UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL DE NUEVA GENERACIÓN USANDO HERRAMIENTAS DE CÓDIGO ABIERTO PARA EL INSTITUTO SUPERIOR TECNOLÓGICO LIBERTAD

Trabajo de titulación previo a la obtención del

Título de Ingeniero de Sistemas

AUTOR: **DIEGO OMAR ESPIN CORRALES**

TUTOR: **JOSÉ LUIS AGUAYO MORALES**

Quito – Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Diego Omar Espin Corrales con documento de identificación Nº 1714743000; manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 01 de agosto del año 2022

Atentamente,

Diego Omar Espin Corrales

1714743000

CERTIFICADO DE SESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Diego Omar Espin Corrales con documento de identificación Nº 1714743000, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Diseño e Implementación de un firewall de nueva generación usando herramientas de código abierto para el Instituto Superior Tecnológico Libertad", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la universidad Politécnica Salesiana quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana

Quito, 01 de agosto del año 2022

Atentamente,

Diego Omar Espin Corrales

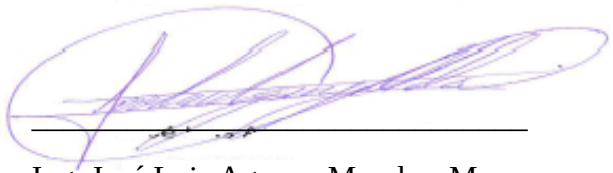
1714743000

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, José Luis Aguayo Morales con documento de identificación No 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL DE NUEVA GENERACIÓN USANDO HERRAMIENTAS DE CÓDIGO ABIERTO PARA EL INSTITUTO SUPERIOR TECNOLÓGICO LIBERTAD, realizado por Diego Omar Espin Corrales con documento de identificación No 1714743000, obteniendo como resultado final el trabajo de titulación bajo la opción Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 01 de agosto del año 2022

Atentamente,



Ing. José Luis Aguayo Morales, Msc

1709562597

DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL DE NUEVA GENERACIÓN USANDO HERRAMIENTAS DE CÓDIGO ABIERTO PARA EL INSTITUTO SUPERIOR TECNOLÓGICO LIBERTAD

DESIGN AND IMPLEMENTATION OF A NEXT-GENERATION FIREWALL USING OPEN-SOURCE TOOLS FOR THE INSTITUTO SUPERIOR TECNOLOGICO LIBERTAD

Diego Espin[1]

Resumen

El diseño del firewall de nueva generación (NGFW) en un ambiente de pruebas para la institución tiene como finalidad asegurar los recursos presentes en su red ante posibles ataques e intrusiones.

Para conseguirlo, se analizó el estado de la infraestructura identificando los posibles riegos a los que esta estaba expuesta, se propuso un nuevo diseño de red debido a las deficiencias que presentaba el actual también, se identificó los activos a los cuales se pretendía asegurar y proteger ante posibles ataques.

Para el diseño del NGFW, se empleó un servidor sobre el cual se virtualizó ambientes de pruebas utilizando herramientas open source como: pfsense, zentyal, proxmox, opnsense, estas fueron configuradas de manera que ayudan a controlar los accesos a los recursos de red y monitoreo del tráfico para identificar posibles comportamientos no deseados también se establecieron perfiles de navegación y reglas de filtrado de contenido.

Los cambios ayudaron a mejorar el rendimiento de la red institucional obteniendo mejores tiempos de respuesta en la transmisión de datos, se pudo garantizar el acceso a recursos compartidos como impresoras, unidades de red, scanners a todo momento sin perjudicar la productividad del personal, hubo una mejora en los accesos a recursos en internet gracias a la optimización del uso del ancho de banda debido a las políticas y perfiles de navegación configuradas en el NGFW.

Pese a la implementación de las soluciones de seguridad sean de pago o gratuitas, es necesario educar a los usuarios para que estén alertas y tomen precauciones para evitar ser víctimas de phishing, programas malignos y ransomware, los cuales son los principales causantes de brechas de seguridad.

Palabras clave, Seguridad de red, Ciberataques, NGFW.

