ethernet:	8

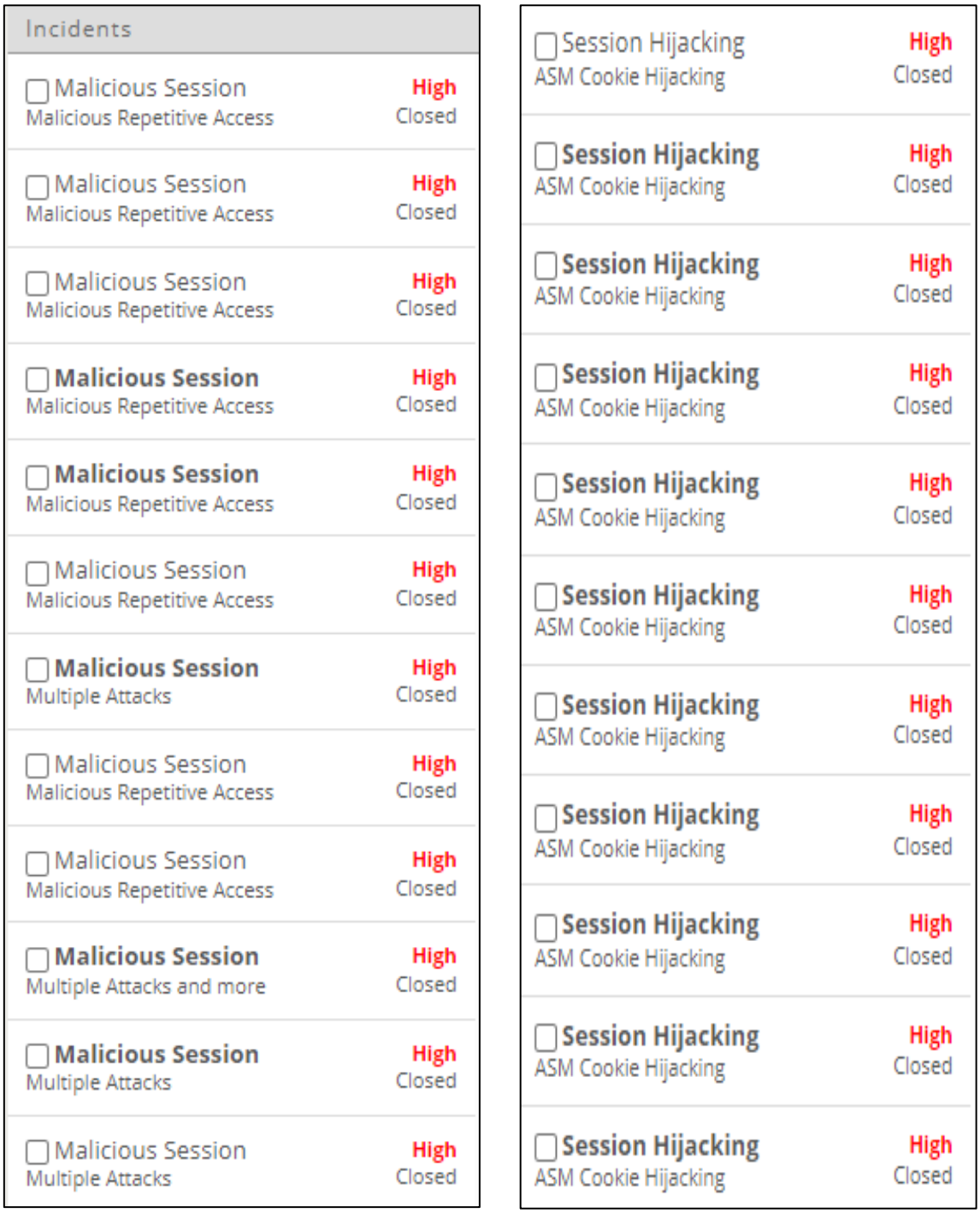
Puertos de fibra Gigabit (SFP):	SFP opcional (SX, LX o cobre)
10 puertos de fibra Gigabit (SFP+):	2 SR o LR (se venden por separado); Conexión directa de cobre 10G opcional
40 puertos de fibra Gigabit (QSFP+):	N / A
Fuente de alimentación:	Uno de 400 W incluido (eficiencia 80 Plus Platinum), opciones de alimentación dual y CC
Consumo típico:	95W (suministro único, entrada de 110V)**
Voltaje de entrada:	90-240 VCA +/- 10 % conmutación automática, 50/60 Hz
Salida de calor típica:	324 BTU/hora (suministro único, entrada de 110 V)**
Dimensiones:	1,75" (4,45 cm) de alto x 17" (43,18 cm) de ancho x 21" (53,34 cm) de profundidad Chasis de montaje en bastidor estándar industrial de 1U
Peso:	20 libras. (9,1 kg) (una fuente de alimentación)
Temperatura de funcionamiento:	32° a 104° F (0° a 40° C)
Humedad relativa operativa:	5 a 85% a 40° C
Aprobación de la agencia de seguridad:	UL 60950-1 2.ª edición CAN/CSA C22.2 No. 60950-1-07 EN 60950-1:2006, 2.ª edición IEC 60950-1:2006, 2.ª edición Evaluada para todos los países CB
Certificaciones/ Estándares de	EN 300 386 V1.5.1 (2010-10) EN 55022:2006 + A1:2007 EN 61000-3-2:2006 EN 61000-3-3:1995 + A1:2000 + A2:2005 EN

