UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

REPORTE FINAL DE ESTADÍA

Estefhany Hernández Ortiz

Implementación y configuración de una red perimetral

EDUCACIÓN SECRETARÍA DE EDUCACIÓN PÚBLICA · UTP COORDINACIÓN GENERAL DE UNIVERSIDADES TECNOLÓGICAS Y POLITÉCNICAS · VERACRUZ GOBIERNO DEL ESTADO · SEV Secretaría de Educación · DET Dirección de Educación Tecnológica del Estado de Veracruz · SEMSyS Subsecretaría de Educación Media Superior y Superior

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

Ingeniería en Redes Inteligentes y Ciberseguridad

Implementación y configuración de una red perimetral

REPORTE FINAL DE ESTADÍA

QUE PARA OBTENER EL GRADO ACADÉMICO DE

INGENIERA EN REDES INTELIGENTES Y CIBERSEGURIDAD

Estefhany Hernández Ortiz

ASESOR ACADÉMICO: DR. LUIS ROLANDO GUARNEROS NOLASCO

ASESOR INDUSTRIAL: LIC. RUPERTO PERALTA DURÁN

CUITLÁHUAC, VER. ABRIL, 2023

ÍNDICE:

Contenido

ÍNDICE DE TABLAS

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

ÍNDICE DE IMÁGENES

Capítulo I Estado del arte

1.1 Introducción

Actualmente, se han presentado una variedad de cambios en el ámbito tecnológico a causa de las necesidades presentadas en las arquitecturas de redes, es decir, las redes internas o empresariales, ya que las organizaciones e instituciones pretenden alcanzar un nivel de seguridad y privacidad sobre sus activos relevantes.

En consecuencia, en el presente trabajo se hace mención a la implementación de una red perimetral (zona desmilitarizada), el cual, hace referencia a un método de defensa o escudo de protección sobre la información (recursos y servicios) de las redes informáticas que son vulnerables a diversos ataques. En otras palabras, este método es una segmentación de la información pública que es accesible desde el exterior, y de la información privada que debe permanecer inaccesible a las redes externas, como es internet.

En este documento, se comprenderá la importancia de la seguridad perimetral en una red de datos, ya que es considerada un factor crítico para incrementar la seguridad y protección sobre la información importante.

1.2 Glosario

1.2.1 DMZ (Zona Desmilitarizada)

Es una zona que se sitúa entre la red interna y las externas, como es la internet, permite las consultas de usuarios en redes externas a los servidores, así como, de servidores hacia la red interna, pero niega las conexiones salientes de la DMZ hacia cualquier otra red que no sea la interna. [2, p.29]

1.2.2 Firewall (Cortafuegos)

Se trata de un sistema encargado de ejecutar reglas como contramedidas ante ataques e intrusiones en la red, además, de ser el responsable de supervisar los paquetes (entrada o descarte), es decir, filtrado de paquetes de datos. Evita que usuarios no autorizados accedan a redes privadas bloqueándolas y negándoles el acceso. Un aspecto importante de los firewalls es, que están configurados para al menos filtrar las comunicaciones según el puerto utilizado. [1, p.23-25]

1.2.3 Router

También conocido como encaminador, este tipo de dispositivo se encarga de controlar el tráfico, para establecer la comunicación entre redes al nivel 3 (capa de red) del modelo OSI. [4, p.17]

1.2.4 Redes LAN (Red de Área Local)

Este tipo de diseño de redes se basa en su área geográfica, generalmente son varios equipos interconectados en entornos pequeños y limitados, por ejemplo, en el hogar, oficinas o edificios. La administración de este tipo de red para conservar un buen funcionamiento, resulta sencillo, es decir, no es demandante. [3, p. 38]

1.2.5 TCP/IP

Protocolo de Control de Transmisión/Protocolo de Internet. Sistema que permite el uso de Telnet, FTP, correo electrónico y otros dispositivos informáticos que no están en la misma red. [1, p.17]

1.2.6 ICMP (Protocolo de mensajes de control de Internet)

Su función es controlar el flujo de comunicación, así como manifestar los errores. [1, p.19]

1.2.7 IPv4

Protocolo de Internet Versión 4. Sirve para identificar a cada máquina dentro de la red.

1.2.8 IDS (Sistema de Detección de Intrusos)

Mecanismo capaz de alertar/informar el tráfico existente en la red, con el propósito de minimizar los peligros que atenten contra la información relevante que comprometa la seguridad de la compañía. [6, p.88]

1.2.9 IPS (Sistema de Prevención de Intrusos)

Establece un conjunto de reglas para determinar posibles amenazas informáticas, generando una alarma para interceptar el tráfico entrante, bloquearlo o descartarlo. [7, p.11]

1.2.10 Suricata

Es un software bajo plataforma Open Source que funciona como IDS/IPS, es la evolución de snort.

1.2.11 VPN (Red Privada Virtual)

Es una arquitectura que permite conectarse a un lugar remoto por medio de una red pública que generalmente es internet. Genera un canal cifrado por donde se transmiten los paquetes, conservando de esa forma, la confidencialidad e integridad de los datos.

1.2.12 OpenVPN

Es una herramienta Open Source que se utiliza para generar VPN. Esta aplicación crea un túnel de conexión punto a punto y con cifrado TLS. También utiliza claves privadas, certificado, etc. para realizar la autenticación en las conexiones. [9, p. 40]

1.2.13 PPPoE (Protocolo Punto a Punto sobre Ethernet)

Protocolo de red utilizado por los ISP que establece una conexión de capa 2, para que los usuarios puedan ingresar a internet por una base local. [4, p.21]

1.2.14 Open Source (Código Abierto)

Software enfocado en la colaboración o liberación de su código fuente para que pueda ser modificado sin restricciones de licencia. [3, p.58]

1.2.15 NAT (Traducción de Dirección de Red)

Estándar que ayuda a realizar traducciones de una o más direcciones IP privadas a públicas para conectar equipos de la red interna hacia una red externa (especialmente internet). [2, p.34]

1.2.16 FreeBSD

Es un sistema operativo avanzado para arquitecturas x86 y amd64 compatibles. Es utilizado para alimentar servidores modernos, escritorios y plataformas embebidas. [2, p.34]

1.2.17 PFSense

Software de código abierto perteneciente a FreeBSD, fue diseñada con el objetivo de implementarse como firewall y enrutador, es administrable desde una interfaz web. [2, p.22]

1.2.18 ACL (Listas de Control de Acceso)

Son un conjunto de reglas que filtran el tráfico entrante o saliente a las interfaces específicas, se basan en las direcciones de origen y de destino, así determinan, si el tráfico es bloqueado o se permite su transmisión a las interfaces del switch. [13, p.19]

1.3 Proyectos exitosos similares

1.3.1 Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo

Este proyecto tiene como objetivo incrementar la seguridad de los servicios académicos en la red telemática de la Universidad Nacional Pedro Ruiz Gallo. [2, p.11]

La naturaleza principalmente es de las telecomunicaciones y se justifica por las siguientes razones: Al implementar un firewall en la gestión de la seguridad perimetral de la red telemática, es necesario considerar como parte de su gestión, los riesgos en el cual se les exige obligatoriamente implementar sistemas que gestionen la seguridad de la información, para mitigar los riesgos operativos asociados a las tecnologías y la continuidad de la gestión de la seguridad perimetral. [2, p.12]

La metodología utilizada en esta investigación es el método cualitativo con su respectiva técnica de investigación que es la entrevista y con las diferentes referencias bibliográficas se intenta obtener información importante que ayude a definir de una manera más clara el proyecto, y la metodología de la investigación a utilizar, es la deductiva.

Tras haber cumplido con el objetivo, se obtienen los siguientes resultados:

- Se detectó la existencia de ataques a cada uno de los 7 servicios que ofrece la red telemática.
- Se implementó y configuró el sistema pfSense para la gestión de la seguridad perimetral.
- Se minimizaron las vulnerabilidades en la red y el servicio de sistema académico.

Afirmando así que la implementación de una zona desmilitarizada aumentó la seguridad perimetral dentro de la red telemática de la Universidad Nacional Pedro Ruiz Gallo. [2, p.41]

1.3.2 Diseño e implementación de una red de datos con seguridad perimetral para una empresa que se dedica al servicio de taxi ejecutivo.

El objetivo de este proyecto es la implementación de una red de datos escalable con equipos de seguridad perimetral que garanticen un elevado índice de protección e integridad en la red, mitigando los posibles riesgos de interconexión en la red de la compañía de taxi ejecutivo Linanfer S.A. [3, p.29]

La implementación de este proyecto es justificable porque al realizar un análisis de la red se traza como propósito obtener una red en óptimas condiciones y sobre todo comprender la importancia de salvaguardar la información de posibles ataques, ya que esta cuenta con grandes cantidades de clientes de los cuales en su mayoría pertenecen al personal de compañías e industrias con las cuales mantienen contratos. [3, p.30]

PPDIOO (Preparar, Planear, Diseñar, Implementar, Operar y Optimizar) es la metodología que será empleada en el proyecto por lo siguiente [3, p.31-33]:

- Se adapta a las necesidades presentadas en el proyecto.
- Permite realizar un firme diseño escalable de la red.
- Con esta metodología se presentarán menos errores en la fase de optimización.

Al concluir el objetivo del proyecto se obtienen los siguientes resultados [3, p.102]:

- Se logró darle un diseño jerárquico a la compañía.
- Se obtuvo una administración favorable para la compañía.

- Se consiguió aprovechar el ancho de banda de la compañía protegiendo los equipos y dispositivos de virus.
- Se ejecutaron pruebas de verificación, conexión y navegación con el servicio de internet y enlace de datos, se realizó el monitoreo de la red realizando ping y obteniendo tiempos de respuesta.

1.3.3 Diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue.

La metodología usada en esta investigación es el método cualitativo con su respectiva técnica de investigación que es la entrevista y con las diferentes referencias bibliográficas se intenta obtener información importante que ayude a definir de una manera más clara el proyecto y la metodología de la investigación a utilizar es la deductiva.

El presente trabajo tiene como objetivo diseñar un mecanismo de seguridad perimetral en la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Puebla, con base en metodologías de seguridad Open Source, con la finalidad de contribuir positivamente en la administración de los sistemas de información.

Se justifica porque las instituciones de gobierno, como lo es el H. Ayuntamiento de Tetelas de Ávilo Castillo requiere lograr una eficiente administración de sus activos físicos y lógicos que a su vez deben ser rápidos, seguros y eficientes, que ayude a obtener un sistema de seguridad, que fortalezca al máximo la seguridad de su infraestructura y disminuir los riesgos posibles a los que se enfrenta día con día.

La metodología implementada será profundizada en un estudio cuantitativo con un alcance descriptivo para llevar a cabo el proceso del proyecto. El alcance descriptivo es el más apto para el desarrollo de la investigación porque se conoce el problema, pero se busca describir fielmente cómo ocurre su magnitud y su alcance en torno al estado actual de la infraestructura de red en el H. Ayuntamiento de Tetelas.

Una vez finalizado la implementación del proyecto, se obtuvo como resultados:

- Se tiene un control más amplio en el uso diario de la información, y los usuarios tienen la capacidad de encontrar cualquier brecha adicional relacionada con la seguridad de los datos.
- Se genero un sistema robusto que mantiene la seguridad en la información, así como la mejor de la infraestructura de la red de datos y el conocimiento necesario para una correcta manipulación de los recursos tecnológicos.

1.4 Citas de proyectos similares

Tabla 1: Proyectos similares

Trabajo o investigación	**Problema**	**Contribución**	**Tecnologías**
Autor: Boris Harold Pitancur Fernández.	El crecimiento de las operaciones de la compañía Corporación Cayman S.A.C, se trasladó a un local más amplio en la zona industrial del Callao, por lo que se le propone una solución para la implementación y diseño de toda la red de datos y seguridad perimetral, bajo un sistema ERP llamado Spring.	Diseño e implementación de una red de datos y seguridad perimetral de la empresa Corporación Cayman S.A.C.	Linux Centos 6.0 IDS. VPN. DMZ.
Autores: Bach. Kenny Esleyther Ruiz Viera. Bach. Wilson Delgado Ramos.	La universidad actualmente cuenta con tecnologías de la información para todos los procesos administrativos, dando lugar a un incremento de ataques externos a sus instalaciones tecnológicas, por ende, es de vital importancia mejorar la gestión de la seguridad perimetral de su red telemática, con bajo costo y mayor eficiencia para detectar incidencias o ataques, dando lugar a fácil mantenimiento y mejora de seguridad a sus procesos operativos con TI de software libre.	Implementación de una solución de seguridad perimetral Open Source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.	DMZ. PFSense. FTP. NAT. VPN. DNS. IDS.
Autores: Jeannelys Belen Carrera Trujillo. Michael Guillermo Sánchez Robalino	En el cantón de Duran en el sector del Recreo se encuentra una compañía dedicada a prestar servicio de taxi ejecutivo llamada Linanfer S.A., presenta diversas falencias, una de las grandes vicisitudes que sobrelleva esta compañía es no contar con un diseño de red escalable y jerarquizado, lo que afecta el rendimiento y optimización en el área tecnológica. Se aspira desagraviar esta necesidad a través de herramientas y recursos tecnológicos Open Source que brindará servicios y soportes de mitigación.	Diseño e implementación de una red de datos con seguridad perimetral para una empresa que se dedica al servicio de taxi ejecutivo.	RouterOS. Proxy. DMZ. IDS. Firewall. IPS. NAT. QoS.

Tabla 2: Proyectos similares

Trabajo o investigación	**Problema**	**Contribución**	**Tecnologías**
Autor: Leonardo José Noriega Vides.	Debido al poco reconocimiento de NetworkBogotá en el ámbito nacional y local. Se identifica la problemática de escaso posicionamiento de marca, para ello la página web, se encargará de difundir actividades, tutoriales y ofrecer servicios que sean de utilidad desde internet. Lo cual es una prioridad, ya que con ello será posible posicionar la comunidad y ser tendencia como proyecto de implementación de redes inalámbricas libres.	Implementación de una red perimetral, sitio web y servidor FTP para la comunidad NetworkBogotá	DMZ. Firewall. OpenWRT. FTP. PPPoE. DNS. Topología MESH
Autores: Fani Yudid Cabrera Vásquez.	Actualmente la institución no cuenta con un sistema de detección de intrusos; otro problema que se debe mencionar es que la universidad tiene ataques informáticos, además que el nivel de seguridad de la red es intermedia lo que genera vulnerabilidades informáticas y para solucionar este detalle se debe obtener un firewall para poder configurar como IDS e IPS.	Diseño de una red de seguridad perimetral basada en Open Source para aplicación de IDS e IPS para el control de amenazas informáticas en la Universidad Técnica de Babahoyo.	DMZ. Subnetting. IPS. VPN. IDS. Firewall. Pasarelas (antimalware) y (antispam)
Autores: María Elisa Mariano Ramos.	Se busca diseñar un mecanismo de seguridad perimetral en la infraestructura de red de H. Ayuntamiento de Tetelas de Ávila Castillo, Puebla; ya que no cuenta con todos los servicios protegidos y modernización	Diseño de seguridad perimetral para la infraestructura de red del H. Ayuntamiento de Teteles de Ávila Castillo, Pue.	SmoothWall. IPFire. Firewall. Fortinet. PFSense. Proxy DMZ.

Capítulo II Acerca del proyecto y de la empresa

2.1 Planteamiento del problema

Actualmente es necesario que cualquier institución implemente mecanismos de seguridad en su red de datos para garantizar un buen nivel de confianza y seguridad en el intercambio o transferencia de la información a través de la red.

En la compañía Avicultores Cordobeses Asociados S.A. de C.V., dedicada a la producción, transformación, distribución y comercialización de insumos para la industria pecuaria y agrícola; está conformada por diversas áreas, donde los usuarios, es decir, los empleados, hacen uso de algún tipo de servicio que otorga la red sin tener un control de la información que se está transmitiendo, suscitando que se conviertan en un blanco fácil para los ataques de terceras personas que utilizan la información para fines inescrupulosos.

Para resolver estos problemas de seguridad presentes, se propone implementar y configurar una red perimetral que separe los equipos que no deben exponerse hacia internet o el exterior, de los equipos que sí deban intercambiar información con internet, a través de herramientas y mecanismos Open Source (que incluya VPN, firewalls para el filtrado de paquetes, colas de tráfico y políticas de seguridad, así como la incorporación de sistemas IDS e IPS) para elevar la seguridad en la red de datos, de forma que se podrá prevenir cualquier ataque que se pueda presentar.

2.2. Objetivos

2.2.1 Objetivo General

Implementar y configurar una red perimetral mediante herramientas Open Source en la compañía de Avicultores Cordobeses Asociados S.A. de C.V. para garantizar la seguridad, funcionamiento óptimo e integridad en los servicios que brinda está a sus usuarios, minimizando los costos, el mantenimiento requerido y disminuyendo así los riesgos a los que se ve expuesta la red de datos.

2.2.2 Objetivos Específicos

- Realizar una evaluación que permita diagnosticar las necesidades de la empresa analizando sus operaciones, recursos, distribución geográfica y servicios que brindan para conocer las vulnerabilidades que presenta.
- Diseñar una red de seguridad perimetral basada en Open Source para aplicación de IDS para el control de amenazas informáticas.
- Crear un diagrama de los flujos lógicos en la red antes de realizar configuraciones,

- Crear y configurar la segmentación de los servicios en la red a través de subnetting con sus respectivas direcciones IP.
- Implementar políticas de seguridad que sean aplicados en los componentes que conformarán la zona desmilitarizada a través de ACL, para el control del tráfico.
- Aplicar un servidor de seguridad perimetral mediante el software pfSense como firewall robusto.
- Implementar un servidor VPN mediante el protocolo de seguridad IPs, con cifrado simétrico aes.
- Implementar un sistema de detección de intrusos a través de la herramienta Suricata.
- Realizar un escaneo de la red utilizando la herramienta Wireshark para observar los paquetes que viajan a través de ella.
- Realizar análisis de resultados de la red para garantizar la gestión de la seguridad.

2.3 Hipótesis

La implementación y configuración de una red perimetral que incluya VPN, firewalls para el filtrado de paquetes, colas de tráfico y políticas de seguridad, así como mecanismos IDS e IPS; incrementará en un 20% la seguridad, disponibilidad e integridad en la red de datos de la empresa Avicultores Cordobeses Asociados S.A. de C.V.

2.4 Justificación del Proyecto

El proyecto que se presenta, surge como resultado de la continua innovación e incremento de las diferentes infraestructuras de red de datos que se comunican hacia el internet, ocasionando, que al mismo tiempo los ataques y amenazas en la seguridad sean de un nivel mayor, generando que la información transmitida sea utilizada por terceras personas.

Ante esta necesidad se demuestra que la implementación de una red perimetral resulta bastante útil en instituciones o empresas que manejen información privada, para brindar el servicio de calidad, seguridad y confidencialidad que los usuarios requieren.

El presente proyecto de titulación tiene como meta brindar una solución definitiva a las complicaciones que se presentan en el área de TIC de la compañía Avicultores Cordobeses Asociados S.A. de C.V. por ello se implementará una red perimetral o más conocida como zona desmilitarizada (DMZ), con la cual se garantiza que la información pública estará separada de la información privada. Mediante el uso de herramientas Open Source, que incluya VPN, firewalls para el filtrado de paquetes, colas de tráfico y políticas de seguridad, como también de los sistemas IDS e IPS, para atenuar las problemáticas ya explicadas.