Abstract

The design of the new generation firewall solution (NGFW) in a test environment developed for the institution aims to secure the resources present in its network against possible attacks and intrusions.

To achieve this, the state of the technological infrastructure was analyzed, identifying the possible risks to which it was exposed, in this process a new network design was proposed due to the deficiencies of the current one, in addition to identifying the sensitive assets to be secured and protected against possible attacks.

For the design of the NGFW, a server was used on which the test environments were virtualized using open-source tools such as: pfsense, zentyal, proxmox, opnsense, these were configured to help us control access to network resources and traffic monitoring to identify possible unwanted behavior, navigation profiles and content filtering rules were also established.

These changes helped to improve the performance of the institutional network by obtaining better response times in data transmission, it was possible to guarantee access to shared resources such as printers, network drives, scanners always without affecting staff productivity, there was an improvement in access to Internet resources thanks to the optimization of bandwidth use due to the policies and browsing profiles configured in the NGFW.

Despite the implementation of security solutions, whether paid or free, it is necessary to educate users to be alert and take precautions to avoid becoming victims of phishing, malware, ransomware, which are the main causes of security breaches.

Keywords, network security, cyberattacks, NGFW.

[1] Estudiante de Ingeniería en Sistemas – Universidad Politécnica Salesiana, Egresado – UPS – sede Quito.

1. Introducción

El adelanto en la tecnología y la automatización de los procesos de negocio dentro de las organizaciones, han sido de gran ayuda para la consecución de varios objetivos comerciales y estratégicos en esta era moderna, el aprovechamiento y explotación de las comunicaciones a través de los sistemas de información publicados en la red permiten la colaboración entre similares dando prestaciones de servicios a nivel global y al alcance de todos ayudando en la consecución de sus objetivos comerciales en menor tiempo y con mayor efectividad (Ibujés Villacís & Benavides Pazmiño, 2018).

El aumento de ciberataques en los últimos años a nivel mundial ha sido un detonante para que las organizaciones implementen mecanismos para proteger sus datos que comparten a través de internet buscando herramientas capaces de protegerlas, estas herramientas deben ser capaces de permitir un constante monitoreo sobre el tráfico generado en la su red o donde tiene desplegados los servicios que prestan, controlar los comportamientos inusuales, presencia de código malicioso, accesos indebidos y cualquier rasgo de tráfico o acción no seguros. (Morales Rojas, 2022).

A medida que estos ataques se vuelven más comunes, las organizaciones han tenido que hacer fuertes inversiones para obtener una o varias soluciones integrales de seguridad, pero, por otro lado, existen otras opciones que pueden ayudar a las organizaciones pequeñas para que implementen también soluciones basadas en software y hardware y a costes bajos, estas pueden ayudar a establecer medidas de prevención para los ataques más comunes.

Las instituciones educativas, estas no están exentas a los diferentes ataques en el ciberespacio, en 2020 la Agencia de Ciberseguridad e Infraestructura CISA, el FBI y MS-ISAC han señalado que existe un incremento considerable de ataques que han afectado a instituciones de educación básica y media, la gran mayoría de estos orientados al robo o secuestro de información (ransomware y malware) y otros a la interrupción de las herramientas usadas para impartir clases en línea (DDoS). Si bien este estudio se lo efectuó en EE. UU., no se descarta que este tipo de comportamientos se extienda a otras regiones debido a la globalización de los servicios y accesos a internet (Harán, 2020).

De acuerdo con (Sophos, 2021), empresa especializada en hardware de seguridad, efectuó una encuesta alrededor de 5400 responsables de TI a nivel mundial, entre estos aproximadamente el 11% pertenecía a instituciones del sector educativo, estos profesionales provenían de regiones como: América, Europa, África - Oriente Medio y Asia. De acuerdo con los resultados de la encuesta, se concluyó que en el último año, el 44% de las instituciones educativas sufrieron afectaciones debido a ransomware, el 58% de las instituciones afectadas afirmaron que su información fue secuestrada o encriptada, 35% de estas instituciones accedió a las exigencias económicas por parte de los ciberdelincuentes desembolsando un promedio de $113000 pero, pese al pago del "rescate" de la información aproximadamente el 32% de esa información comprometida quedó inaccesible, la inversión total que este sector desembolsó para la rectificación de este tipo de ataques fue la cifra mas alta de los sectores que formaron parte de la encuesta y supero los 2 millones de dólares.

