OFICINA DE POSGRADOS

Tema:

SOFTWARE DEFINED WIDE AREA NETWORKING (SD-WAN) COMO MECANISMO DE SEGURIDAD EN ACCESOS WAN

Proyecto de Investigación y Desarrollo previo a la obtención del título del Magister en Ciberseguridad

Línea de Investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

JONATHAN FERNANDO QUEZADA HARO

Director:

ING. ALBERTO ARELLANO

Ambato – Ecuador

Marzo 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

***SOFTWARE DEFINED WIDE AREA NETWORKING* (SD-WAN) COMO MECANISMO DE SEGURIDAD EN ACCESOS WAN**

Línea de Investigación:

Seguridad de la Información: Tiene como objeto de investigación el manejo y aseguramiento de la información, aborda temas relacionados con el conjunto de herramientas, buenas prácticas, controles, directrices, métodos de gestión de riesgos, que utiliza para proteger los activos dentro de una organización.

Autor:

JONATHAN FERNANDO QUEZADA HARO

Alberto Leopoldo Arellano, Ing. Msc — f.____
CALIFICADOR

Darío Javier Robayo Jacome, Msc. — f.____
CALIFICADOR

Jose Marcelo Balseca Manzano, Msc — f.____
CALIFICADOR

Padre Juan Carlos Acosta, Mg. — f.____
DIRECTOR UNIDAD ACADEMICA

Hugo Rogelio Altamirano Villaroel, Dr. — f.____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2021

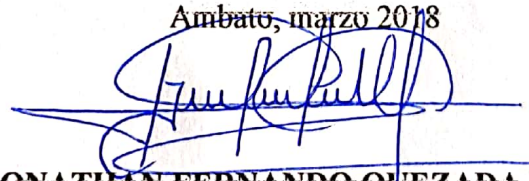
DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JONATHAN FERNANDO QUEZADA HARO,** con **CC. 180407525-5,** autor del trabajo de graduación intitulado: "*SOFTWARE DEFINED WIDE AREA NETWORKING* (SD-WAN) COMO MECANISMO DE SEGURIDAD EN ACCESOS WAN", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD,** en la escuela de **Postgrados.**

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respeta los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respeta las políticas de propiedad intelectual de Universidad

Ambato, marzo 2018



JONATHAN FERNANDO QUEZADA HARO

CC. 180407525-5

AGRADECIMIENTO

Agradezco a Dios y a mis padres por brindarme esa oportunidad de existir en este mundo, a mi hermano y a mi familia por ser quienes siempre me alientan a seguir adelante y a todos quienes conforman la Maestría en Ciberseguridad de la Pontificia Universidad Católica del Ecuador Sede Ambato – Primera Cohorte.

De manera especial quiero agradecer a mi Tutor Ing. Mg. Alberto Arellano por sus inestimables aportes en el desarrollo del trabajo de titulación que gracias a su guía y apoyo, se logró cumplir el objetivo planteado. Y primordialmente a mi madre que siempre, se ha preocupado por mí, me ha inculcado valores que no he olvidado y por ser el apoyo incondicional en todos los momentos de mi vida.

DEDICATORIA

A Dios por darme un día más de vida y brindarme las fuerzas necesarias para seguir adelante.

A mi madre Angélica que ha sido mi apoyo incondicional para alcanzar este importante éxito profesional en mi vida, a mi hermano Alexander que siempre ha estado pendiente en todo momento.

A mi amado hijo Cristopher Alejandro, por ser la luz y alegría de mis días y sobre todo el motor que me impulsa a siempre seguir adelante, a mi compañera de viaje Mayrita quien es el eje fundamental en mi desarrollo personal y profesional.

Jonathan

RESUMEN

Los departamentos de tecnologías de la información, se percatan, que los enlaces de comunicación entre el sitio matriz y las agencias son vulnerables a riesgos informáticos; ocasiona pérdida de tráfico a los usuarios que utilizan servicios críticos para la organización, como son la videoconferencia o la transferencia de archivos importantes; empieza a perder la calidad de la comunicación experimenta cortes o degradación en el servicio.

La necesidad de ancho de banda que existe en las oficinas remotas ya sea dentro de un país o entre diferentes países, cada día va en aumento; y una de las tendencias actuales para mejorar la experiencia del usuario es ir directamente a sus aplicaciones en la nube. Por lo tanto, el objetivo del trabajo de investigación es aplicar buenas prácticas de seguridad en una arquitectura de *Software Defined Wide Area Networking* (SD-WAN), para reducir los riesgos informáticos que son víctimas las organizaciones. Como resultado de este trabajo, se espera presentar a las organizaciones un conjunto de buenas prácticas en una arquitectura *Software Defined Wide Área Networking* (SD-WAN) que permita minimizar los riesgos informáticos y brindar alta disponibilidad; control y calidad a las comunicaciones, selección dinámicamente el mejor camino entre el sitio matriz y las agencias a un costo menor.

Palabras clave: Software Defined Wide Area Networking, riesgos informáticos, vulnerables, infraestructuras.

ABSTRACT

The Information Technology departments realize that the communication links between the main site and the agencies are vulnerable to IT risks, causing loss of traffic to users who use critical services for the organization, such as videoconferencing or the transfer of important files, and the quality of the communication starts to be lost, experiencing outages or degradation of the service.The need for bandwidth that exists in remote offices either within a country or between different countries, is increasing every day; and one of the current trends to improve the user experience is to go directly to their applications in the cloud. Therefore, the objective of this study is to apply good security practices in a Software Archirecture Defined Wide Area Networking (SD-WAN), in order to reduce the IT risks that organizations are victims of. As a result of this study, it is expected to present to the organizations a set of best practices in a Software Archirecture Defined Wide Area Networking (SD-WAN) that allows minimizing IT risks and providing high availability, control and quality in communications, dynamically selecting the best path between the main site site and the agencies at a lower cost.

***Keywords**: Software Defined Wide Area Networking, IT risks, vulnerable, infrastructures.*

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXO

INTRODUCCIÓN

La gestión de la red y la seguridad en el acceso a las aplicaciones en la actualidad, se ha convertido en la principal preocupación de las empresas, es así como la red de área amplia definida por software SD-WAN ha transformado la industria y la forma en que las empresas distribuidas hacen negocios. Aunque SD-WAN tiene muchos beneficios, también presenta muchos desafíos, incluida la falta de seguridad y el rendimiento impredecible (Palo Alto Networks, 2020).

El propósito de la red de área amplia definida por software SD-WAN es interconectar las redes de área local (LAN) en las ubicaciones centrales de una organización, como la sede central y los centros de datos, así como en las ubicaciones remotas. Los transportes y la tecnología de la WAN han evolucionado, y en los últimos años, las ofertas basadas en la conmutación de etiquetas multiprotocolo MPLS e Internet han desplazado a las demás opciones, la SD-WAN ha continuado este desplazamiento, permite la mercantilización tanto del MPLS como de Internet (Rouse, 2020).

Antecedentes

Hoy en día, los departamentos de TI están bajo presión para hacer más con menos; es decir, administrar más sitios y clientes con presupuestos limitados y un equipo relativamente pequeño, todo sin reducir la confiabilidad y la seguridad. El alto costo de la conectividad WAN empresarial, el soporte y el personal, combinados con el crecimiento de aplicaciones de transmisión de datos con gran ancho de banda y servicios basados en la nube, está obligada a que muchos administradores de red a busquen soluciones alternativas (Sánchez, 2019).

SD-WAN es un nuevo modelo distinto al tradicional con el que la red hace frente a los desafíos actuales.

El enfoque es la conectividad de la red, reduce costes operativos y mejorar el uso de recursos para implementaciones en varios sitios.

Debido a que las redes *Multiprotocol Label Switching* (MPLS) que una vez conectaron organizaciones de múltiples sitios a través de vastas distancias, ya no son la mejor solución; por sus costos elevados y la latencia que experimentan en sus comunicaciones (Majdoub, 2017).

Las organizaciones generan pérdidas de toda la comunicación; ya sea por la desconexión del enlace, o por el uso masivo por parte de los usuarios de las aplicaciones y servicios de la organización en la nube. Otra alternativa de conectividad para organizaciones que mantienen agencias distanciadas geográficamente es la arquitectura SD-WAN que ofrece ventajas como reducción de costos y eficiencia en la comunicación (Coronel, 2020). Sin embargo, el análisis de los riesgos de seguridad en esta arquitectura no ha sido estudiado experimentalmente; por lo que si bien es cierto ofrece ventajas tecnológicas, aún no habla de evidencias científicas desde la perspectiva de la ciberseguridad (Naula, 2020).

Con este antecedente el problema científico, se expresa como una pregunta: ¿Cómo configurar una arquitectura SD-WAN para reducir los riesgos informáticos?

Un conjunto de buenas prácticas configuradas en una arquitectura de red de área amplia definida por software reducirá los riesgos informáticos en las organizaciones.

La presente investigación tiene como objetivo aplicar buenas prácticas de seguridad en una arquitectura de *SD-WAN* para reducir los riesgos informáticos, pertenecientes a las empresas que brindan servicios tecnológicos de seguridad y proporcionan visibilidad del uso de aplicaciones en la red como la capacidad de controlar la seguridad en los accesos de los usuarios a esas aplicaciones en el Ecuador.

Además para lograr el cumplimiento de este proyecto de desarrollo, se plantea los siguientes **objetivos específicos:**

- Analizar las bases teóricas de *Software Defined Wide Area Networking* (SD-WAN) relacionadas con los riesgos informáticos.

- Diagnosticar el estado actual de los riesgos informáticos en arquitecturas de *Software Defined Wide Area Networking* (SD-WAN).
- Verificar el funcionamiento de una arquitectura de *Software Defined Wide Area Networking* (SD-WAN) bajo buenas prácticas de seguridad evidencia la reducción de riesgos informáticos.

Metodología de la Investigación

El tipo de investigación, que se utiliza para el desarrollo del presente proyecto es la cuasi experimental, el estudio está basado en implementaciones de escenarios simulados en entornos virtualizados para defender si un conjunto de buenas prácticas configuradas en una arquitectura de una red de área amplia definida por software reducirá los riesgos informáticos en las organizaciones.

Metodología de Desarrollo

La metodología aplicada es PPDIOO, la cual rige en lineamientos propuestos por Cisco para administración de red.

Como muestra en la figura 1, el seguimiento de este ciclo de vida propuesto que ayuda a cumplir objetivos trazados como son la disminución del costo total de administración de la red y aumento de disponibilidad de la red a su vez mejora en agilidad para implementación de cambios en la estructura de la red. El ciclo de vida es útil para la implementación de nuevas redes, así como para actualizaciones en redes existentes. Los elementos que conforman el ciclo de vida forman un círculo sin fin, por ejemplo, el paso de optimización conlleva a realizar actividades como identificar cambios, validar en la infraestructura existente; misma que conllevarían a iniciar desde el paso de preparación (Guerra, 2016).

Figura 1. Fases de Metodología PPDIOO

Fuente: (Guerra, 2016)

Fases del ciclo de vida PPDIOO

Fase I: Preparar

Se identifican los requerimientos que el usuario final va a demandar a la red, estas son: aplicaciones a usar, número de usuarios que va a tener la red, la demanda que va a tener cada una de las aplicaciones dentro de la red, entre otras. Con estos parámetros, se caracteriza los puntos importantes que describen cuál será el uso de la red.

Fase II: Planea

Se orienta a los requerimientos de la red, es decir aquí analiza y obtiene toda la información de la red existente (patrones de tráfico, tipo de tráfico que circula por la red, direccionamiento, enrutamiento, etc.). Con estos parámetros, se propone una arquitectura de diseño que pueda cumplir con todos los requerimientos obtenidos en la fase de preparación.

Fase III: Diseñar

Esta enfocada al desarrollo de la arquitectura lógica como física de la red, incorpora protocolos y tipo de equipos con modelos concretos a usar, también estipula el cableado estructurado, y todo esto en base a los requerimientos técnicos y empresariales obtenidos en fases anteriores.

Fase IV: Implementar

La red construye de acuerdo con las especificaciones obtenidas en las fases anteriores, mantiene una descripción de cada paso y del tiempo estimado para la implementación. Finalmente realizan pruebas de campo para verificar el diseño de esta.

Fase V: Operar

La red mantiene en funcionamiento y monitoreada con el fin de verificar su rendimiento, y así poder dar apertura a una futura optimización de la red misma.

Fase VI: Optimizar

Se proponen cambios en el diseño de la red siempre que el rendimiento, se degrade con el tiempo y sus requerimientos sean más exigentes, todo esto en base a una administración proactiva que identifica y resuelve los problemas antes que sucedan (Sean Wilkins, 2020).

Recopilación de requisitos de red

El proceso de recopilación de requisitos, se divide en cinco pasos. Durante estos pasos (en lenguaje de proyectos denominado hitos), el diseñador analiza el proyecto con el personal del cliente para determinar y reunir los datos necesarios, incluye la documentación apropiada, sigue los pasos:

- Identificar las aplicaciones de red y servicios de red planificados.

- Determinar los objetivos de la organización.
- Determinar las posibles limitaciones de la organización.
- Determinar los objetivos técnicos.
- Determinar las limitaciones técnicas a ser tomadas en cuenta.

Se realiza una investigación de casos de uso de las tecnologías de red de área amplia definida por software SD-WAN, por lo tanto, los elementos de una configuración SD-WAN funcionan juntos, donde permiten:

- Agrupar las interfaces físicas Ethernet que comparten un destino común en una interfaz lógica SD-WAN.
- Especificar las velocidades de enlace.
- Especificar los umbrales a los que un camino deteriorado (o un apagón o una caída de tensión) hacia una SD-WAN garantiza la selección de un nuevo mejor camino.
- Especificar el método de selección de esa nueva mejor ruta.
- Esta vista indica las relaciones entre los elementos de un vistazo.

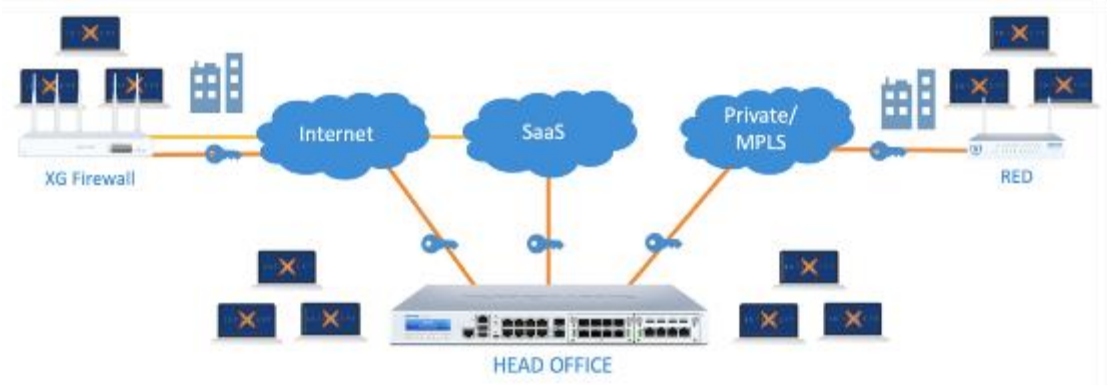


Figura 2. Conexión de agencias a través de SD-WAN

Fuente: (Sophos XG, p.4)

La red de área amplia definida por software controla que los enlaces acordes al tráfico que generan tomen túneles VPN específicos o el acceso sea directo a Internet debido a que ciertas aplicaciones o servicios toman de una agencia a un concentrador o de una agencia a

Internet. Agrupar las rutas de modo que, si una conexión deteriora, el *firewall* selecciona una nueva mejor ruta (Palo Alto Networks, 2020).

- Un perfil SD-WAN especifica la interfaz física y el tipo de enlace de esa interfaz (ADSL / DSL, módem de cable, Ethernet, fibra, LTE/3G/ 4G/ 5G, MPLS, microondas /radio, satélite, Wifi, u otro). En el perfil de SD-WAN, se especifica las velocidades máximas de carga y descarga (en Mbps) de la conexión del proveedor de internet. También cambiar si el *firewall* monitorea la ruta con frecuencia o no; donde el *firewall* supervisa todos los enlaces de forma predeterminada (Palo Alto Networks, 2020).
- Enrutamiento de las aplicaciones sobre el mejor enlace mediante reglas de *firewall* o enrutamiento basado en políticas.
- Una interfaz virtual SD-WAN es un túnel VPN o un grupo directo de internet constituido con una o más interfaces que forman una interfaz SD-WAN virtual numerada a la que enrutar el tráfico. Las rutas que pertenecen a una interfaz SD-WAN van todas a la misma WAN de destino y son todas del mismo tipo ya sea mediante un túnel de acceso directo a internet o una VPN IPSec (Palo Alto Networks, 2020).

Justificación

En la actualidad, todas las organizaciones y personas son víctimas de los cibercriminales, dado que en la actualidad están mejor organizados y las amenazas son cada día más sofisticadas, es imperativo contar con capacidades para realizar una evaluación de ciberseguridad a las redes SD-WAN.

Con el diagnóstico de ciberseguridad a la red SD-WAN, se permitirá garantizar la seguridad al interconectar las redes de área local (LAN) en ubicaciones remotas de una organización, como la sede central y los centros de datos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1 Comunicaciones SD-WAN

Una Red de área amplia definida por software es un nuevo enfoque de conectividad con la tecnología de la WAN. Administra diferentes tipos de conexiones, incluye el MPLS, banda ancha, y *Long Term Evolution* (LTE); apoyar la comunicación de aplicaciones alojadas en los centros de datos, nubes públicas y privadas, y ruta de tráfico optimizar el camino en tiempo real (Lessing, 2020).

Los ejecutivos de TI recurren a las redes de área amplia definida por software para obtener una conectividad rápida y fiable con múltiples nubes y agencias.

Según la (Corporación Internacional de Datos, 2020) son el principal proveedor mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, casi el 95% de las empresas usan actualmente la tecnología de SD-WAN o planean empezar a usarla dentro de 24 meses como muestra en la figura 3.

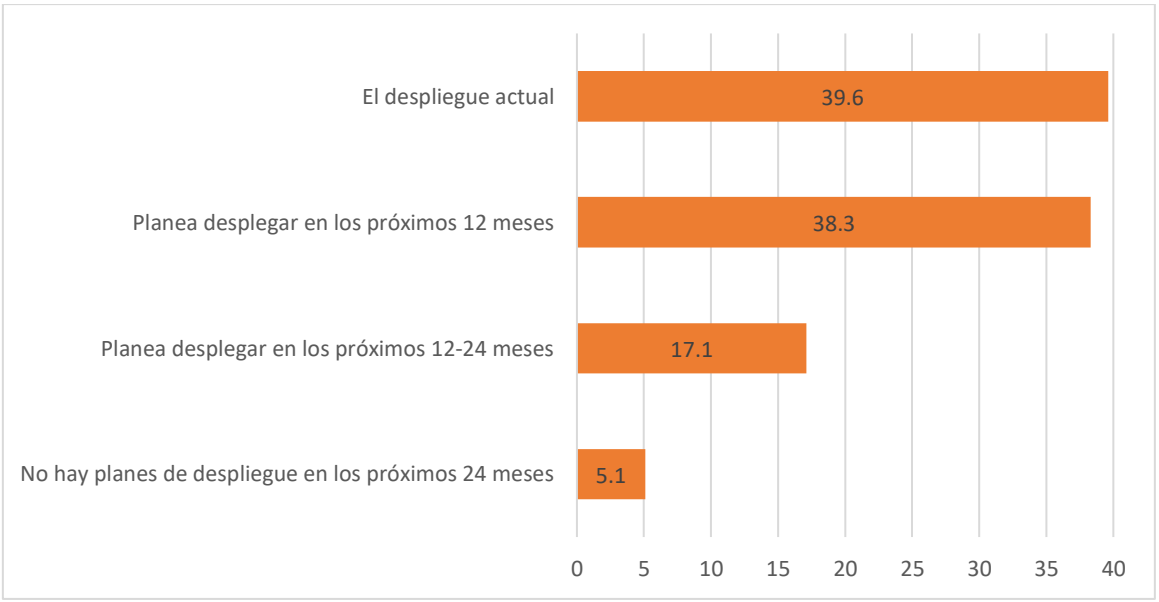


Figura 3. Traducido de IDC´s Software Defined WAN Survey, August 2018

Fuente: (International Data Corporation (IDC), 2020)

Gartner muestra una definició

n de lo que es una red de área amplia definida por software SD-WAN en la figura 4.

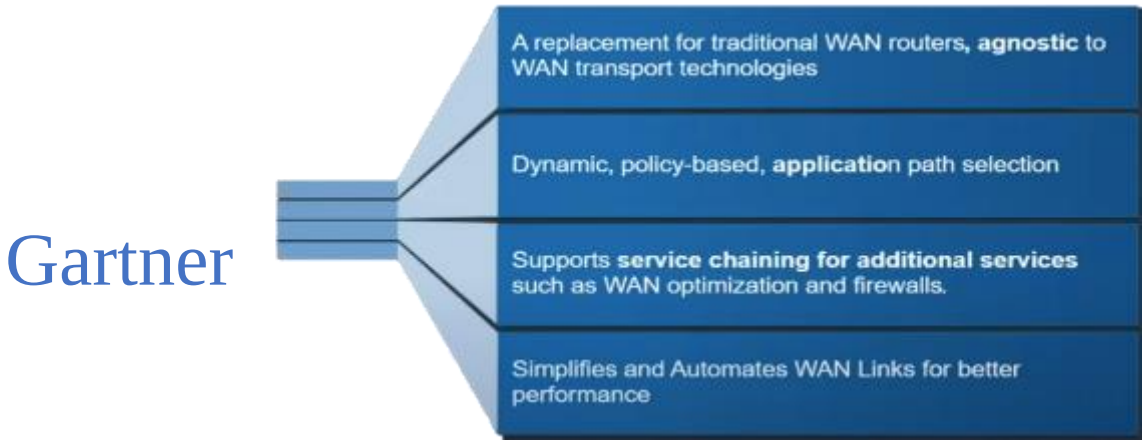


Figura 4. Definición de SD-WAN, Gartner MG

Fuente: Gartner (Septiembre 2020)

En septiembre de 2020, Gartner predice que la tecnología SD-WAN, se incluirá hasta en un 75% en la infraestructura para 2020 como muestra en la figura 5, y que el gasto en productos SD-WAN superará el gasto en enrutamiento tradicional para 2022, se muestra como líder de la solución a VMware y Fortinet (Gartner Research, 2020).

Figura 5. Cuadrante Mágico de Gartner para las infraestructuras de Borde

Fuente: Gartner (Septiembre 2020)

1.1.1 Características de SD-WAN

Una Red de área amplia definida por software permite tener diferentes tipos de servicios y conexiones como datos, internet y LTE o de una red MPLS tradicional, separa el plano de control del de datos, es decir, si pierde conexión a su plataforma de control los servicios funcionan sin ningún inconveniente, añade una sensación de mejora al usuario final (Palo Alto Networks, 2020).

Tiene una administración centralizada y mediante software, que permite la resolución de problemas de manera sencilla.

El Funcionamiento de la tecnología SD-WAN crece a medida que el número de dispositivos en las agencias aumentan y las aplicaciones, se vuelven más intensivas en ancho de banda, las empresas, se ven obligadas a gastar más para satisfacer esta demanda. Como resultado, las arquitecturas tradicionales de WAN con conmutación de etiquetas multiprotocolo MPLS tienden a consumir ancho de banda al transportar el tráfico de las agencias a la nube, lo que hace que los enfoques de WAN heredados sean ineficaces. El futuro de las empresas distribuidas es una red de área amplia definida por el software, que utiliza enlaces de productos básicos y permite gestionar y controlar de forma inteligente la conectividad entre las agencias. Sin embargo, con sus beneficios, la tecnología SD-WAN también trae muchos desafíos, como la falta de seguridad, el bajo rendimiento y la complejidad (Palo Alto Networks, 2020).