2.5 Alcances y limitaciones

2.5.1 Alcances

El presente trabajo, pretende implementar y configurar una zona desmilitarizada para la red de datos de la compañía Avicultores Cordobeses Asociados S.A. de C.V. donde se configurarán los servicios que serán restringidos y permitidos para los usuarios de la compañía, es decir que cuente con políticas de seguridad implementadas en la red y las herramientas Open Source ya mencionadas. Todo esto considerando un límite de 15 semanas.

2.5.2 Limitaciones

- Procesos largos de configuración, debido a la falta de hardware en los equipos de la red de datos.
- Falta de disposición de acuerdo al tiempo requerido para trabajar en las necesidades de la empresa.
- Falta de información sobre las características y equipos de cada departamento.
- Dificultad al configurar los servicios que implementará la red perimetral.

2.6 La empresa

2.6.1 Historia de la empresa

Avicultores Cordobeses Asociados fue fundado desde 1979 en la localidad de Paraje Nuevo, Veracruz. Actualmente es una empresa dedicada a la producción y comercialización de ganado, pollo en pie y pollo procesado. Avicultores Cordobeses Asociados tiene una cultura basada en la integridad y la excelencia.

2.6.2 Misión, visión, objetivos y procesos que realizan en la empresa

Ser una organización líder en la producción, transformación, distribución y comercialización de insumos para la industria pecuaria, agrícola y posicionarlo ante el consumidor, de la manera más directa, profesional y eficiente, haciendo posible la existencia y evolución.

Ofrecen elementos de producción pecuaria y los medios para obtener el máximo rendimiento genético en aves, ganado de carne, ovino y porcino a través de:

- Servicios técnicos y de asesoría.
- Un producto sano y de calidad.
- Alimentos balanceados.
- Medicinas veterinarias.
- Materias primas.
- Implementos avícolas.

Capítulo III Metodología PPDIOO

La metodología PPDIOO posee su origen bajo los lineamientos propuestos en el ciclo de vida de una red, ayudando a cumplir objetivos trazados.

La intervención metodológica servirá para la implementación y desarrollo del proyecto, comenzando con la preparación y planeación, los cuales dan un soporte para la elección de las herramientas con las que se va a trabajar y la recopilación de requerimientos, seguidamente se procede con el diseño para dar lugar a la implementación y operación de la red planteada y finalmente optimizar dicha red.

En esta ocasión se tomó en consideración su uso por la comodidad que ofrece sobre la estructuración de las tareas a realizar, de esa manera cumpliendo el objetivo de organizar y facilitar el trabajo a realizar, documentando todo lo que sea realizado en cada etapa.

3.1 Preparación

“Fase de Preparación, involucra temas de presupuesto, estrategia de red”.

3.2 Planeación

“Fase de Planeación, involucra evaluación de la red, análisis de deficiencias”.

Se identifica los requerimientos de red, realizando una evaluación de esta, donde se determinan las deficiencias en la arquitectura. Posteriormente se elabora un plan de proyecto para administrar las tareas, los recursos y la asignación de responsables destinados a cada actividad. Este plan de proyecto es seguido durante todas las fases del ciclo.

3.3 Diseño

“Fase de Diseño, involucra el diseño de la solución (productos, servicios)”.

En esta fase se toman decisiones sobre la infraestructura de red, analizando la mejor distribución física y lógica de los equipos a implementar, permitiendo así, desarrollar un diseño detallado que comprenda requerimientos técnicos y de negocios, obtenidos desde las fases anteriores.

3.4 Implementación

“Fase de Implementación, involucra la puesta en marcha de la solución”.

Durante este paso se realiza un plan de despliegue que incluya los plazos de ejecución. Cada paso en la implementación debe incluir una descripción, guía de implementación y el tiempo estimado para completarla, además de la

documentación de los escenarios en caso de falla e información de referencia adicional.

3.5 Operación

“Fase Operativa, involucra el mantenimiento de la red”.

La implementación real y la verificación del diseño tienen lugar durante este paso. Correlacionándose directamente a la fase de “implementación” ya que esta fase es la prueba final de diseño. Este paso incluye administración y monitoreo de los componentes de la red, mantenimiento de ruteo, administración de actualizaciones, desempeño, e identificación y corrección de errores de red.

3.6 Optimización

“Fase de Optimización, involucra la administración proactiva de la red”.

En la etapa de optimización, se efectúa una administración proactiva, identificando y corrigiendo errores detectados. Es necesario que se documente toda acción realizada en esta fase ya que es probable que se genere una modificación sobre el diseño.

Capítulo IV Desarrollo del proyecto

4.1 Preparación

Se realizó una investigación respecto a qué necesidades se presentaban.

Para ello, se llevó a cabo un diagnóstico sobre la red corporativa con el propósito de identificar el estado actual de esta y de esa forma detectar las necesidades que está presente, así como determinar las soluciones a implementar.

Tabla 3: Diagnóstico sobre la red corporativa

Necesidades presentadas	Soluciones o implementaciones
• Ataques de ransomware al realizar una sesión remota, ya que se encripta la información transferida. • Presencia de virus que generan la pérdida de información y entorpecimiento en la comunicación. • Problemas de redundancia (bucle en la capa 2) en los switches.	• Subnetting para organización de las diferentes redes que existen en la empresa. • Reglas de acceso para el filtrado de direcciones y mejorar la seguridad en la red empresarial. • Firewall open source para bloquear accesos no autorizados, pero sin interrumpir la comunicación. • VPN para el acceso remoto que evite ataques de terceras personas con intenciones perjudiciales. • IDS e IPS para detectar y prevenir las intrusiones en la red.

4.2 Planeación

En esta fase, se realizó un cronograma de actividades a seguir, el cual consta de diferentes pasos repartidos durante un lapso de tiempo, describiendo las tareas que se deberán realizar para lograr el objetivo. El cual se muestra a continuación:

SEMANA	ACTIVIDAD / OBJETIVOS ESPECÍFICOS DEL PROYECTO
1	Elaborar un diagnostico de necesidades.
2	Selección de metodología a aplicar.
3	Elaborar el mapa de red para la seguridad perimetral.
4	Crear y configurar la segmentación de los servicios en la red a través de subnneting con sus respectivas direcciones IP

Ilustración 1: Cronograma de actividades

4.3 Diseño

Durante la fase de diseño se calculó las direcciones de red con base en la dirección raíz que se tiene en la red corporativa, tomando en cuenta la cantidad de host que conforman la red, además, se desarrolló el diseño físico y lógico de la red.

En esta tabla se muestra el número de subred, la dirección de subred, el prefijo, la máscara, las direcciones IP utilizables y por último el broadcast de cada una de las subredes.

Tabla 4: Subredes de la arquitectura de red corporativa

#	Dirección de red	Prefijo	Submáscara	1ra IP	Última IP	Broadcast
1	192.168.0.0	/26	255.255.255.192	192.168.0.1	192.168.0.62	192.168.0.63
2	192.168.0.64	/26	255.255.255.192	192.168.0.65	192.168.0.126	192.168.0.127
3	192.168.0.128	/26	255.255.255.192	192.168.0.129	192.168.0.190	192.168.0.191
4	192.168.0.192	/26	255.255.255.192	192.168.0.193	192.168.0.254	192.168.0.255

Se realizó un esquema de red físico de acuerdo a la problemática que la empresa presenta utilizando la herramienta de diagramación online Lucid chart, en la cual se consideró la más apropiada distribución de los elementos a implementar.

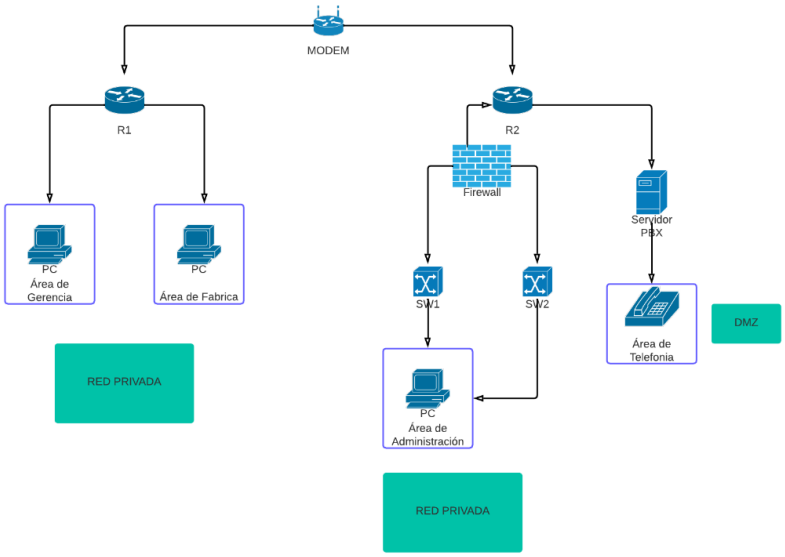


Ilustración 2: Diseño físico de red

El diagrama lógico se realizó en la herramienta lucid chart de igual forma que el esquema físico, en este, se analizó la mejor distribución lógica de la red, que incluye especificaciones técnicas como el direccionamiento IP, los elementos de seguridad, etc.

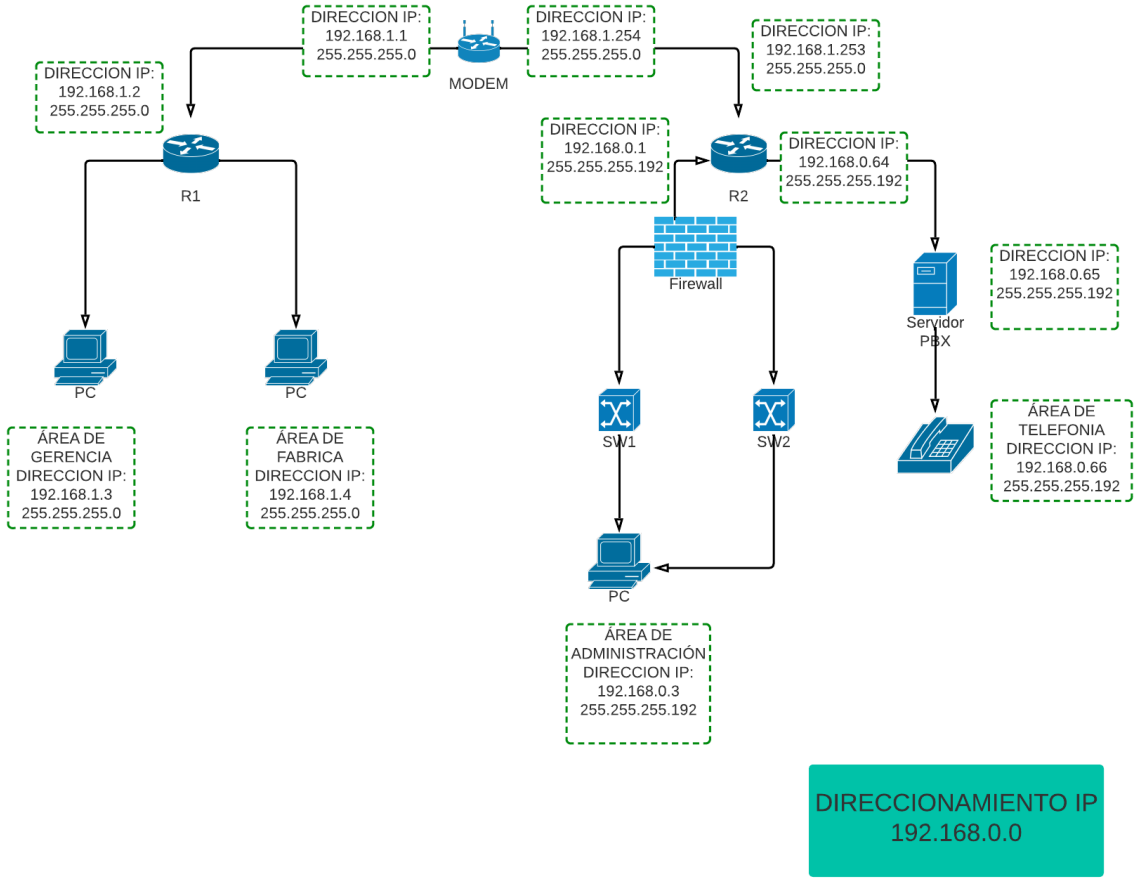


Ilustración 3: Diseño lógico de red

4.4 Implementación

Se configuró una red perimetral con herramientas como firewall basado en PFsense, sistema de detección de intrusiones en base a la implementación de un servidor de Suricata en Ubuntu 20.04 LTS, una VPN con la aplicación OpenVPN. Mecanismos y servicios de red, como reglas para el control de acceso mediante ACLs, organización y segmentación de la red mediante subnetting y la reconfiguración del servicio de voz IP con Elastix.

4.4.1 Configuración de Subneteo en la red.

Para el Subneteo de la red, se utilizó el router CISCO RV042G, donde se ingresaron las 4 subredes diseñadas con anterioridad. Los datos a especificar son, el identificador de la subred y la submáscara:

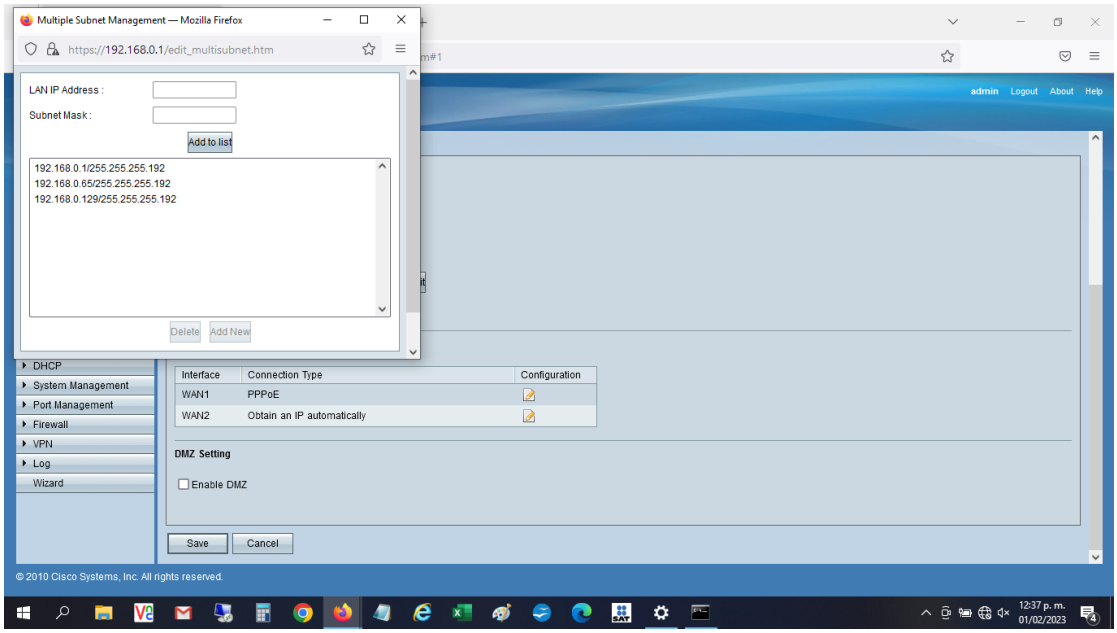


Ilustración 5: Ingreso de subredes en el router

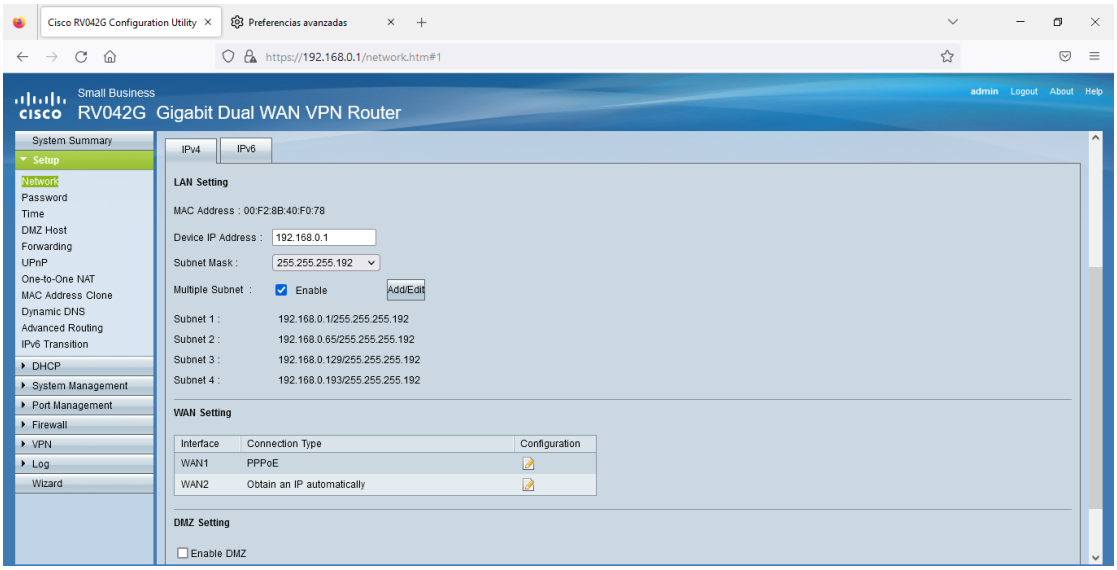


Ilustración 4: Visualización de las subredes creadas

4.4.2 Reconfiguración del servidor y los clientes de voz IP.

Para realizar los cambios se accedió a la interfaz gráfica de Elastix, y se editaron parámetros de red, como la dirección IP del host, del Gateway y sobre la interface

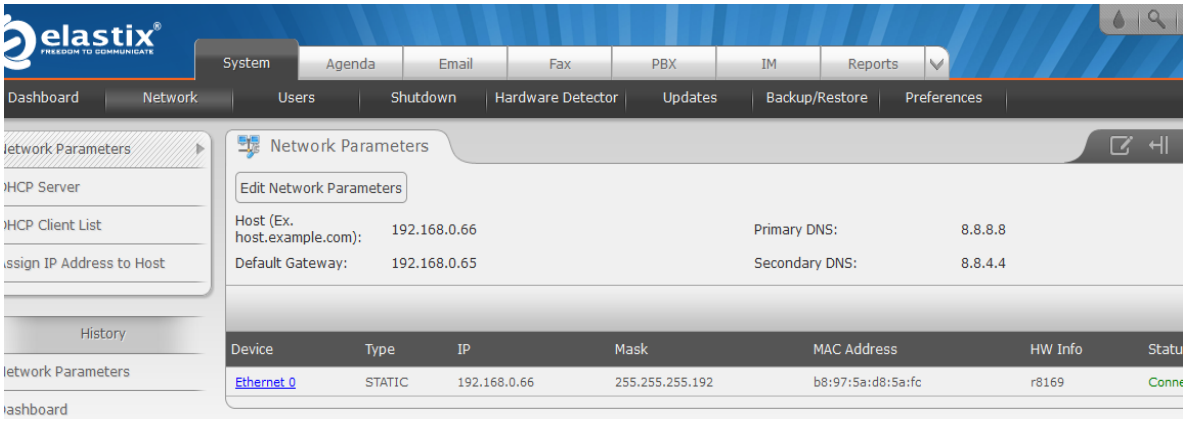


Ilustración 6: Interfaz gráfica de Elastix

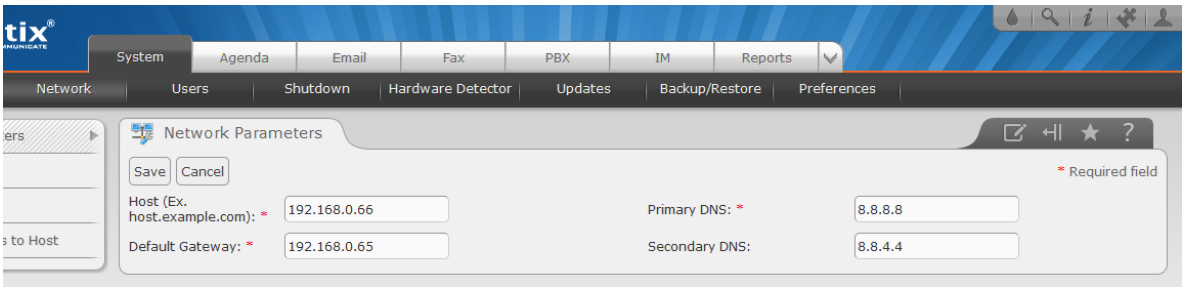


Ilustración 7: Modificaciones en los parámetros del servidor VoIP

También se realizaron modificaciones sobre las SIP troncales y las extensiones para que los clientes realizarán llamadas hacia el exterior y viceversa.

```
disallow=all
allow=ulaw
canreinvite=no
context=from-pstn
dtmfmode=Auto
host=192.168.0.83
incominglimit=1
nat=yes
port=5061&5061
qualify=yes
type=peer
```

Ilustración 8: Parámetros de la SIP trunk

4.4.3 Configuración del firewall pfSense

Para ello, se realizó la instalación del software pfSense en virtualbox.