De aquí la importancia de asegurar la información, proponer planes y herramientas que permitan mitigar cualquier tipo de amenazas sobre las redes de datos, plantear políticas de seguridad en las diferentes organizaciones, hacer participe de estas a los usuarios para que tengan conocimiento de las

amenazas a las que se enfrentan y no sean víctimas de los diferentes ataques todo con el objetivo de mantener a salvo los datos y proteger los servicios que ofertan.

La solución firewall propuesta para la institución a más de las funciones de análisis de tráfico y bloqueo de puertos, será capaz de identificar el tipo de tráfico generado por las aplicaciones, lo que le caracteriza y es una de las ventajas que ofrece un firewall de nueva generación.

El diseño de esta solución es a través del uso de herramientas open-source o gratuito, así la institución no tendrá que destinar un presupuesto enorme para su despliegue a futuro.

2. Métodos y Materiales

2.1. Materiales

Hardware: La institución dispone de dos servidores en los cuales se instalarán las herramientas necesarias para controlar la red institucional y otro en el cual se crearon los ambientes de pruebas donde vamos a diseñar el NGFW.

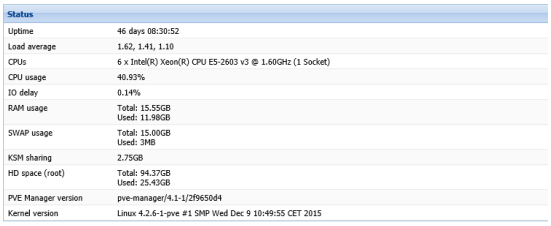


Figura 1. Servidor para gestión de red (Principal):

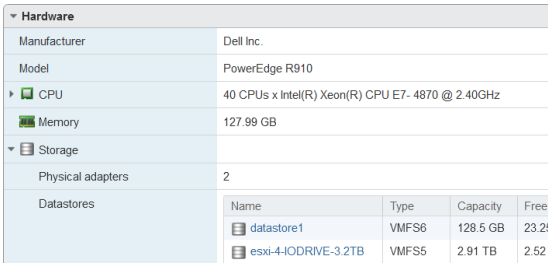


Figura 2. Servidor para ambientes de pruebas:

Software: de acuerdo con la propuesta se evaluaron varias herramientas open source, de las cuales se seleccionaron:

VMware ESXI v6.7: con un licenciamiento gratuito el cual fue utilizado para crear las máquinas virtuales que proporcionaron el ambiente de pruebas.

PROXMOX: sistema operativo similar a ESXI open source para virtualizar los ambientes para la gestión de red.

Zentyal v4.0: distribución Linux basada en Debian que hace la función de enrutamiento y firewall perimetral.

OPNSense v21.7: distribución de Linux basada en FreeBSD que presta funciones de enrutamiento gestión de redes y firewall perimetral.

PfSense v2: también basada en FreeBSD con funciones de enrutamiento y firewall perimetral.

Snort: sistema de detección y prevención de intrusiones.

OpenVPN: servicio para conexiones VPN.

Portal Cautivo: módulo adicional para opnsense para crear acceso a la red wifi a través de un portal de autenticación.

2.2. Métodos

2.2.1. Rediseño de red

El diseño de la solución para el aseguramiento de la red de datos y protección de la información de la institución surgió a partir del incremento de ciberataques a las distintas organizaciones y en especial al sector educativo (Harán, 2020).

Se procedió con un levantamiento de toda la información referente a la infraestructura tecnológica de la institución en donde surgieron necesidades urgentes, previas a la preparación de los ambientes de pruebas para el diseño del NGFW, una de estas y muy importante fue el rediseño de la red a través de una segmentación de la misma,

aprovechando las ventajas que ofrece esta práctica ayudó a solventar las constantes perdidas de conectividad, congestión de red y el bajo rendimiento en general que se presentaba constantemente en la institución.