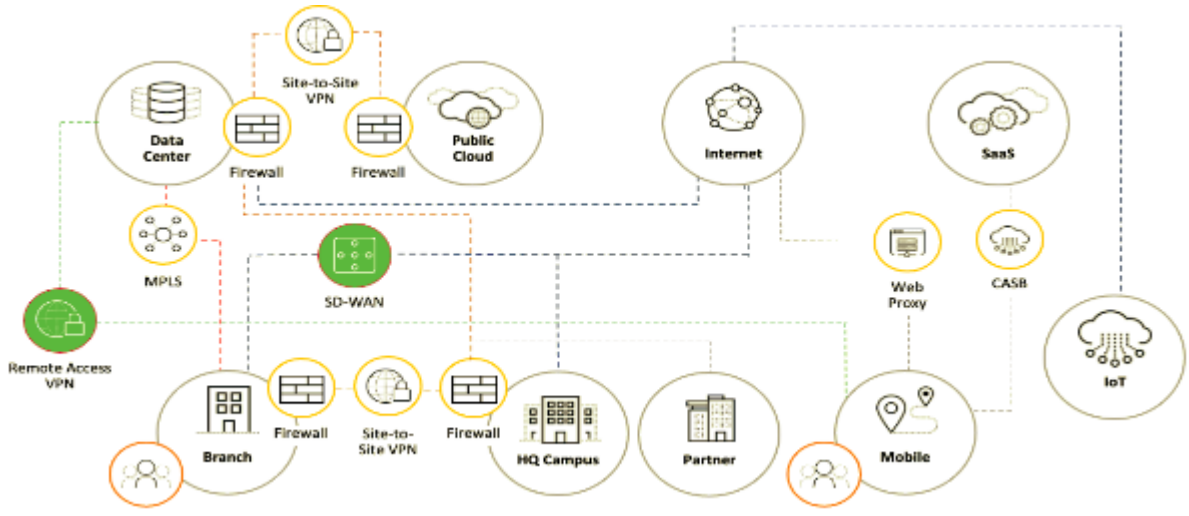


Figura 6. Tecnología SD-WAN

Fuente: Palo Alto (2020)

Como muestra en la figura 6 la tecnología SD-WAN centralizan en el CE de manera física múltiples enlaces de diferentes tecnologías y servicios con el objetivo de ser visto como un único enlace lógico, producto de la suma del ancho de banda de los mismos. Con la concentración de canales permite garantizar el funcionamiento de las aplicaciones independiente que presente un retardo, intermitencias en uno de los enlaces, debido a que los paquetes son enviados de manera automática por el mejor canal, para lo cual consideran los siguientes parámetros: latencia de WAN a WAN, verifica el *throughput* y la calidad del enlace (Palo Alto Networks, 2020).

1.1.2 Arquitectura

Una red de área amplia definida por el software proporciona visibilidad en el uso de aplicaciones y en la red como la capacidad de controlar el acceso de los usuarios a esas aplicaciones. Al inspeccionar la información de sesión y de carga útil del tráfico que atraviesa el *firewall*, se identifica las aplicaciones y proporciona un control granular de las mismas. Esta visibilidad también es esencial para que la tecnología SD-WAN proporcione una selección inteligente de la ruta por aplicación como muestra en la figura 7 (Palo Alto Networks, 2020).

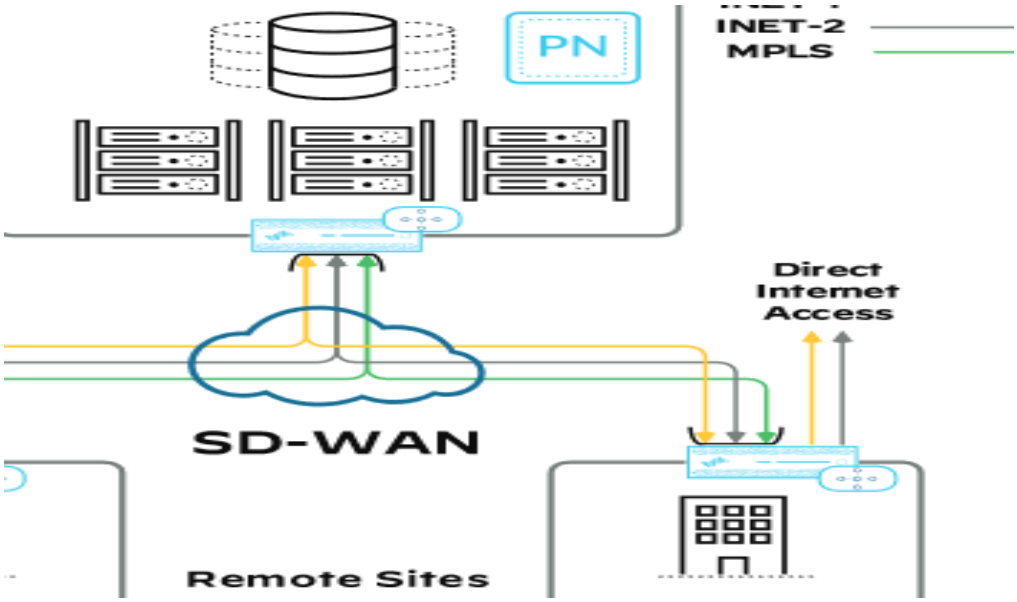


Figura 7. Conexión segura SD-WAN

Fuente: Palo Alto (2020)

Además de las capacidades uno de los retos es proporcionar una seguridad integral a las organizaciones que implementan esta tecnología de comunicación de la siguiente manera:

- Permitir de forma segura a los usuarios, el contenido y las aplicaciones incluidas las aplicaciones SaaS, clasifica todo el tráfico independientemente del puerto.
- Reducir el riesgo de un ataque mediante el uso de un modelo de aplicación positiva, permite todas las aplicaciones deseadas y bloquea todo lo demás.
- Aplicar políticas de seguridad para bloquear los exploits de vulnerabilidad conocidos, virus, *spyware*, *botnets* y otros malware desconocidos, como las amenazas persistentes avanzadas.

1.1.2 Seguridad

Uno de los pioneros en la adopción de tecnologías de área amplia definida por software es Cisco el cual ofrece una gama completa de funciones de seguridad integrada que aborda el cumplimiento de una manera integral al ofrecer un conjunto de controles de seguridad (Cisco, 2020).

Tabla 1. Controles de Seguridad Cisco SD-WAN

Componentes	**Controles de seguridad**
Plano de control	Modelo de seguridad de confianza cero
Plano de datos	Capas de seguridad integradas en las instalaciones y en la nube
Plano de gestión	Control de acceso basado en roles y ACL
Plataforma	Hardware, software y solución confiables

Fuente: Cisco SD-WAN

1.2 Eficiencias de conexión

Una red de área amplia definida por el software ofrece a las organizaciones que cuentan con múltiples agencias distribuidas geográficamente una serie de beneficios:

- **Mayor flexibilidad y agilidad**: con SD-WAN, las organizaciones tienen más opciones de conectividad, como el Internet de banda ancha, que es más rápida que las redes MPLS. Configurar, desplegar y administrar las redes MPLS lleva mucho tiempo para la mayoría de las organizaciones. La SD-WAN remedia este desafío porque separa el control de los servicios de red del transporte, permite que Internet esté disponible en una región determinada sin limitarse a la cobertura proporcionada por el portador del MPLS (Palo Alto Networks, 2020).

Figura 8. Despliegue de tecnología SD-WAN

Fuente: Palo Alto (2020)

- **Mejora de la experiencia del usuario**: sin SD-WAN, la conexión de las agencias a las aplicaciones en la nube es costosa. Las redes WAN tradicionales tienen que *backhaul* el

tráfico a la sede o al centro de datos corporativos, normalmente a través del MPLS. Esto lleva a una pobre experiencia de usuario (Palo Alto Networks, 2020).

- **Costo reducido:** la SD-WAN lleva a un sustancial ahorro de costes en:

    - Adquisición de hardware, software y soporte. Según Gartner, las empresas ahorran hasta un 40% en cinco años.
    - Personal para administrar, solucionar problemas y proveer equipos WAN.
    - Gastos de la red. Debido a que la SD-WAN complementa o sustituye el costoso MPLS con conectividad de banda ancha, el tráfico, se enrutada en base a la mejor opción de costo versus rendimiento.

1.3 Casos de uso

En las revisiones de las definiciones de casos de uso que implementan en las redes de área amplia definida por software no, se consideran implementaciones a nivel local porque no existen, sin embargo, se investigó casos de éxito en países que cuentan con tecnologías avanzadas donde promueven y apoyan a la protección de la información y a la gestión de la seguridad según el modelo de defensa en profundidad.

Los dos casos de uso más importantes identificados en la investigación son los siguientes:

- **Educación**

    Para el sector educativo, se ha hecho una revisión de trabajos de grado, postgrado a nivel nacional, pero al ser una tecnología nueva no, se ha implementado en Ecuador, sin embargo, el Ministerio de Educación de Canadá estableció un proyecto de modernización de banda ancha que hará la transición de todas las escuelas de Ontario de MPLS a banda ancha. Para aliviar la complejidad de la infraestructura académica y reducir significativamente el costo de MPLS, muchos distritos escolares canadienses recurren a la solución *Secure* SD-WAN

para permitirles cumplir con las regulaciones de privacidad y protección mientras mejoran los entornos de aprendizaje dentro de sus distritos para ambos estudiantes. y personal (Sophos, 2020).

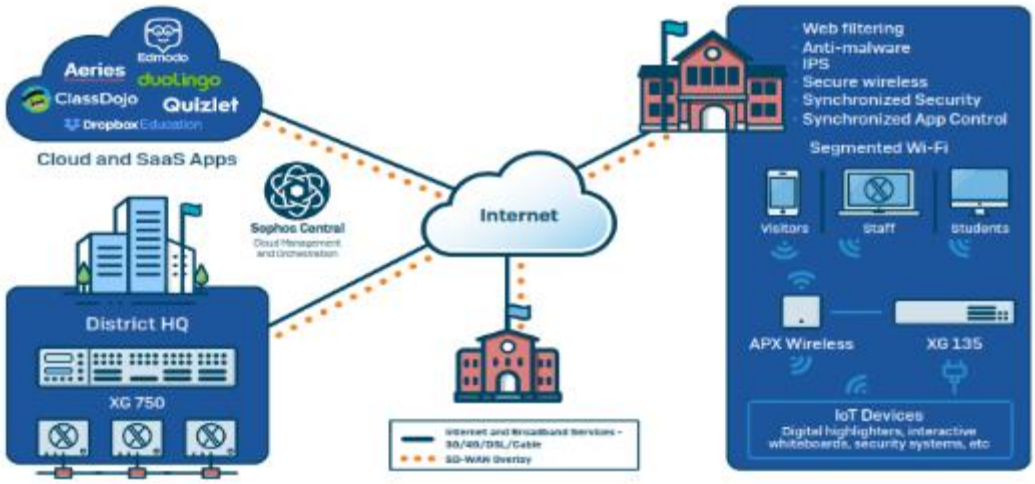


Figura 9. Tecnología SD-WAN entorno de la educación

Fuente: Sophos XG (Enero 2020 p. 6)

Desde esta perspectiva expuesta en la figura 9, nacen nuevas características enfocadas a la educación en escuelas primarias y secundarias, o distritos escolares, consolidado en un único distrito para proporcionar educación a los estudiantes.

- Servicios bajo demanda donde, se permite la implementación de servicios de red basados en aplicaciones bajo demanda, optimiza su tiempo de despliegue.
- Optimización del tráfico para proporcionar una gestión eficiente del tráfico, basada en los requisitos establecidos por el alumno y también mejora el ancho de banda y la experiencia del alumno.
- Servicios a prueba de fallos, su principal objetivo ayudar en caso de una pérdida parcial o total de los elementos de la red, proporciona sistemas redundantes, recuperación de desastres y rutas alternativas.

- La automatización del servicio facilita al controlador la programación eventos que requieren diferentes tipos de *QoS,* usa una variable gestión de ancho de banda.
- Conectar las escuelas y las sedes en su distrito escolar primario o secundario
- Intercambiar de forma segura información personal de estudiantes y profesores y transacciones financieras.
- Gestionar el crecimiento continuo de nuevos dispositivos de acceso a la red, tanto personal como de la escuela.
- Mantenerse al día con las cambiantes tecnologías y aplicaciones educativas en la red (Sophos, 2020).

Según menciona Fortinet (2019), líder mundial en soluciones de ciberseguridad amplias, integradas y automatizadas, anunció que cuatro instituciones académicas en Canadá, incluidas la Junta Escolar del Distrito de Niagara, la Junta Escolar Católica del Distrito de Londres, la Junta Escolar del Distrito de Kawartha Pine Ridge y Upper Grand La Junta Escolar del Distrito está mejora significativamente el rendimiento y la visibilidad de la WAN mediante la implementación de la solución FortiGate Secure SD-WAN de Fortinet.

La solución SD-WAN utiliza la agregación del ancho de banda del túnel para maximizar la utilización del ancho de banda y garantizar el rendimiento sin comprometer el ancho de banda de otras aplicaciones en la red. La solución también es capaz de detectar y reportar el ancho de banda WAN en tiempo real. Estas capacidades permiten a las escuelas cumplir con el requisito del Ministerio de Educación de 1 megabit por segundo por alumno, lo que reduce los costos y aumenta la velocidad y el rendimiento de los dispositivos en la red (Sophos, 2020).

A medida que las instituciones académicas buscan proteger a sus estudiantes y entornos de aprendizaje de las crecientes amenazas de IoT y la interconectividad, se destaca una solución. La solución SD-WAN de Fortinet ofrece a los distritos escolares de Canadá la oportunidad de pasar fácilmente de las redes MPLS a la banda ancha para cumplir con los requisitos del Ministerio de Educación de 1 Mbps por estudiante. Con la banda ancha rápida de Fortinet, las medidas de seguridad integradas y la rentabilidad, los educadores líderes están en mejores

condiciones de brindar acceso a Internet confiable, rápido, seguro y asequible en la escuela (Fortinet, 2020).

- **Finanzas**

El segundo caso de uso, se enfoca en las instituciones financieras como bancos, cooperativas de crédito y corredores de bolsa empresas que prestan servicios financieros personales y corporativos, uno de los Banco Comunitarios *Points West Community Bank*, con sede en Nebraska, tiene agencias localizadas en tres estados: Nebraska, Wyoming y Colorado realizaron una migración a la tecnología SD-WAN como, se muestra en la figura 10 (Sophos, 2020).

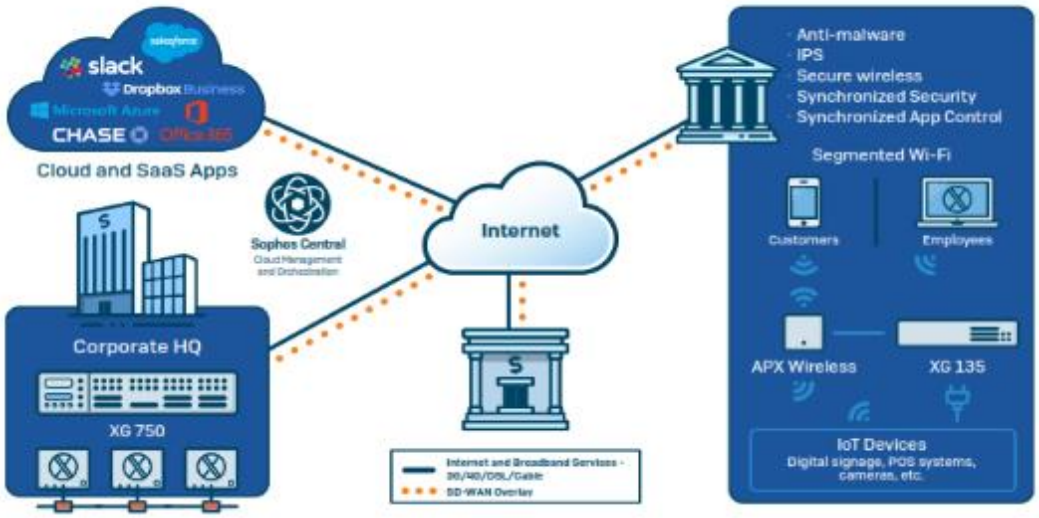


Figura 10. Caso de uso SD-WAN finanzas

Fuente: Sophos XG (Enero 2020 p. 10)

El equipo de Points West evaluó una variedad de tecnologías SD-WAN, el 95% del tráfico va de un sitio a otro y realiza lo siguiente:

- Conectar las agencias locales, estatales y nacionales que comparten grandes cantidades de información confidencial de los clientes cada día.

- Proteger los datos personales y empresariales y las transacciones financieras de las amenazas cibernéticas.
- Mantener el crecimiento continuo de la IO conectada con dispositivos como cajeros automáticos y cámaras de seguridad.
- Habilitar nuevas tecnologías y aplicaciones en la red, tales como banca móvil, firmas electrónicas, señalización digital y videos (Sophos, 2020).

El segundo caso de éxito de SD-WAN en las instituciones financieras, se encontró en *Stearns Bank* con sede en St. Cloud, Minnesota. Con la implementación de SD-WAN el ingeniero de infraestructura de Stearns Bank dijo: Nuestros centros de datos hablan como si estuvieran en el mismo edificio. Retroceder en tiempo real, hacer pruebas de recuperación de desastres y compartir bases de datos entre agencias (Stearns Bank, 2016).

CAPÍTULO II

DISEÑO METODOLÓGICO

2.1 Tipos de investigación

La metodología aplicada es la cuasiexperimental, se implementarán escenarios simulados en entornos virtualizados para defender si un conjunto de buenas prácticas configuradas en una arquitectura de una red de área amplia definida por el software reducirá los riesgos informáticos en las organizaciones.

Tipos de recolección de información

La investigación surge a partir de los distintos problemas identificados en las conexiones entre las oficinas remotas y la oficina matriz. Cabe mencionar que al ser una nueva tecnología no, se encontraron implementaciones en Ecuador, sin embargo, se encontró en el Ministerio de Educación de Canadá un proyecto de modernización de banda ancha que hará la transición de todas las escuelas de Ontario de MPLS a banda ancha. Para aliviar la complejidad de la infraestructura académica y reducir significativamente el costo de MPLS, muchos distritos escolares canadienses recurren a la solución Secure SD-WAN de Fortinet para permitirles cumplir con las regulaciones de privacidad y protección mientras mejoran los entornos de aprendizaje dentro de sus distritos para ambos estudiantes y personal (Fortinet, 2020).

2.2 Método de Investigación

2.2.1 Investigación Inductiva

Una vez recolectadas las implementaciones realizadas en cada caso de uso, se identificó que comparten determinadas características como los son la reducción de costos con referencia a la tecnología de MPLS y no han profundizado en el estudio de la seguridad.

La metodología pretende sacar conclusiones a partir de observaciones. Estas conclusiones, se convierten en leyes generales si, se consideran válidas para todos los casos semejantes, siempre de lo general a lo particular.

2.2.2 Investigación Deductiva

La metodología deductiva empleada, se incluye en la realización y presentación de una arquitectura de red de área amplia definida por el software donde, se probarán ciertas características específicas, aplicar buenas prácticas de seguridad para reducir los riesgos informáticos en las organizaciones.

2.2.3 Investigación Exploratoria

En la investigación, se identifica que esta nueva tecnología de red de área amplia definida por el software reduce la inversión que realiza el departamento de Tecnologías de la Información para conectar el sitio matriz con todas sus agencias. Es importante mencionar, que la investigación exploratoria impulsa el desarrollo de un estudio de la seguridad del cual se extraigan resultados y una conclusión (Sean Wilkins, 2020).

Herramientas de Software:

A continuación, se listan las herramientas a ser utilizadas en la etapa de pruebas a los diferentes escenarios, que se implementaran:

VMware vSphere: Es un hipervisor *bare*-metal gratuito que permite virtualizar múltiples sistemas operativos en un solo servidor físico consolidar sus aplicaciones utilizar menos hardware. https://my.vmware.com/en/web/vmware/evalcenter?p=free-esxi7 (Vmware, 2016).

Sophos XG: La arquitectura del XG *firewall* está diseñada para ofrecer niveles extremos de visibilidad, protección y rendimiento para ayudar a abordar algunos de los mayores retos a los,

que se enfrentan los administradores de redes hoy en día. https://www.sophos.com/es-es/products/next-gen-*firewall*.aspx (Sophos, 2020).

Palo Alto: Es un dispositivo de seguridad de red perimetral que otorga o rechaza el acceso de la red interna, a los flujos de tráfico entre una zona externa que no es de confianza y una zona interna o red lan que es de confianza. https://support.paloaltonetworks.com/Support/Index (Palo Alto Networks, 2020).

Sophos SD-RED: Es un dispositivo que facilita la extensión de su red segura a otras ubicaciones. No requiere de habilidades técnicas en el emplazamiento remoto; basta con introducir el ID del dispositivo en el dispositivo de *firewall* de Sophos y enviarlo. Nada más enchufar y conectar a Internet el dispositivo, este pondrá en contacto con su *firewall* y establecerá un túnel VPN seguro dedicado. https://www.fastvue.co/sophos/download (Sophos, 2020).

Centos 8: Está diseñado para situaciones en las que la estabilidad es primordial. No encontrará las mejores y más recientes funciones y aplicaciones llamativas en CentOS, pero podrá ejecutar sus aplicaciones web prácticamente sin tiempo de inactividad. https://www.centos.org/download (Linux, 2020)**.**

MikroTik: El RouterOS es el sistema operativo del hardware del RouterBOARD. Tiene todas las características necesarias para un ISP - enrutamiento, cortafuegos, gestión de ancho de banda, punto de acceso inalámbrico, enlace backhaul, puerta de enlace hotspot, servidor VPN y más. https://mikrotik.com/download (Vunkers, 2020).

Windows 10: Es un sistema operativo de Microsoft para computadoras personales, tabletas, dispositivos integrados y dispositivos de Internet de las cosas. https://www.microsoft.com/en-us/software-download/windows10ISO.

Kali Linux: Es un proyecto de código abierto mantenido y financiado por Offensive Security, un proveedor de servicios de prueba de penetración y capacitación en seguridad de la información de clase mundial.

Nikto: Es un escáner de servidor web de código abierto que realiza pruebas exhaustivas contra servidores web para varios elementos, incluidos más de 6700 archivos / programas potencialmente peligrosos, verifica versiones desactualizadas de más de 1250 servidores y problemas específicos de la versión en más de 270 servidores.

Slow HTTP Test: Es una herramienta que permite simular distintos tipos de ataques de denegación de servicio (DoS), en la capa de aplicación. Funciona en la mayoría de los sistemas operativos, tales como Linux, OSX y Windows. SlowHTTPTest, se usa desde una interfaz de línea de comandos. El código fuente de SlowHTTPTest está disponible en github.

Parametros a configurar para el ataque DoS:

- H: envía las cabeceras similares como lo hace slowloris.
- i 10: indica el intervalo de conexiones cada 10 segundos.
- r 200: se realizarán 200 conexiones por segundo.
- t GET: el tipo de peticiones será modo GET.
- u URL: La url o dirección ip a la que realiza la prueba
- x 24: número de bytes generados randómicamente en cada conexión
- p 3: tiempo que espera para una nueva conexión

Metasploit: Es una herramienta que viene instalada en la suite de kali Linux la cual es utilizada para descubrir vulnerabilidades que estan ocultas en los equipos con Sistema operativos windows, linux y mac utiliza una variedad de herramientas y utilidades. Metasploit le permite entrar y vulnerar la seguridad de los equipos de una organización tal y como lo hace un hacker y utiliza los mismos métodos para auditar e infiltrarse en redes y servidores siguen una serie de pasos como, se detalla en los anexos.

Nmap: Es una aplicación de código abierto y gratuito el cual, se utilizad en windows, linux y mac y es útil para el descubrimiento de redes y la auditoría de seguridad.

Amap: Es una herramienta de primera generación para el escaneo. Intenta identificar aplicaciones incluso si ejecuta sobre un puerto diferente al normal. También identifica aplicaciones basados en no ASCII. Esto logra al enviar paquetes activadores, y consulta las respuestas en una lista de cadenas de respuesta (Quezada, 2019).

- La opción -b de amap imprime los banners en ASCII, en caso alguna sea recibida.
- La opción -q de amap implica que todos los puertos cerrados o con tiempo de espera alto NO serán marcados como no identificados, y por lo tanto no serán reportados.

MobaXterm: Es una herramienta de conexión remota. En una sola aplicación de Windows, proporciona un montón de funciones que adaptan a los programadores, web masters, administradores de TI.

SSH Tunneling: El túnel SSH, también llamado SSH Port Forwarding, es una técnica utilizada para crear un túnel encriptado a través de una conexión SSH. Un túnel SSH tiene una variedad de usos, tales como evitar los mecanismos de restricción o encriptar el tráfico no encriptado. Por ejemplo, si en un lugar de trabajo existen restricciones para asegurar que los empleados no puedan navegar a ciertos sitios, se podría establecer un túnel de SSH a través de la computadora de la casa de un empleado para dirigir el tráfico a un sitio restringido. Aunque la creación de túneles de SSH es una función útil y legítima del protocolo de SSH, tiene un potencial diferente desde la perspectiva de un atacante (Zone, 2020).

2.3 Metodología de Desarrollo

Con el objetivo de identificar los posibles riesgos informáticos que dispone una organización, se aplicó este método apoya las siguientes técnicas:

2.3.1 Preparar

Para el desarrollo de esta fase, se realizaron revisiones de casos de uso y de casos de éxito fuera del país donde, se han identificado una serie de parámetros que son de importancia para el diseño de la red, a continuación, se exponen los siguientes parametros:

- **Servicios y Aplicaciones**

Las aplicaciones en común que utilizan las organizaciones para enviar y recibir archivos entre sus diferentes sucursales son utilizadas en los casos de éxito analizados son las aplicaciones que las empresas consideran como críticas por la información que transfieren.

- **Seguridad en los Accesos**

Con base al análisis de las implementaciones realizadas en el ámbito de educación y finanzas, la tecnología de red de área amplia definida por software reduce los costos y la dificultad de implementación referente a otras tecnologías, es decir, se tiene una diferencia notable en la disponibilidad de los accesos a las aplicaciones de la oficina matriz, pero a nivel de seguridad no, se ha profundizado mucho debido a que se trata de una nueva tecnología.