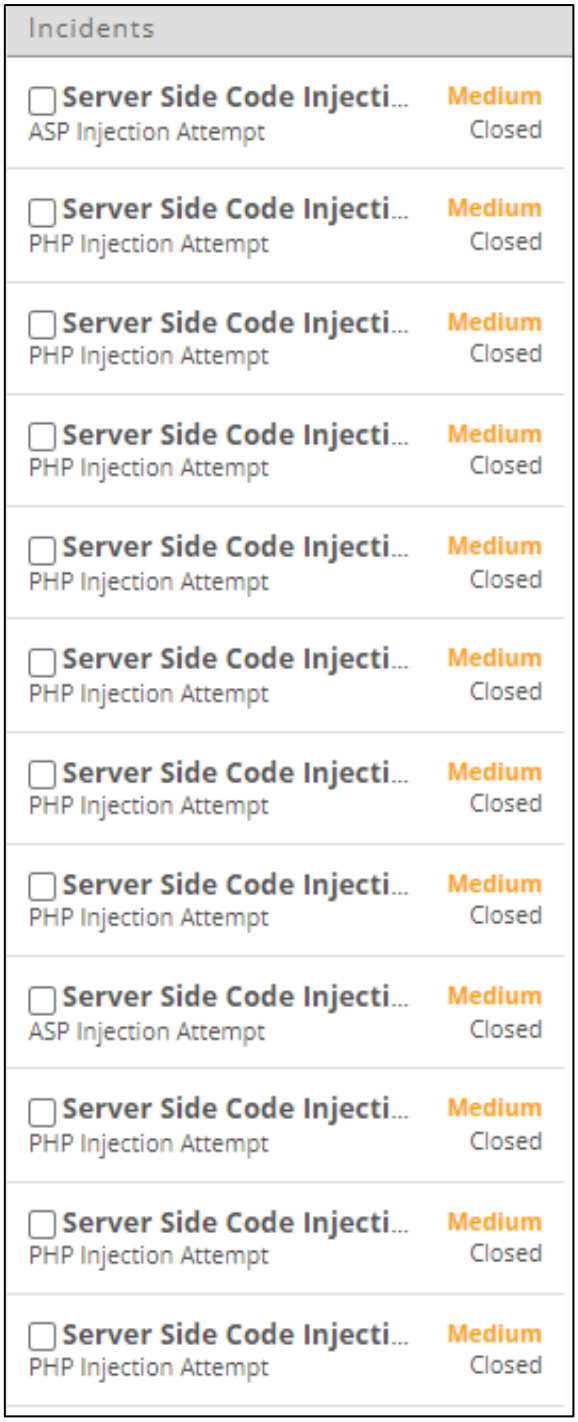
ANEXO 3. BALANCEO DE SERVIDORES DE CORREO EXCHANGE 2016