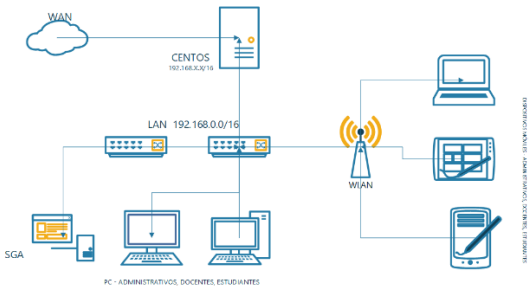


Figura 3. Diagrama de red inicial

El nuevo diseño de red además de cumplir con lo antes mencionado brinda un nivel inicial de seguridad pues ayuda a controlar los accesos a las diferentes VLANS y por ende a los recursos compartidos, también aporta características como: funcionalidad, escalabilidad, adaptabilidad y administración correcta de todos los activos.

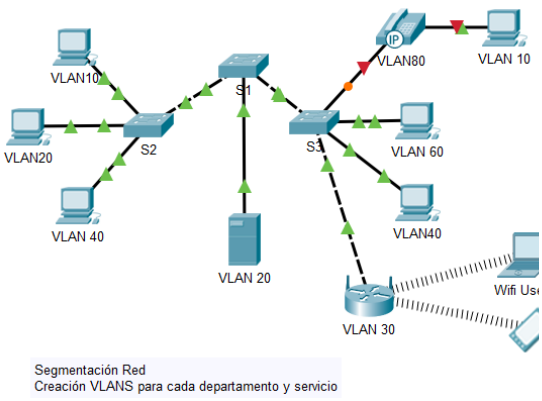


Figura 4. Diagrama de red segmentado.

Para el control de la red se cambió el sistema operativo del servidor principal (CENTOS) a PROXMOX en el cual se crearon dos máquinas virtuales una con Zentyal el cual estaba destinado a reemplazar las funciones de un enrutador y a su vez como firewall perimetral.

En este se configuraron todas las interfaces de red de acuerdo con el nuevo diseño, un servidor DNS para los aplicativos alojados localmente, objetos los cuales representan a uno o varios elementos de red facilitando la gestión al momento de configurar la red, también se creó reglas básicas para poder compartir y bloquear el acceso a los diferentes recursos compartidos.

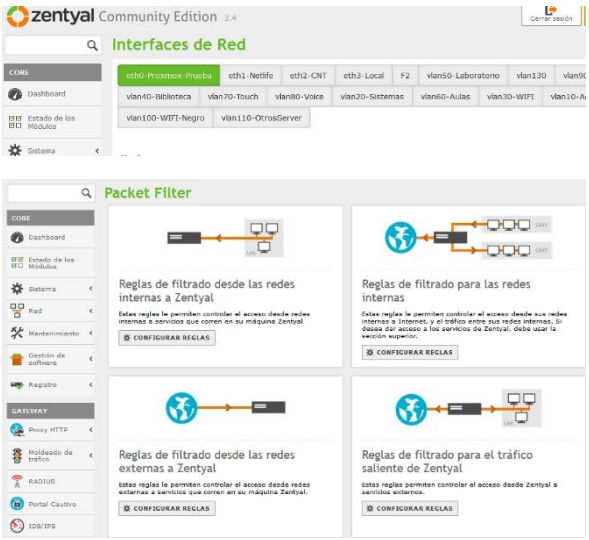


Figura 5. Servidor Zentyal, Router y Gestión de red

Adicional se configuro un balanceo de carga para prevenir un posible fallo de uno de los ISP o a su vez redirigir cierto tráfico para que tenga salida por una de las interfaces WAN y no saturar el ancho de banda.

Figura 6. Balanceo de carga en Zentyal

2.2.2. Ambiente de pruebas

Con el segundo servidor (DELL Power Edge R910), se procedió a crear los ambientes de pruebas preparando máquinas virtuales necesarias, para probar cada funcionalidad del NGFW.