2.3.2 Planear

Según las investigaciones que realizaron, las empresas que han implementado esta nueva tecnología fue debido a los costos elevados que les representaba renovar su tecnología actual, es decir, sigue la comunicación entre sitios remotos que encuentran en cualquier parte del mundo con la oficina remota.

Se requiere además tener mayor disponibilidad en las conexiones entre los diferentes puntos y la oficina central, esto, se podía realizar con la tecnología MPLS que contaban, pero los costos eran demasiado elevados para tener un segundo o tercer enlace que provea esta disponibilidad en el caso que llegue a fallar en enlace principal.

Otro de los requerimientos que los dueños solicitan es mejorar los tiempos de respuesta en las comunicaciones de los sitios remotos con la oficina matriz, esto debido a que las conexiones viajaban actualmente por canales MPLS que no tenían un ancho de banda considerable justamente por los costos elevados, ahora si las conexiones, se dan directamente por el canal de internet los resultados mejoran notablemente.

2.3.3 Diseñar

Con las limitaciones encontradas en los diseños de red MPLS actuales debido a trabajan solo en capa 3 del modelo OSI, el nuevo diseño de conectividad que propone entre las diferentes agencias ubicadas en cualquier parte el mundo con la oficina matriz tiene previsto mejorar la experiencia de estas comunicaciones y aplicar un conjunto de buenas prácticas configuradas en una arquitectura de red de área amplia definida por software (SD-WAN) para reducir los riesgos informáticos en las organizaciones.

- **Diseño de la Topología de Red**

El diseño de las redes de área amplia definida por software implementada en un entorno virtualizado emulan las conexiones SD-WAN que tiene enlaces de internet para permitir el acceso a los servicios internos como sitios web o aplicaciones, los dos enlaces que conectan a dos proveedores de internet diferentes, con este diseño, se quiere simplificar las operaciones de las redes y poder automatizar muchas de las acciones, las políticas en las a métricas de comportamiento de red utiliza políticas de seguridad realiza una caracterización de mis aplicaciones en la wan.
Para armar una arquitectura de la wan y de las aplicaciones, tener claro los siguientes puntos:

- Aplicaciones y servicios que van a utilizar.
- La redundancia de la red.
- La disponibilidad de la red.
- Tipo de administración que va a dar a una red.

A continuación, en la figura 11, se muestra la topología de red propuesta para la conexión de dos agencias con el sitio matriz mediante una conectividad de red de área amplia definida por software SD-WAN.

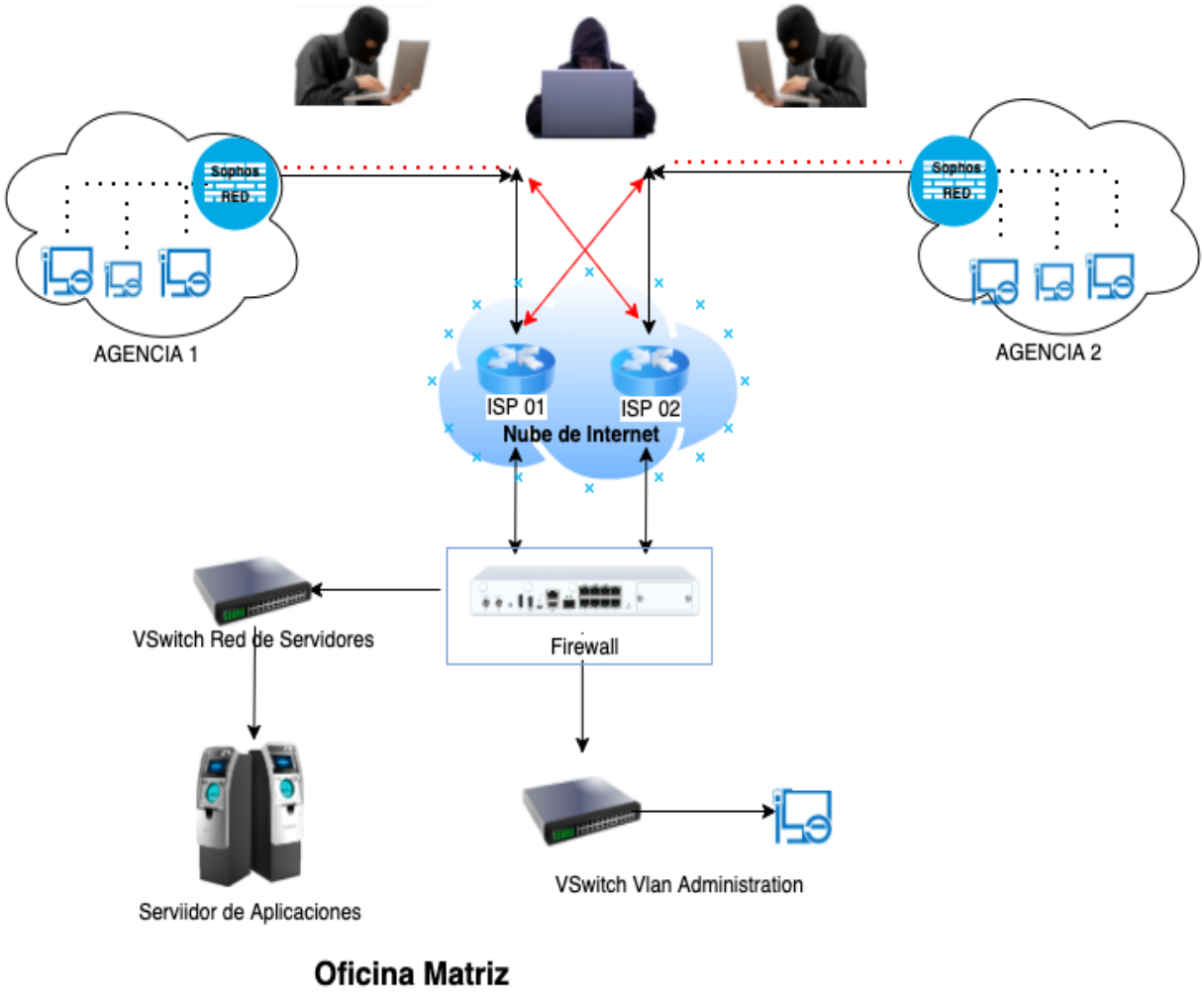


Figura 11. Arquitectura de comunicación SD-WAN

Fuente: elaboración propria

- **Direccionamiento Lógico ipv4**

Para el desarrollo del diseño de las redes internas de oficina matriz y sus agencias presenta la siguiente información de direcciones de clase B y C.

Tabla 2. Direccionamiento ipv4

Zona	**Descripción**	**Subred ipv4**	**Máscara**	**Gateway**
Administración	Gestión del *Firewall*	192.168.129.0	/24	192.168.129.225
Red	Sophos Red Agencia 01	172.16.17.0	/24	172.16.17.1
Red	Sophos Red Agencia 02	172.16.20.0	/24	172.16.20.1

Fuente: elaboración propia

Para la configuración de los proveedores de internet y datos, se realiza un análisis de los proveedores a nivel nacional que brindan estos servicios donde, se destacan Telconet, Claro, Cnt, entre otros. En la tabla 3, se muestra el direccionamiento asignado a cada servicio.

Tabla 3. Direccionamiento ipv4 que otorga cada proveedor

Punto a Punto				
Matriz			Agencias	
Origen	Proveedor	Subred	Destino	Subred
Oficina Matriz	Internet	200.7.206.88/29	Agencia 1	181.39.156.118/29
		181.39.14.136/29		

		200.7.206.88/29	Agencia 2	190.216.99.24/29
		181.39.14.136/29		

Fuente: elaboración propia

- **Simulación de SD-WAN**

En términos generales para realizar la simulación de la red área amplia definida por software, se utiliza la versión 6.7.0 de VMware esxi, el mismo que permite desarrollar simulaciones de diferentes sistemas operativos en un mismo equipo como muestra en la figura 12.

Figura 12. Servidor VMware esxi

Fuente: VMware VDC Fundamentals p.23

Conexiones de los equipos para la simulación: Se realiza la simulación en el software de virtualización VMware esxi de acuerdo con el diseño propuesto, que consta de una oficina matriz con dos agencias debido a que evaluará la seguridad en las conexiones SD-WAN.

El aprovisionamiento de los equipos virtualizados con sus respectivos estados, se muestra en la figura 13.

Figura 13. Equipos virtualizados

Fuente: elaboración propia

La configuración de los conmutadores virtuales del host, se detalla en la figura 14.

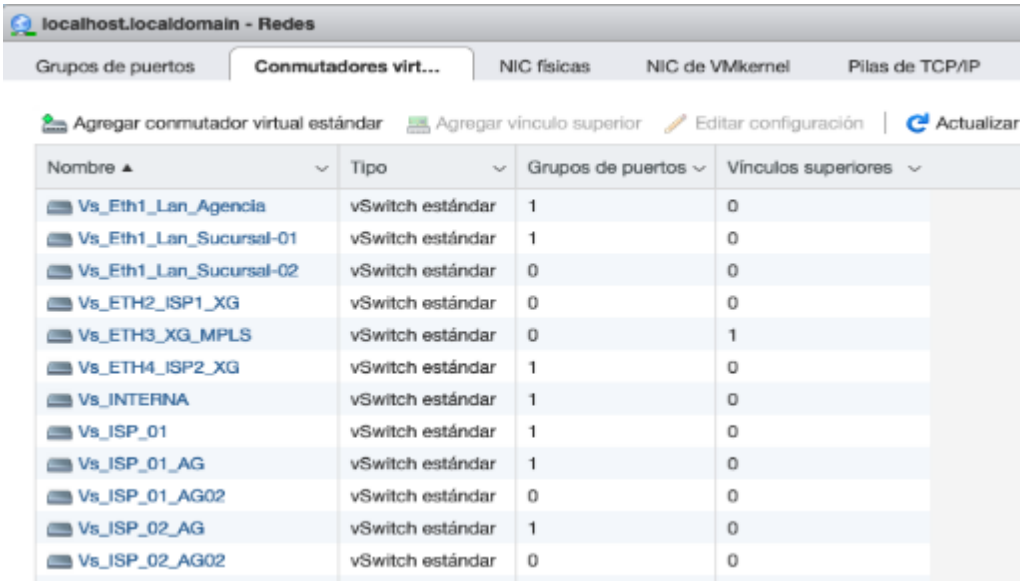


Figura 14. Listado de conmutadores virtuales

Fuente: elaboración propia

La configuración de los grupos de puertos virtuales del host, se detalla en la figura 15.

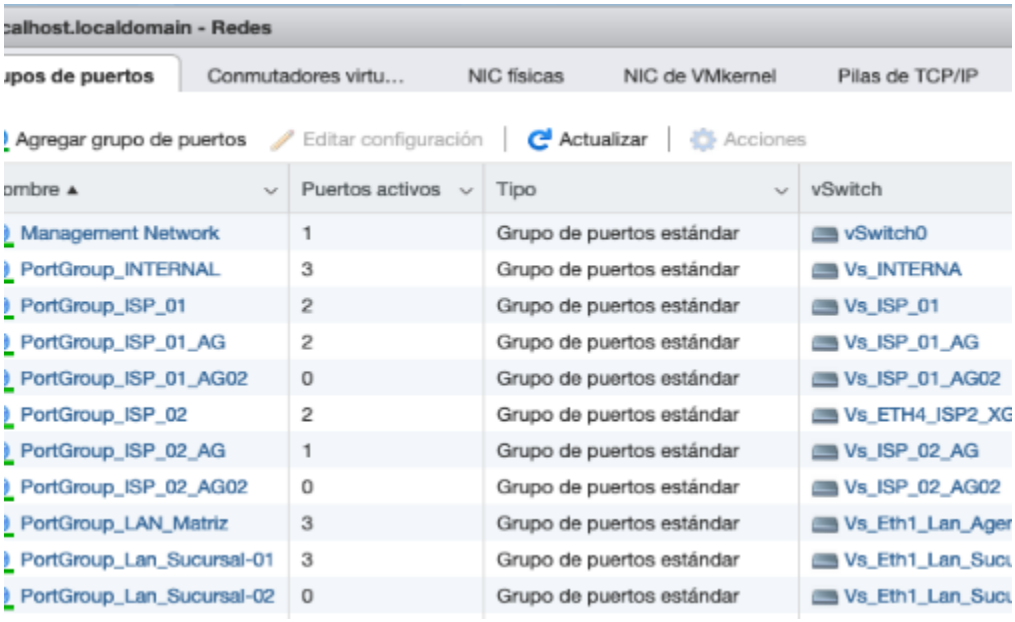


Figura 15. Listado de grupo de puertos

Fuente: elaboración propia

2.3.5 Implementar

Una vez que los casos de uso, se han examinado y han definido los componentes utilizados, se implementa tres escenarios mediante los cuales conectan agencias remotas ubicadas en cualquier parte del mundo con la oficina matriz.

Escenario 1: Acceso a Servicios internos a través de una publicación por regla de *firewall*.

Se configura una regla *Destination Network Address Translation* (DNAT) para publicar un servicio web de la oficina Matriz como, se muestra en la figura 16, esta publicación, se la realizó en un puerto diferente donde, se intenta ocultar el puerto origen en el que escucha el servidor interno.

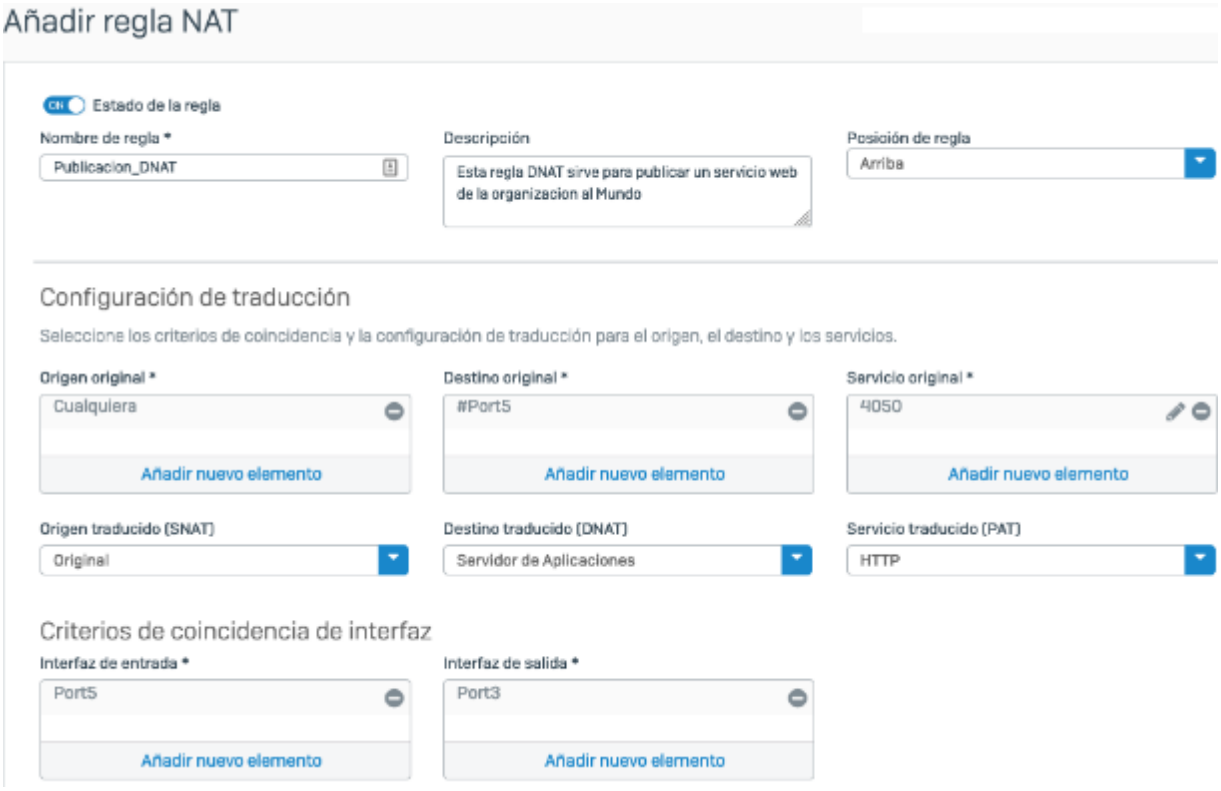


Figura 16. Creación regla DNAT

Fuente: elaboración propia

Se configura una regla de *firewall* para que permita el acceso al servicio, que se está publicado en la regla DNAT, para lo cual, se agrega nombre y descripción de la regla como se muestra en la figura 17.

Figura 17. Creación de regla de *Firewall*

Fuente: elaboración propia

En la figura 18, se configura un puerto desconocido para realizar la publicación de un servicio web, esto con el objetivo de crear un distractor para los cibercriminales.

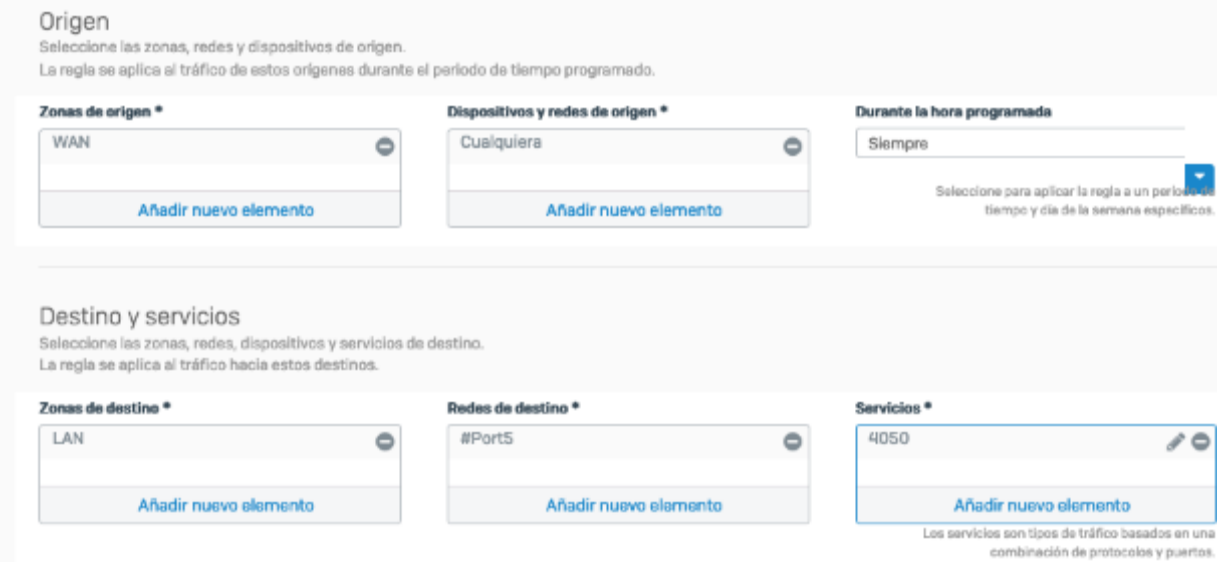


Figura 18. Puertos permitidos en una regla de *Firewall*

Fuente: elaboración propia

Escenario 02: Acceso a Servicios internos a través de una VPN IPSec entre Matriz y las agencias.

Para configurar una VPN IPSec entre dos sitios la oficina matriz y sus diferentes agencias que están ubicadas en cualquier parte del mundo es necesario llenar el siguiente formulario para crear una política de conexión entre los dos sitios, en la tabla 4, se define las direcciones ip públicas con las que establecerán el Túnel VPN IPSec.

Tabla 4. Direccionamiento ip público de los *firewalls*

Información VPN-IPSec	***Firewall* Matriz**	***Firewall* Agencia**
Dirección ip Pública	200.7.206.90	181.39.156.119
Descripción del Dispositivo	Sophos XG Version: SFOS 18.0.3 MR-3	Strata Palo Alto

Fuente: elaboración propia

En la tabla 5, se configura los parámetros de la fase 1 y 2 que tienen los mismos en los dos dispositivos.

Tabla 5. Parámetros de negociación Túnel VPN IPSec

Propiedades del Tunnel		***Firewall* Matriz**	***Firewall* Agencia**
Fase 1	Método de Autenticación	Clave previamente compartida	Clave previamente compartida
	Esquema de cifrado	IKEv1 / IKEv2	IKEv1 / IKEv2
	Grupo Diffie-Hellman	14 (DH2048)	14 (DH2048)
	Algoritmo de cifrado	AES 128/256	AES 128/256
	Algoritmo Hashing	SHA 256/512	SHA 256/512
	Tiempo de vida (para la renegociación)	28800 seconds	28800 seconds
	Llave o certificado pre compartido	Contraseña de 12 caracteres incluye letras mayúsculas, minúsculas, números y caracteres especiales.	
Fase 2	Algoritmo de encriptación ESP	AES 128/256	AES 128/256
	Algoritmo de autenticación ESP	SHA 256/512	SHA 256/512
	Grupo Diffie-Hellman	14 (DH2048)	14 (DH2048)
	Tiempo de vida (para la renegociación)	28800 seconds	28800 seconds

Fuente: elaboración propia

En la tabla 6, se agregan los host o redes completas que accede mediante el Túnel VPN IPSec, se detalla los servicios que van a consumir.

Tabla 6. Información de las redes internas a compartir

Regla de acceso VPN	**Origen**	**Destino**	**Servicios**
Regla #1	Agencia 01	Equipo en oficina matriz	HTTP

Fuente: elaboración propia

Configuración de VPN IPSec

Se configura en general del Túnel VPN IPSec en la oficina matriz, como, se observa en la figura 19.

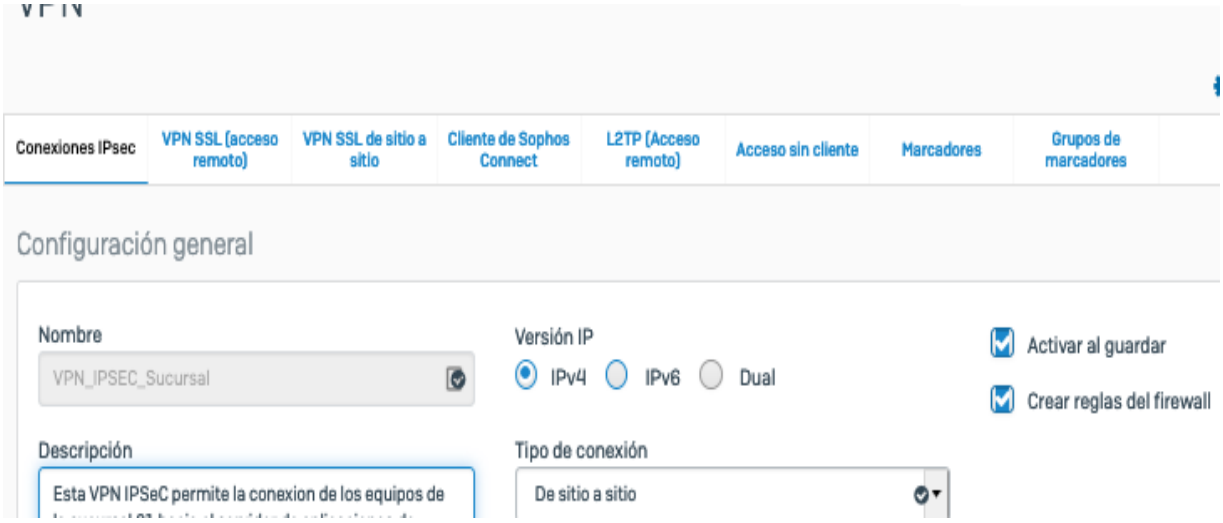


Figura 19. Definición del nombre para la política VPN IPSec

Fuente: elaboración propia

Como, se muestra en la figura 20, el tipo de autenticación y la política, se configura de manera similar en los dos *firewalls* para que pueda completar correctamente la Fase 1 del Túnel VPN IPSec.

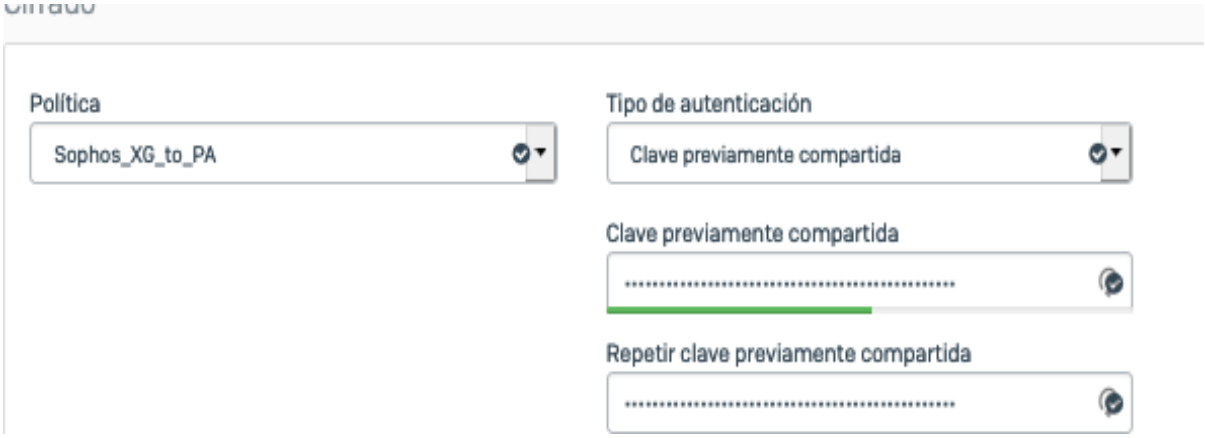


Figura 20. Configuración de tipo de autenticación

Fuente: elaboración propia

En la figura 21, se muestra la configuración de la puerta de enlace donde, se agrega la dirección ip pública con la que va a establecer el Túnel VPN IPSec y de la misma manera agregar los hosts/segmentos de red que van a ser compartidos a través de este.