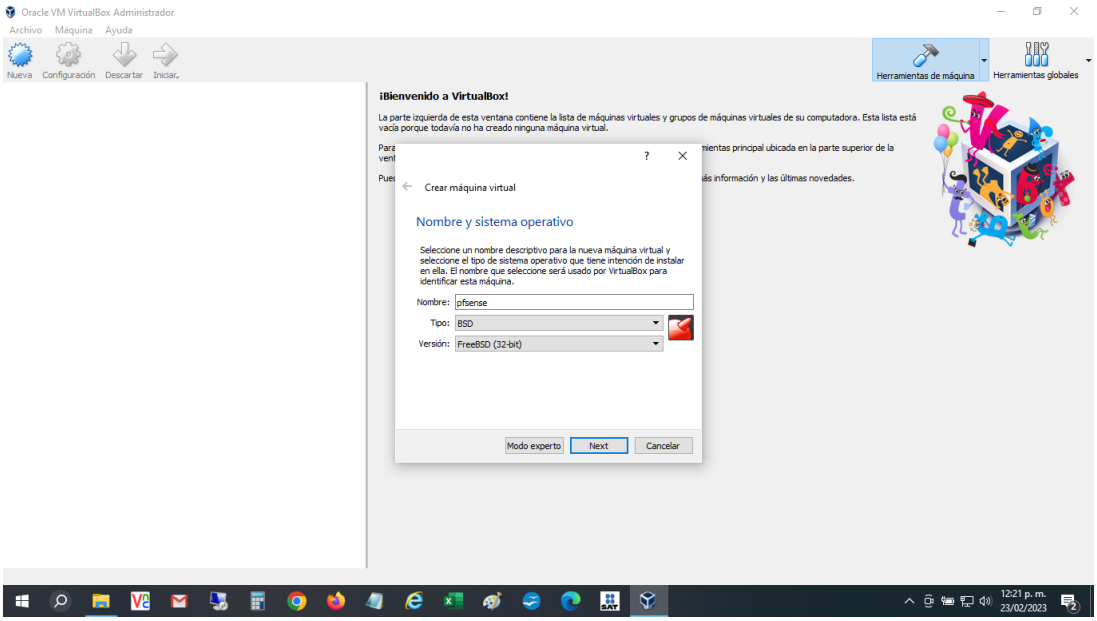


Ilustración 9: Creación del firewall pfSense

El tipo de instalación que se designó a la máquina virtual fue “standard kernel”

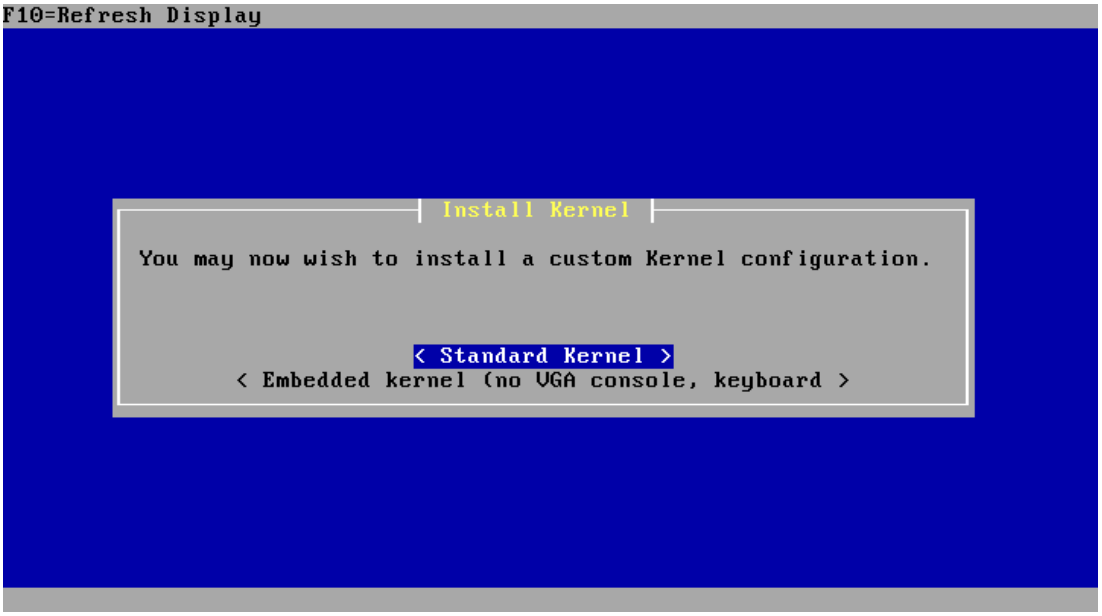


Ilustración 10: Proceso de instalación de pfSense

Se configuraron los parámetros de las interfaces de red (LAN, DMZ y WAN) del firewall.

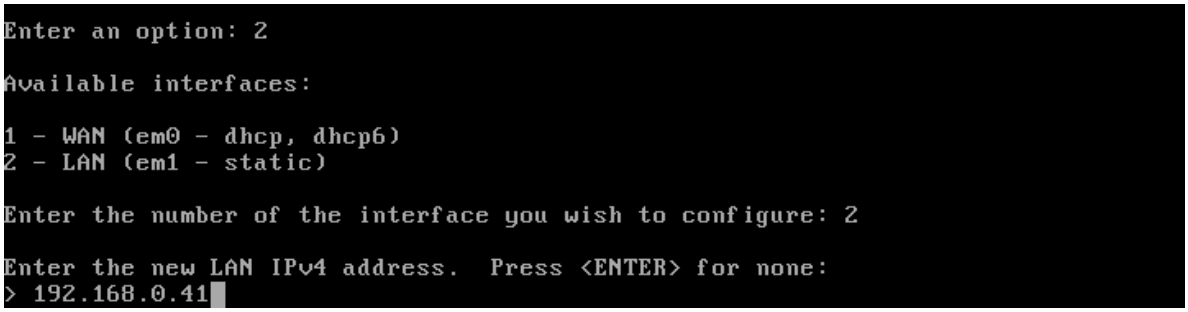


Ilustración 11: Configuración de las interfaces del firewall

Además, se habilitó la interfaz gráfica para permitir la creación de reglas para el control de paquetes que supervisa el firewall y la priorización del tráfico.

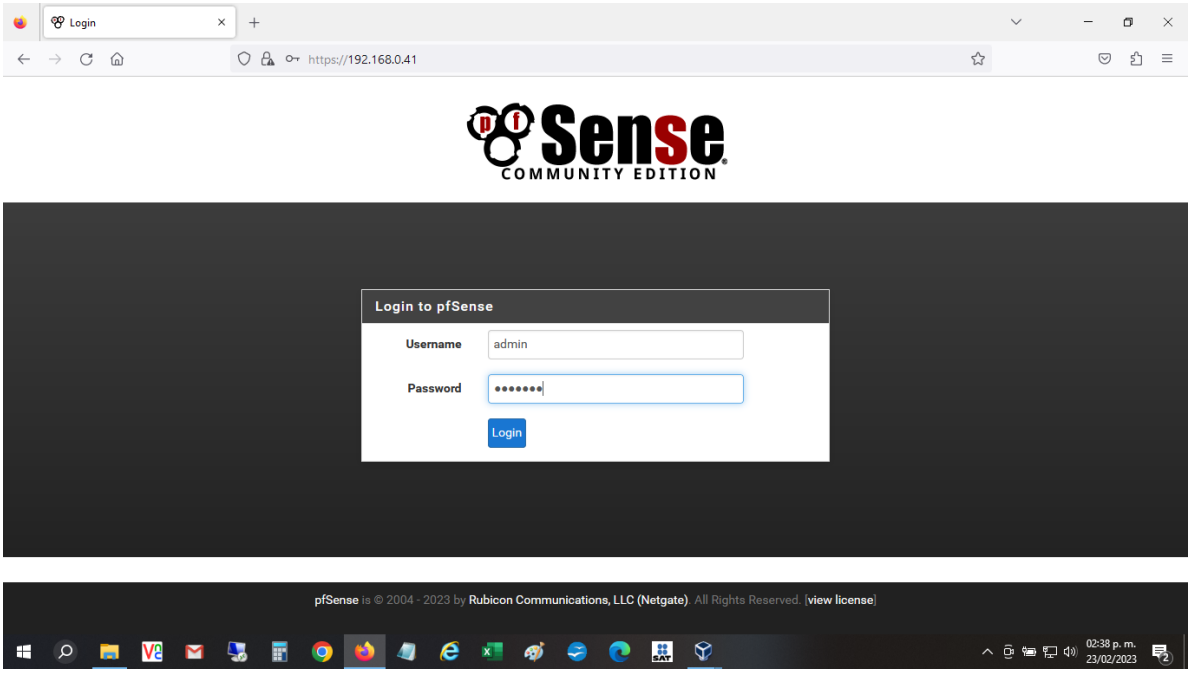


Ilustración 12: Interfaz gráfica de pfSense

4.4.4 Implementación de reglas ACL en el router.

Para agregar reglas ACL en el router Cisco RV042G, se llenaron campos donde se especifica el tipo de acción que tendrá la regla, el servicio, la interfaz de origen y de destino a supervisar, entre otras cuestiones.

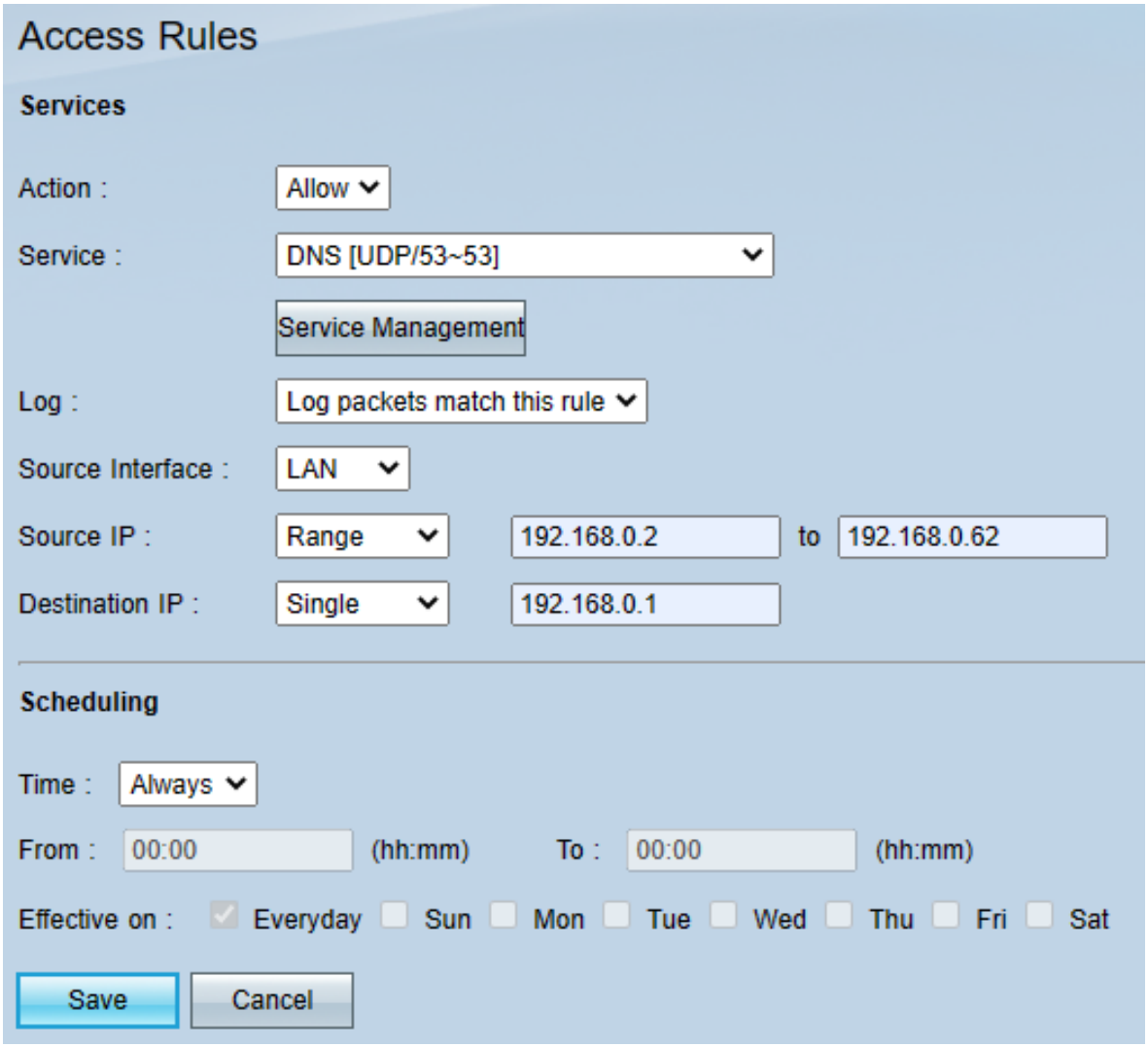


Ilustración 13: Creación de ACLs en el router

Una vez registradas las reglas, se les asigna una prioridad y se habilitan.

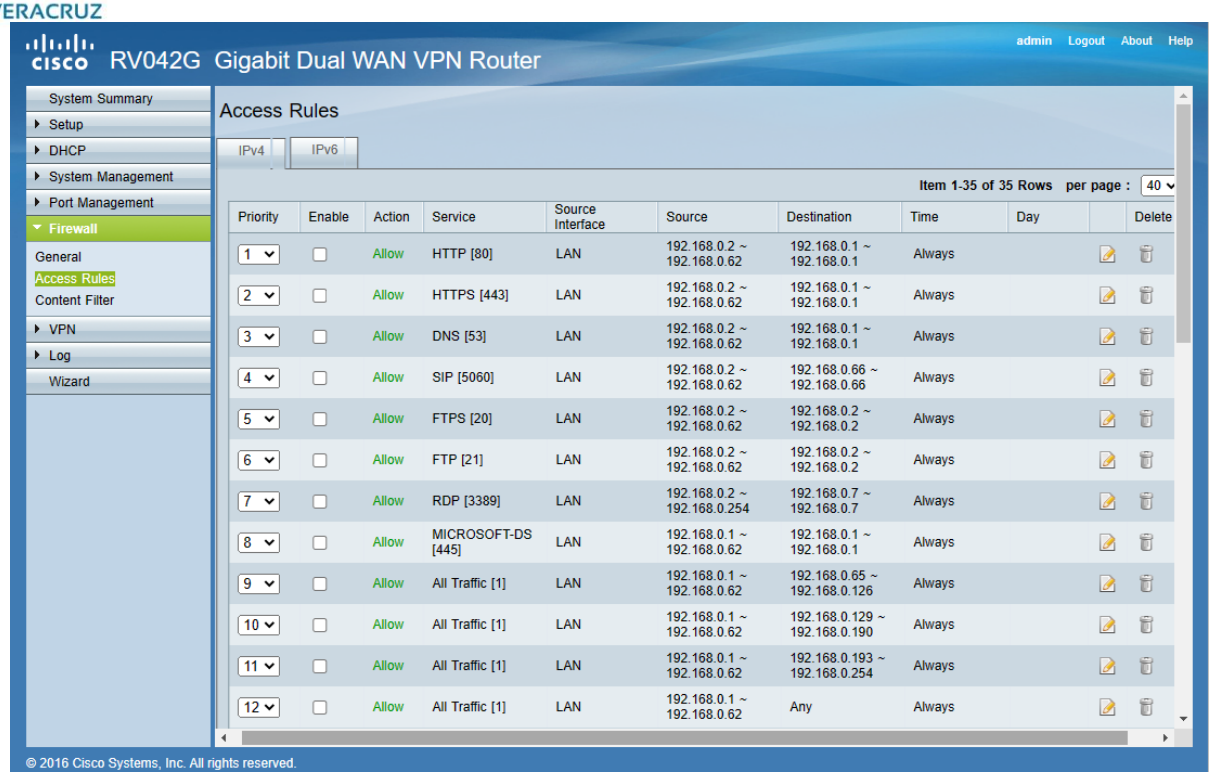


Ilustración 14: Reglas ACLs en el router

4.4.5 Instalación de Wireshark

Para Wireshark, se descargó el instalador de Windows de 32 bits y se procedió a ejecutarlo.