Se usaron varias maquina virtuales con el S.O. PfSense en donde se configuró los módulos de IDP/IPS, filtrado Web, VPN, Portal Cautivo, también se creó una máquina virtual que serviría como cliente de nuestra red con S.O. Windows 10.

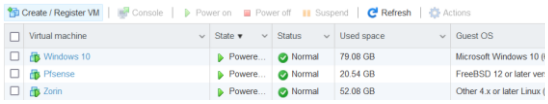


Figura 7. Maquinas virtuales para el diseño de NGFW

En PfSense, se configuró un acceso VPN mediante el servicio de OpenVPN para poder usar recursos de la sede matriz en las otras sedes y viceversa, adicional para acceder de manera segura y controlada a la red institucional y mantener controlada y monitoreada esa conexión.

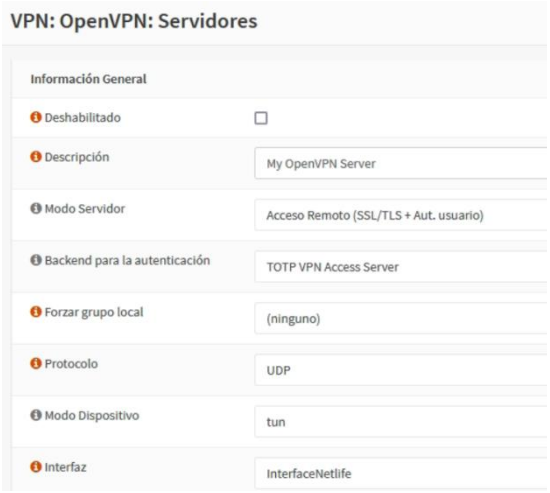


Figura 8. Configuración del servicio VPN

Se creo un portal cautivo para autenticar a los dispositivos y usuarios que se conectan a la red Wi-Fi de estudiantes e invitados asignado una cuota de tiempo para que pueda hacer uso del servicio.

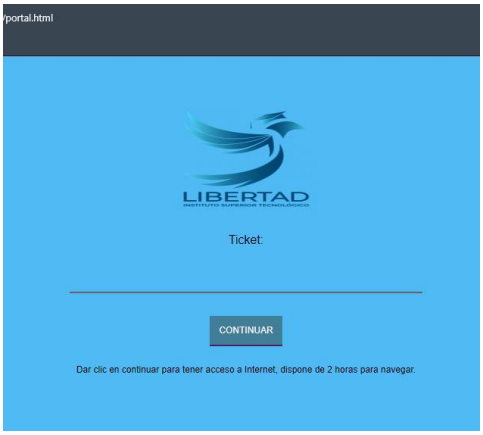


Figura 9. Portal para autenticación de usuarios Wifi a través de un TOKEN

Para el módulo de detección y prevención de intrusiones IDS/IPS, se utilizó SNORT que es una herramienta de código abierto desarrollada para monitorear el tráfico de red en tiempo real, una de las funciones de SNORT es censar todos los paquetes que son transportados por la red y verificar su comportamiento de manera que si actúan de manera inapropiada o no acorde a su algoritmo presente en las definiciones de SNORT este alerta al administrador de red mediante mensajes en su interfaz de monitoreo y dependiendo de las reglas que se han configurado puede bloquear el tráfico de estos paquetes.

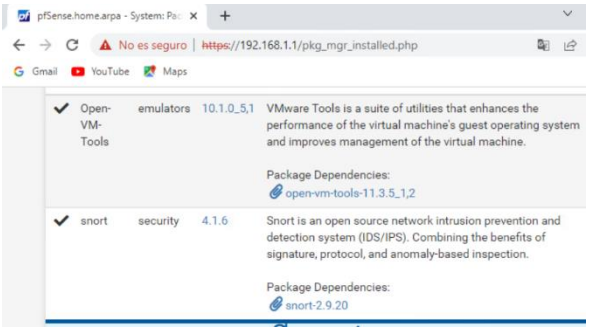


Figura 10. Instalación de paquete SNORT

Una de las principales ventajas de SNORT es que se puede analizar el tráfico en la capa 7 (Aplicación) del modelo OSI, identificando contenido web o tráfico que generan las diferentes aplicaciones o programas en un equipo esto gracias a OpenAppID de cisco.