Figura 21. Configuración de redes internas a compartir

Fuente: elaboración propia

En la figura 22, se corrobora que el Túnel VPN IPSec configurado en oficina matriz, se establece de manera satisfactoria.

Figura 22. Conexión exitosa del Túnel VPN IPSec

Fuente: elaboración propia

***Firewall* Agencia**

Después de configurar el Túnel VPN IPSec en la oficina matriz, se continúa con la configuración general del Túnel VPN IPSec en la agencia 01, como, se observa en la figura 23, se crea dos objetos que son asociados a la dirección ip pública del *Firewall* de Matriz y el otro objeto asociado al segmento de red interno de la agencia.

Definicion de objetos:

- Red Agencia: Definir el segmento de red interna que desea compartir por el túnel vpn IPSec.

- VPN-IPSec- *Firewall* Matriz: Crear un objeto donde, se agregue la Dirección ip pública del *firewall* con el que va a levantar el túnel.

Figura 23. Definición de objetos en *Firewall* de agencias

Fuente: elaboración propia

Como, se muestra en la figura 24, se define un nombre para el nuevo túnel, que se va a crear y definir la versión de IKE, en muchas ocasiones la mayoría de los *firewalls* soportan únicamente IKEv1 por lo que es recomendable que la misma versión, se seleccione en los dos *firewalls*, a continuación, elegir el tipo de ip como estática debido a que esto permite una configuración más sencilla.

A continuación, se selecciona el método de autenticación de los dos *firewalls* seleccionar la clave pre-compartida la cual, se utiliza en los dos *firewalls* para que puedan autenticar correctamente y pueda completar correctamente la Fase 1 del túnel VPN IPSec.

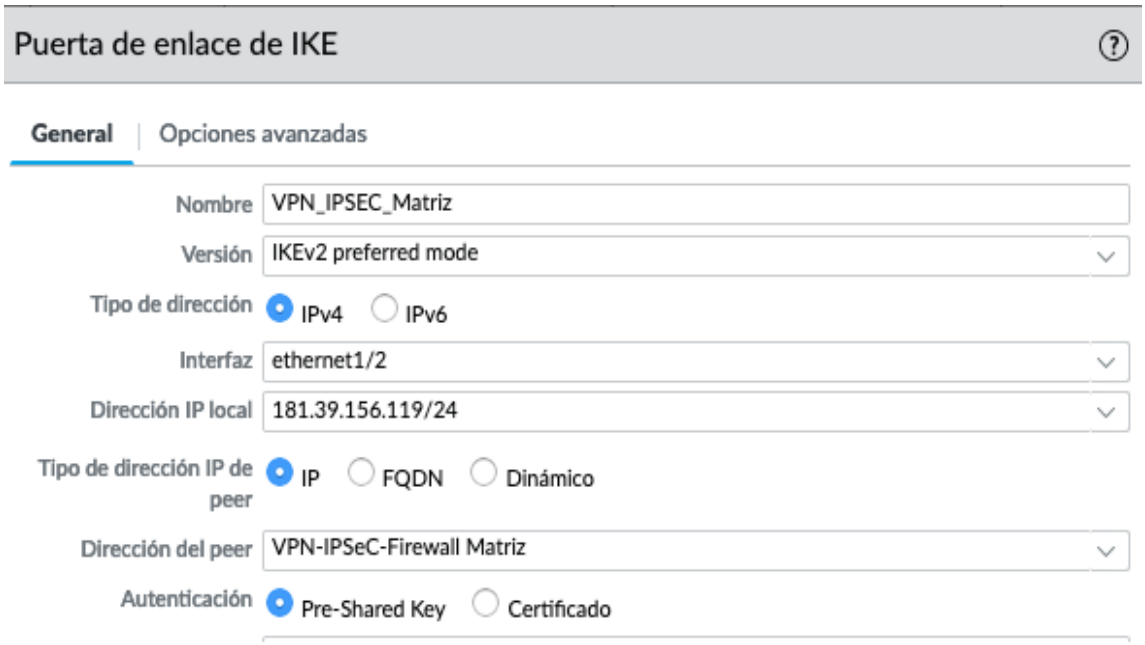


Figura 24. Configuración de parámetros de conexión y autenticación

Fuente: elaboración propia

En la figura 25, se muestra los parámetros de opciones avanzadas donde, se define las siguientes opciones:

- El modo pasivo impide que esta puerta de enlace haga negociaciones salientes y responda sólo a las solicitudes de negociación.
- NAT Trasversal permite la encapsulación UDP en los protocolos IKE en caso de que al menos una de las pasarelas esté detrás de una pasarela NAT.
- El modo de cambio está en automático de forma predeterminada, pero establece en Main si ambos pares están en una dirección ip estática o agresiva si cualquiera de los dos pares está en una dirección ip dinámica.
- El perfil de IKE Crypto, se establece el perfil que ha creado anteriormente.
- La detección de pares muertos es un latido que identifica los pares VPN no disponibles para ayudar a restaurar los recursos.
- El trabajo de comprobación de IKEv2 es similar al DPD, pero cada paquete, se cuenta durante la actividad y sólo después de que el mismo ha estado inactivo durante la

cantidad de tiempo configurada, se envía un paquete vacío para determinar la vida. (Palo Alto Networks, 2020)

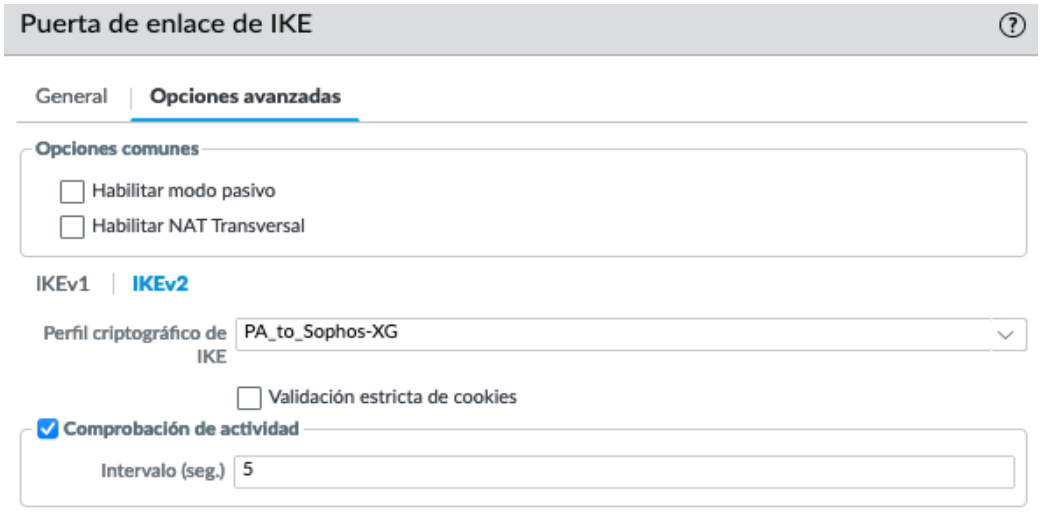


Figura 25. Configuración de fase 2 VPN IPSec

Fuente: elaboración propia

En la figura 26, se muestra la configuración del Túnel IPSec que levanta la conexión con la oficina matriz.

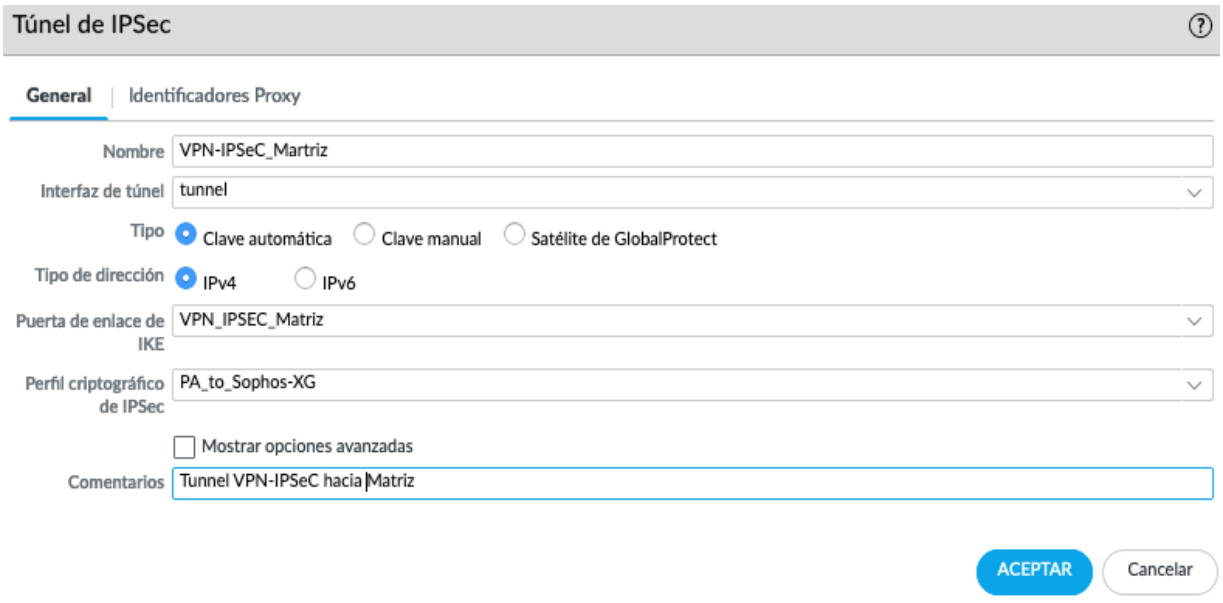


Figura 26. Selección de puerta de enlace y política

Fuente: elaboración propia

A continuación, en la figura 27, se agrega los segmentos de red o host que serán compartidos por el Túnel VPN IPSec.

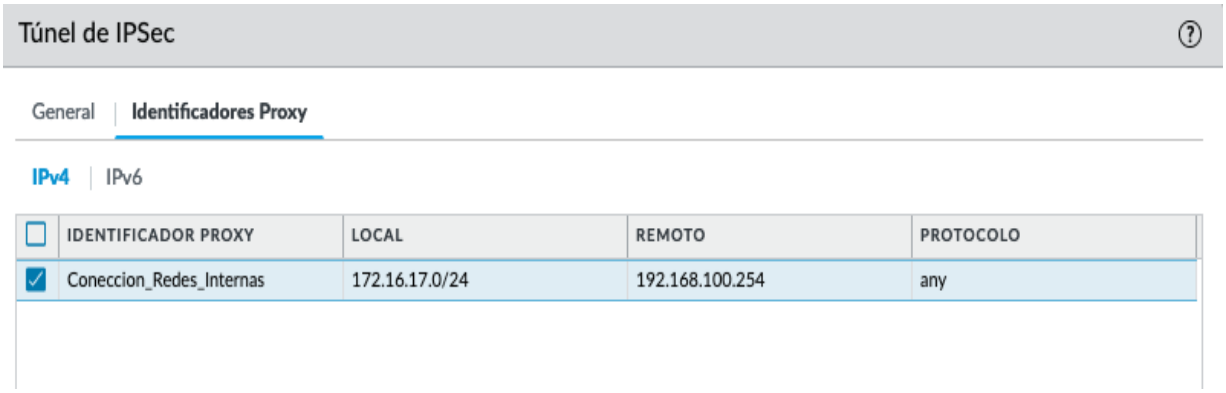


Figura 27. Configuración de redes internas a compartir

Fuente: elaboración propia

Finalmentet, en la figura 28, se corrobora que el Túnel VPN IPSec configurado en la agencia, se establece de manera satisfactoria un túnel cifrado con la oficina matriz.

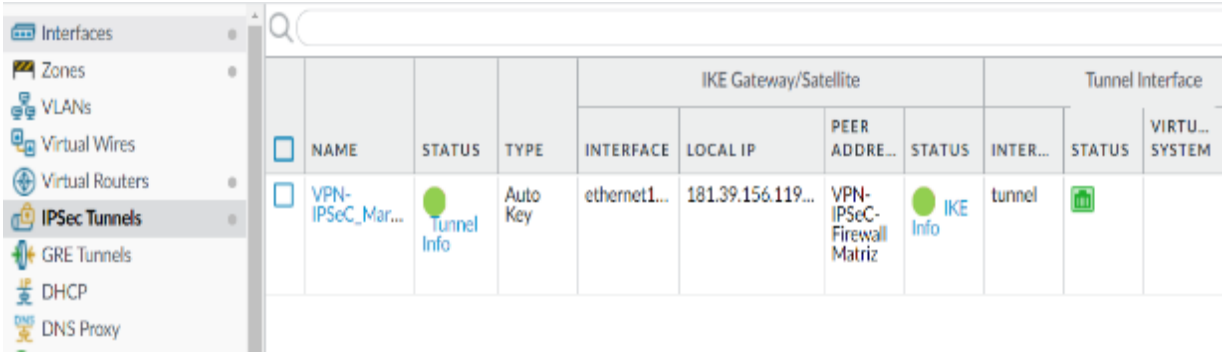


Figura 28. Conexión exitosa Túnel VPN IPSec

Fuente: elaboración propia

Escenario 03: Acceso a servicios internos a través de una red de área amplia definida por el software desde las agencias 01 y 02 hacia Matriz.

Configuración del *Firewall* Sophos XG en Oficina Matriz**.**

- **Aprovisionamiento de Sophos Red**

Se configura un Sophos RED en un Sophos XG *Firewall*, las opciones de configuración elegidas por el administrador, se cargan en los servidores de aprovisionamiento de Sophos. La configuración es poco más que los siguientes elementos:

- Dirección ip del *firewall* Sophos XG.
- Modo de enlace ascendente WAN (DHCP, ip estática).
- Si, se elige el modo de enlace ascendente estático, la configuración de la dirección RED WAN (dirección, máscara de red, puerta de enlace predeterminada y servidor DNS).
- Opcionalmente, configuración de conexión de banda ancha móvil para hardware RED.
- Código de desbloqueo.

Existe un código de desbloqueo que no almacena en el dispositivo Sophos Red, que utiliza para evitar que un Sophos Red que está en uso sea redirigido accidental o maliciosamente. Se proporciona el código de desbloqueo correcto para que los servidores de aprovisionamiento acepten una nueva configuración para un Sophos Red. Inicialmente, el código de desbloqueo está en blanco, hasta que haya conectado un Sophos Red a un Sophos XG *firewall* una vez.
La primera vez que configura un dispositivo Sophos Red en el *firewall*, el código de desbloqueo, se deja en blanco. Cada vez que un Sophos Red, se conecta a un nuevo cortafuegos, se ingresa el código de desbloqueo anterior para mover el Sophos Red. Una vez que la configuración, se envía al servidor de aprovisionamiento, emite un nuevo código de desbloqueo y muestra en la Consola de administración de Sophos XG *firewall*. (Sophos, 2020)

- **Instrucciones de Configuración de Sophos RED**

Esta sección describe los pasos básicos necesarios para agregar un nuevo RED a un Sophos XG *firewall* manualmente. En algunos casos, se necesitan opciones de configuración más detalladas, pero esto está fuera del alcance de este documento.

Antes de agregar el dispositivo sophos RED, se activa el servicio del RED. Vaya a Servicios del sistema > RED y habilite el estado del RED. El nombre de la organización, la ciudad, el país y el correo electrónico. Haga clic en Aplicar para activar el servicio RED.

En esta pestaña, habilitar Force TLS 1.2 para mayor seguridad o activar la desautorización automática del dispositivo. La desautorización automática de dispositivos es una característica que permite que un dispositivo RED, se desvincule del *firewall* después de un período de inactividad; esto es para evitar que alguien mueva un dispositivo RED a otra ubicación sin el conocimiento del administrador del sistema. Un dispositivo que pierde su conexión con Sophos XG *Firewall* después de que haya transcurrido el período de desautorización, necesita que alguien con acceso de administrador reactive el RED antes de usarlo. (Sophos, 2020)

- **Adición de RED al *firewall* de Sophos XG**

Como, se observa en las figuras 29, 30 y 31, en el *Firewall* Sophos XG de la oficina Matriz, se configura el dispositivo Sophos Red ubicado en la agencia 01 de la siguiente manera:

- En la Consola de administración acceder al apartado de Red y accede a Interfaces.
- Clic en agregar interfaz.
- Seleccionar Agregar RED.
- Configurar la interfaz RED.
- Ingresar un nombre de la agencia descriptivo en el campo Nombre de agencia.
- Seleccionar el tipo de dispositivo Sophos Red.
- Ingresar el ID del Sophos Red. Solicitar el ID al equipo de Sophos Soporte.
- Si el dispositivo se ha configurado anteriormente en otro Sophos XG *firewall*, se requiere un código de desbloqueo para guardar la configuración. El código de desbloqueo, se encuentra en el *firewall* al que se conectó el Sophos Red por última vez, en la Consola de administración o Web admin, si estaba previamente conectado a un Sophos XG.

- En el campo de ip / nombre de host del cortafuegos configurar la dirección ip pública de la agencia remota, si desea, se implementa un nombre de dominio totalmente calificado o una dirección ip pública, que se pueda resolver públicamente.
- Permitir que el modo de enlace ascendente permanezca configurado como DHCP si es posible. Elegir una dirección estática si no hay opción para DHCP. Al configurar una dirección ip estática, tenga en cuenta que el Sophos Red, se conecta a una red DHCP al menos una vez para descargar la configuración. Si, se elige una dirección estática, aparecen campos adicionales para la dirección ip, máscara de red, ip de puerta de enlace y servidores DNS.

- Hacer click en Guardar.

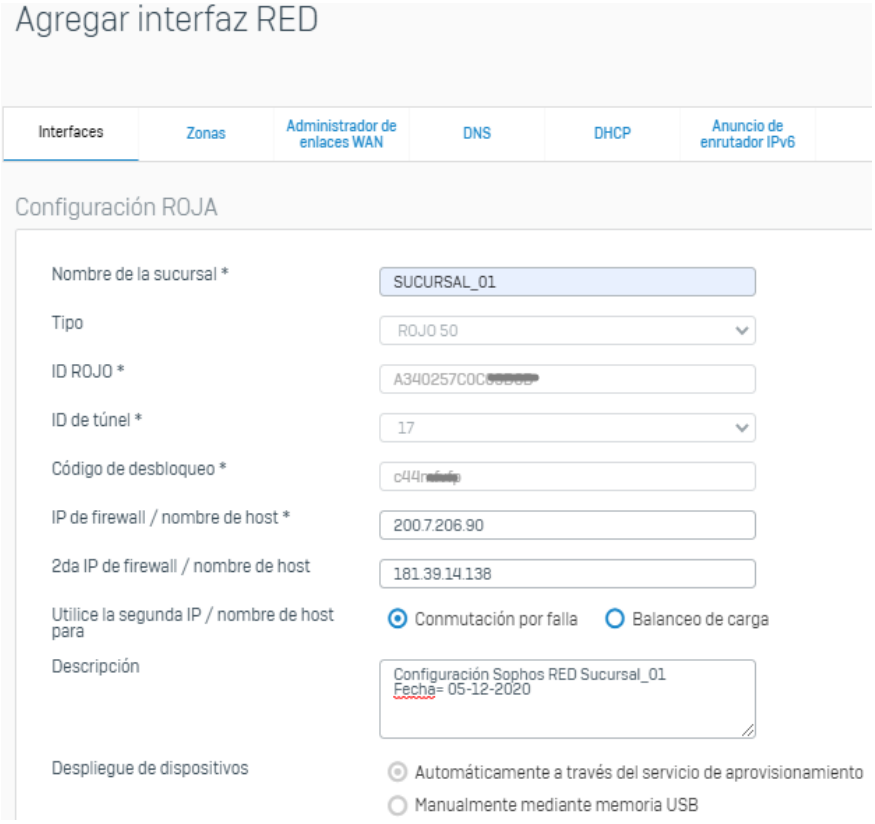


Figura 29. Interfaz asignada para Sophos Red

Fuente: elaboración propia

En la figura 30, se define el modo de configuración en Estándar / Unificado, en este modo, la red remota esté completamente administrada por Sophos XG *firewall*, a través de RED.

El servidor de seguridad Sophos XG *firewall* ofrece DHCP para la LAN remota, y es posible que RED sea el único dispositivo que conecte la LAN a Internet. Si bien otro enrutador, se ubica frente al dispositivo Sophos RED, no hay una ruta paralela alrededor del RED hacia Internet.

Figura 30. Red ipv4 Agencia 01

Fuente: elaboración propia

En la figura 31, se observa que el dispositivo Sophos red de la agencia 01, se conecta de manera satisfactoria al Sophos XG de oficina matriz.

Figura 31. Estado de conectividad de Sophos Red

Fuente: elaboración propia

- **Crear una Zona de Seguridad**

Todo el tráfico seleccionado, se enruta a Sophos XG *firewall* y las reglas del *firewall* lo permiten o no lo permiten. Los dispositivos Sophos Red, se controlan en función de las zonas de las que son miembros y refinar aún más mediante reglas de *firewall* para redes dentro de cada zona.

Al crear un Sophos Red y configurarlo para que sea miembro de la red LAN, las reglas de *firewall* no, se crean automáticamente. El *firewall* Sophos XG identificó que el Sophos Red era miembro de la Zona LAN y luego le aplicó las mismas reglas que aplicaba al resto de la LAN. Para mantener una mayor separación entre la LAN y las redes del Sophos Red, usar una zona existente como VPN o Wifi o crear una nueva llamada RED como, se observa en la figura 32, para dar una separación de zonas de manera lógica.

Una zona es una o más interfaces virtuales o físicas, que se han combinado en un grupo. Esta colección de interfaces generalmente representa un segmento de la red que tiene los mismos requisitos de política de seguridad. Esto permite que un administrador aplique fácilmente reglas de políticas a todas las interfaces en una zona a la vez.

Para crear una nueva zona:

- Acceder al apartado de red, dirigirse a zonas y clic en agregar.
- Completar el nombre de la nueva zona.
- Seleccionar el tipo de zona.
- Las zonas LAN son más seguras, están destinadas a proteger los recursos privados, mientras que las zonas DMZ tienen menos restricciones de seguridad. Consulte la ayuda en línea para obtener más detalles sobre la diferencia entre estas dos opciones.
- En Acceso al dispositivo, elegir qué servicios, se ofrecen en esta zona. Incluso si la regla de *firewall* lo permite, DNS, Web Proxy y otros tipos de acceso enumerados aquí no están disponibles para la zona a menos que estén habilitados.
- En el apartado de administración, se edita los permisos en la zona, vaya a administración, acceso al dispositivo para modificar o eliminar la configuración.

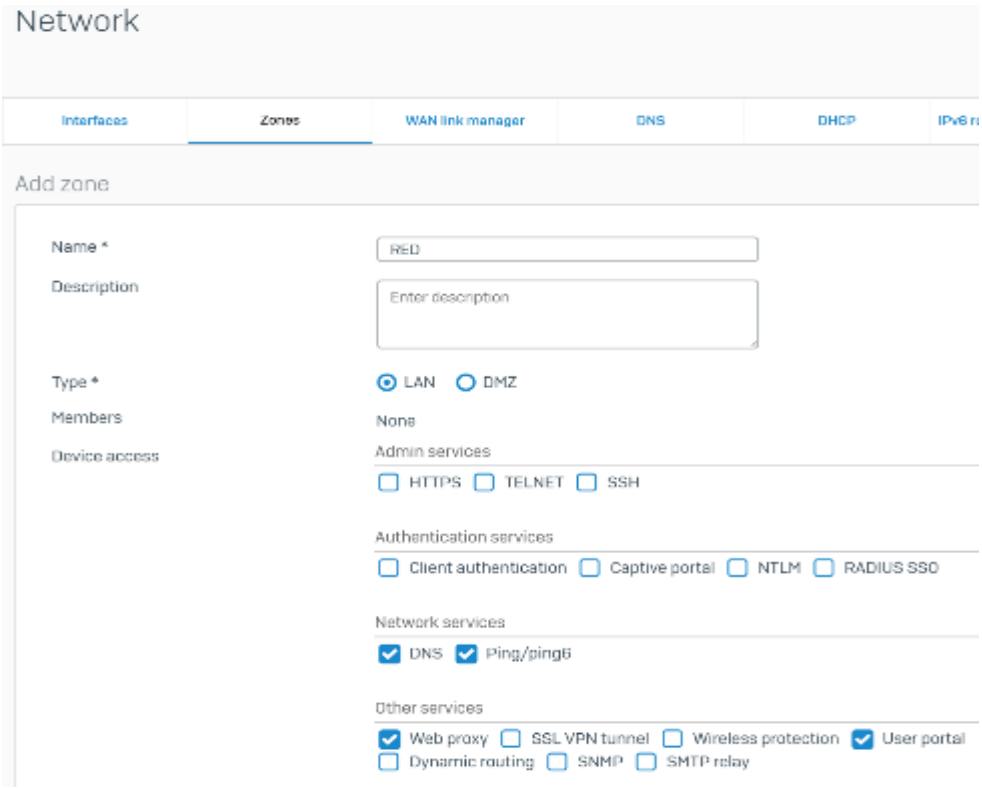


Figura 32. Zona de seguridad Sophos Red

Fuente: elaboración propia

- **Crea una regla de *firewall***

Las reglas de *firewall* determinan cómo, se enruta el tráfico si, se usa una zona existente. Verifique que las reglas, que se aplican a la zona no rompan la seguridad de sus redes internas. Tenga cuidado al seleccionar zonas existentes, algunas de ellas, como la zona VPN.