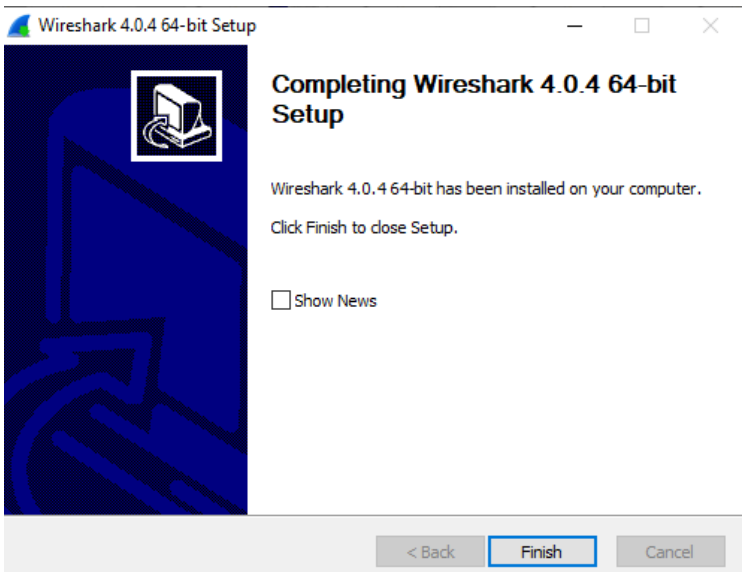


Ilustración 15: Instalación de Wireshark

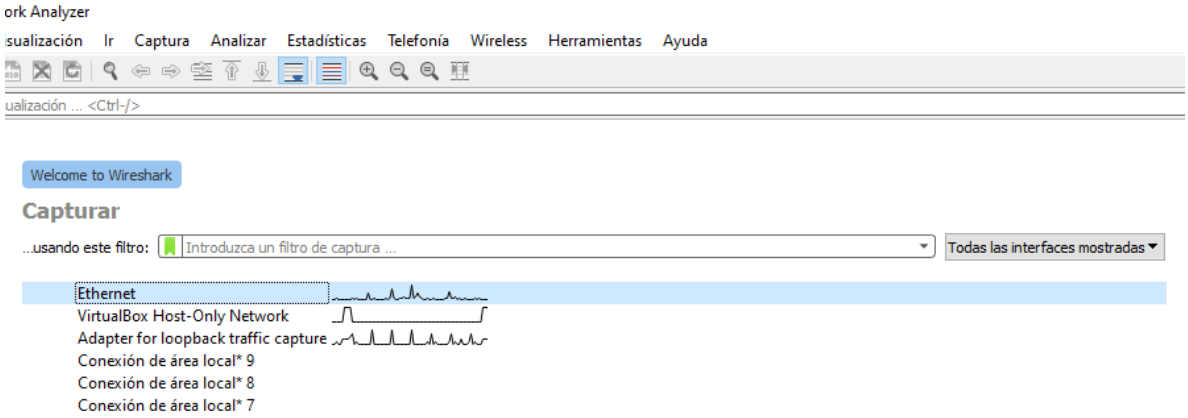


Ilustración 16:Interfaz de Wireshark

4.4.6 Configuración de reglas de firewall en pfSense

Para añadir reglas en el firewall es necesario especificar la acción que realizará la regla, así como la interfaz, el protocolo, la interfaz de origen y de destino.

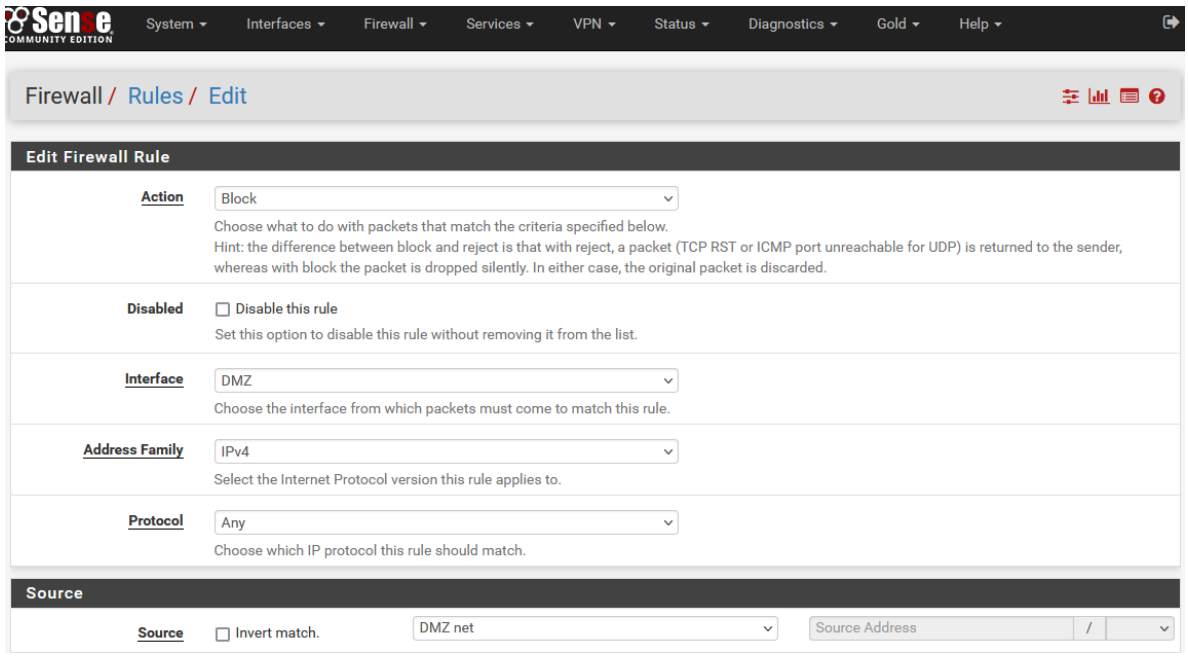


Ilustración 17: Configuración de parámetros en las reglas del firewall

Las reglas que se agregaron en el firewall son las siguientes:

Interface DMZ:

- El tráfico de la DMZ hacia Internet (WAN) será permitido.
- El tráfico de la DMZ hacia la LAN será bloqueado.

Interface LAN:

- El tráfico del host 192.168.0.4 hacia la DMZ por TCP 22 será permitido.
- El tráfico de la LAN hacia la DMZ por UDP 5060,5061 será permitido.
- El tráfico de la LAN hacia la DMZ por TCP 80,443 será permitido.
- El tráfico de la LAN hacia la DMZ por UDP 53 será permitido.
- El tráfico de la LAN hacia la WAN será permitido.
- El tráfico de la LAN hacia la DMZ será bloqueado.

Interface WAN:

- El tráfico de la WAN hacia la DMZ por UDP 5060,5061 será permitido.
- El tráfico restante será bloqueado.

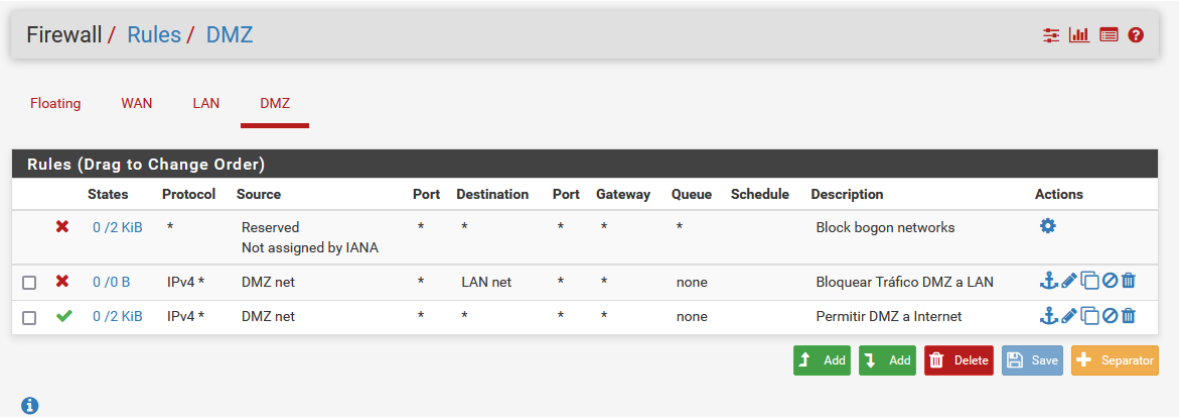


Ilustración 18: Reglas de la interface DMZ

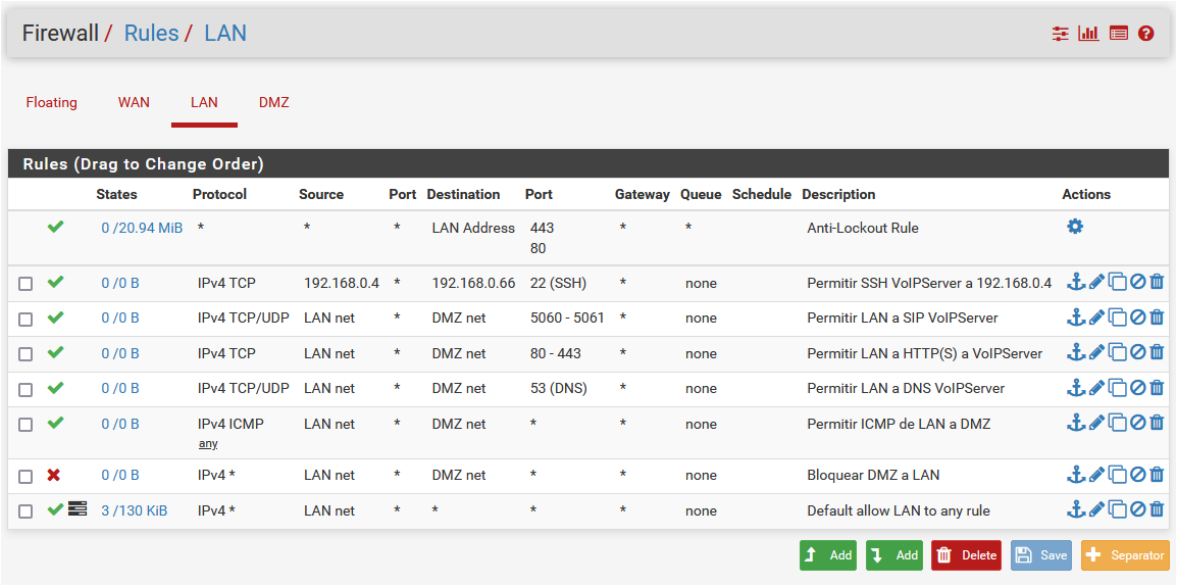


Ilustración 19: Reglas de la interface LAN

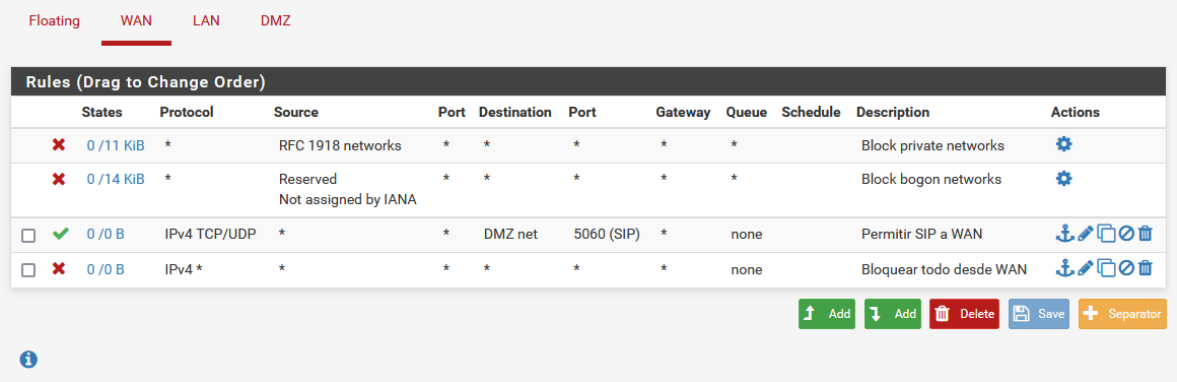


Ilustración 20: Reglas de la interface WAN

4.4.7 Configuración de la priorización del tráfico

Para realizar la priorización del tráfico, es necesario indicar en el firewall el número de conexiones LAN, así como de conexiones WAN

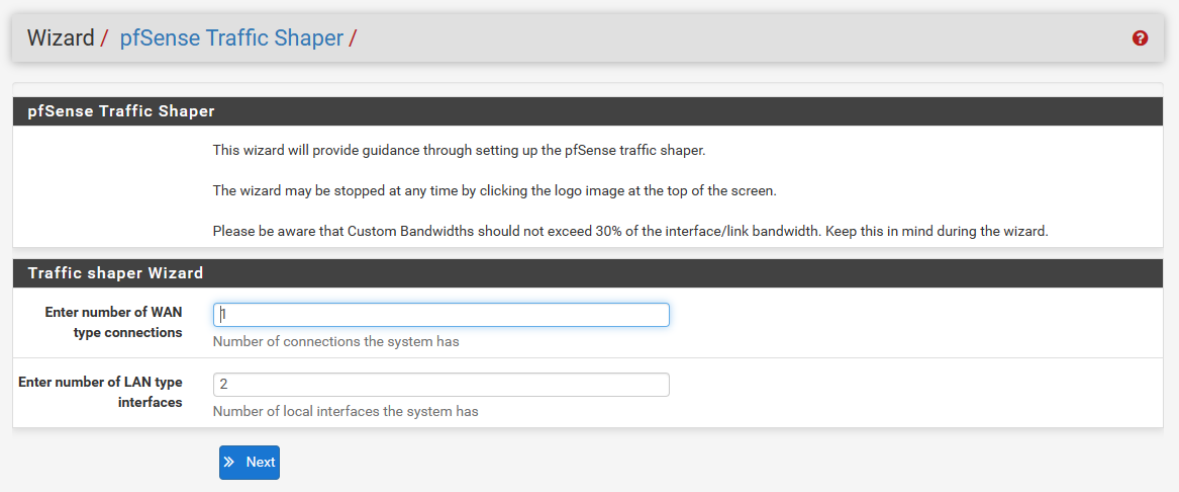


Ilustración 21: Asignación de conexiones a priorizar

Priorizamos el tráfico de VoIP.

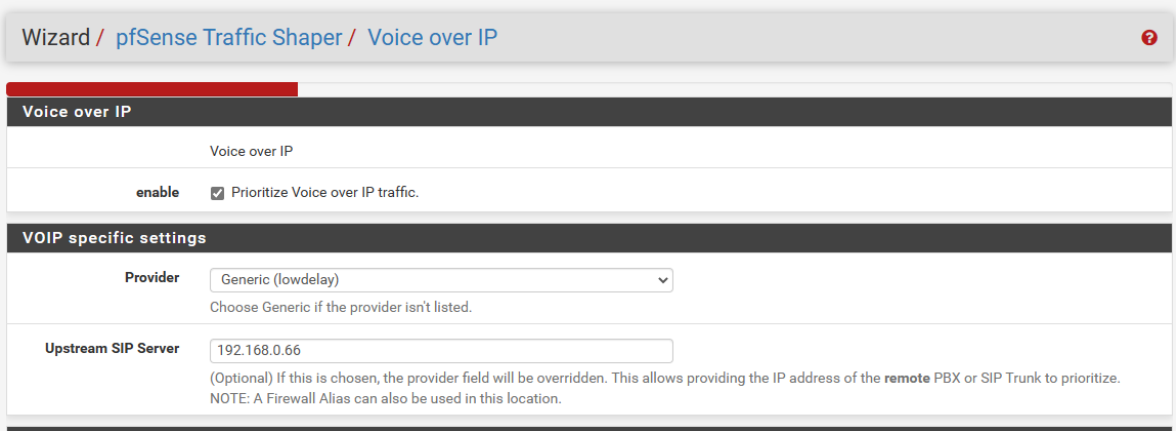


Ilustración 22: Priorización del tráfico VoIP

En el caso del tráfico de videojuegos no será priorizado.

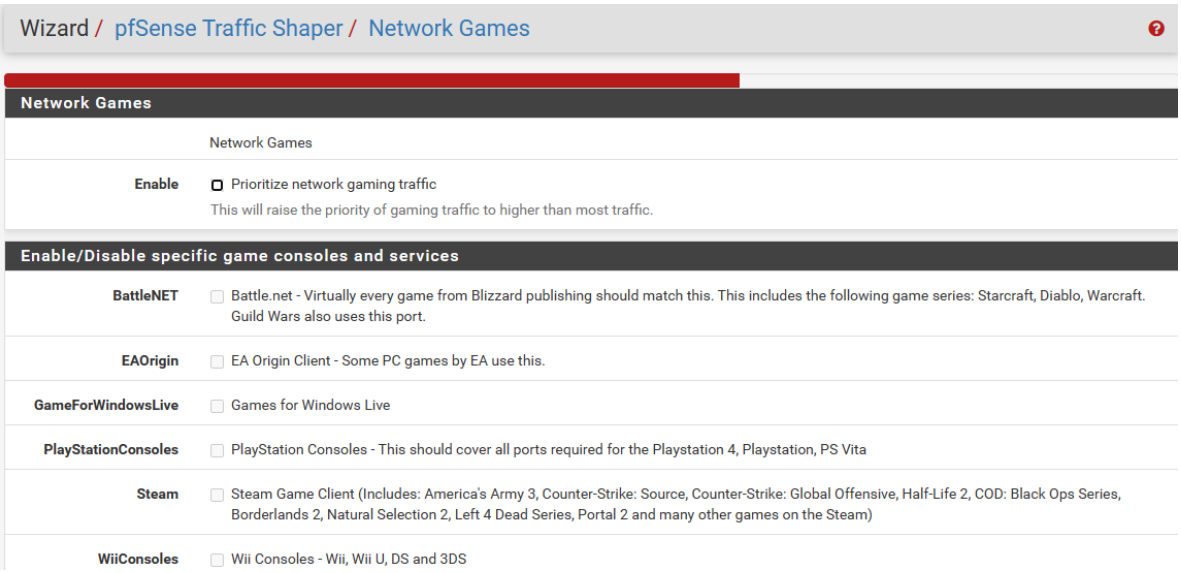


Ilustración 23: Relegar del tráfico de videojuegos

Priorización de protocolos como: MSRDP, PCAnywhere, VNC, PPTP, IPSEC, RTSP, RTMP, DNS, ICMP, SNMP, etc.

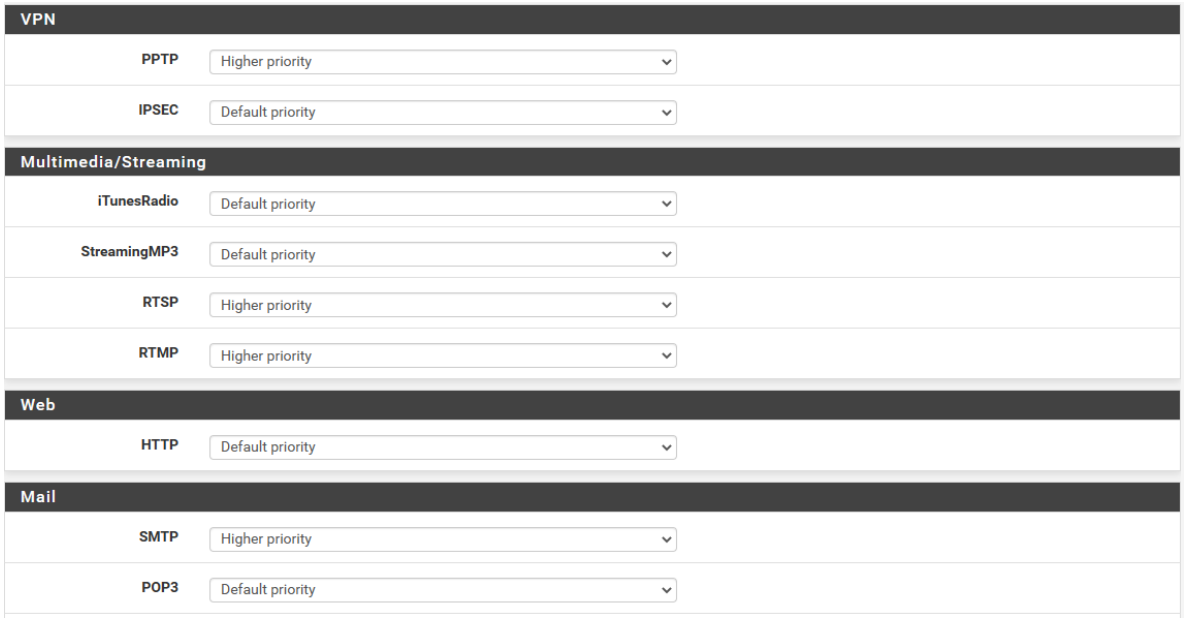


Ilustración 24: Priorización del tráfico de protocolos

4.4.8 Configuración del servidor OpenVPN

En las siguientes tablas se detallan los diferentes tipos de protocolos VPN y sus características [10, p.25-28]:

Tabla 5: Protocolos que se utilizan en una VPN

Protocolos VPN	IP-sec	WireGuard	OpenVPN
Diseño	Complejo	Simple	Complejo
Confidencialidad	Sí	Sí	Sí
Costo	Alto	Bajo	Medio
Cifrado	Modo de transporte y modo de túnel utilizados	ChaCha20-poly1305, cifrado simétrico	TLS (AES/BF)
Integridad	Sí	Sí	Sí
Velocidad	Rápido	Muy rápido	Rápido
Autenticación	Protocolo AH y ESP	Poly1305	TLS
Seguridad	Bueno	Más seguro que IP-Sec	Bueno
Puerto	UDP 500 y TCP	UDP 51820	UDP 1194

Tabla 6: Ventajas y desventajas de OpenVPN

OpenVPN	
Ventajas	Desventajas
Estabilidad.	No es compatible con IPSec, el estándar actual para soluciones VPN.
Multiplataforma, conocido por su portabilidad.	OpenVPN realiza una conjunción de soluciones a nivel de capa 2, capa 3 y capa 7 las cuales no son un estándar de VPN.
OpenVPN admite el transporte IPv6.	Hay pocos fabricantes de hardware que lo integran en sus soluciones.
Hace uso de OpenSSL.	
Hace uso de la autenticación SSL/TLS y el protocolo ESP de IPSec para el transporte seguro de túneles a través de UDP.	