Para configurar SNORT, se debe descargar las reglas de filtrado predefinidas y gratuitas disponibles para la comunidad, el único requisito es registrarse de manera gratuita en su portal, generando para cada usuario un código OinkMaster el cual se debe registrar en el módulo de SNORT.

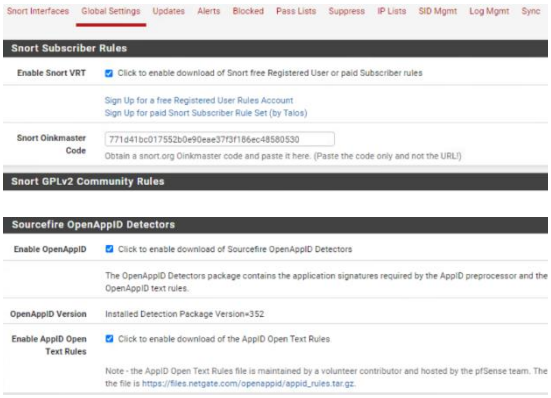


Figura 11. Configuración OinkMaster, para uso de definiciones de distribución libre

Una vez configurado el código se debe habilitar la descarga de las reglas gratuitas y en el caso de este ambiente las que corresponden a OpenAppID.

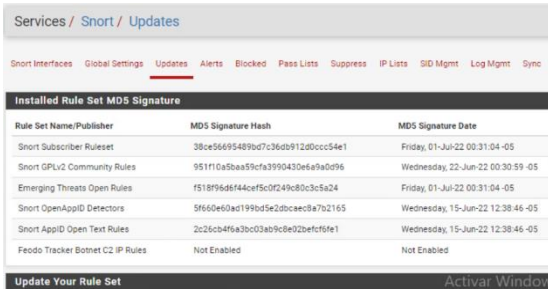


Figura 12. Habilitación de descargas de actualizaciones de definiciones y reglas

Luego se configuran las interfaces que van a ser censadas con SNORT por cada interface se crea una instancia de manera que a cada interfaz le podemos configurar reglas diferentes.

Figura 13. Configuración de interfaces a ser monitoreadas

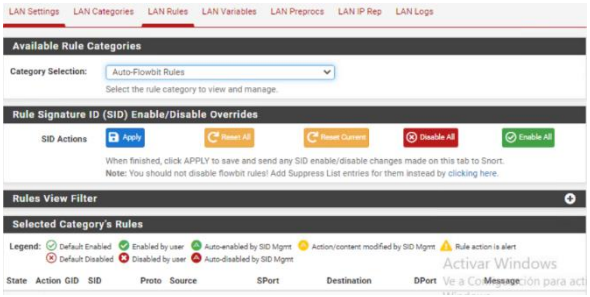


Figura 14. Creación de reglas de filtrado SNORT

Una vez que se a configurado todas las interfaces se define las reglas de filtrado permitiendo al sistema el análisis e identificación los paquetes de la red y tomar las acciones definidas para cada aplicación o contenido.

SNORT es una capa adicional de seguridad que podemos añadir a pfsense,

Para una mejor administración, debemos documentar todos los cambios y reglas que vamos incluyendo

3. Resultados

Con el rediseño de red y la implementación del servidor Zentyal para gestionar y monitorear la red mejoró la velocidad de conexión entre los diferentes dispositivos interconectados.