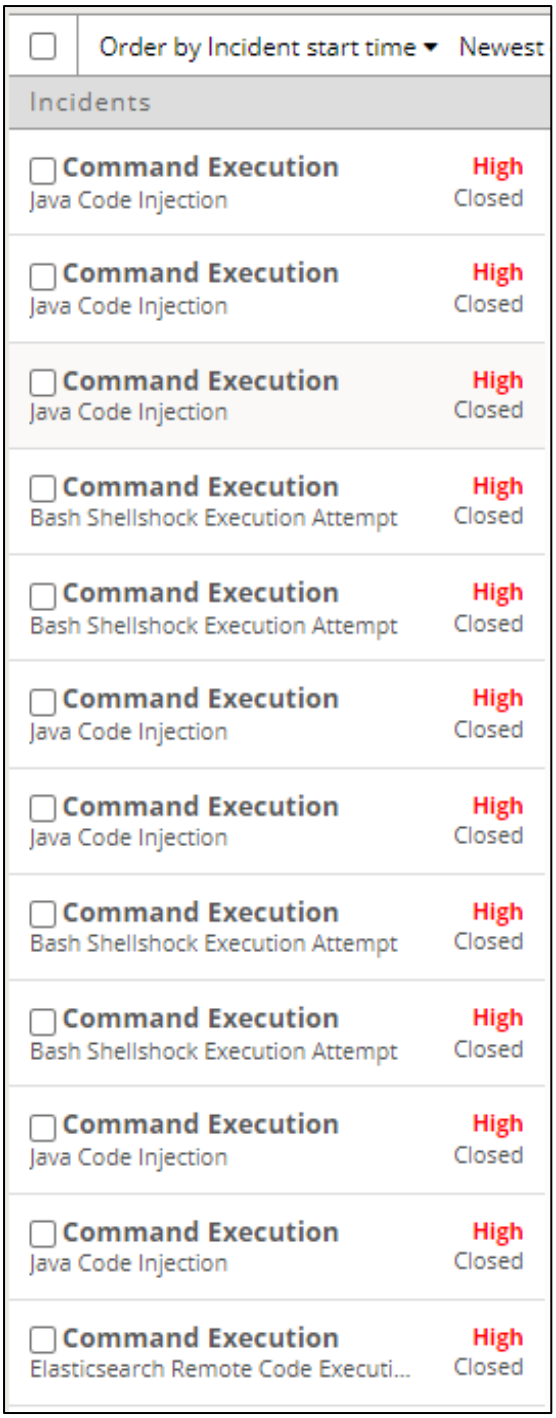
```
# show ltm pool Pool_Exchange_2016
-------------------------------------------------------------------------
Ltm::Pool: Pool_Exchange_2016
-------------------------------------------------------------------------
Status
  Availability          : available
  State                 : enabled
  Reason                : The pool is available
  Monitor               : gateway_icmp
  Minimum Active Members : 0
  Priority Groups       : 0/0/0 (highest/current/lowest)
  Current Active Members : 3
  Available Members     : 3
  Total Members         : 3
  Total Requests        : 7.5T
  Servers mail          : 10.20.100.108,10.20.100.109,10.20.100.110

Traffic                                                      ServerSide
  Bits In                                                         9.6T
  Bits Out                                                      249.1G
  Packets In                                                    662.1M
  Packets Out                                                   385.7M
  Current Connections                                               10
  Maximum Connections                                              204
  Total Connections                                             26.8M
```

ANEXO 4. VALIDACIÓN ATAQUES MALICIOSOS MITIGADOS POR F5 BIG IP




Incidents
Server Side Code Injecti...
ASP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
ASP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed
Server Side Code Injecti...
PHP Injection Attempt
Medium
Closed


Order by Incident start time
Newest
Incidents
Command Execution
Java Code Injection
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Bash Shellshock Execution Attempt
High
Closed
Command Execution
Bash Shellshock Execution Attempt
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Bash Shellshock Execution Attempt
High
Closed
Command Execution
Bash Shellshock Execution Attempt
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Java Code Injection
High
Closed
Command Execution
Elasticsearch Remote Code Executi...
High
Closed