De acuerdo a lo descrito anteriormente, se tomó la decisión de optar por el protocolo OpenVPN, ya que es muy bueno en la encriptación de datos, además de ser multiplataforma y con una buena velocidad.

Para la implementación de OpenVPN se utilizó la versión 2.4.9

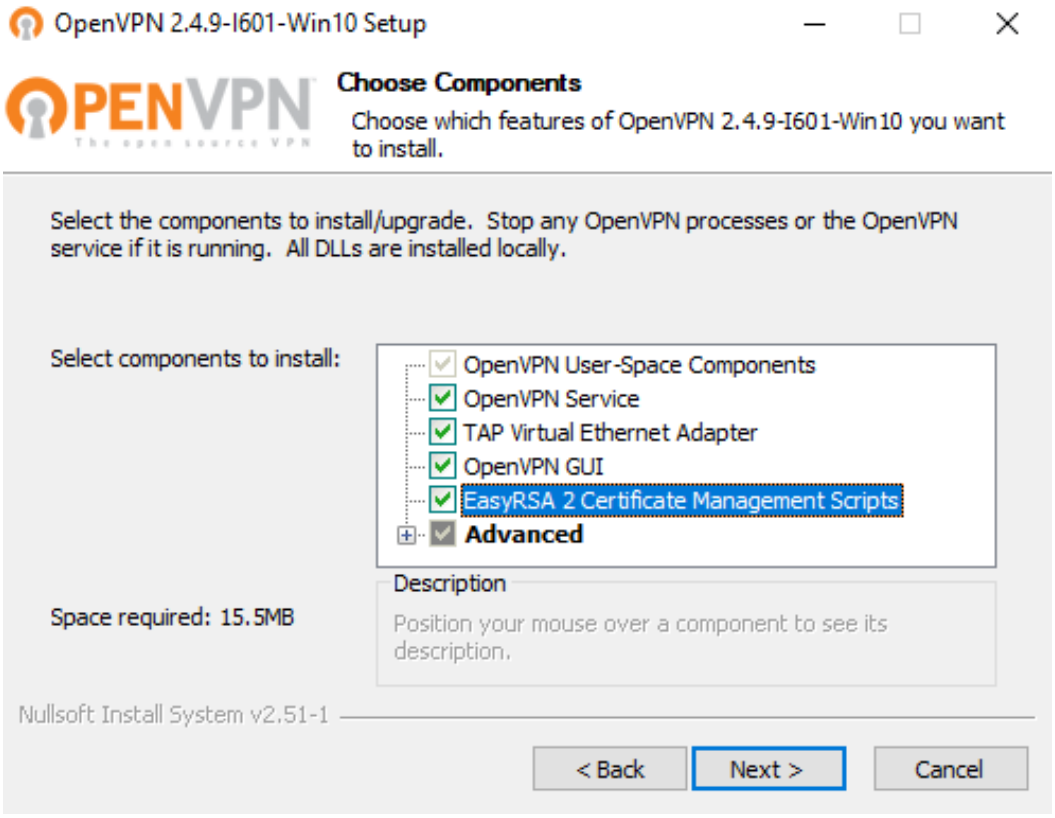


Ilustración 25: Instalación de OpenVPN

Para que el servidor OpenVPN sea funcional se deben realizar modificaciones en las variables del archivo "var" qué especifican la zona geográfica donde se encontrara.

```
set KEY_COUNTRY=MX
set KEY_PROVINCE=VE
set KEY_CITY=Paraje Nuevo
set KEY_ORG=Avicultores Cordobeses Asociados
set KEY_EMAIL=informatica@grupoaca.com
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Ilustración 26: Modificación del archivo var de OpenVPN

Para el servidor y los clientes de este mecanismo se crean claves de la autoridad de certificación (CA), también llaves y certificados, y se generan los parámetros de Diffie Hellman (DH)

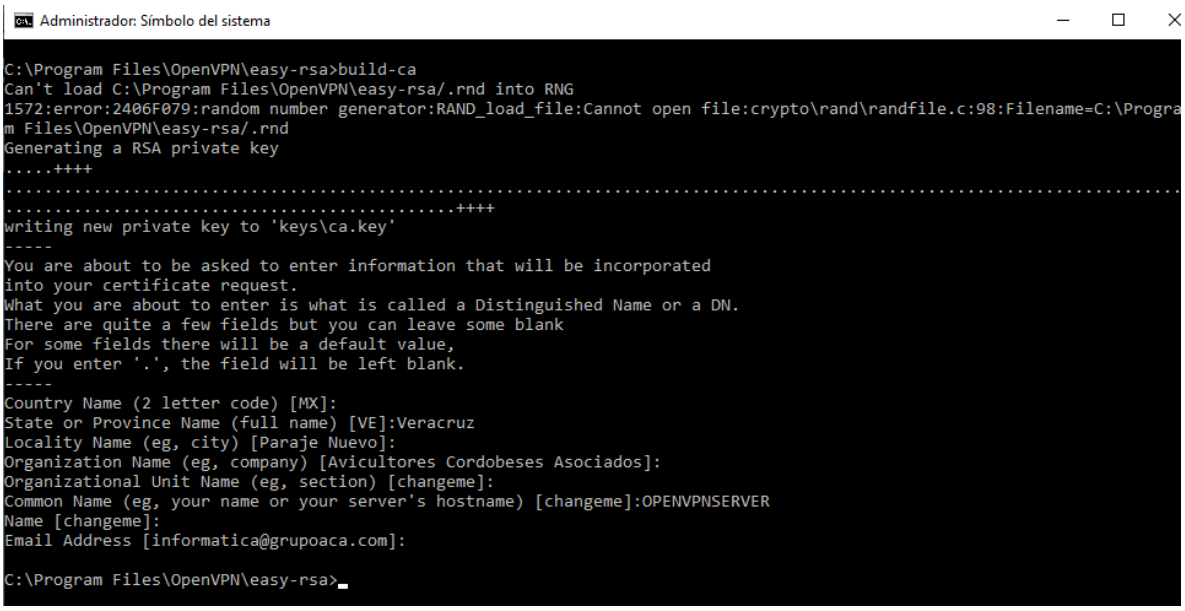


Ilustración 27: Creación de la clave CA

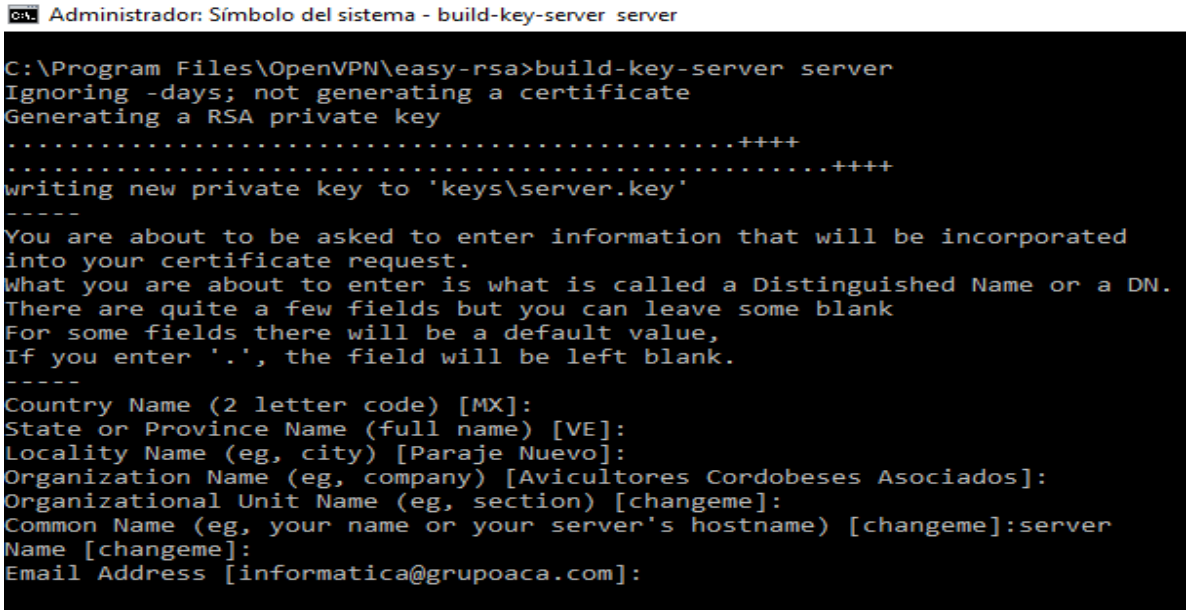


Ilustración 28: Creación de certificados y llaves para el servidor

Ilustración 29: Creación del parámetro DH

En el archivo de configuración de OpenVPN debemos especificar las rutas donde se encuentran los certificados y llaves creadas, así como también el rango de IPs que se asignan a los clientes remotos.

```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).

ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\server.crt"
key "C:\\Program Files\\OpenVPN\\config\\server.key"
dh "C:\\Program Files\\OpenVPN\\config\\dh2048.pem"

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
```

Ilustración 30: Archivo de configuración de OpenVPN

Como ya se había mencionado, OpenVPN hace uso de la autenticación TLS, y esta se debe crear, de acuerdo a como se observa en la siguiente imagen.

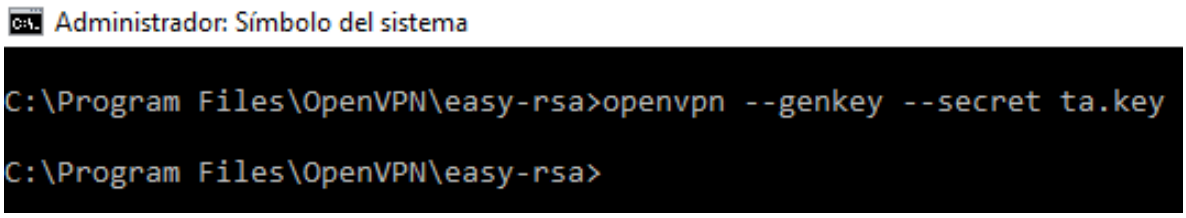


Ilustración 31: Creación de la clave estática de OpenVPN

Por último, se establece la conexión tanto en el servidor como en el cliente.

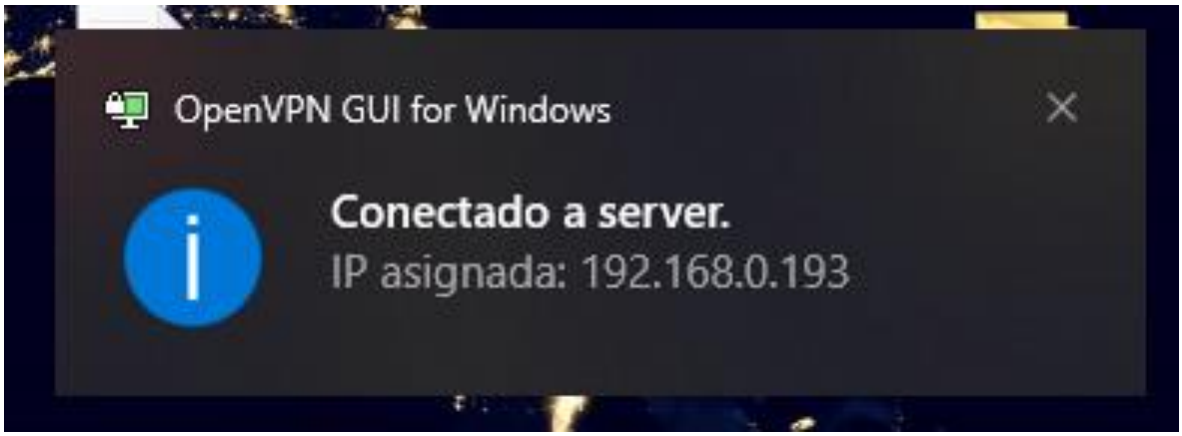


Ilustración 32: Conexión VPN a servidor

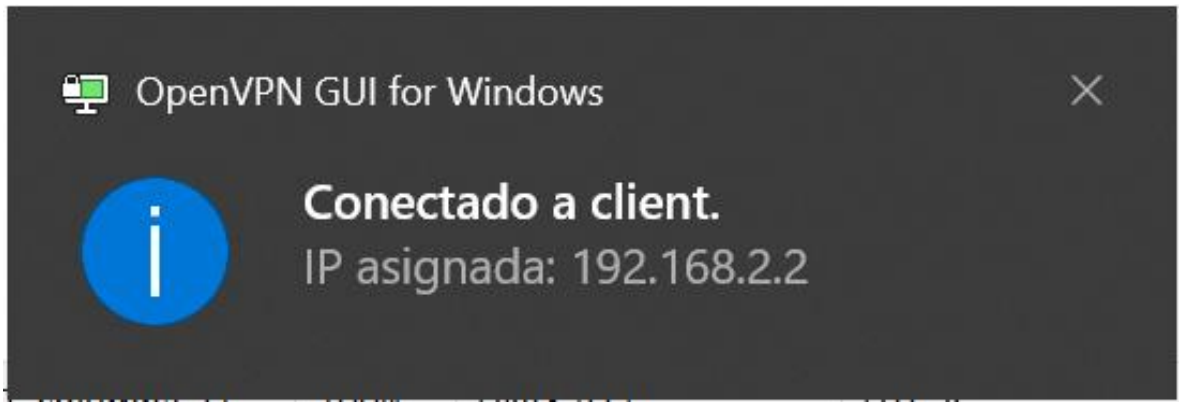


Ilustración 33: Conexión VPN a cliente

4.4.9 Implementación de Suricata como IDS

Para la implementación de Suricata, se utilizó el sistema operativo Ubuntu 20.04 LTS, donde se realizan las configuraciones.

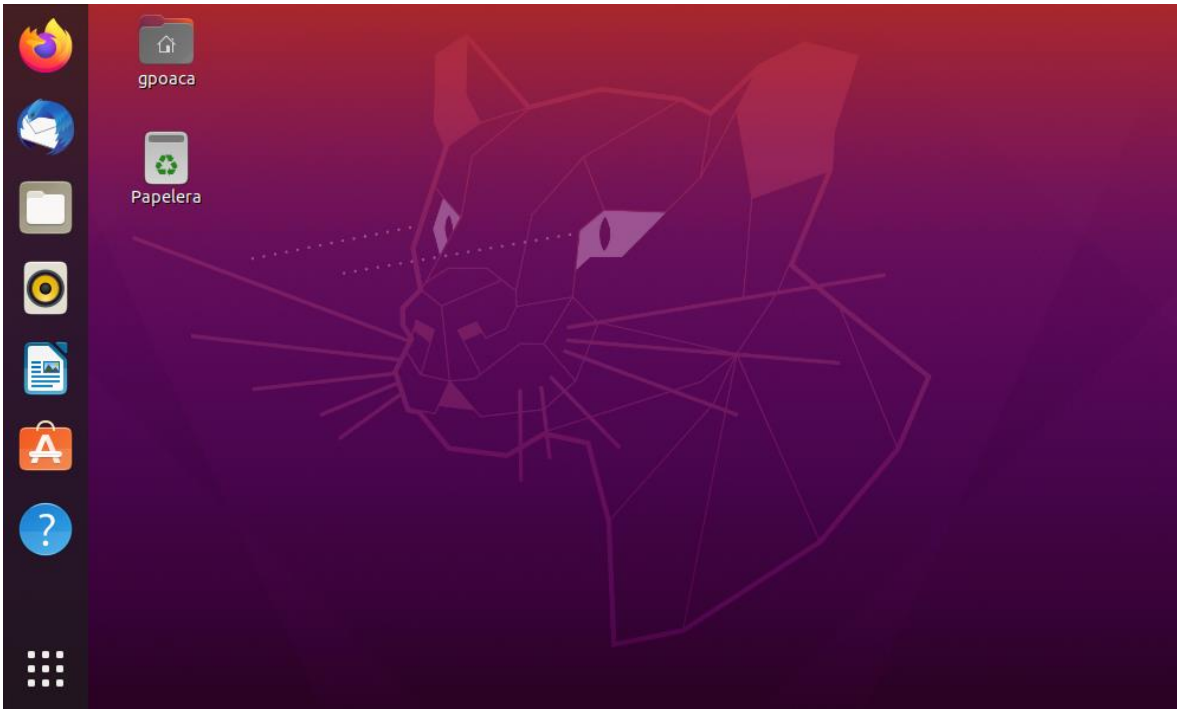


Ilustración 34: Instalación de Ubuntu

En Ubuntu se instala la última versión de suricata, para ello se utiliza el comando que se muestra en la siguiente imagen.

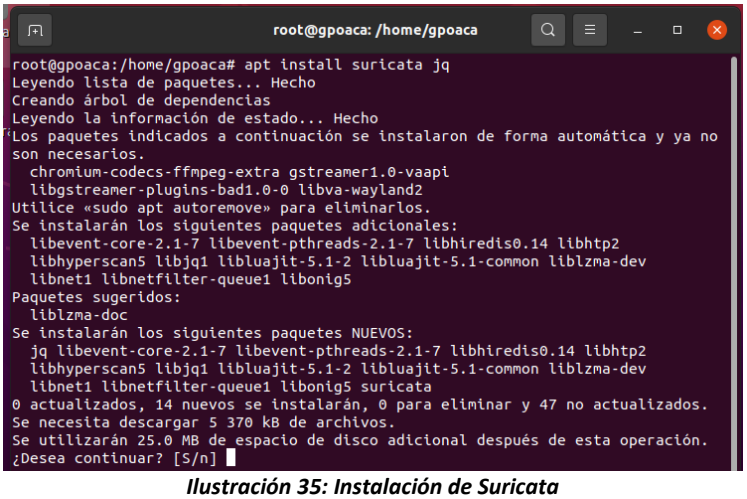


Ilustración 35: Instalación de Suricata

En el archivo de configuración de suricata.yaml se modifican las variables de las redes internas y externas, además, del parámetro que indica donde se almacenan los registros logs de suricata, el fichero donde se escriben las reglas y la interface donde se realizará el análisis.