En la figura 33, se ha creado una nueva regla de *firewall* para usar con la nueva zona del dispositivo sophos RED.

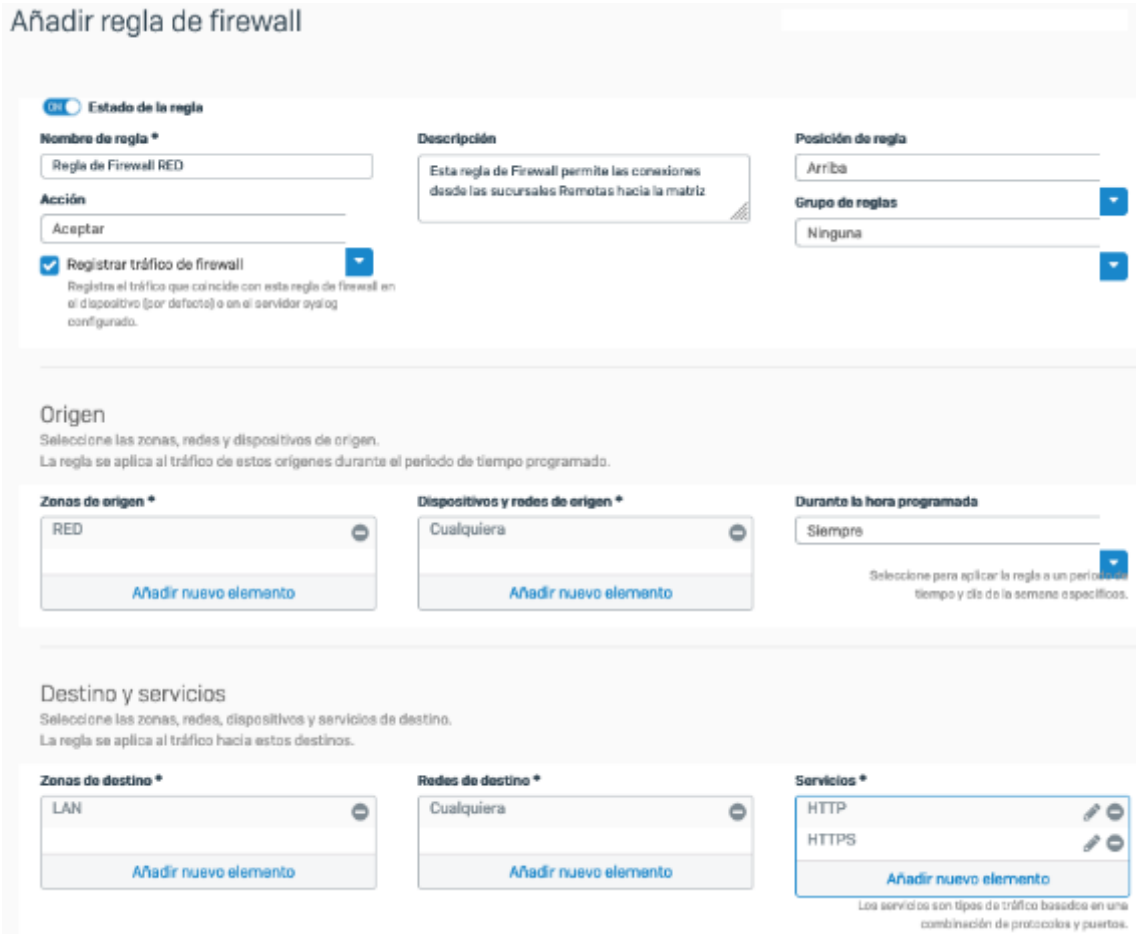


Figura 33. Creación de regla de *firewall*

Fuente: elaboración propia

No hay una forma única de construir reglas de *firewall* RED. La ventaja del dispositivo RED es la libertad de tratarlo como cualquier otra interfaz de red en un *firewall* y configurarlo de la misma manera.

- **Escenarios de implementación**

Si el primer enlace de comunicación falla, se levantará el Túnel dinámicamente con el segundo enlace de internet que esté configurado en Sophos XG.

- Nombre de host de Sophos XG *Firewall* = Conmutación por error
- Enlace ascendente RED = Conmutación por error

En la figura 34, el dispositivo Sophos RED establece una conexión entre RED_WAN1 y SFOS_WAN1.

Figura 34. Actividad Agencia Oficina Matriz

Fuente: KB de Sophos XG

En la figura 35, si SFOS_WAN1 está inactivo: RED_WAN1, se conectará a SFOS_WAN2

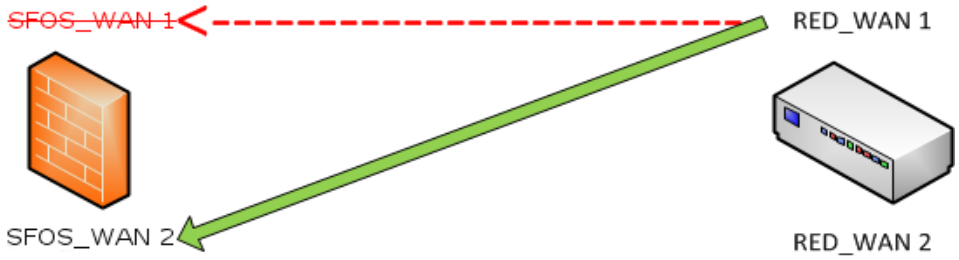


Figura 35. ISP 01

Fuente: KB de Sophos XG.

En la figura 36, si SFOS_WAN1 y RED_WAN1 están inactivos: RED_WAN2, se conectará a SFOS_WAN2

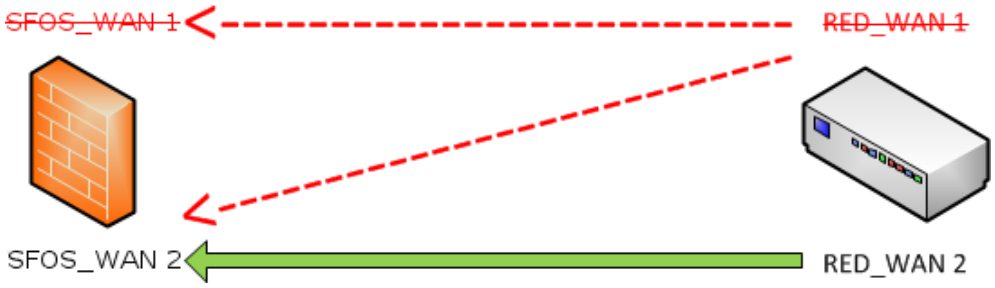


Figura 36. ISP 02

Fuente: KB de Sophos XG

- **Puertos que utiliza el dispositivo Sophos RED**

Tabla 7. Requerimientos de Sophos Red

Dispositivo	**Puertos/Servicios**
Sophos RED	TCP 3400
	UDP 3410

Fuente: KB de Sophos XG

CAPÍTULO III

3.1 Análisis de los resultados de la investigación

Resumen de las pruebas

En este capítulo, se detalla un resumen de las pruebas realizadas referentes al acceso que proviene desde dos agencias remotas hacia oficina matriz para consumir un aplicativo.

3.1.1 Operar

Escenario 01: Acceso a servicios internos como http a través de una publicación por Regla de *firewall*.

Agencia 01:

Pruebas de conectividad entre la agencia 01 y la oficina matriz, la figura 37 muestra una prueba de ping que corrobora que existe comunicación entre la agencia 02 y la oficina matriz.

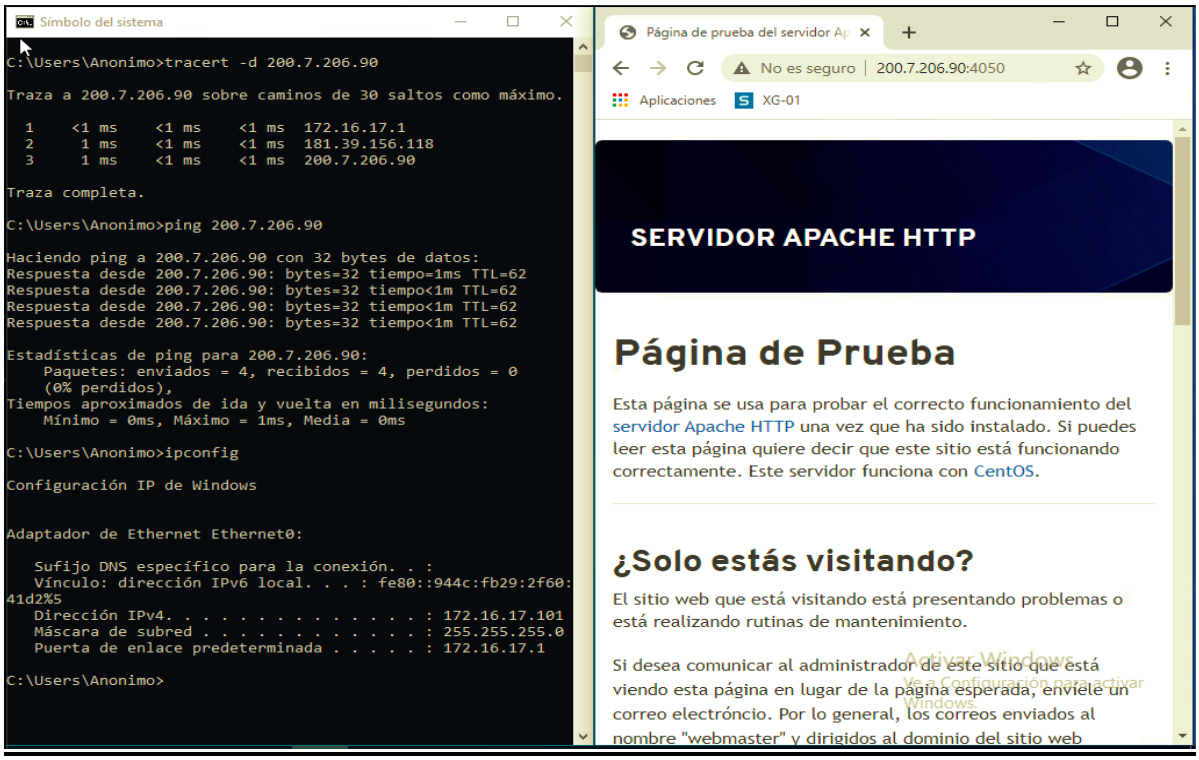


Figura 37. Conectividad agencia 01 y oficina matriz

Fuente: elaboración propia

Revisión de registros de acceso en el *Firewall* Sophos XG de oficina matriz donde, se observa que las consultas que envía la agencia 01 hacia servidor de aplicaciones ubicado en oficina matriz son marcadas como permitidas como, se muestra en la figura 38.

Figura 38. Revisión de registros de acceso

Fuente: elaboración propia

Agencia 02:

Pruebas de conectividad entre la agencia 02 y la oficina matriz, la figura 39 muestra una prueba de ping que corrobora que existe comunicación entre la agencia 02 y la oficina matriz.

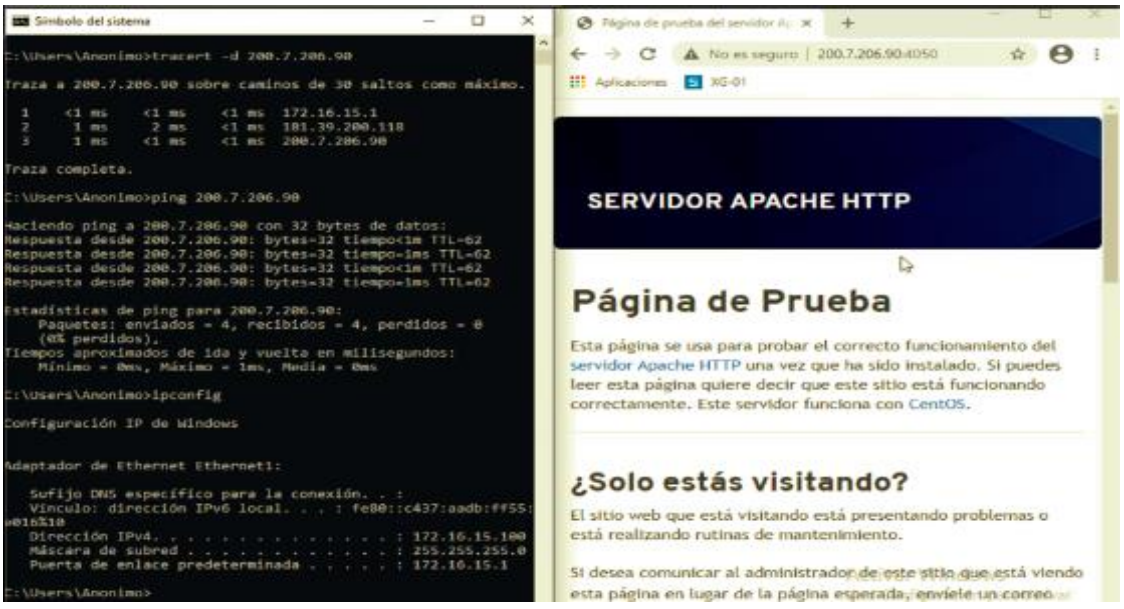
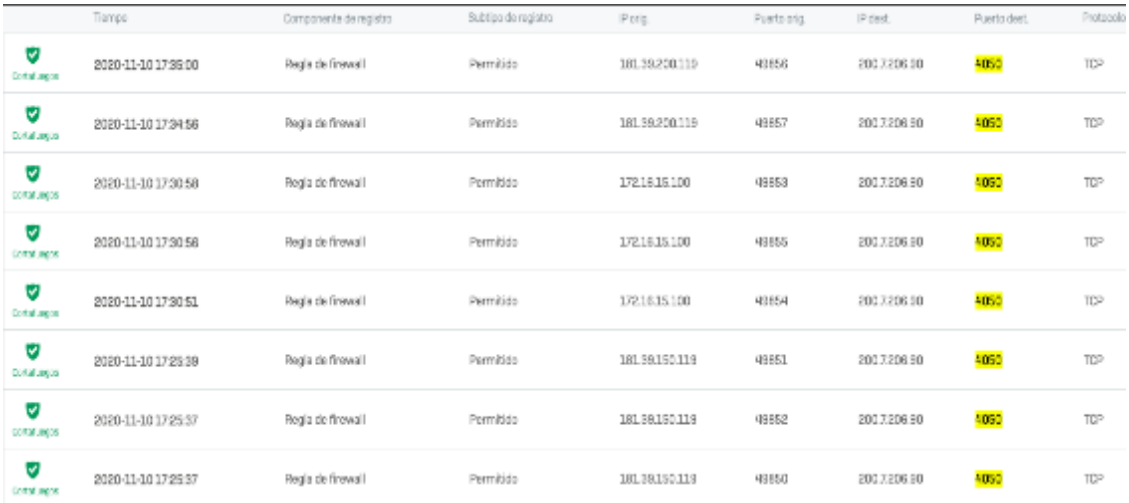


Figura 39. Conectividad agencia 02 y oficina matriz

Fuente: elaboración propia

Revisión de registros de acceso en el *firewall* Sophos XG de oficina matriz donde, se observa que las consultas que envía la agencia 01 hacia servidor de aplicaciones ubicado en oficina matriz son marcadas como permitidas como, se muestra en la figura 40.



	Tiempo	Componente de registro	Subtipo de registro	IP org.	Puerto org.	IP dest.	Puerto dest.	Protocolo
	2020-11-10 17:35:00	Regla de firewall	Permitido	181.39.230.119	49856	200.7.206.90	4050	TCP
	2020-11-10 17:34:56	Regla de firewall	Permitido	181.39.230.119	49857	200.7.206.90	4050	TCP
	2020-11-10 17:30:58	Regla de firewall	Permitido	172.16.15.100	49853	200.7.206.90	4050	TCP
	2020-11-10 17:30:56	Regla de firewall	Permitido	172.16.15.100	49855	200.7.206.90	4050	TCP
	2020-11-10 17:30:51	Regla de firewall	Permitido	172.16.15.100	49854	200.7.206.90	4050	TCP
	2020-11-10 17:25:39	Regla de firewall	Permitido	181.39.150.119	49851	200.7.206.90	4050	TCP
	2020-11-10 17:25:37	Regla de firewall	Permitido	181.39.150.119	49852	200.7.206.90	4050	TCP
	2020-11-10 17:25:37	Regla de firewall	Permitido	181.39.150.119	49850	200.7.206.90	4050	TCP

Figura 40. Revisión de registros de acceso

Fuente: elaboración propia

Uno de los principales ataques informáticos de los que son víctimas las organizaciones son los ataques de denegación de servicio, donde el objetivo del ataque es apagar una máquina o red de destino, haciéndola inaccesible para los usuarios previstos. Los ataques DoS logran esto inundar el objetivo con tráfico donde envían información que desencadena un bloqueo.

Si un cibercriminal detecta que un sitio web está activo, él ejecuta el ataque DoS con la herramienta *Slowhttptest* al sitio web objetivo y dejar inaccesible el sitio para los usuarios de las agencias.

En la figura 41, se muestra que el servicio que está alojado en la oficina matriz y que es accesible desde las agencias, se muestra como disponible.

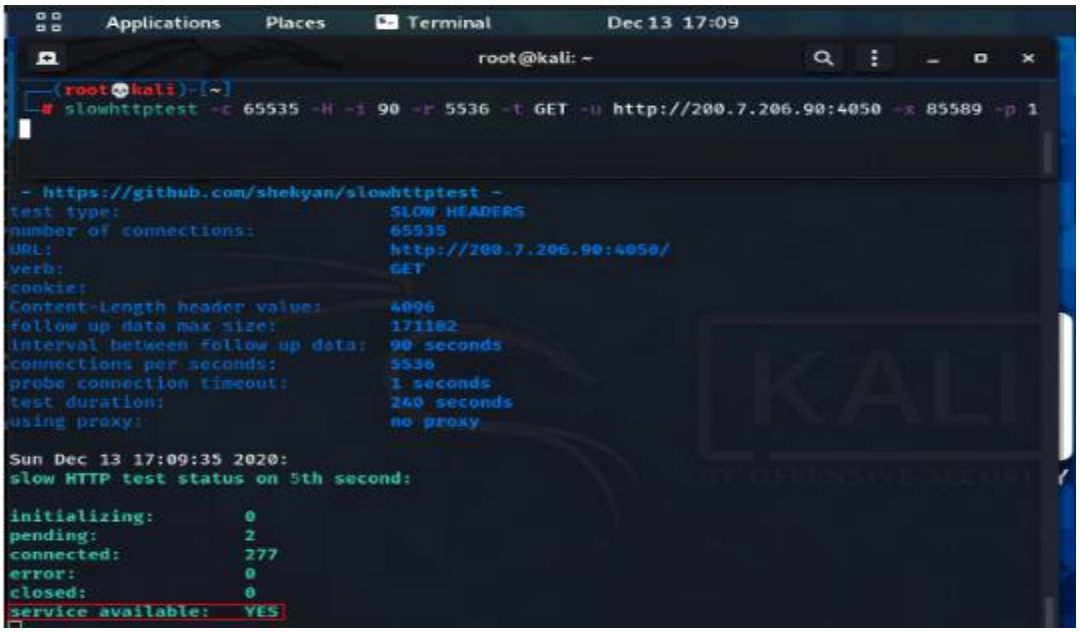


Figura 41. Ejecución de un ataque DoS

Fuente: elaboración propia

Sin embargo, después de 5 segundos de haber ejecutado el ataque, se observa en la figura 42 que es sitio ya no está disponible para ser accedido desde las agencias 01 y 02.

Figura 42. Ataque exitoso DoS

Fuente: elaboración propia

Luego, que se confirma que el ataque a un pilar de la seguridad que es la confidencialidad ha sido exitoso, se realizan pruebas de acceso desde las agencias remotas, estos ya con resultados negativos debido a que no, se accede y consumir el servicio que está ubicado en oficina matriz.

En la figura 43, se expone las pruebas de acceso desde la Agencia 01.

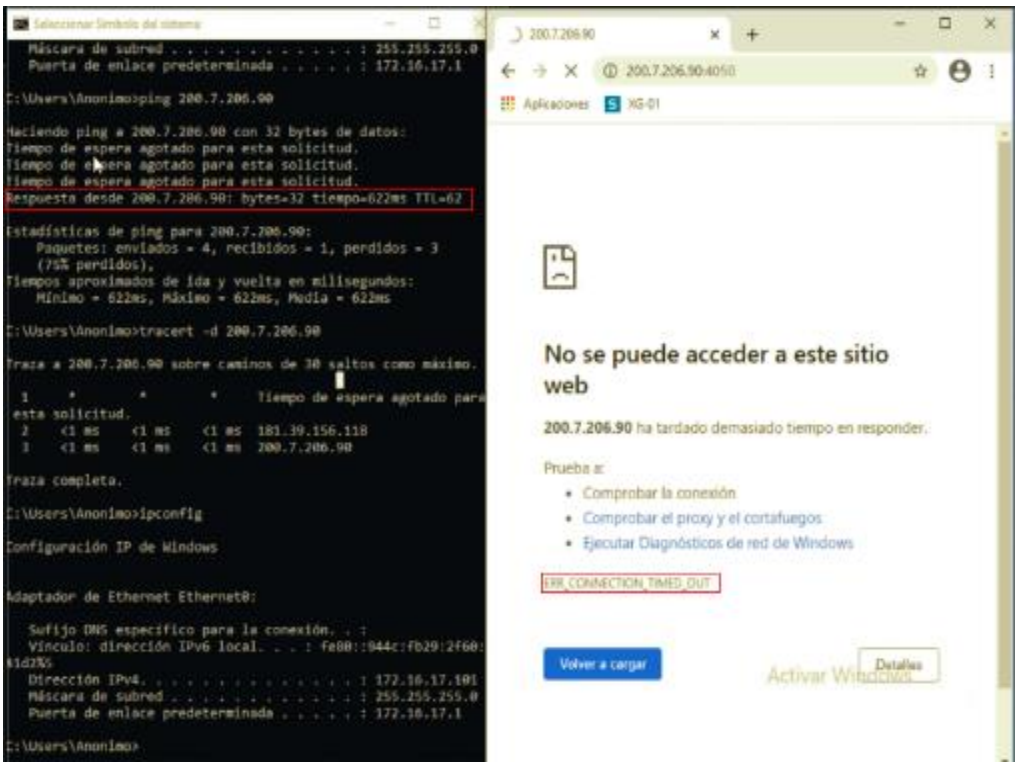


Figura 43. Conexión fallida desde agencia 01 a oficina matriz

Fuente: elaboración propia

En la figura 44, se visualiza las pruebas de acceso desde la Agencia 02 donde, se corrobora que el servicio ya no está disponible.