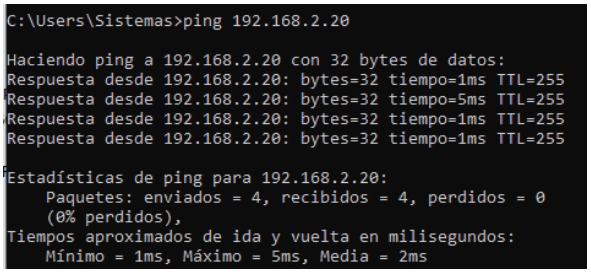


Figura 15. Pruebas de conexiones LAN, posterior al rediseño de red

Antes de esto existía la problemática de que muchos usuarios accedían a la red institucional sin el debido control, ocasionando una saturación e intermitencias,

los tiempos de respuesta eran elevados como se puede constatar en la siguiente figura:

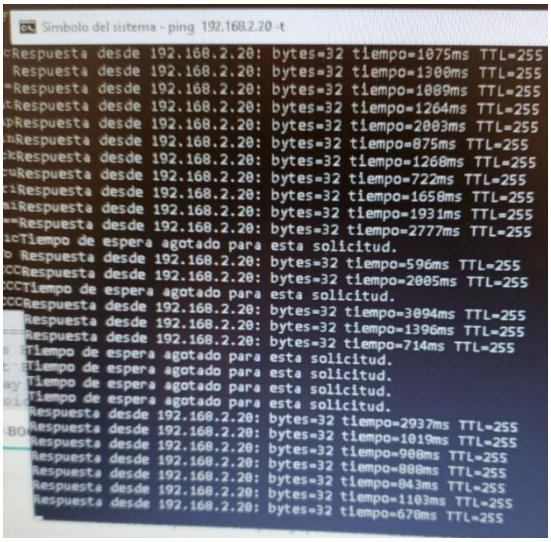


Figura 16. Pruebas de conexiones LAN, posterior al rediseño de red

Con la ayuda de las políticas de navegación en Zentyal, OPNSense, PfSense y reglas en definidas en SNORT, se puden crear perfiles de navegación para cada interfaz o VLAN creadas en el diseño de red permitiendo optimizar y aprovechar el uso del ancho de banda en la institución.

Inicialmente solo con el rediseño de red se empezó a ver resultados como este:

Medida de velocidad de AB antes del rediseño de red, no se tenía control de los dispositivos que accedían a la red, tampoco se controlaba el acceso a internet por parte de los usuarios.

Figura 17. Medición de AB inicial

Medición luego del rediseño de red, en este punto ya se tiene lista segmentación de la red adicional con la ayuda de PfSense se implementó un portal cautivo para controlar y autenticar usuarios en las conexiones WiFi:

Figura 18. Medición de AB luego de segmentación

Medición creando reglas en SNORT para bloqueo de aplicaciones como Streaming, Redes Sociales y otro contenido no necesario:

Figura 19. Medición de AB, aplicando políticas de filtrado web

Como se puede notar, la solución planteada para la institución ha sido de gran ayuda para la optimización de la red y posterior aseguramiento de la misma.

Adicional podemos constatar en los servidores instalados el estado y consumo de recursos.

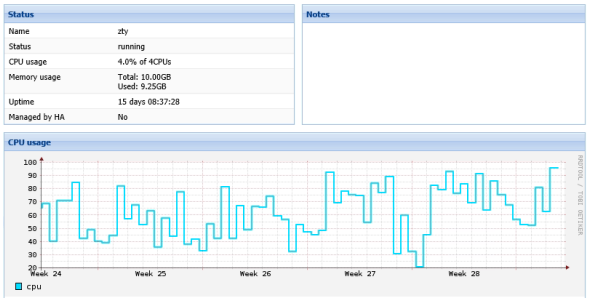


Figura 20. Monitoreo de recursos servidor principal

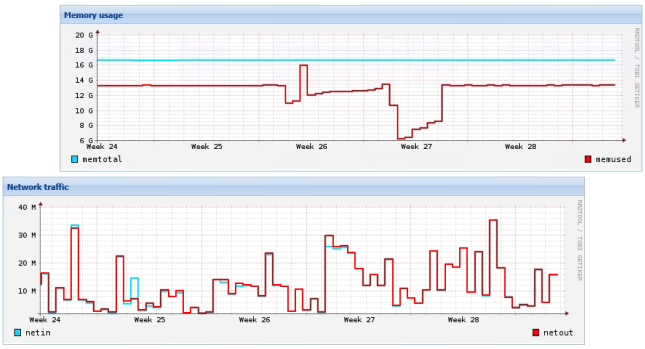


Figura 21. Estadísticas de uso de AB total

4. Discusión

Con la segmentación de la red se logró una mejor administración de los recursos proporcionando conexiones mucho más rápidas y acceso a recursos compartidos para optimizar tiempos y mejorar la productividad del personal.