```
##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    HOME_NET: "[192.168.0.0/24]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
```

Ilustración 36: Archivo de configuración de Suricata

En el fichero my.rules que se encuentra en la ruta ““/etc/suricata/rules”, se añaden las reglas que estará monitorizando el sistema IDS.

```
root@gpoaca: /home/gpoaca
 GNU nano 4.8                    /etc/suricata/rules/my.rules                    Modificado
alert icmp any any -> any any (msg: "ICMP Packet found"; sid:2000001; rev:1;)
drop tcp any any -> any any (msg: "facebook esta bloqueado"; content:"facebook"; sid:1000002; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 80 (msg: "petición GET"; flow:established, to_server ; content:"GET"; http_method; sid:9999; rev:2;
alert tcp any any -> any 22 (msg:"Conexión SSH Detectada"; flow:to_server; app-layer-protocol:ssh; sid:2271009; rev:1;)


###Nmap
alert tcp any any -> any !22 (msg:"Nmap FIN Scan"; flags:F; sid:1000008; rev:1;)
alert tcp any any -> any !22 (msg:"Nmap NULL Scan"; flags:0; sid:1000009; rev:1;)
alert udp any any -> any any (msg:"Nmap UDP Scan"; sid:1000010; rev:1;)
alert tcp any any -> any !22 (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1;)
alert tcp any any -> any !22 (msg:"NMAP TCP Scan"; sid:1000005; rev:2;)
alert icmp any any -> any any (msg:"NMAP ping sweep Scan"; dsize:0; sid:1000004; rev:1;)
```

Ilustración 37: Reglas de Suricata

Para ejecutar las reglas se introduce el comando “suricata -c /etc/suricata.yaml -s /etc/suricata/rules/my.rules -i enp0s3”