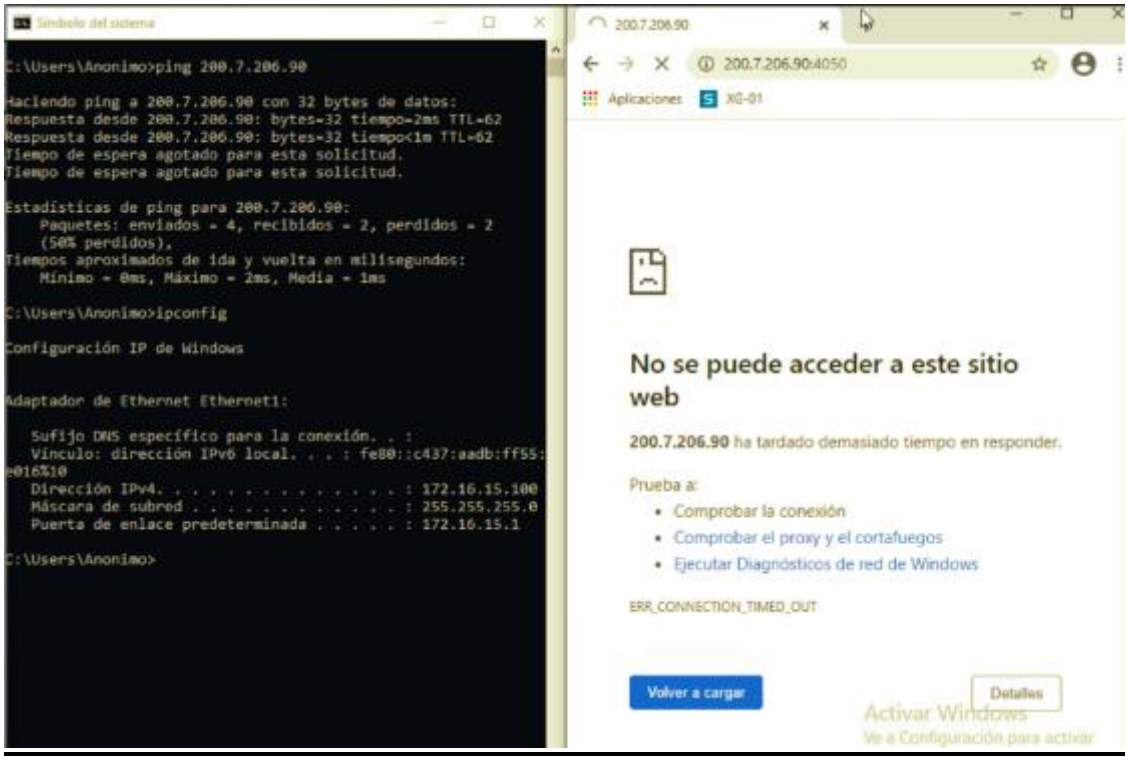


Figura 44. Conexión fallida desde agencia 02 a oficina matriz

Fuente: elaboración propia

Escenario 02: Acceso a Servicios internos a través de una VPN IPSec entre Matriz y las agencias.

Pruebas de conectividad entre la agencia 01 y la oficina matriz, la figura 45 muestra el proceso, que se realiza entre las dos direcciones ip públicas para levantar el Túnel VPN IPSec y una vez, que se ha validado que las configuraciones tanto en la fase uno como en la fase dos son las mismas en los dos *firewalls,* se comparten los segmentos de red o únicamente host a través del túnel.

Si, se comparte solo equipos puntuales en el Túnel VPN IPSec hay que tener presente que cada vez, que se agregue un nuevo host para ser compartido a través del Túnel presentara una pérdida

de paquetes entre los dos puntos esto debido a, que se actualizan las tablas de rutas en los dos *firewalls* tanto en oficina matriz y de la agencia.

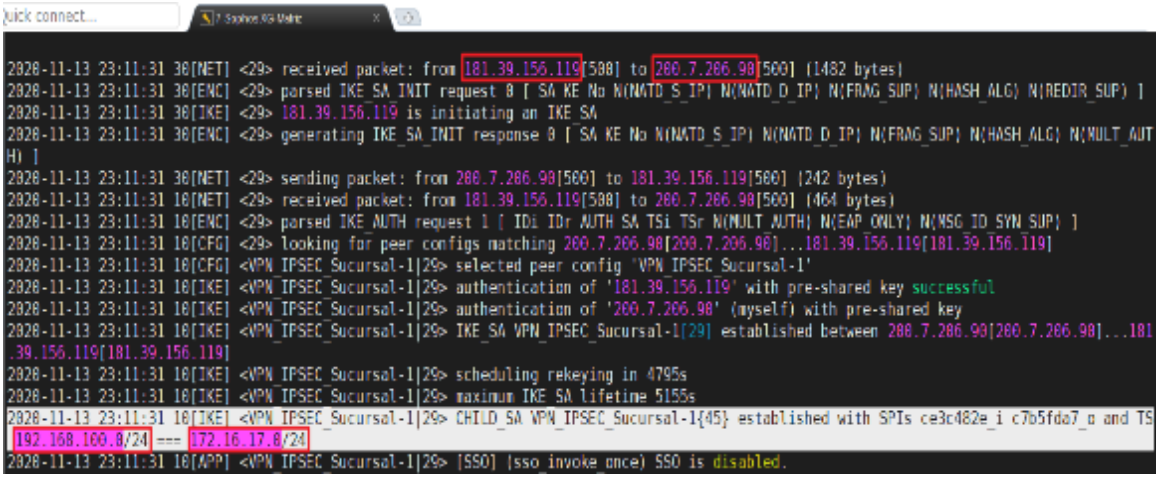


Figura 45. Establecimiento de Túnel VPN IPSec

Fuente: elaboración propia

Pruebas de conectividad entre la agencia 01 y la oficina matriz, la figura 46 muestra una prueba de ping que corrobora que existe comunicación entre la agencia 02 y la oficina matriz.

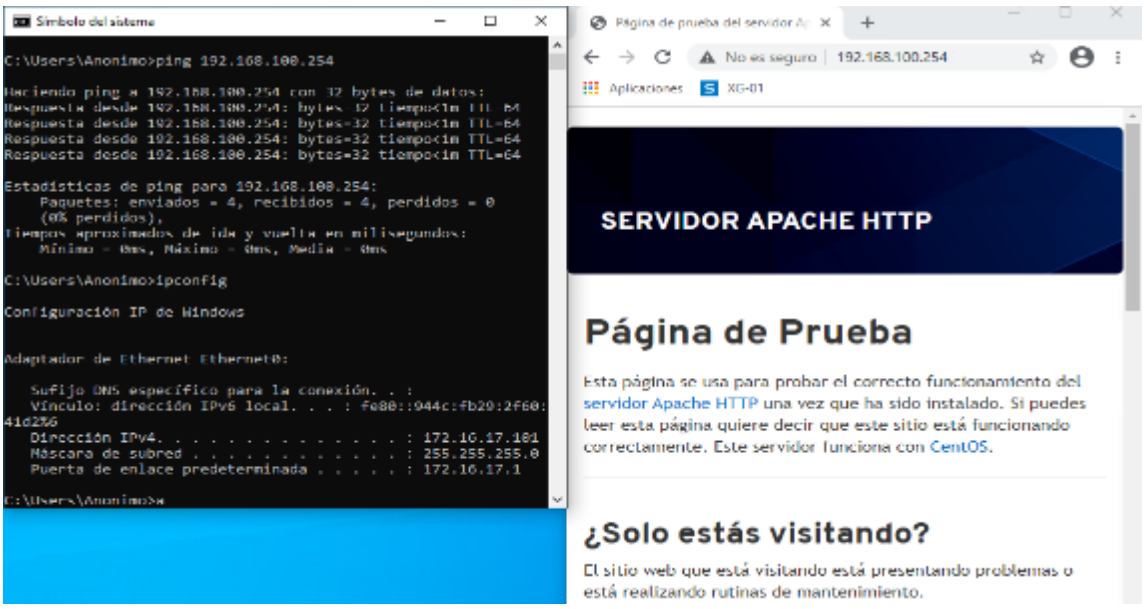


Figura 46. Prueba de ping y acceso al servicio en oficina matriz

Fuente: elaboración propia

Los ataques DoS que son originados por los usuarios internos, logran esto al inundar el objetivo con tráfico donde envian información que desencadena un bloqueo.

Si un empleado descontento detecta que un nuevo sitio web que está activo, él ejecuta el ataque DoS con la herramienta *Slowhttptest* al sitio web objetivo y dejar inaccesible el sitio para los usuarios de las agencias.

En la figura 47, se muestra que el servicio que está alojado en la oficina matriz y que es accesible desde las agencias, se muestra como disponible.

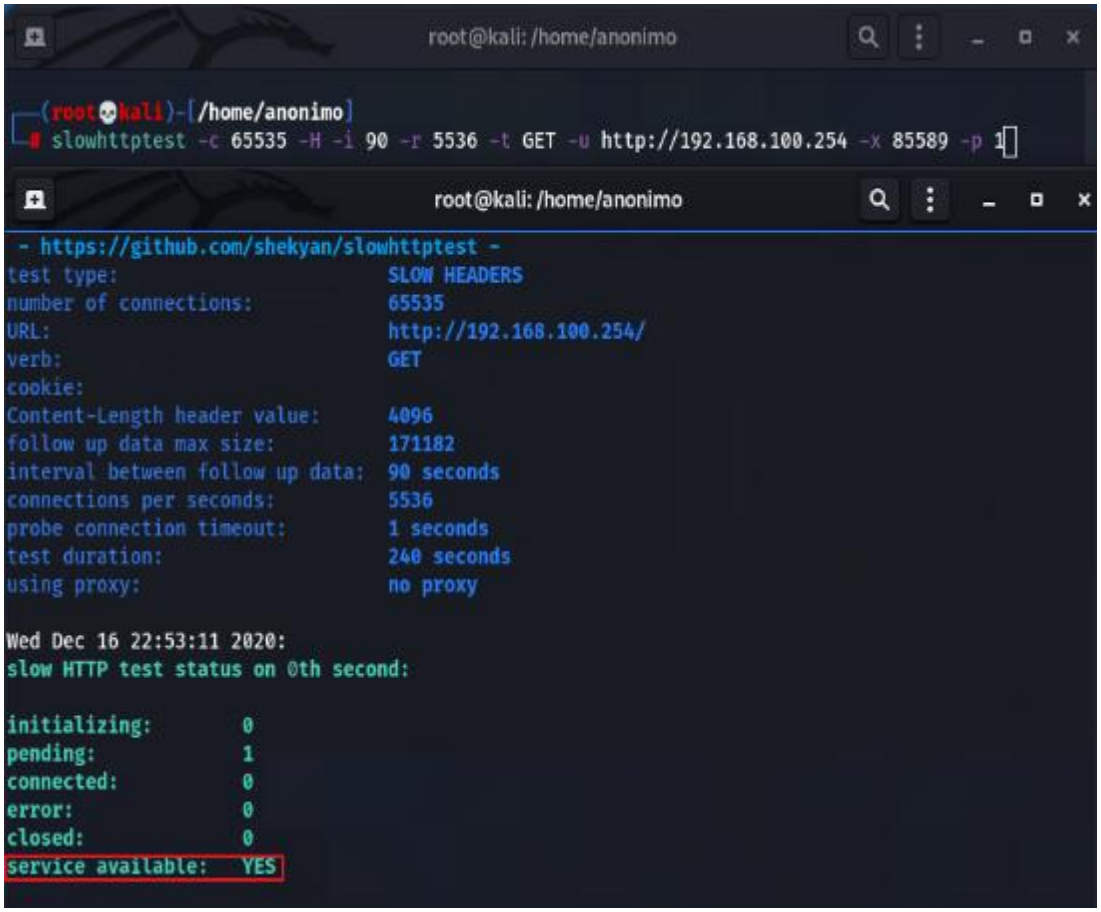


Figura 47. Ejecución de un ataque DoS interno

Fuente: elaboración propia

Sin embargo, después de 10 segundos de haber ejecutado el ataque, se observa en la figura 48 que es sitio ya no está disponible para ser accedido desde la agencia 01.

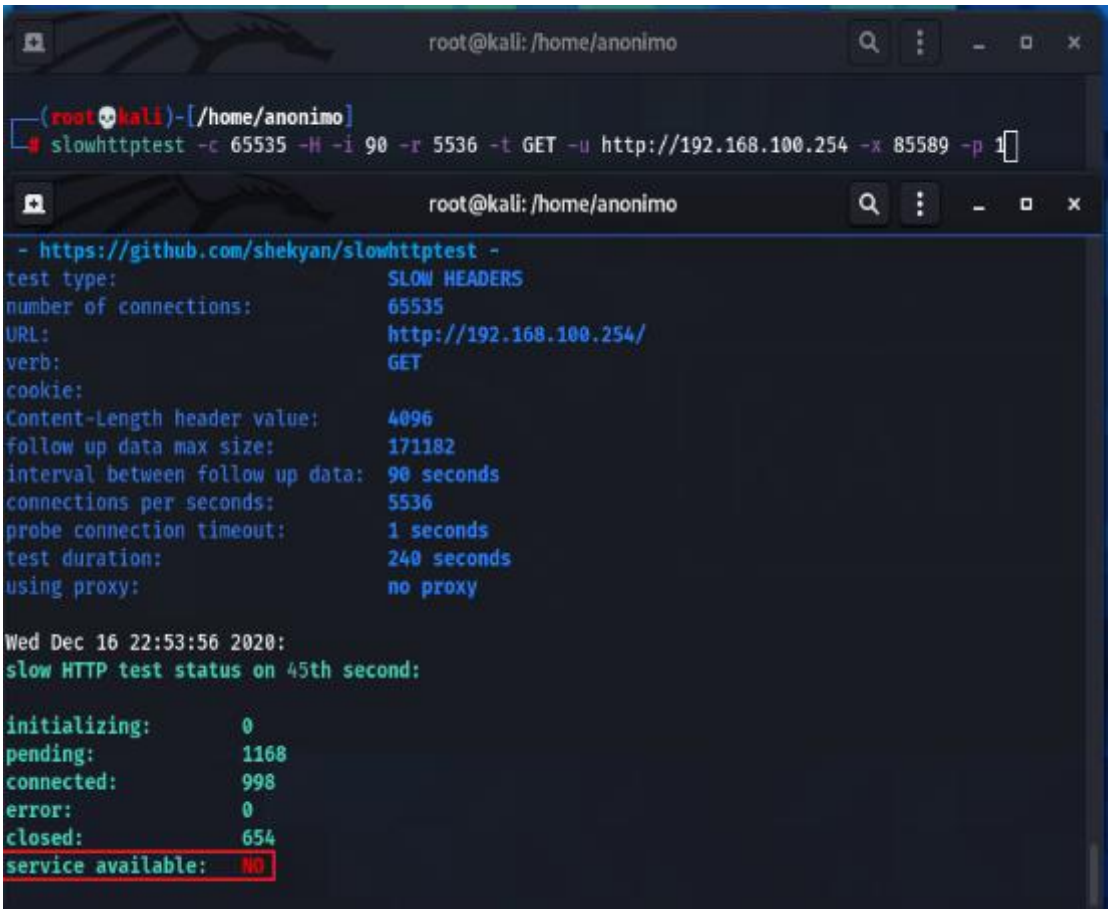


Figura 48. Ataque DoS interno exitoso

Fuente: elaboración propia

Luego, que se confirma que el ataque a un pilar de la seguridad que es la confidencialidad ha sido exitoso, se realizan pruebas de acceso desde la agencia remota, estos ya con resultados negativos debido a que no, se accede y consumir el servicio que está ubicado en oficina matriz.

En la figura 49, se expone las pruebas de acceso desde la Agencia 01.

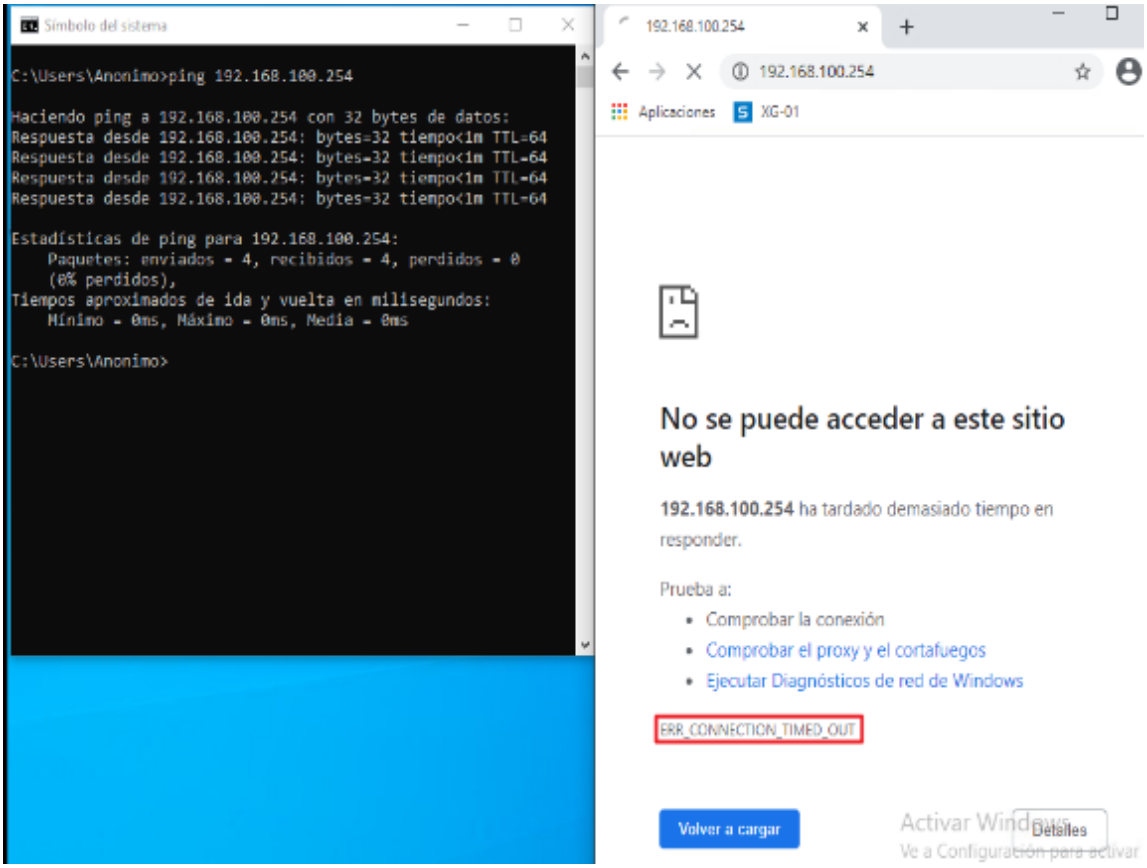


Figura 49. Conexión fallida desde agencia 01 hacia oficina matriz

Fuente: elaboración propia

Escenario 3: Acceso a servicios internos a través de una red de área amplia definida por el software desde las agencias 01 y 02 hacia Matriz.

Se aprovechan los múltiples enlaces del proveedor de internet para escalar la capacidad y reducir los costos, que se presentan con los enlaces de datos. La selección de rutas y la detección de apagones son por aplicación para garantizar el mejor rendimiento y experiencia de usuario para aplicaciones críticas.

De forma predeterminada, se logra una conmutación por error de hasta tres segundos como, se muestra en la figura 50, entre enlaces lo que garantiza el mejor rendimiento posible de las aplicaciones.

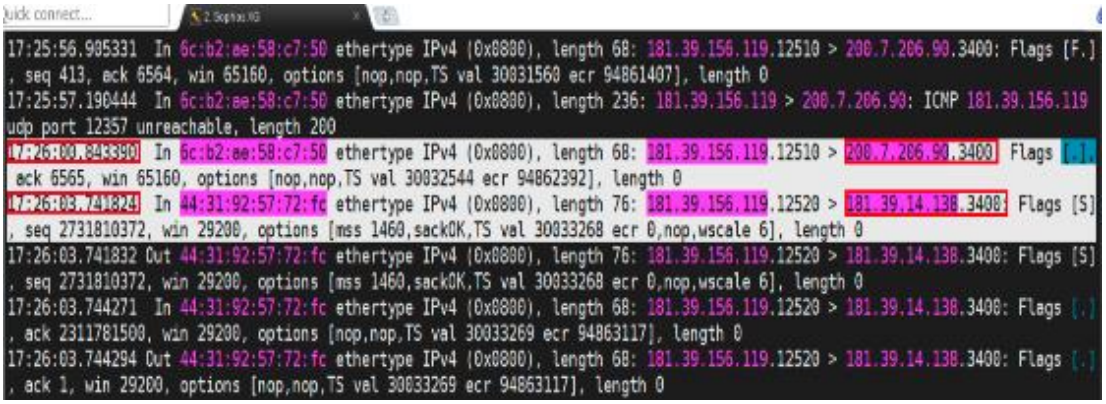


Figura 50. Conmutación de túneles dinámicos SD-WAN

Fuente: elaboración propia

Si el enlace principal, se encuentra nuevamente disponible la sucursal vuelve a crear el Túnel de manera dinámica, en la figura 51, se observa que el tiempo de conmutación entre el enlace principal con el secundario es de un segundo.

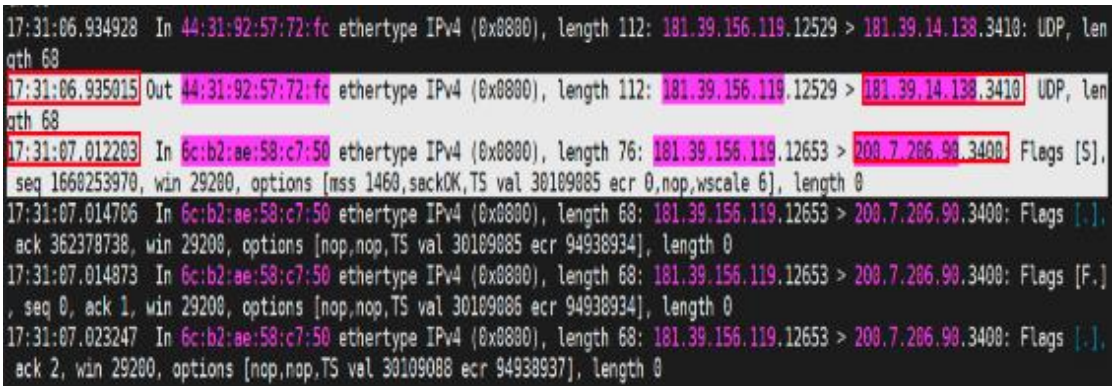


Figura 51. Restablecimiento de túnel dinámico SD-WAN enlace principal

Fuente: elaboración propia

Si permite puertos para las conexiones desde las agencias remotas hacia la oficina matriz, somos propensos a los riesgos informáticos debido a que existen los protocolos de tunelización que

ocultan un paquete completo dentro del datagrama y existe la posibilidad de un mal uso. La tunelización, se utiliza a menudo para superar los *firewall* poco sofisticados o mal configurados al incluir protocolos bloqueados dentro de los protocolos que el *firewall* permite como, se muestra en la figura 52.

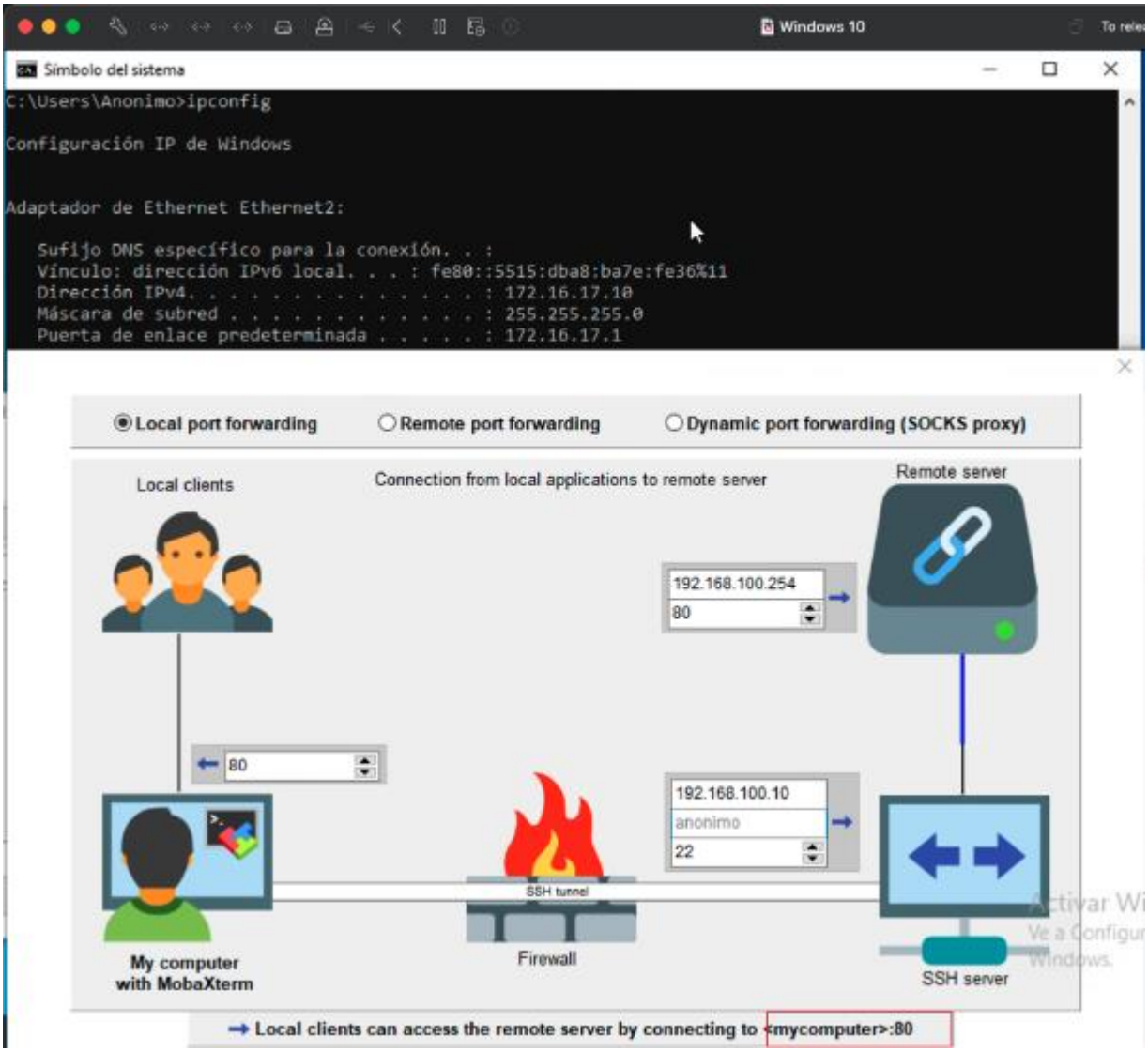


Figura 52. Conexión equipo no autorizado mediante túnel SHH

Fuente: elaboración propia

Con ssh tunneling, se elude un *firewall* de aplicaciones web y de red, encapsula túneles ssh. En la figura 53, la cual indica la captura de tráfico de la conexión desde un equipo de una agencia

a un equipo no autorizado de oficina matriz, pasa desapercibido y aprovecha para robar información confidencial de las compañías.