La protección de activos en donde se alojan los servicios a los que accede la comunidad que conforma la institución, así como su información tienen un gran valor no solo económico sino sustancial para la institución y su funcionamiento.

La socialización de los cambios efectuados y los informes detallados de todo lo que se ha desarrollado con este proyecto se entregó a la dirección de información y tecnologías de la institución.

Como parte del aseguramiento de activos se propuso desplegar en el parque tecnológico un listado de buenas prácticas para seguridad informática:

a) Contraseñas seguras
b) Software Legal y actualizado
c) Proveer de Antivirus a los equipos.
d) Establecer un cronograma de copias de seguridad de las BDD.
e) Filtrado de contenido, de acuerdo con las funciones de cada área
f) Campañas se socialización a usuarios para evitar ataques de phishing y malware.

5. Conclusiones

Para implementar soluciones de seguridad dentro de una institución, es de suma importancia identificar el nivel de criticidad de los activos que interactúan en la red así, establecer diferentes capas de aseguramiento de estos.

La segmentación de una red es primordial dentro de las organizaciones, a través de esta se transportan grandes cantidades de datos y ayuda en temas de seguridad para evitar que una amenaza que se haya introducida dentro de una institución no se propague sobre toda su red, aislando ese segmento y protegiendo a los demás.

El presente trabajo expuso algunas herramientas de software libre disponibles para diseñar una solución de protección de las redes institucionales, sin embargo, el despliegue de estas requiere de gran esfuerzo del personal a cargo debido a la falta de soporte directo que se lo debe encontrar en las comunidades del ciberespacio.

Aunque muchas organizaciones invierten fuertes sumas de dinero en equipamiento y personal técnico calificado, no están exentas de ataques, esto se debe en gran parte al comportamiento de los usuarios; en el manejo que dan a recursos de red y el acceso a la información de internet, muchos de los ataques más comunes son de phishing y malware, los cuales pueden ser originados por un usuario final o un cliente que abrió un correo o un menaje a través de una red social. Muchas de las empresas efectúan pruebas de phishing con sus empleados y aún existe una gran cantidad de estos que siguen cayendo en esta "trampa".

6. Referencias

Harán, J. M. (12 de 11 de 2020). *Advierten sobre el crecimiento de ciberataques a instituciones de educación inicial y primaria.* Obtenido de welivesecurity.com: https://www.welivesecurity.com/la-es/2020/12/11/advierten-crecimiento-ciberataques-apuntan-instituciones-educacion-inicial-primaria/

Ibujés Villacís, J. M., & Benavides Pazmiño, M. A. (2018). Contribución de la tecnología a la productividad de las pymes de la industria textil en Ecuador. *Cuadernos de Economía*, 140-150.

Jiménez Alegria, L. C. (2016). Implementación de un sistema de Seguridad (IDS/IPS) Open Source basado en Raspberry para Red del Ministerio Público Sede Puno.

Luvezute Kripka, R. M. (2015). La investigación documental sobre la investigación cualitativa : conceptos y caracterización. *Revista De Investigaciones UNAD*, 55–73.

Martin Roesch. (25 de 02 de 2014). *https://blogs.cisco.com.* Obtenido de Cisco Announces OpenAppID – the Next Open Source 'Game Changer' in Cybersecurity: https://blogs.cisco.com/security/cisco-announces-openappid-the-next-open-source-game-changer-in-cybersecurity

Morales Rojas, J. G. (2022). *Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial, Tesis de Licenciatura.* Bogotá: Universidad piloto de Colombia.

Sophos. (2021). *El estado del ransomware en el sector educativo 2021.* Monográficos de Sophos.