ANEXO 5. VALIDACIÓN DE CONEXION DE MÚLTIPLES USUARIOS

```
show sys connection virtual-server VS-Exchange_2016
Sys::Connections
IP Public             IP Server        Selft IP              Server mails       Type
130.205.163.37:56924  20.6.25.154:443  168.200.127.10:54458  10.20.100.108:443  tcp  5
123.210.103.36:57702  20.6.25.154:443  168.200.127.10:57702  10.20.100.109:443  tcp  3
142.200.102.28:33328  20.6.25.154:443  168.200.127.10:43810  10.20.100.110:443  tcp  5
110.240.105.38:37486  20.6.25.154:443  168.200.127.10:52306  10.20.100.110:443  tcp  3
144.202.163.35:50040  20.6.25.154:443  168.200.127.10:52244  10.20.100.108:443  tcp  3
150.200.103.35:38612  20.6.25.154:443  168.200.127.10:52178  10.20.100.109:443  tcp  4
155.200.173.35:54064  20.6.25.154:443  168.200.127.10:54064  10.20.100.109:443  tcp  3
162.200.107.38:52670  20.6.25.154:443  168.200.127.10:38353  10.20.100.109:443  tcp  4
112.204.132.33:45276  20.6.25.154:443  168.200.127.10:9777   10.20.100.108:443  tcp  5
114.200.113.38:56660  20.6.25.154:443  168.200.127.10:2608   10.20.100.110:443  tcp  4
167.201.144.37:49164  20.6.25.154:443  168.200.127.10:9010   10.20.100.110:443  tcp  9
119.200.153.37:42212  20.6.25.154:443  168.200.127.10:23265  10.20.100.109:443  tcp  5
122.207.165.35:45666  20.6.25.154:443  168.200.127.10:33937  10.20.100.109:443  tcp  2
130.220.169.36:41304  20.6.25.154:443  168.200.127.10:32018  10.20.100.108:443  tcp  4
125.200.172.37:41432  20.6.25.154:443  168.200.127.10:31537  10.20.100.110:443  tcp  6
146.210.194.33:59732  20.6.25.154:443  168.200.127.10:33569  10.20.100.109:443  tcp  4
147.200.187.38:58662  20.6.25.154:443  168.200.127.10:33315  10.20.100.110:443  tcp  6
159.200.131.38:45566  20.6.25.154:443  168.200.127.10:31864  10.20.100.108:443  tcp  4
116.280.100.37:37174  20.6.25.154:443  168.200.127.10:23920  10.20.100.108:443  tcp  4
155.200.102.28:56570  20.6.25.154:443  168.200.127.10:31990  10.20.100.110:443  tcp  3
153.241.153.38:55610  20.6.25.154:443  168.200.127.10:38002  10.20.100.109:443  tcp  5
176.221.199.34:48894  20.6.25.154:443  168.200.127.10:48894  10.20.100.110:443  tcp  4
171.200.190.34:53206  20.6.25.154:443  168.200.127.10:9889   10.20.100.110:443  tcp  4
191.200.111.35:48862  20.6.25.154:443  168.200.127.10:9488   10.20.100.109:443  tcp  6
180.202.128.33:52954  20.6.25.154:443  168.200.127.10:54655  10.20.100.110:443  tcp  4
178.200.103.37:43504  20.6.25.154:443  168.200.127.10:54758  10.20.100.108:443  tcp  3
129.250.137.35:42150  20.6.25.154:443  168.200.127.10:51873  10.20.100.108:443  tcp  5
183.182.111.35:55550  20.6.25.154:443  168.200.127.10:51942  10.20.100.109:443  tcp  4
185.200.193.36:42968  20.6.25.154:443  168.200.127.10:51894  10.20.100.110:443  tcp  5
192.201.173.77:33668  20.6.25.154:443  168.200.127.10:61970  10.20.100.109:443  tcp  4
195.200.102.32:52670  20.6.25.154:443  168.200.127.10:61778  10.20.100.110:443  tcp  4
197.212.143.27:42444  20.6.25.154:443  168.200.127.10:61755  10.20.100.108:443  tcp  4
```

3% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 3% Base de datos de Internet
- Base de datos de Crossref
- 0% Base de datos de trabajos entregados
- 0% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.untels.edu.pe Internet	2%
2	community.f5.com Internet	<1%
3	repositorio.unsaac.edu.pe Internet	<1%
4	learn.microsoft.com Internet	<1%
5	repository.usta.edu.co Internet	<1%
6	cybertesis.unmsm.edu.pe Internet	<1%
7	doku.pub Internet	<1%
8	dspace.ups.edu.ec Internet	<1%

9	informatica.upla.edu.pe Internet	<1%
10	patents.google.com Internet	<1%
11	repositorio.ucsg.edu.ec Internet	<1%
12	repositorioacademico.upc.edu.pe Internet	<1%
13	oa.upm.es Internet	<1%
14	repository.unad.edu.co Internet	<1%
15	shop.growhit.com Internet	<1%
16	video.aoljobs.com Internet	<1%
17	dccia.ua.es Internet	<1%
18	scribd.com Internet	<1%
19	securityfocus.com Internet	<1%