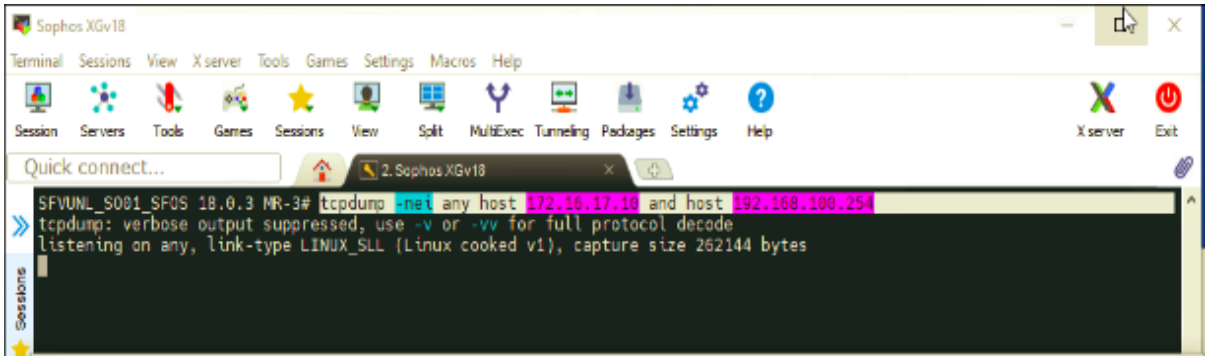


Figura 53. Captura de logs conexión tunneling

Fuente: elaboración propia

Como muestra en la figura 54, una vez, que se establece la conexión desde la computadora de la agencia hacia un equipo no autorizado en la oficina matriz el usuario mal intencionado utiliza cualquier script que permita transferirse archivos confidenciales y eliminar cualquier tipo de información rápidamente.

Figura 54. Conexión exitosa a un equipo no autorizado mediante túnel SSH

Fuente: elaboración propia

El uso de protocolos de tunelización también dificulta la realización de tareas como la inspección profunda de paquetes, donde la infraestructura de red busca datos sospechosos en el datagrama, o el filtrado de entrada / salida, que comprueba la cordura de las direcciones de destino de los datos para evitar posibles ataques.

3.1.2 Optimizar

Escenario 3: Acceso a servicios internos a través de una red de área amplia definida por el software configurada bajo buenas prácticas de Seguridad.

Se proponen los siguientes cambios a configurar en una red de área amplia definida por el software para mitigar los ataques informáticos y reducir los riesgos informáticos en los accesos a los servicios internos a través de los accesos WAN de los que son víctimas las organizaciones:

- En las reglas de *firewall* y políticas SD-WAN, se limita el acceso solo a equipos específicos, servicios necesarios como, se muestra en la figura 55, evita las configuraciones genéricas.

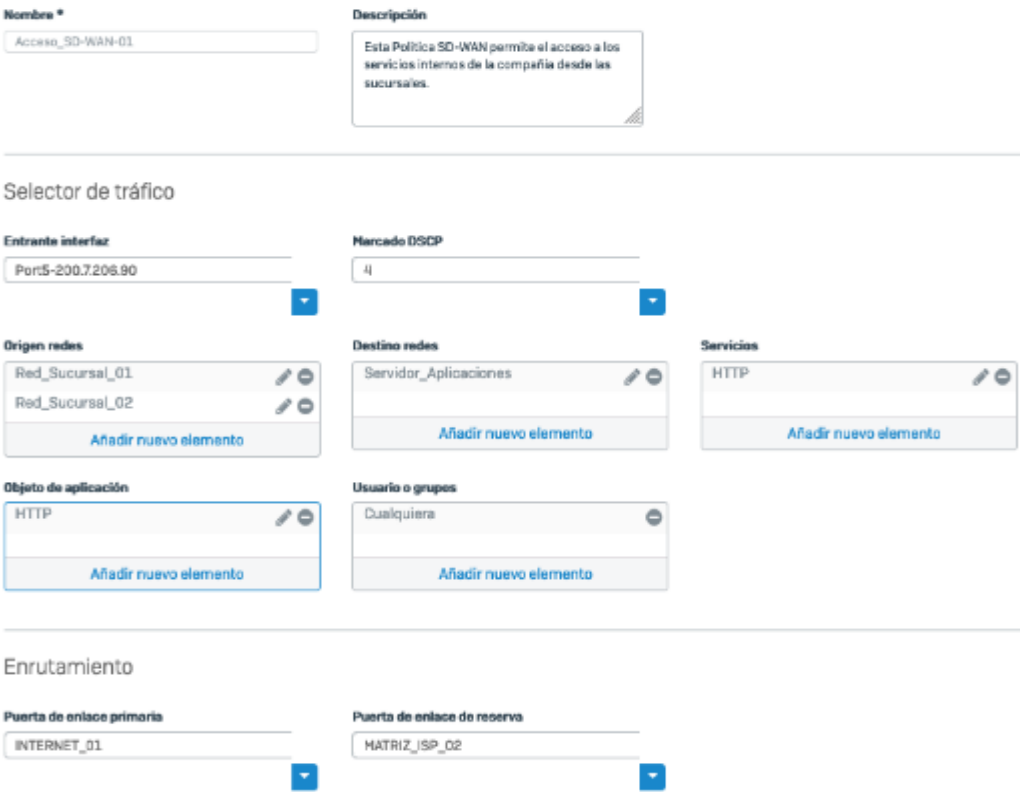


Figura 55. Configuración de política SD-WAN bajo buenas prácticas de seguridad

Fuente: elaboración propia

Esta configuración, que se apega a buenas prácticas de seguridad en las configuraciones y garantiza un nivel de seguridad superior siempre tomar como referencia la arquitectura de seguridad, cero confianza (Zero Trust) la cual es una iniciativa estratégica que ayuda a reducir riesgos informáticos, el concepto de confianza de la arquitectura de red de una organización detalla “nunca confiar, verificar siempre".

Tabla 8. Comparativos de tecnologías de acceso WAN

Tecnologías / Parámetros	SD-WAN	DNAT	VPN IPSec
Complejidad	Simplifica significativamente la complejidad de la administración a través de Sophos XGv18 donde proporciona un tablero gráfico fácil de usar desde el cual, se monitorea, configura y mantiene todos los dispositivos y enlaces operativos.	Si la seguridad no está integrada las aplicaciones publicadas necesitan opciones adicionales de seguridad.	La política, que se configura para el túnel vpn IPSec tiene que ser la misma en los dos *firewalls* y cada vez, que se necesite agregar un nuevo equipo al túnel hacerlo en los dos *firewalls* y esto ocasiona una pérdida de conexión en el túnel.
Visibilidad	Amplia visibilidad y gestión de las	Visibilidad de las aplicaciones que son publicadas a internet	El enrutamiento de paquetes limita la

	aplicaciones críticas para la organización.	con riesgo que sean vulneradas.	visibilidad de las aplicaciones.
Reconocimiento de Rutas	Prioriza automáticamente el enrutamiento de aplicaciones en todo el ancho de banda en función del usuario y aplicación específicos.	Crear una regla de *Firewall* por cada host interno, que se quiera publicar en internet.	Por cada nueva ruta, que se quiera agregar al Túnel el *Firewall* experimentara una Perdida de paquetes hasta que actualice el nuevo host/red a compartir.
Rendimiento y disponibilidad	Levanta Túneles de manera dinámica donde ofrece un rendimiento óptimo para las aplicaciones y garantiza la disponibilidad en todo momento.	Su rendimiento esta conforme al ancho de banda de internet y no garantiza disponibilidad debido a que solo tiene un punto de falla.	Ofrece un ancho de banda limitado, comparte el canal de internet con el tráfico de navegación de los usuarios y un solo punto de falla
Escalabilidad	Simplifica la orquestación y el aprovisionamiento de nuevas sucursales con inteligencia de enrutamiento, asegurar	Acoge las conexiones que originan desde cualquier parte del mundo por lo que es necesario elaborar un presupuesto para	Algunos fabricantes de *Next Generation Firewalls* son limitados debido a que no son compatibles en los protocolos de seguridad.

	la red automáticamente.	garantizar un buen ancho de banda con el proveedor de internet.	
Seguridad	Las VPN basadas en IPSec son universales para todas las SD-WAN. Dado que una SD-WAN utiliza la Internet pública además de las conexiones MPLS, se requiere un túnel VPN o IPSec para, como mínimo, garantizar que no, se interfiera el tráfico entre el remitente y el receptor.	No es recomendable realizar publicaciones de sitios web o aplicaciones a través de una regla DNAT, debido a, que se expone a que el servicio sea accedido desde cualquier parte del mundo y es propensos a recibir ciberataques.	*Internet Protocol Security* garantiza que la información que es compartida desde la oficina matriz hacia sucursal es segura e inaccesible para terceros. Utiliza diferentes niveles de cifrado para garantizar la confidencialidad de la información.

Fuente: elaboración propia

Se ha realizado un comparativo de los fabricantes de *Next Generation Firewall* más conocidos que comercializan la tecnología de red de área amplia definida por software, realizar una valoración de sus características.

Tabla de valoración:

Tabla 9. Valoración de Fabricantes en SD-WAN

Parameros	**Valoración**
Limit ado	●
Bueno	● ●
Muy bueno	● ● ●
Excelente	● ● ● ●

Fuente: elaboración propia

Tabla comparativa de fabricantes:

Tabla 10. Comparativo de SD-WAN en *Firewalls* de Próxima Generación

Fabricantes / Características	Fortinet	Cisco Meraki	Palo Alto	Sophos XG
Redundancia en conexión (Balanceo de enlaces, conmutación por erro, preservación de sesiones)	● ● ●	● ●	● ● ●	● ●
Por la ruta de la aplicación (lista de aplicaciones, simplicidad)	● ● ●	● ●	● ● ● ●	● ● ●
Medición de la calidad (Enlace, latencia, jiter, pérdida, capacidad)	● ● ● ●	● ● ●	● ● ● ●	● ●
Calidad de Servicio (por aplicación, colas de prioridad, esfuerzo del instalador)	● ● ● ●	● ●	● ● ● ●	● ●
Visibilidad del tráfico	● ●	● ●	● ●	● ● ●

(indicadores de salud, indicadores de eventos, monitores de flujo, informes)				
Encriptación y análisis de Tráfico	●	● ● ● ●	● ●	●

Fuente: Sophos 2020

En la figura 56, se muestra la evolución de los diferentes fabricantes en el cuadrante de líderes de Gartner desde el año 2019 al 2020 referente a la tecnología de red de área amplia definida por software.

Gartner no respalda a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no aconseja a los usuarios de tecnología que seleccionen solo a los proveedores con las calificaciones más altas u otra designación.

Las publicaciones de investigación de Gartner consisten en las opiniones de la organización de investigación de Gartner y no interpretarse como declaraciones de hechos. Gartner niega todas las garantías, expresas o implícitas, con respecto a esta investigación, incluidas las garantías de comerciabilidad o idoneidad para un propósito particular.

Este gráfico fue publicado por Gartner, Inc. como parte de un documento de investigación más amplio, se evalua en el contexto de todo el documento. (Gartner, 2020)

Evolución del cuadrante mágico de Gartner:

- Publicado en octubre 2019
- Publicado septiembre 2020

Figura 56. Evolución del Cuadrante Mágico de Gartner para las infraestructuras SD-WAN

Fuente: Gartner (Septiembre 2020)

CONCLUSIONES

- El análisis de las bases teóricas de SD-WAN relacionadas con los riesgos informáticos identificó los principales casos de éxito implementado las redes de área amplia definida en software en el ámbito de educación y de finanzas fuera del país y determinar las principales características, aplicativos, plataformas y posibles ataques que tienen en esta nueva tecnología.

- El diagnóstico del estado actual de los riesgos informáticos en arquitecturas SD-WAN muestran los resultados de los ataques realizados, se concluye que un cibercriminal toma ventaja de las configuraciones por defecto, se dejan en los equipos perimetrales al momento de realizar publicaciones de servicios internos, si es por una regla DNAT, los ataques serán originados desde Internet, si la publicación es a través de una política SD-WAN, los ataques muchas veces, se originan desde la red de las agencias, siempre buscan un objetivos en común el cual es atacar contra un pilar fundamental de la seguridad que es la disponibilidad y dejan inaccesible a un servicio web o aplicativo interno de la organización.

- La verificación del funcionamiento de una arquitectura SD-WAN bajo buenas prácticas de seguridad evidencia la reducción de riesgos informáticos que son víctima las organizaciones y adicional tener alta disponibilidad en los accesos a nuestros servicios publicados a través de los enlaces de Internet. En referencia a la figura 50, si el enlace de Internet número uno queda inaccesible por cualquier motivo de manera inmediata las configuraciones de SD-WAN levanta el túnel con el segundo enlace de internet y garantiza la disponibilidad del servicio para las personas que lo consumen, y si vuelve a estar operativo el primer enlace de internet, se establecerá nuevamente el túnel de manera dinámica lo cual garantiza el uso del mejor enlace para la conexión con las aplicaciones críticas de la organización.

- Con una red de área amplia definida por software, se muestra calidad de las aplicaciones críticas, debido a que las organizaciones buscan visibilidad en tiempo real de la aplicación el tráfico y el rendimiento para mantener la calidad de las sesiones de las aplicaciones comerciales y prioriza las aplicaciones críticas para la organización.

RECOMENDACIONES

- Adoptar esta arquitectura de red de área amplia definida por software en las organizaciones del país, disponen de una administración centralizada y mejora la calidad de las conexiones entre la oficina matriz y las sucursales, se encuentran ubicadas en diferentes partes del mundo levantan túneles dinámicos los cuales reducirían el trabajo a los Administradores de TI.

- El uso de una arquitectura de red de área amplia definida por software, se implementará el modelo de seguridad *Zero-Trust* el cual ayuda a mitigar los riesgos informáticos reduce las brechas de seguridad y elimina el concepto de confianza en la arquitectura de red de una organización. Siempre es importante fomentar el principio de seguridad "nunca confiar, siempre verificar"

- Se mejora los tiempos de convergencia en una red de área amplia definida por software si implementán detección de fallas BFD para que la convergencia sea extremadamente rápida en los túneles dinámicos, sin embargo, esto valida en los datashet de los Next Generation *Firewall* para confirmar si es soportado por los fabricantes.

BIBLIOGRAFÍA

Aucay, F. R. (2020). Esquema de comunicación con SDWAN de los puntos de atención en la Cooperativa Jardín Azuayo. ISSN:2550-682X.

Cisco. (2020). Qué es SD-WAN. Retrieved from https://www.cisco.com/c/es_mx/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html

Coronel, R. (2020). SD-WAN, principales conceptos y modelo de funcionamiento. Retrieved from https://ostec.blog/es/seguridad-perimetral/sd-wan-conceptos-funcionamiento/

Corporación Internacional de Datos. (2020, Noviembre 11). La voz de la industria Digital. Retrieved from https://ametic.es/es/asociado/idc-research-espana#:~:text=International%20Data%20Corporation%20(IDC)%20es,telecomunicaciones%20y%20tecnolog%C3%ADa%20de%20consumo.

Fortinet. (2020, Mayo 2019). How SD-WAN Solutions Help Canadian Schools with WAN-Edge Transformation. Retrieved from https://www.fortinet.com/blog/business-and-technology/how-sdwan-solutions-help-canadian-schools-remain-compliant

Gartner Research. (2020). Transforming Networking for the Cloud Era with SD-WAN.

Gartner. (2020, Septiembre). It's a Hat Trick! VMware Named a Leader in Gartner 2020 Magic Quadrant for WAN Edge Infrastructure. Retrieved from https://sdwan.vmware.com/sd-wan/gartner-magic-quadrant-wan-edge-infrastructure-sdwan-2020

Gordeychik, S. (2018). Sergey Gordeychik. Retrieved from https://www.researchgate.net/publication/328900172_SD-WAN_Threat_Landscape

Guerra, P. (2016). “PROPUESTA DE METODOLOGÍA PARA LA IMPLEMENTACIÓN DE PROYECTOS DE REDES – CASO DE ESTUDIO INSTITUCIÓN FINANCIERA LOCAL.

Guevara, J. (2017). Diseño de la red de campus de la empresa ¨equipos y suministros de Telecomunicaciones equysum" de la ciudad¨.

Guevara, J. (2017). Diseño de ña red de campus de la empresa ¨equipos y suministros de Telecomunicaciones equysum de la ciudad¨.

International Data Corporation (IDC). (2020, Octubre 05). IDC Technology Spotlight: Threat Visibility and Management Are Critical in Managed Security Services. Retrieved from https://business.comcast.com/community/browse-all/details/threat-visibility-and-management-are-critical-in-managed-security-services

Julián Guevara. (2017). Diseño de la red de campus de la empresa ¨equipos y suministros de Telecomunicaciones equysum" de la ciudad¨.

Lessing, M. (2020, Marzo 10). sdx central. Retrieved from https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/

Linux, C. (2020, Enero). The CentOS Project. Retrieved from https://www.centos.org/

Majdoub, M. (2017). A Fast Bit-Level MPLS-Based Source Routing Scheme in Software Defined Networks: SD-WLAN. Computer Science.

Naula, R. (2020). Diseño de una solución SD-WAN (Software Define Wide Area Network) para alta capacidad aplicada al laboratorio de la Facultad Técnica de la UCSG. Retrieved from http://repositorio.ucsg.edu.ec/handle/3317/15601

Nguyen, T. A. (2018). Retrieved from Anhnt162 Cisco Sdwan: https://www.scribd.com/presentation/417004001/Anhnt162-Cisco-Sdwan

Palo Alto Networks. (2020). PAN-OS Secure SD-WAN. Santa Clara.

Quezada, A. E. (2019). Hacking con Kali Linux. Lima.

Rouse, M. (2020). WAN definida por software (SD-WAN). New York .

Sánchez, B. (2019). Análisis de factibilidad técnico y económico entre una red MPLS Traffic Engineering (TE) con IPSEC y una red Sd-Wan moderna. Retrieved from http://repositorio.espe.edu.ec/xmlui/handle/21000/15877

SCC. (2019). SD-WAN: ¿QUÉ ES? Retrieved from https://www.sccenlared.es/sd-wan-que-es/

Sean Wilkins. (2020). Cisco's PPDIOO Network Cycle. Retrieved from https://www.ciscopress.com/articles/article.asp?p=1697888&seqNum=2

Sophos. (2020). Making the Move to SD-WAN with Sophos: Six Use Cases. United Kingdom.

Sophos. (2020, Diciembre 11). Sophos XG Firewall: RED (Remote Ethernet Device) technical training guide. Retrieved from https://support.sophos.com/support/s/article/KB-000036699?language=en_US#RED-Technical-Overview

Stearns Bank. (2016). Partners with Ecessa for Secure Connections Using SD-WAN. Stearns Bs, Florida, Georgia.

Vmware. (2016). Data Center Viftualization Fundamntals. California.

Vunkers. (2020). Vunkers IT Experts. Retrieved from https://www.vunkers.com/productos/mikrotik/#:~:text=%3EMikroTik%20RouterOS%20es%20el%20sistema,acceso%2C%20servidor%20VPN%20y%20m%C3%A1s.

Zone, R. (2020, Junio 04). SSH Tunneling: Manual para crear un túnel SSH y navegar seguro. Retrieved from https://www.redeszone.net/tutoriales/servidores/ssh-tunneling/

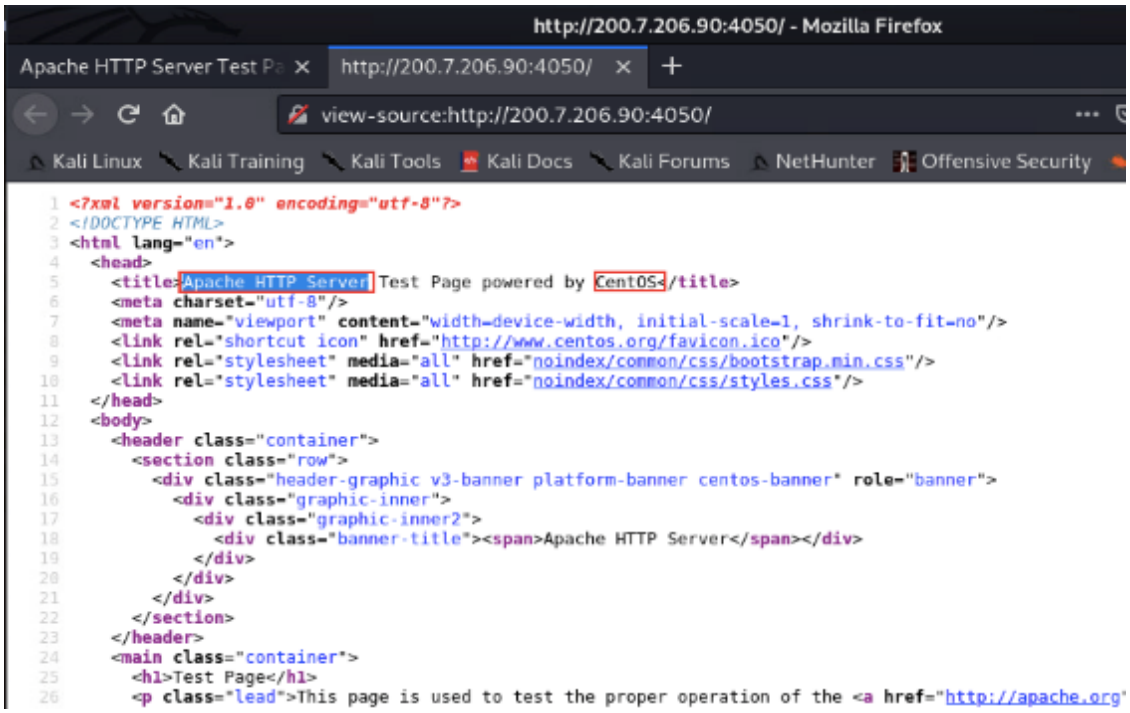
ANEXO 1

Se utilizó el ciclo de vida de un ciberataque para el desarrollo de los tres escenarios el cual es una secuencia de pasos que un atacante sigue metódicamente para infiltrarse en la red de una organización y extraer datos importantes y confidenciales de ella.

Fase 1:

Reconocimiento: Los cibercriminales estudian cuidadosamente sus ataques, de una forma que investigan, identifican y seleccionan objetivos, muchas veces extrae información pública de las organizaciones desde el perfil de LinkedIn de un empleado hasta información en la *Deepweb* y *Darkweb.*

Para este proyecto de investigación, se observa el código fuente de la página web, se determina que es un servidor web apache y que funciona en CentOS.

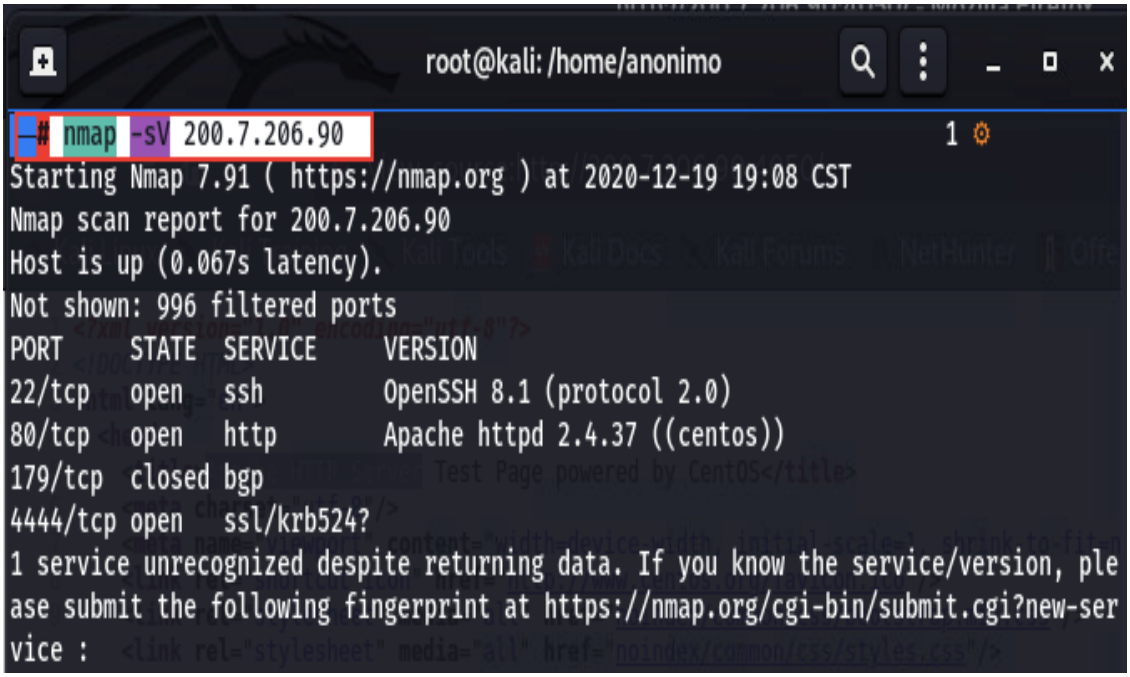


Fase de Reconocimientos web

Fuente: elaboración propia

Escaneo: A continuación, los cibercriminales utilizan nmap para determinar cuáles son los puertos abiertos que las organizaciones utilizan para realizar sus publicaciones, determinan las versiones de los servicios de esos puertos públicos en el perímetro.

Herramienta 1: Nmap



Escaneo de puertos al *Firewall* Perimetral

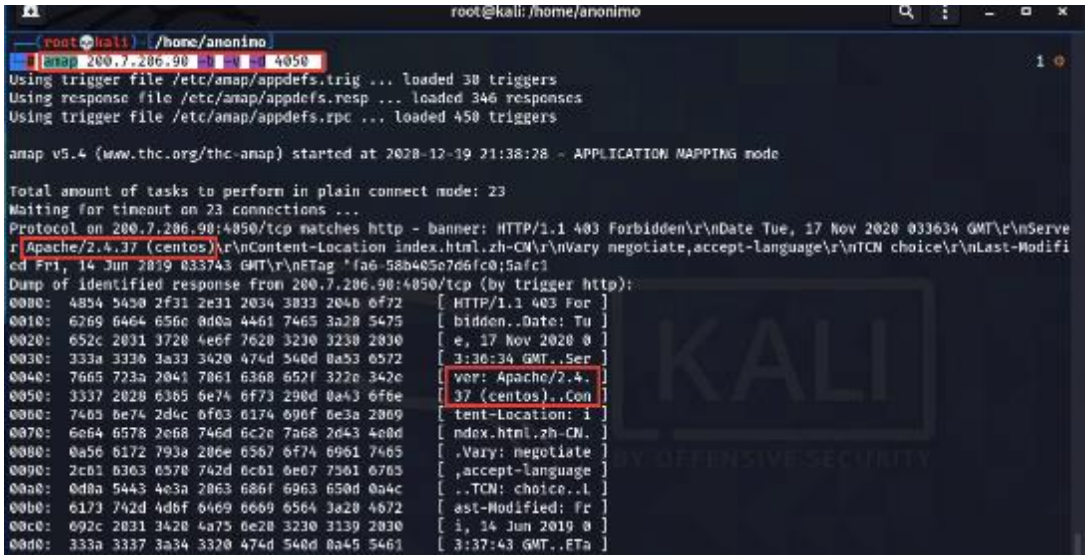
Fuente: elaboración propia

Herramienta 2: Amap

Es una herramienta entrega información valiosa a los cibercriminales, identifican qué servicio web o aplicativo esta publicado a internet incluso si el administrador de red de la organización realiza esa publicación en un puerto desconocido, como es nuestro caso en el puerto 4050 TCP.

Datos importantes encontrados por la herramienta:

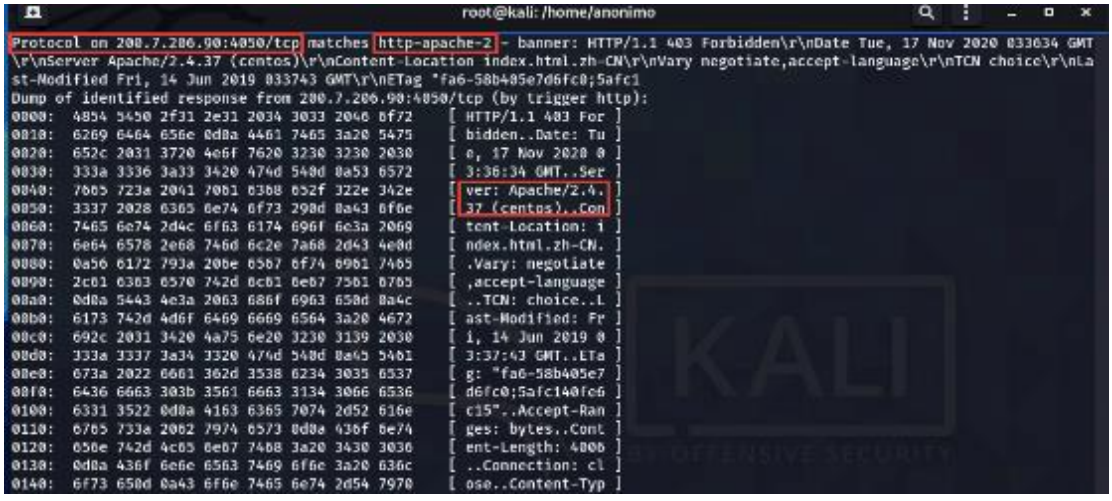
- Servidor web apache.
- Sistema operativo del host CentOS.



Información importante en la fase de enumeración

Fuente: elaboración propia

Se observa el banner con información de la dirección ip publica por donde se ha publicado el servicio web, se observa nuevamente la información de servidor web y Sistema operativo del equipo:

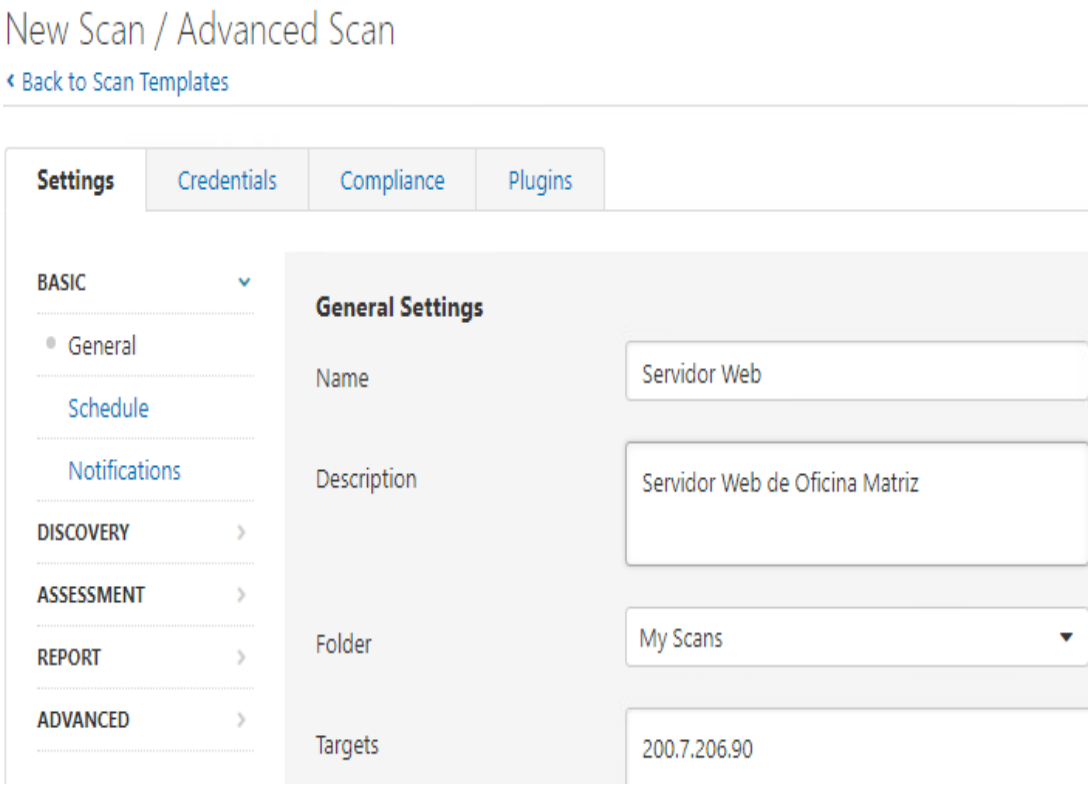


Banner del servidor Apache

Fuente: elaboración propia

Identificar Vulnerabilidades: Despues de recolectar suficiente información de la organización víctima, se identifica sus debilidades es decir que vulnerabilidades tiene y

cuales podrían aprovechan, esto realiza con la herramienta de Nessus que es una suite muy completa que realiza análisis de vulnerabilidades a sitios web.

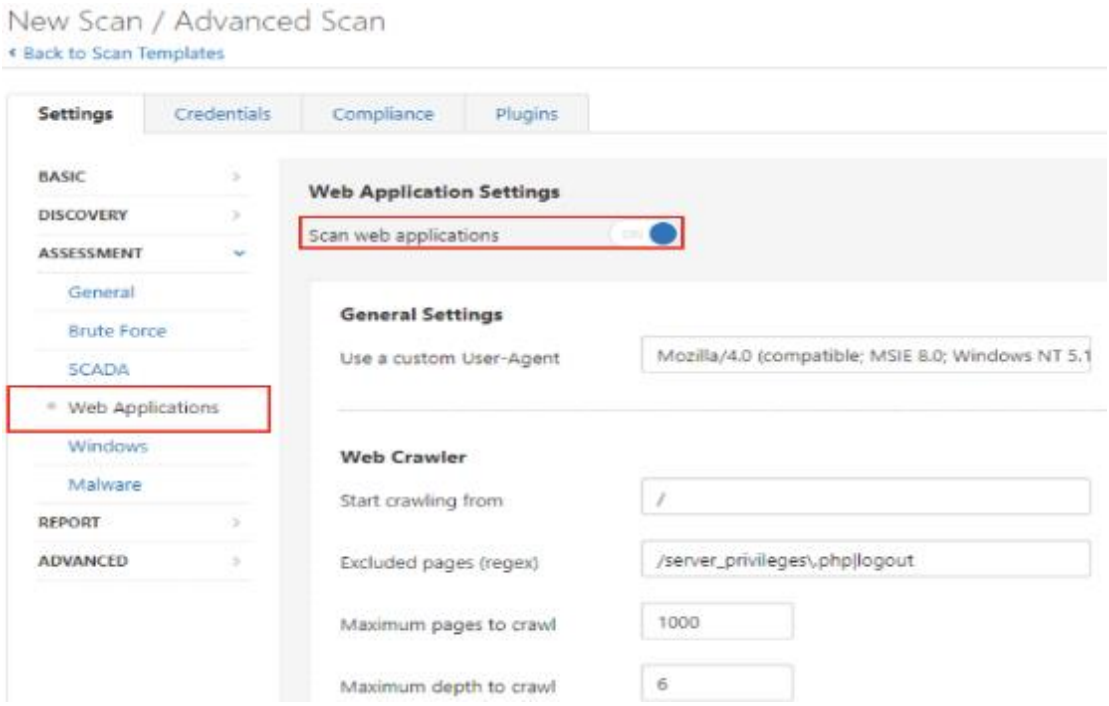


Definición del host a escanear

Fuente: elaboración propia

Una vez que personalizan el escaneo con la dirección ip del host utiliza plug-ins, debido a que Nessus usa una arquitectura servidor-cliente donde el servidor realiza controles de seguridad del equipo cliente.

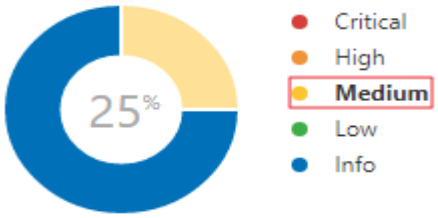
La mayoría de las aplicaciones web contienen vulnerabilidades de seguridad. En muchas ocasiones las formas simples de crear una aplicación web son propensas a ataques de inyección de SQL, DoS y ataques de secuencias de comandos entre sitios, así como a otras vulnerabilidades menos comunes.



Activación del Pluguin para el escaneo de Servidores Web

Fuente: elaboración propia

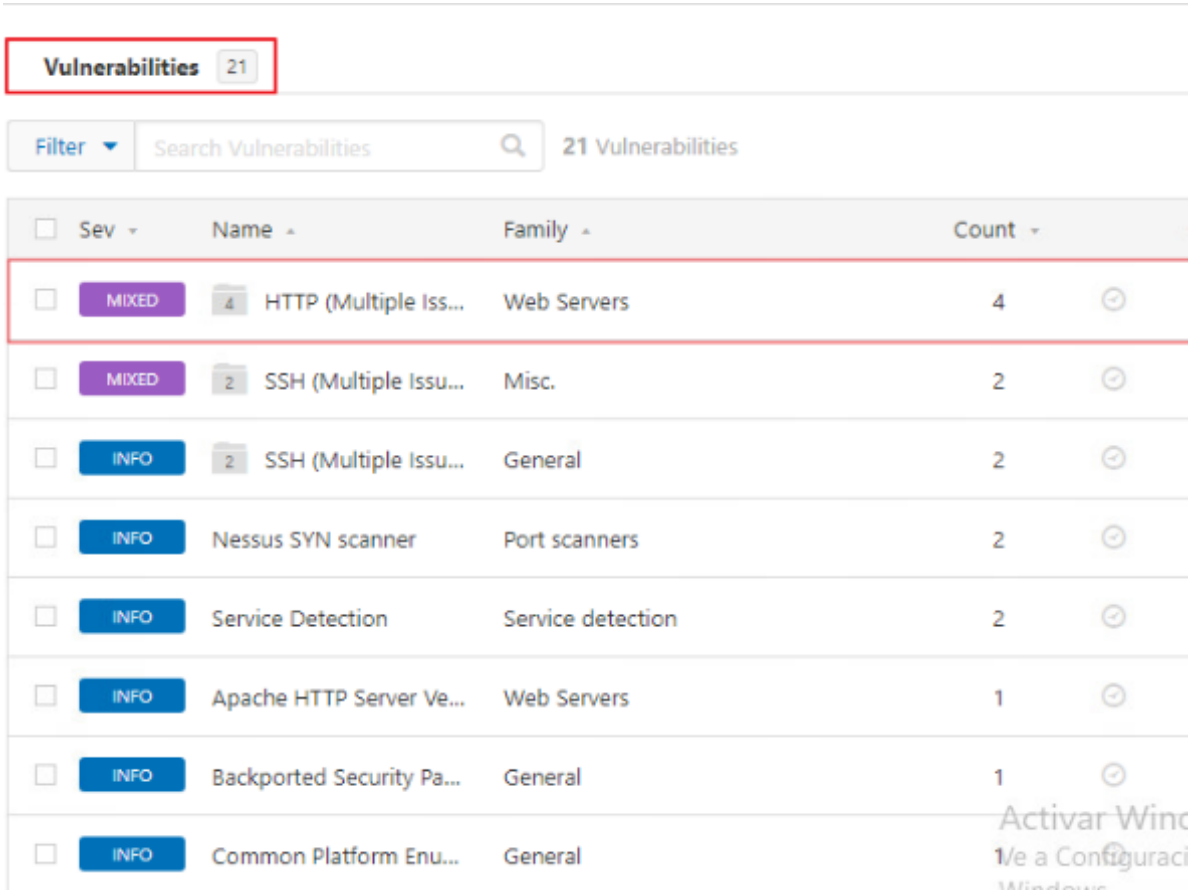
Se observa un resumen de las vulnerabilidades medias.



Resumen de vulnerabilidades medias

Fuente: elaboración propia

Una vez que finaliza el escaneo del host muestra las vulnerabilidades más relevantes, se estudió las vulnerabilidades de HTTP o SSH.



Resultados del Analisis de Vulnerabilidades

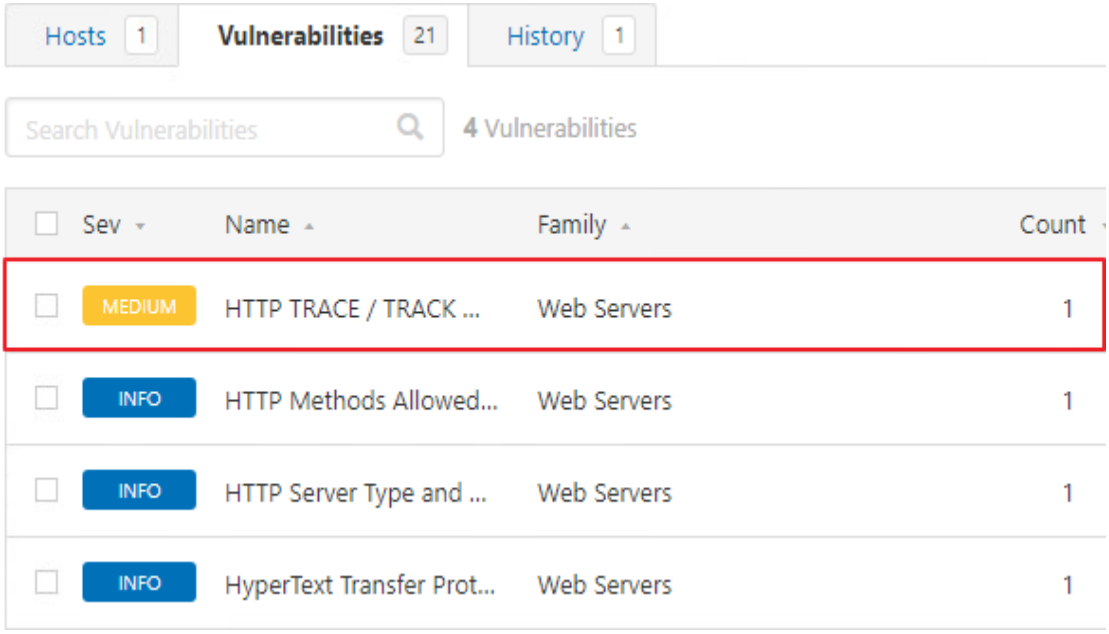
Fuente: elaboración propia

Para esta ocasión, se indago con mayor detalle la vulnerabilidad de rastreo HTTP / TRACK.

Descripción:

El servidor web remoto soporta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que utilizan para depurar las conexiones del servidor web.

Nessus es un escáner de vulnerabilidades que aparte de encontrar las vulnerabilidades presenta la solución:



Seguimiento de vulnerabilidad en HTTP

Fuente: elaboración propia

Solución:

Deshabilite estos métodos de HTTP. Consulte la salida del plugin para obtener más información.

Links de información para la solución:

- https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
- http://www.apacheweek.com/issues/03-01-24
- https://download.oracle.com/sunalerts/1000718.1.html

Explotación/Ataque: Una vez que el atacante identifica los puertos y servicios de las publicaciones a utilizar, cualquier herramienta de hacking y utilizarlas contra una aplicación o sistema vulnerable, normalmente utilizan un kit de explotación como lo es Metasploit.

Para realizar una explotación exitosa al cibercriminal le toma semanas e inclusos meses para estudiar sus objetivos y encontrar un punto de entrada inicial en la organización.

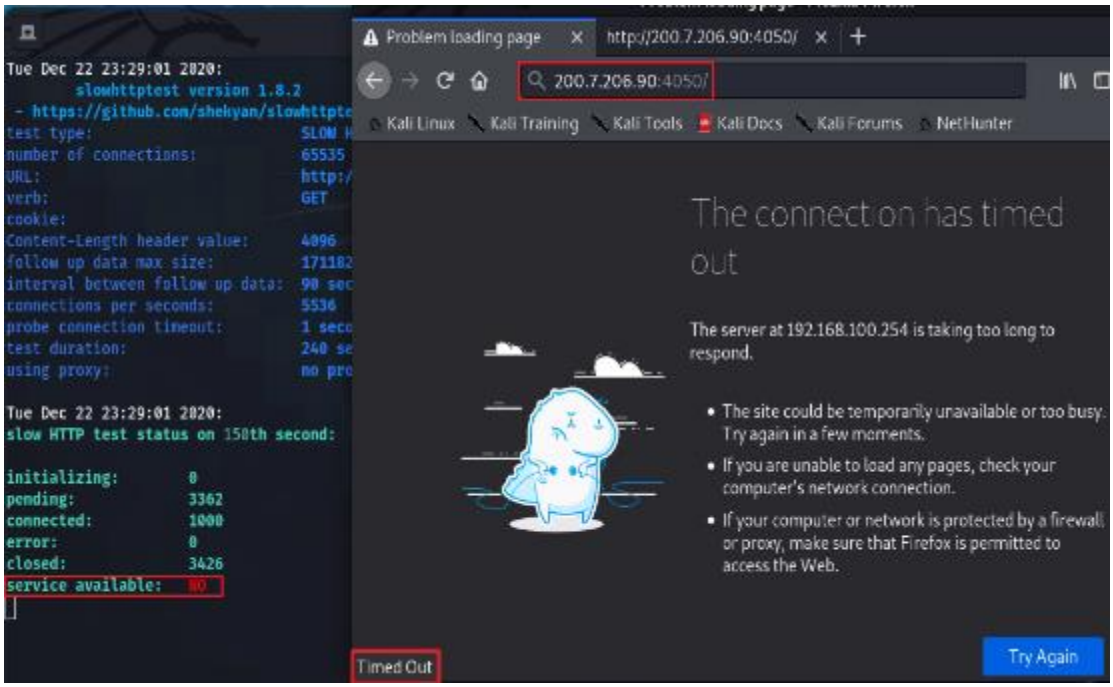
Para esta fase, se utilizó el framework de Metasploit:

Herramienta Metasploit

Fuente: elaboración propia

Al tratarse de un servicio web con una versión actual estable: 2.4.46 no se encontraron vulnerabilidades criticas ni altas solo, se identificaron vulnerabilidades medias.

Se ejecutó un ataque DoS para afectar a la disponibilidad del sitio web y dejarlo fuera de servicio, así logran así afectar un pilar importante de la triada de la seguridad.



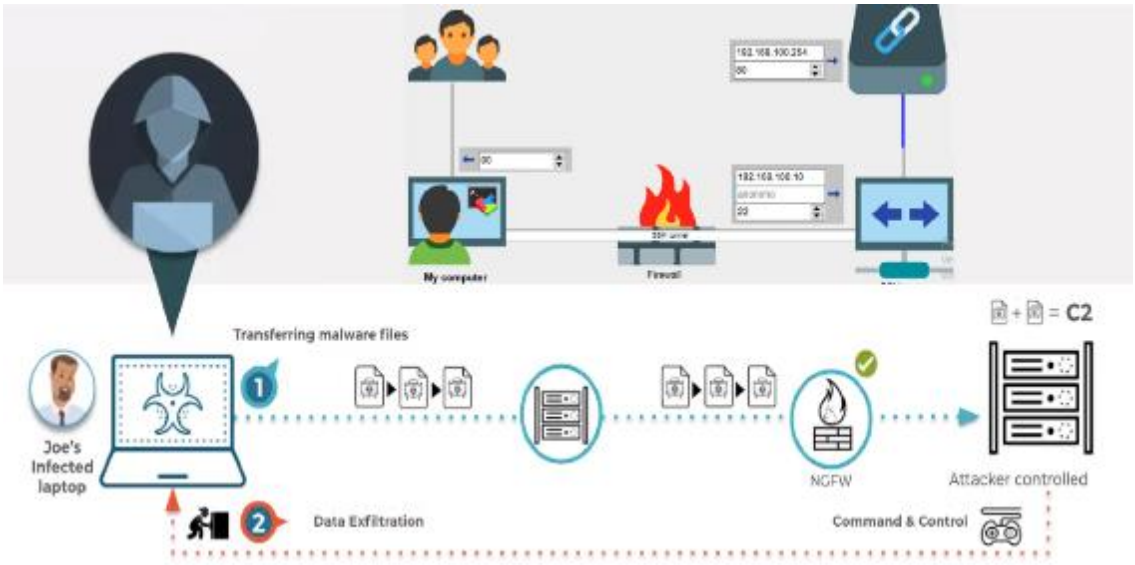
Sitio inaccesible por ataque DoS

Fuente: elaboración propia

Robo de Información: El SSH Tunneling es un vector de ataque aprovecha las configuraciones por defecto que dejan los administradores de los *Firewalls* para robar información confidencial e importante de la organización.

Con ssh Tunneling, se estableció una conexión a una tercera máquina la cual no tiene acceso por reglas de *Firewall*, una vez que nuestra maquina establezca una conexión por

ssh al equipo que tiene permisos de allí, se accede al túnel el cual estableció previamente entre la maquina destino y la tercera máquina.



Exfiltración de Datos por ssh tunneling

Fuente: elaboración propia