```
root@gpoaca: ~
root@gpoaca:~# suricata -c /etc/suricata/suricata.yaml -s /etc/suricata/rules/my.rules -i enp0s3
5/4/2023 -- 13:20:39 - <Notice> - This is Suricata version 6.0.10 RELEASE running in SYSTEM mode
5/4/2023 -- 13:20:39 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
```

Ilustración 38: Ejecución de las reglas de suricata

4.5 Operación

Se realizó pruebas y testeos del proyecto:

4.5.1 Pruebas del funcionamiento de subnetting configurado en el router.

Se aplica una dirección IPv4 a los equipos que conformarán las subredes y se hace una prueba de verificación mediante un ping.

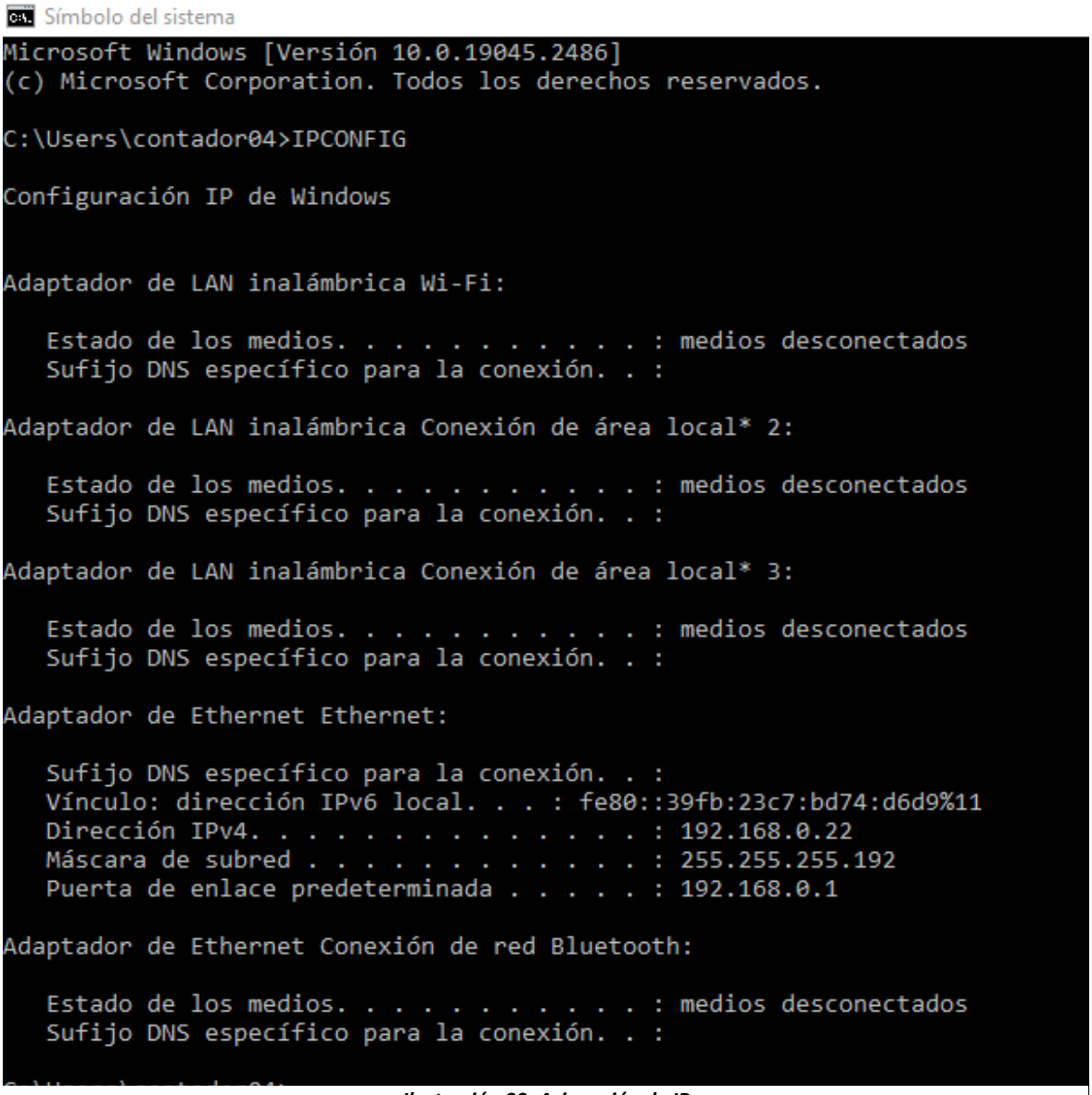


Ilustración 39: Asignación de IP

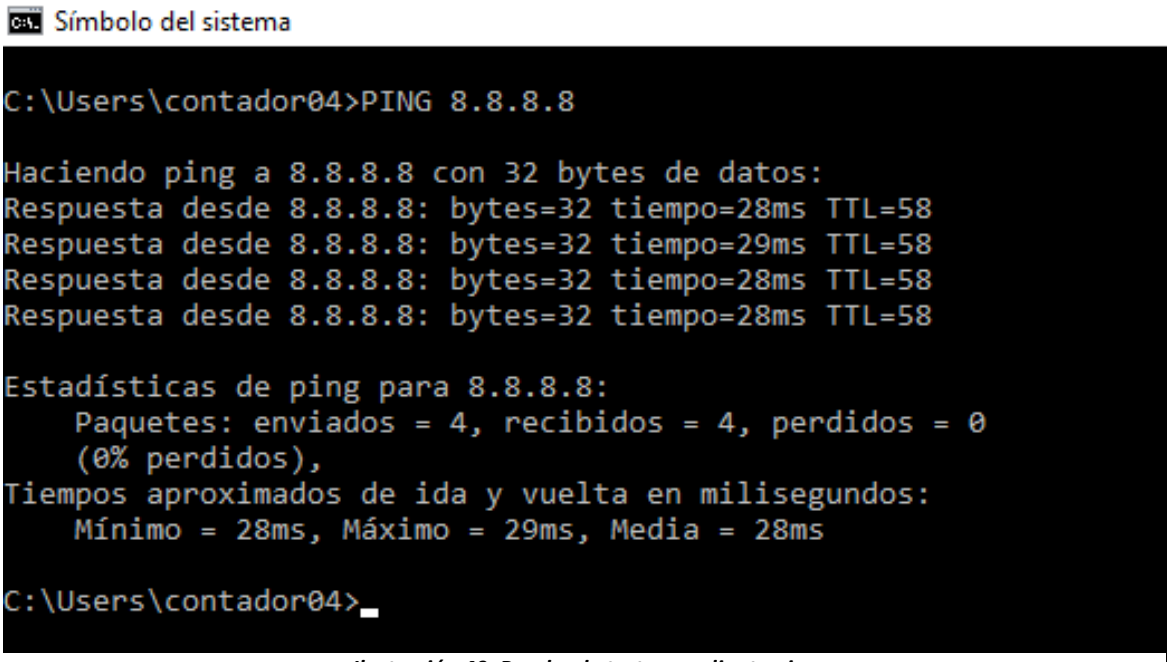


Ilustración 40: Prueba de testeo mediante ping

4.5.2 Funcionamiento y monitorización de wireshark

Para capturar los paquetes en wireshark, se escribe el protocolo en la barra de filtrado para iniciar la captura de paquetes.

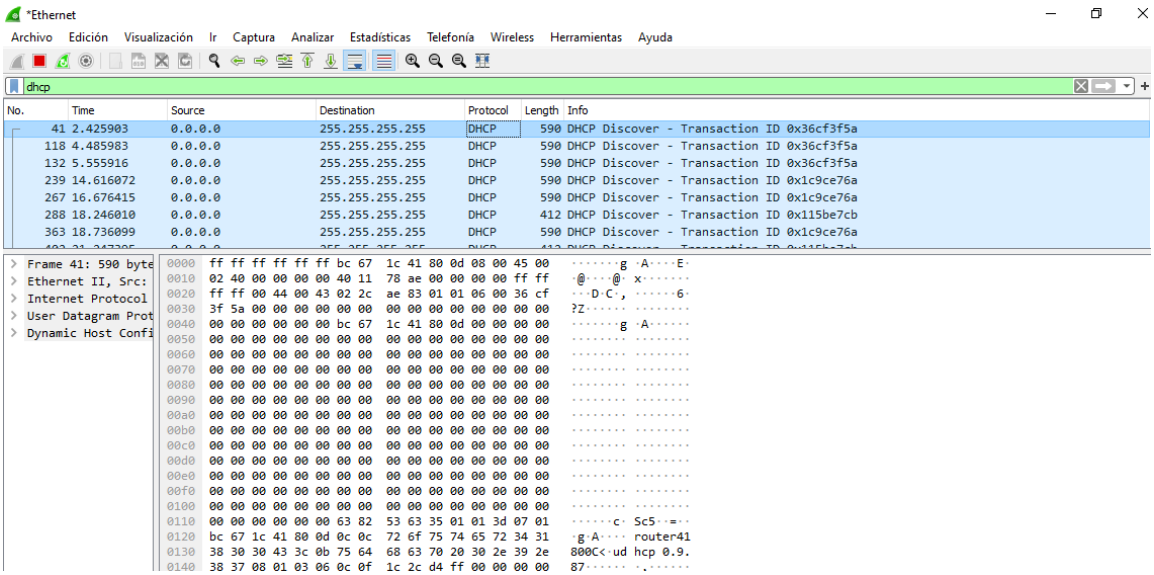


Ilustración 41: Funcionamiento de Wireshark

4.5.3 Aplicación de las reglas para priorizar el tráfico en pfSense

Se generan con éxito las reglas para priorizar el tráfico en el firewall.

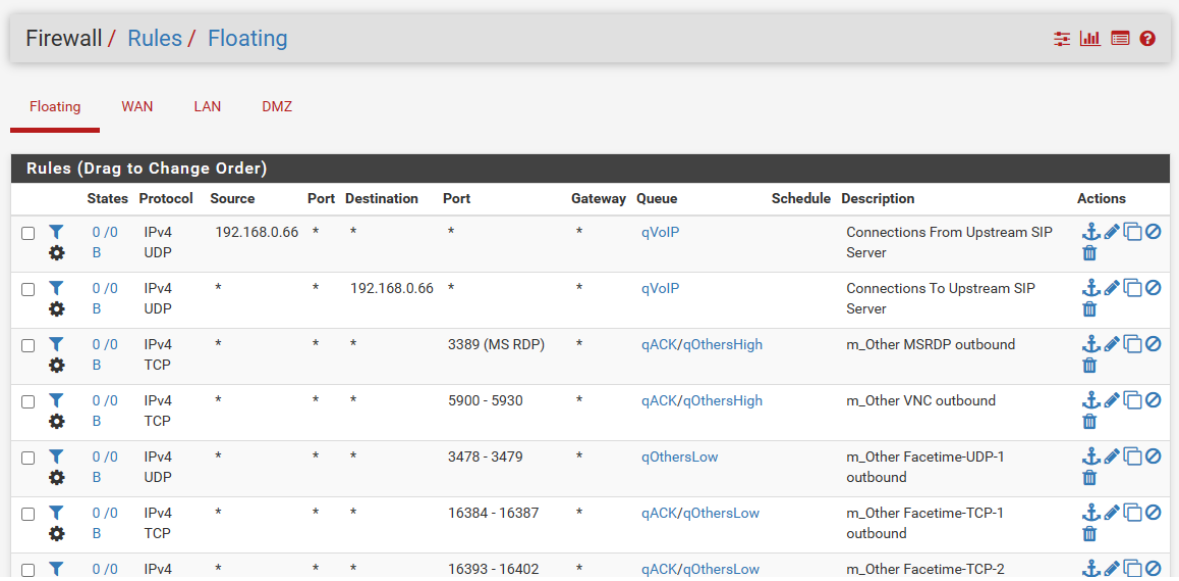


Ilustración 42: Reglas de priorización del tráfico

4.5.4 Prueba de funcionamiento de OpenVPN

Se establece la conexión tanto en el servidor como en el cliente.

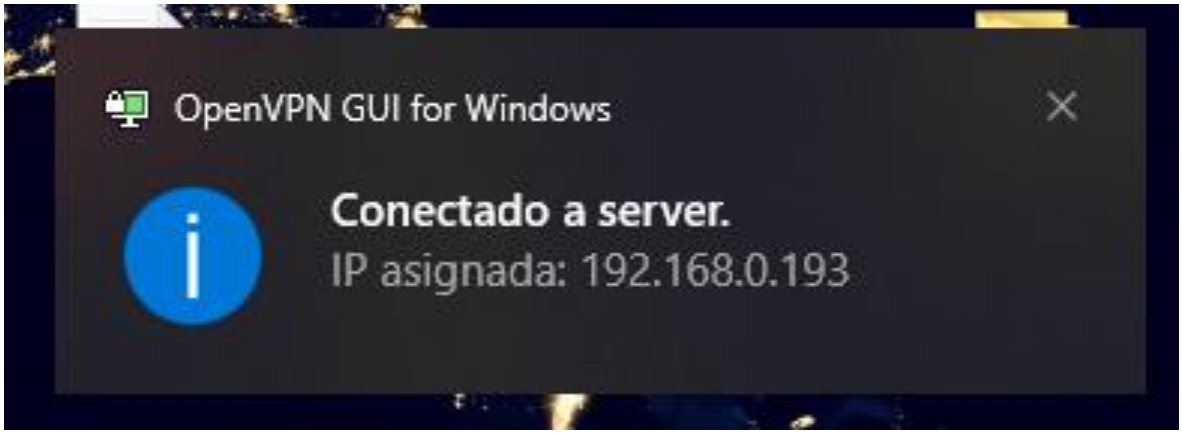


Ilustración 43: Conexión del servidor OpenVPN

Ilustración 44: Conexión del cliente OpenVPN

4.5.5 Generar las alertas de los paquetes en el IDS Suricata

En el fichero log podemos visualizar el registro de alertas que generan las reglas indicadas en el sistema IDS.

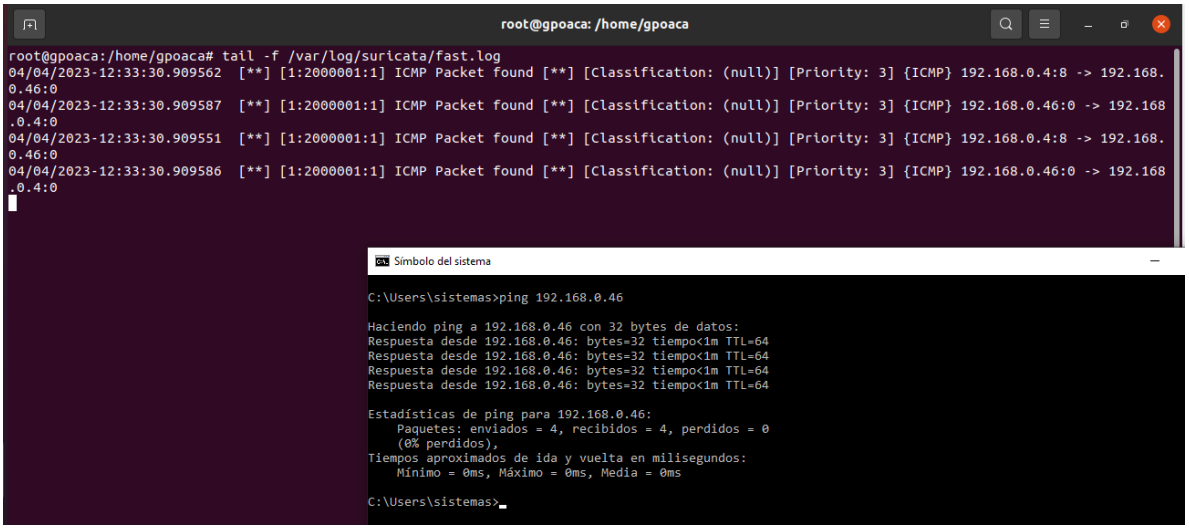


Ilustración 45: Alertas de los paquetes ICMP

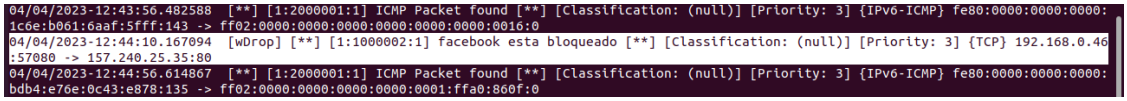


Ilustración 46: Alertas de las peticiones a sitios web

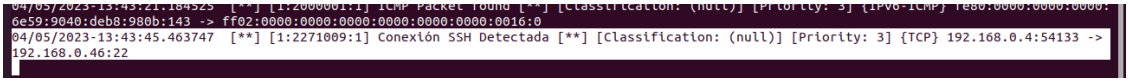


Ilustración 47: Alertas de conexiones SSH

Ilustración 48: Generación de alertas a los escaneos de puertos con NMAP

4.6 Optimización

Debido a que las configuraciones de los servicios resultaron complejas tanto por la IP pública variable y el enrutador con certificados de seguridad obsoletos. Se aconseja contratar una IP pública fija para que la interface que se configura tanto en el servidor de firewall como el servidor de VPN no presente problemas de filtrado y de conexión respectivamente, y así mismo permita que pfSense realice un balanceo de cargas ya que la arquitectura originalmente cuenta con dos conexiones WAN y de esa forma mejorar la calidad de trabajo para los clientes de la red interna.

Para el caso del enrutador se recomienda obtener un enrutador con más funciones como lo es, que sea capaz de realizar configuraciones de VLANs y de activación de puertos para permitir con eficacia la entrada de conexiones clientes de OpenVPN.

Capítulo V Evaluación de resultados y conclusiones

5.1 Evaluación de resultados

En relación al objetivo que se enlistó como:

- Realizar una evaluación que permita diagnosticar las necesidades de la empresa analizando sus operaciones, recursos, distribución geográfica y servicios que brindan para conocer las vulnerabilidades que presenta.

Podemos decir que se cumplió al 100% ya que se realizó un diagnóstico donde se analizaron los ataques que se han ido presentando a lo largo de la vida de la red corporativa, así como la identificación de las causas por las que surgen esos ataques y las soluciones ante las necesidades presentadas.

- Diseñar una red de seguridad perimetral basada en Open Source para aplicación de IDS para el control de amenazas informáticas.

Podemos decir que se cumplió al 100% ya que todas las herramientas implementadas durante el ciclo de este proyecto son basadas en código libre (pfSense, OpenVPN y suricata, el cuál es un sistema de detección de intrusiones).

- Crear un diagrama de los flujos lógicos en la red antes de realizar las configuraciones.

Podemos decir que se cumplió al 100% porque se realizó un diagrama, así como también tablas sobre la distribución lógica, es decir las direcciones IP, las interfaces, los puertos, etc. de cada componente que conforma la red.

- Crear y configurar la segmentación de los servicios en la red a través de subnetting con sus respectivas direcciones IP.

Podemos decir que se cumplió al 100% porque fue configurado satisfactoriamente las subredes creadas para la organización de los componentes de la red, en el enrutador, además de que se generaron tablas que indican los rangos de cada subred, así como su identificar, la submáscara de red, el broadcast y la puerta de enlace.

- Implementar políticas de seguridad que sean aplicadas en los componentes que conformarán la zona desmilitarizada a través de ACL, para el control del tráfico.

Podemos decir que se cumplió al 100% debido a las configuraciones ingresadas tanto al enrutador como al firewall, es decir, las reglas para el control de acceso, que determinan la entrada o descarte de paquetes de acuerdo a la especificación

de las reglas. Terminando de una forma en que los clientes externos puedan acceder a los equipos de la DMZ y viceversa, pero denegando cualquier intento de ingreso del exterior hacia la red interna.

- Aplicar un servidor de seguridad perimetral mediante el software pfSense como firewall robusto.

Podemos decir que se cumplió en un 100% ya que fue posible la instalación y el acceso a la interfaz gráfica del software pfSense, además de que se consiguió implementar ACLs para las tres interfaces que fueron configuradas (DMZ, WAN y LAN). También se obtuvo un buen funcionamiento en la priorización del tráfico que se presenta en las redes LAN y WAN, ya que se presentó una mejora en la velocidad de la transmisión de información de la red.

- Implementar un servidor VPN mediante el protocolo de seguridad IPs, con cifrado simétrico aes.

Podemos decir que se cumplió en un 80% ya que se tuvo que optar por otras soluciones en cuanto a la implementación de un servicio de VPN ya que por el tipo de complejidad y la falta de tiempo que se presentó, no resultó posible la implementación de una VPN mediante Docker con cifrado aes. Esto debido en gran medida a la arquitectura que posee el enrutador, ya que no era posible configurar los puertos para permitir la entrada de clientes VPN. Por esta razón se decidió implementar un servidor VPN basado en OpenVPN.

- Implementar un sistema de detección de intrusos a través de la herramienta Suricata.

Podemos decir que se cumplió al 100% ya que se generan alertas sobre el tráfico en la red (ICMP, sitios web, escaneo de puertos, SSH) y se reportaban estas alertas en los archivos log del sistema suricata.

- Realizar un escaneo de la red utilizando la herramienta Wireshark para observar los paquetes que viajan a través de ella.

Podemos decir que se cumplió en un 100% ya que se permitía el análisis y captura de los paquetes de la red.

- Realizar análisis de resultados de la red para garantizar la gestión de la seguridad.

Podemos decir que se cumplió en un 100% porque al implementar los sistemas y mecanismos mencionados en este proyecto, la velocidad y la calidad de la red mejoró, además de que los ataques y el robo de la información por parte de terceras personas se vio minimizado.

5.2 Conclusiones

Después de finalizar la implementación de una red perimetral en la empresa Avicultores Cordobeses Asociados S.A. de C.V. se observó lo siguiente:

- La combinación entre pfSense e IDS (Suricata) ocasionó que la seguridad en la red sea más robusta, porque uno de los sistemas realiza acciones contra posibles ataques, mientras que la otra alerta sobre una amenaza presente. Y mediante los logs podemos notificar a la empresa de lo que está sucediendo y en consecuencia generar registros y planes de acción para evitar en un futuro situaciones similares.
- Por el sistema OpenVPN se tiene un acceso controlado a todos los servicios que brinda la red interna, ya que esta otorga una forma segura de acceder a los recursos de la empresa desde cualquier parte del mundo.
- Con las reglas de acceso configuradas en el enrutador y el firewall se logró que la red cuente con una seguridad perimetral, además de las configuraciones de priorización sobre el tráfico que mejoran la gestión de la infraestructura, la velocidad de transmisión y disminuyen la pérdida de paquetes, así como la disminución de intrusiones y vulnerabilidades.
- Tanto la distribución de los equipos en el flujo lógico y físico de la red, como la implementación de mecanismos de seguridad, resultan en una mejora del funcionamiento de los servicios que brinda la red corporativa de Avicultores Cordobeses Asociados S.A. de C.V.

Es indispensable que cualquier red tome en consideración la aplicación de la seguridad informática, debido al crecimiento de las comunicaciones, porque las necesidades también incrementan. Un sistema perimetral facilita a los administradores de la red a mantener la disponibilidad, eficacia y seguridad sobre la red.

Anexos

Diagnóstico de la red.

INTRODUCCIÓN:

El siguiente reporte presenta la información obtenida del diagnóstico de la empresa Avicultores Cordobeses Asociados, realizado el día 13 de enero del 2023 con el ingeniero de sistemas Ruperto Peralta Durán, al cual se le realizó una serie de preguntas para determinar la seguridad de la información, basándose en los pilares y políticas de seguridad, es decir, la disponibilidad, integridad, confidencialidad y autenticación de la red empresarial.

OBJETIVO:

Identificar el estado actual de la red en la empresa Avicultores Cordobeses Asociados, detectando las necesidades que esta presente y así desarrollar un plan de acción para implementar mecanismos que reduzcan los incidentes y mejoren la calidad de trabajo.

PERSONAS QUE INTERVINIERON:

- Entrevistadores:
  - TSU. Estefhany Hernández Ortiz
- Entrevistados:
  - Lic. Ruperto Peralta Durán.
  - Lic. Manlio Díaz Crivelli.

NECESIDADES O PROBLEMÁTICAS PRESENTADAS:

- Existen equipos fuera de la oficina que acceden remotamente a la red empresarial para gestiones de trabajo, al no contar con mecanismos de seguridad que protejan la información transferida, se presentan ataques como la encriptación de la información (ransomware) o la presencia de virus que generan la pérdida de información de forma temporal, la interrupción de los servicios y el entorpecimiento de la comunicación.
- Debido a la falta de organización en las direcciones IP de la empresa se presenta congestión en la red administrativa empresarial, es decir, la reducción de la calidad del servicio ya que el enlace o nodo de red transporta más datos de los que puede manejar, produciendo el retraso en la cola, la pérdida de paquetes o el bloqueo de conexiones.
- Los switches presentan problemas con la redundancia (bucle en la capa 2) provocando los siguientes problemas:
  - Inestabilidad de la base de datos MAC: Se produce por recibir copias de la misma trama en diferentes puertos del switch. El switch consume los recursos para resolver la inestabilidad, afectando el reenvío de datos.

- Tormentas de difusión: Se produce cuando existen tantas tramas de difusión atrapadas en un bucle de capa 2. Como consecuencia no hay ancho de banda disponible y la red deja de estar disponible.
- Transmisión de varias tramas: Varias copias de la misma trama provocan errores en protocolos de capa superior que asumen que la transmisión ha fallado.

SOLUCIONES O IMPLEMENTACIONES:

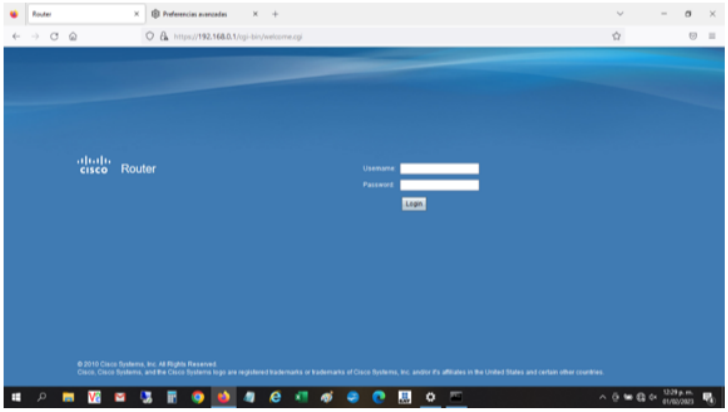
- Se lleva a cabo el uso de subnetting para organizar las diferentes redes que existen en la empresa, es decir, clasificar el tráfico de red en distintas categorías y facilitar la aplicación de políticas de seguridad, para obtener una mejor prestación de servicios. Consiste en dividir una red, sea de clase A, B o C, en dos o más subredes.
- Para evitar el acceso de terceras personas en la red se propone implementar reglas de acceso para el filtrado de direcciones y mejorar la seguridad que cumple un papel fundamental para preservar la integridad de la información.
- Implementación de un firewall basado en software de código abierto para bloquear accesos no autorizados a ordenadores, pero sin interrumpir la comunicación entre el ordenador y otros servicios autorizados.
- Implementación de un VPN para que los equipos del exterior pertenecientes a encargados del área de redes puedan acceder a la red mediante un túnel virtual que mantenga la seguridad de la comunicación, evitando el ataque de personas con intenciones perjudiciales.
- IDS (Sistema de Detección de Intrusos) se encarga de inspeccionar la actividad en la red en busca de comportamientos inusuales que puedan indicar un ataque o mal uso de la red, e IPS (Sistema de Prevención de Intrusos) que ejerce control de acceso la cual analiza los datos del ataque y actúa en consecuencia.

Registro de implementación

REGISTRO DE IMPLEMENTACIÓN:

Entregable:	Configuración de subneteo en la red.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	01/02/2022 – 03/02/2022
Evidencia y Descripción	

1. Para el Subneteo de la red, se utilizó un router CISCO RV042G, al cual, se accede mediante un navegador. En la barra de búsqueda de mozilla Firefox se coloca la dirección IP (192.168.0.1) y "admin" como usuario y contraseña por defecto.



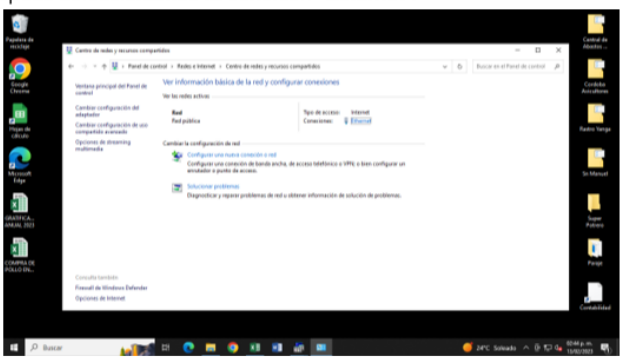
Entregable:	Asignación de dirección IP a impresoras.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	06/02/2022 – 06/02/2022
Evidencia y Descripción	

1. Para asignar una dirección IP a una impresora, en este caso marca "RICOH", deslizamos la interface, hasta encontrar la opción "herramientas usuario". Procedemos a dar clic en esa opción.

2. Una vez realizado el paso anterior, hacemos clic en la opción "características máquina"

Entregable:	Asignación de dirección IP a computadoras.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	06/02/2022 – 08/02/2022
Evidencia y Descripción	

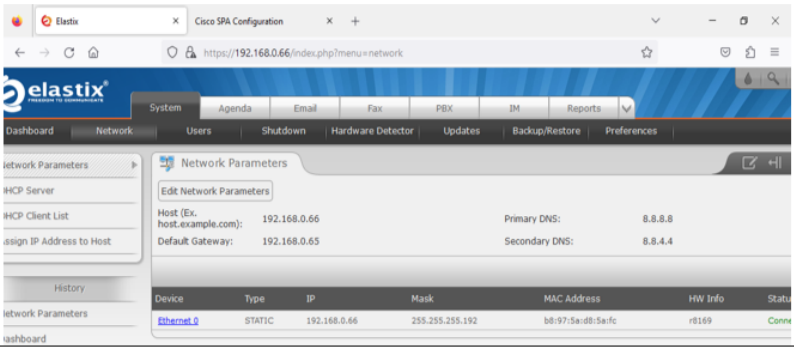
1. Para asignar una dirección IP a una computadora, en este caso marca "RICOH", nos dirigimos al apartado "centro de redes y recursos compartidos" del panel de control.
2. Después seleccionamos la conexión "Ethernet".



3. Se abrirá una ventada sobre el estado de la conexión Ethernet, a continuación

Entregable:	Correcciones en el servidor de VoIP
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	20/02/2022 – 24/02/2022
Evidencia y Descripción	

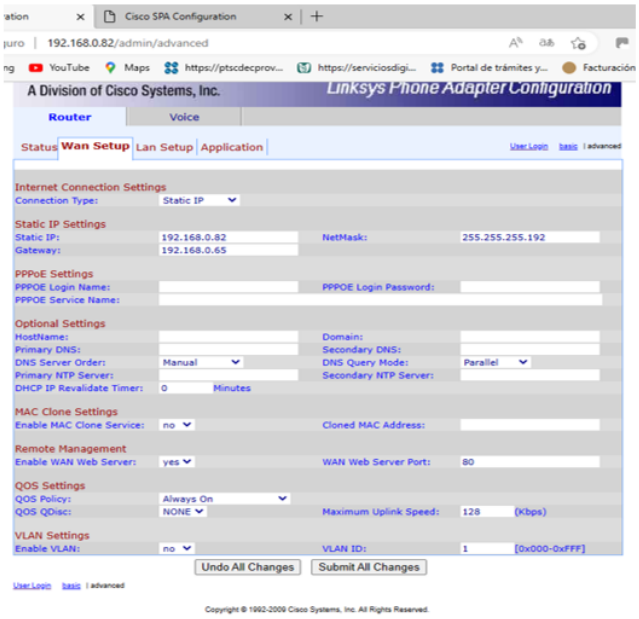
1. Para realizar los cambios se accedió a la interfaz gráfica de Elastik, a continuación, nos dirigimos a la opción network de la pestaña system.
2. Damos clic en el botón "edit network parameters" para hacer el cambio de direcciones IP.



3. Se realizaron los siguientes cambios:

Entregable:	Correcciones en los linksys de VoIP.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	20/02/2022 – 24/02/2022
Evidencia y Descripción	

1. De igual forma que con el servidor de VoIP, accedemos a la interfaz gráfica del linksys a modificar mediante su dirección IP.
2. Nos posicionamos en la opción wan setup de la pestaña router donde cambiamos la información de los campos en el apartado Static IP Settings.
   a. Static IP: 192.168.0.82
   b. Gateway: 192.168.0.65
   c. NetMask: 255.255.255.0
3. Aplicamos los cambios haciendo clic en el botón Submit All Changes.



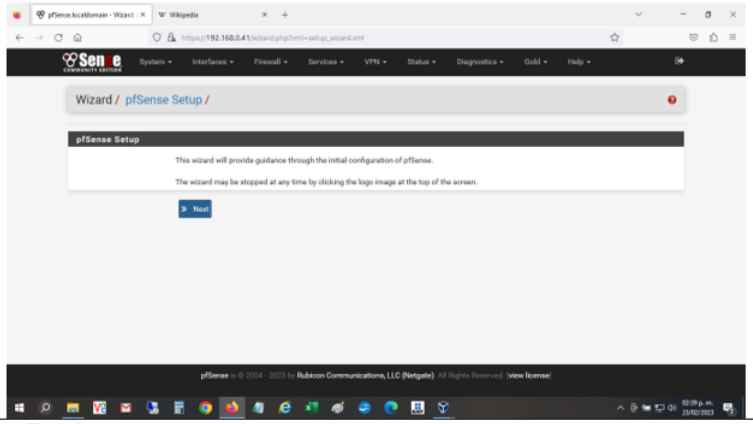
Entregable:	Correcciones en los teléfonos de VoIP.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	20/02/2022 – 24/02/2022
Evidencia y Descripción	

1. Para un teléfono de tipo Denwa se realizan los cambios de la siguiente forma:
2. Nos dirigimos a la pestaña "RED" y en los campos de ajustes WAN se actualiza lo siguiente; hacemos clic en aplicar:
   a. Dirección IP: 192.168.0.70
   b. Máscara de red: 255.255.255.192
   c. IP del Gateway: 192.168.0.65

3. Después, en la pestaña de VoIP se modifica solamente la dirección del servidor (192.168.0.66), hacemos clic en aplicar para finalizar.

Entregable:	Configuraciones iniciales de pfSense.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	23/02/2022 – 24/02/2022
Evidencia y Descripción	

1. Se nos mostrará un asistente de configuración, será visible solo la primera vez que accedamos a la interface del firewall.
2. En la bienvenida e información del soporte damos clic en next.

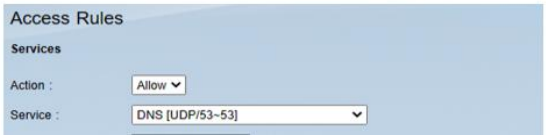


3. En información general introducimos lo siguiente:
   a. Hostname: el nombre de nuestro firewall.
   b. Domain: el nombre del dominio de la empresa.
   c. Primary DNS Server: 8.8.8.8

Entregable:	Implementación de las reglas de acceso.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	27/02/2022 – 27/02/2022
Evidencia y Descripción	

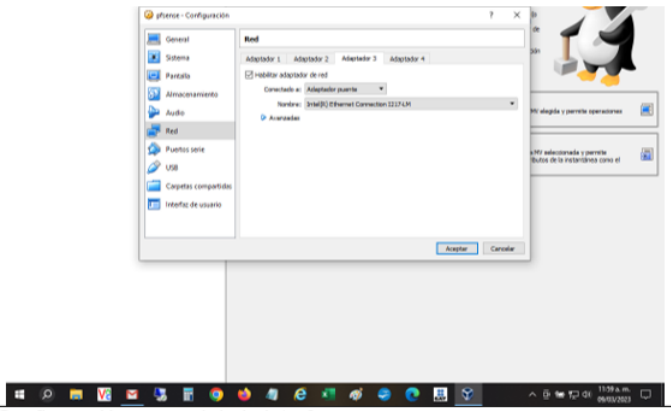
1. Accedemos al router RV042 por medio de un navegador web y nos dirigimos a la pestaña firewall, donde seleccionamos la opción “Access Rules”.

2. Para agregar una nueva regla, hacemos clic en “Add”.
3. En los campos de la ACL se refiere a lo siguiente:
   a. Action: La acción ya sea permitir o denegar sobre el tráfico de datos.
   b. Service: El tipo de protocolo y puerto de internet.
   c. Source interface: La interfaz de origen que se va a filtrar.
   d. Source IP: La red de origen o las direcciones IP que se van a filtrar.
   e. Destination IP: La red de destino o las direcciones IP que se van a filtrar.
   f. Scheduling: El tiempo/intervalo en que la regla estará en funcionamiento.



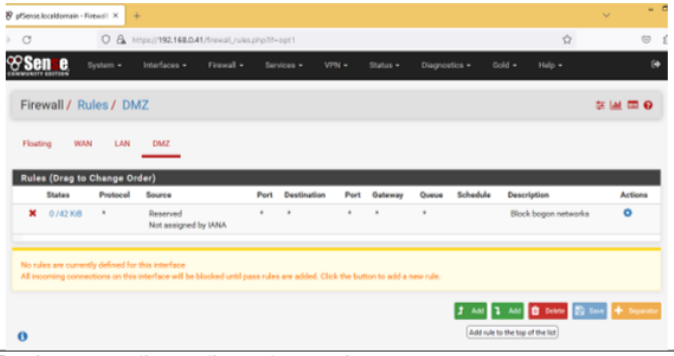
Entregable:	Activación de la interfaz DMZ.
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	06/02/2022 – 09/02/2022
Evidencia y Descripción	

1. Se crea una interfaz en nuestro firewall activando el adaptador 3 y se especifica lo siguiente en los campos faltantes:
    a. Attached to: Adaptador puente



Entregable:	Reglas de Firewall
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	06/02/2022 – 09/02/2022
Evidencia y Descripción	

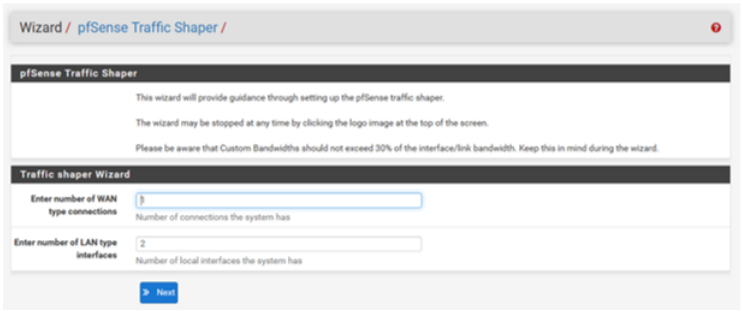
1. Nos dirigimos a la pestaña Firewall y hacemos clic en rules.
2. Abrimos la pestaña DMZ.
3. Para agregar reglas damos clic en el botón add (arriba).



4. En el campo action se tienen tres opciones:

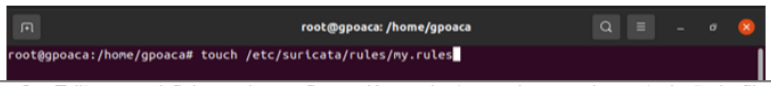
Entregable:	Priorización del tráfico
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	13/03/2022 – 14/03/2022
Evidencia y Descripción	

1. Nos dirigimos a la pestaña Firewall y en Traffic Shaper > Wizards, hacemos clic en Multiple Lan/Wan.
2. Indicamos lo siguiente:
   a. Number of WAN: 1
   b. Number of LAN: 2
   c. Hacemos clic en next.

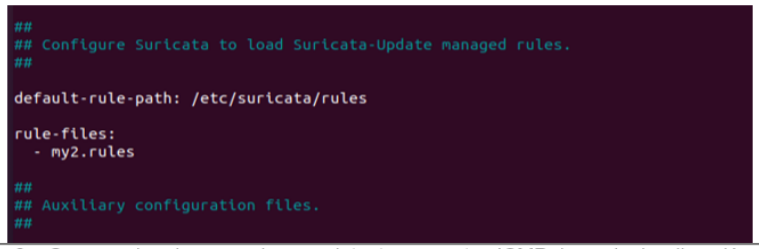


Entregable:	Configuración de reglas para el filtrado de suricata
Responsable	Estefhany Hernández Ortiz.
Fecha inicio y fin	27/03/2022 – 31/03/2022
Evidencia y Descripción	

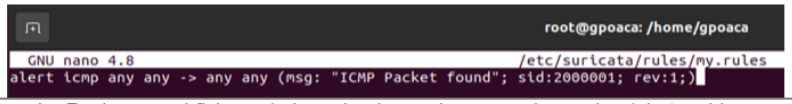
1. Creamos un archivo en la ruta "/etc/suricata/rules", con el siguiente comando:
   a. touch /etc/suricata/rules/my.rules



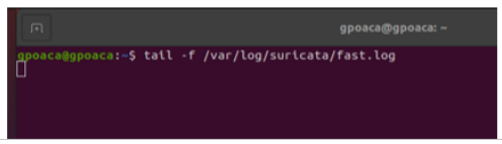
2. Editamos el fichero de configuración suricata.yaml y en el apartado "rule-files" modificamos como se muestra a continuación.



3. Creamos la primera regla para detectar paquetes ICMP de cualquier dirección de origen y destino a cualquier puerto, en el fichero "my.rules".
   a. Alert icmp any any -> any any (msg: "ICMP Packet found"; sid:2000001; rev:1;)



4. Revisamos el fichero de logs donde se almacenan las reglas (alertas, bloqueos, etc.) del servicio con el comando "tail -f /var/log/suricata/fast.log"
5. Reiniciamos el servicio con el comando "service suricata restart", para que se actualicen los cambios.



Reglas de control de acceso

1. Las redes que no son de administración ni gerencia solo deben tener acceso a internet, DNS y al servidor SIP, no a las demás redes.

Ip access-list extended FABRICA_ACA

Permit tcp 192.168.0.128 0.0.0.63 host 192.168.0.129 range 80 443

Permit tcp 192.168.0.128 0.0.0.63 host 192.168.0.129 eq 53

Permit tcp 192.168.0.128 0.0.0.63 host 192.168.0.66 eq 5060

Deny ip 192.168.0.128 0.0.0.63 192.168.0.0 0.0.0.63

Deny ip 192.168.0.128 0.0.0.63 192.168.0.64 0.0.0.63

Deny ip 192.168.0.128 0.0.0.63 192.168.0.192 0.0.0.63

permit ip 192.168.0.128 any

Interface g0/3

Ip access-group FABRICA_ACA in

Ip access-list extended TELEFONIA_ACA

Permit tcp 192.168.0.64 0.0.0.63 host 192.168.0.65 range 80 443

Permit tcp 192.168.0.64 0.0.0.63 host 192.168.0.65 eq 53

Permit tcp 192.168.0.64 0.0.0.63 host 192.168.0.66 eq 5060

Deny ip 192.168.0.64 0.0.0.63 192.168.0.0 0.0.0.63

Deny ip 192.168.0.64 0.0.0.63 192.168.0.128 0.0.0.63

Deny ip 192.168.0.64 0.0.0.63 192.168.0.192 0.0.0.63

Permit ip 192.168.0.64 any

Interface g0/2

Ip access-group TELEFONIA_ACA in

2. El área administrativa y gerencia 2 tienen acceso a internet, DNS, SIP, FTPS, RDP y a las demás subredes.

Ip access-list extended ADMINISTRATIVA_ACA

Permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.1 range 80 443

Permit udp 192.168.0.0 0.0.0.63 host 192.168.0.1 eq 53

Permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.66 eq 5060

Permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.2 eq 21

Permit tcp 192.168.0.0 0.0.0.63 host 192.168.0.7 eq 3389

permit ip 192.168.0.0 0.0.0.63 192.168.0.64 0.0.0.63

permit ip 192.168.0.0 0.0.0.63 192.168.0.128 0.0.0.63

permit ip 192.168.0.0 0.0.0.63 192.168.0.192 0.0.0.63

Permit ip 192.168.0.0 0.0.0.63 any

Interface g0/1

Ip access-group ADMINISTRATIVA_ACA in

3. El área de administración puede acceder a routers y las demás áreas no.

ip access-list standard ADMINISTRACION_SISTEMAS

permit 192.168.0.0 0.0.0.63

deny any

line vty 0 4

access-class ADMINISTRACION-SISTEMAS in

---configurar en vty---

REGLAS DE CONTROL DE ACCESO EN EL FIREWALL.

Interface DMZ:

- El tráfico de la DMZ hacia Internet (WAN) será permitido.
- El tráfico de la DMZ hacia la LAN será bloqueado.

Interface LAN:

- El tráfico del host 192.168.0.4 hacia la DMZ por TCP 22 será permitido.
- El tráfico de la LAN hacia la DMZ por UDP 5060,5061 será permitido.
- El tráfico de la LAN hacia la DMZ por TCP 80,443 será permitido.
- El tráfico de la LAN hacia la DMZ por UDP 53 será permitido.
- El tráfico de la LAN hacia la WAN será permitido.
- El tráfico de la LAN hacia la DMZ será bloqueado.

Interface WAN:

- El tráfico de la WAN hacia la DMZ por UDP 5060,5061 será permitido.
- El tráfico restante será bloqueado.

Segmentación de la red

INTRODUCCIÓN.

En el siguiente trabajo se lleva a cabo el proceso para obtener una segmentación o Subneteo en la red actual. Este método se define como la división en las direcciones de red completas en partes de menor tamaño; principalmente se emplean por los siguientes beneficios:

- Reducir el tamaño de los dominios de broadcast, creando pequeñas redes con menos tráfico.
- Permitir que las LAN en distintas ubicaciones geográficas se comuniquen a través de los routers.
- Proporcionar seguridad mejorada separando una LAN de otra.

OBJETIVO.

Realizar una segmentación en la red corporativa de la empresa Avicultores Cordobeses Asociados, haciendo uso del Subneteo como método para obtener una mejor administración en las direcciones IP y una mejor calidad en los servicios de la red.

SEGMENTACIÓN DE LOS SERVICIOS EN LA RED A TRAVÉS DE SUBNETTING.

Clase de red:

La red empresarial actualmente cuenta con una clase c (indicada por el prefijo /24).

Submáscara de red actual:

La submascara de red actual es: 255.255.255.0 (un total de 24 bits encendidas).

Número de host por cada red:

Se pretende obtener subredes que abarquen alrededor de 60 host por cada una.

Proceso de obtención:

$$2^x - 2 \geq 60\ (host)$$

$$2^x \geq 60 + 2$$

$$2^x \geq 62$$

$$x = 6\ (bits\ apagados)$$

Submáscara de red nueva:

De acuerdo al calculo anterior y tomando en cuenta que el límite de bits son 32, se determina que la nueva submáscara contara con un prefijo /26, por lo tanto, la nueva submáscara es: 255.255.255.192

Tamaño de bloque:

Para obtener el tamaño de bloque se deben restar a el ultimo octeto de la nueva submáscara (192), el número 256.

$$TB = 256 - 192$$

$$TB = 64$$

TABLA DE DIRECCIONAMIENTO.

#	Dirección de red	Prefijo	Submáscara	1ra IP	Última IP	Broadcast
1	192.168.0.0	/26	255.255.255.192	192.168.0.1	192.168.0.62	192.168.0.63
2	192.168.0.64	/26	255.255.255.192	192.168.0.65	192.168.0.126	192.168.0.127
3	192.168.0.128	/26	255.255.255.192	192.168.0.129	192.168.0.190	192.168.0.191
4	192.168.0.192	/26	255.255.255.192	192.168.0.193	192.168.0.254	192.168.0.255

Tabla de direccionamiento

TABLA DE DIRECCIONAMIENTO DE LA PRIMERA SUBRED (ADMINISTRATIVA):

#	Dirección IP	Submáscara	Usuario	Puesto	
1	192.168.0.1	255.255.255.192	Router		
2	192.168.0.2	255.255.255.192	Servidor de Archivos		
3	192.168.0.3	255.255.255.192			
4	192.168.0.4	255.255.255.192	Ruperto Peralta		
5	192.168.0.5	255.255.255.192			
6	192.168.0.6	255.255.255.192	Recepción Teresa		
7	192.168.0.7	255.255.255.192	Escritorio remoto		
8	192.168.0.8	255.255.255.192			
9	192.168.0.9	255.255.255.192	Impresora oficina		
10	192.168.0.10	255.255.255.192			
11	192.168.0.11	255.255.255.192	Lizbeth Trujillo	Contadora	
12	192.168.0.12	255.255.255.192	María de los Ángeles	Facturación	
13	192.168.0.13	255.255.255.192	María Yolanda Sánchez	Compras (alimentos)	
14	192.168.0.14	255.255.255.192	Nicolas Vázquez	Jefe Recursos humanos	
15	192.168.0.15	255.255.255.192	Teodoro Cortez	Contador	
16	192.168.0.16	255.255.255.0			
17	192.168.0.17	255.255.255.192	Reyna Román	Auxiliar contable	
18	192.168.0.18	255.255.255.0			
19	192.168.0.19	255.255.255.0			
20	192.168.0.20	255.255.255.192	Juan Miguel Luna	Comercialización	
21	192.168.0.21	255.255.255.0			
22	192.168.0.22	255.255.255.192	Yadira Román	Auxiliar contable	
23	192.168.0.23	255.255.255.192		Incubadora	
24	192.168.0.24	255.255.255.192			
25	192.168.0.25	255.255.255.0			
26	192.168.0.26	255.255.255.0			

TABLA DE DIRECCIONAMIENTO DE LA SEGUNDA SUBRED (TELEFONIA):

#	Dirección IP	Submáscara	Usuario	Puesto	Extensión	
1	192.168.0.65	255.255.255.192	Router			
2	192.168.0.66	255.255.255.192	Servidor VoIP			
3	192.168.0.67	255.255.255.192	Ruperto Peralta	Sistemas	101	
4	192.168.0.68	255.255.255.192	Jaime Crivelli	-	102	
5	192.168.0.69	255.255.255.192	Claudina Crivelli	Directora	103	
6	192.168.0.70	255.255.255.192	Teodoro Cortez	Contador General	109	
7	192.168.0.71	255.255.255.192	Recepción		111	
8	192.168.0.72	255.255.255.192	Elizabeth Morales	Caja	113	
9	192.168.0.73	255.255.255.192	Nicolas Vazquez	Recursos Humanos	116	
10	192.168.0.74	255.255.255.192	Yolanda Sanchez		119	
11	192.168.0.75	255.255.255.192	Nestor	Fabrica	205	
12	192.168.0.76	255.255.255.192	Armando Morales	Gerente	222	
13	192.168.0.77	255.255.255.192	Gely Ortiz	Facturación	229	
14	192.168.0.78	255.255.255.192	Miguel Luna	Ventas	231	
15	192.168.0.79	255.255.255.192	Miriam	Incubadora	233	
16	192.168.0.80	255.255.255.192	Lizbette	Contadora	118	
17	192.168.0.81	255.255.255.192	Deposito San Manuel		160	
18	192.168.0.82	255.255.255.192	Linksys Voip		155	
19	192.168.0.83	255.255.255.192	Linksys Voip		106	
20	192.168.0.84	255.255.255.192	Vigilancia		221	
21	192.168.0.85	255.255.255.192				
22	192.168.0.86	255.255.255.192				
23	192.168.0.87	255.255.255.192				
24	192.168.0.88	255.255.255.192				
25	192.168.0.89	255.255.255.192				
26	192.168.0.90	255.255.255.192				

TABLA DE DIRECCIONAMIENTO DE LA TERCERA SUBRED (FABRICA):

#	Dirección IP	Submáscara	Usuario	Puesto	Extensión	
1	192.168.0.129	255.255.255.192	Router			
2	192.168.0.130	255.255.255.192	Arnold Gomez Tapia	Jefe Producción		
3	192.168.0.131	255.255.255.192	Ciro Rafael Hernández	Encargado		
4	192.168.0.132	255.255.255.192	Roberto Valdivia	Dosificador		
5	192.168.0.133	255.255.255.192	Impresora			
6	192.168.0.134	255.255.255.192				
7	192.168.0.135	255.255.255.192				
8	192.168.0.136	255.255.255.192				
9	192.168.0.137	255.255.255.192				
10	192.168.0.138	255.255.255.192				
11	192.168.0.139	255.255.255.192				
12	192.168.0.140	255.255.255.192				
13	192.168.0.141	255.255.255.192				
14	192.168.0.142	255.255.255.192				
15	192.168.0.143	255.255.255.192				
16	192.168.0.144	255.255.255.192				
17	192.168.0.145	255.255.255.192				
18	192.168.0.146	255.255.255.192				
19	192.168.0.147	255.255.255.192				
20	192.168.0.148	255.255.255.192				
21	192.168.0.149	255.255.255.192				
22	192.168.0.150	255.255.255.192				
23	192.168.0.151	255.255.255.192				
24	192.168.0.152	255.255.255.192				
25	192.168.0.153	255.255.255.192				
26	192.168.0.154	255.255.255.192				

UNIVERSIDAD TECNOLÓGICA DEL CENTRO DE VERACRUZ

Bibliografía

[1] B. H. Pitancur Fernández, "Diseño e implementación de una red de datos y seguridad perimetral de la empresa corporación cayman s.a.c.", Tesis de licenciatura, Universidad Tecnológica del Perú, Lima, 2019. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5933/B.Pitancur_Programa_Especial_Titulacion_Titulo_Profesional_2019.pdf?sequence=1&isAllowed=y

[2] K. E. Ruiz Vieira, "Implementación de una solución de seguridad perimetral open source en la red telemática de la universidad nacional pedro ruiz gallo", Tesis de licenciatura, Universidad de Lambayeque, Chiclayo, 2018. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repositorio.udl.edu.pe/bitstream/UDL/122/3/UNIVERSIDAD-DE-LAMBAYEQUE.pdf

[3] J. B. Carrera Trujillo, "Diseño e implementación de una red de datos con seguridad perimetral para una empresa que se dedica al servicio de taxi ejecutivo.", Tesis de licenciatura, Universidad de Guayaquil, Guayaquil, 2019. Accedido el 14 de febrero de 2023. [En línea]. Disponible: http://repositorio.ug.edu.ec/bitstream/redug/45012/1/B-CINT-PTG-N.457%20Carrera%20Trujillo%20Jeannelys%20%20Belén%20.%20Sánchez%20Robalino%20Michael%20Guillermo.pdf

[4] L. J. Noriega Vides, "Implementación de una red perimetral, sitio web y servidor ftp para la comunidad networkbogotá", Tesis de licenciatura, Universidad Cooperativa de Colombia, Bogotá, 2020. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repository.ucc.edu.co/server/api/core/bitstreams/ff3b1e97-ab12-4115-ac80-bb001dcce325/content

[5] J. Tello, "Implementación de un sistema de seguridad perimetral, basado en el modelo safe de cisco para la gestión de la infraestructura de redes y comunicaciones en la empresa agrofrutos trading S.A.", Tesis de licenciatura, Universidad César Vallejo, Piura, 2021. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/92548/Justiniano_TEAP-SD.pdf?sequence=1&isAllowed=y

[6] J. J. Marín Valencia, A. Patiño Valencia y J. C. Acevedo Bedoya, "Implementación de un sistema de seguridad perimetral informático usando vpn, firewall e ids", *Revista Universidad Católica de Oriente*, vol. 31, n.º 45,

pp. 84–99, 2020. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://revistas.uco.edu.co/index.php/uco/article/view/284/370

[7] F. Y. Cabrera Vásquez, "Diseño de una red de seguridad perimetral basada en open source para aplicación de ids e ips para el control de amenazas informáticas en la universidad técnica de Babahoyo", Tesis de licenciatura, Universidad Técnica de Babahoyo, Babahoyo, 2022. Accedido el 14 de febrero de 2023. [En línea]. Disponible: http://dspace.utb.edu.ec/bitstream/handle/49000/13035/E-UTB-FAFI-SIST-000377.pdf?sequence=1&isAllowed=y

[8] F. Morales, S. Toapanta y R. M. Toasa, "Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información", *Revista Ibérica de Sist. y Tecnologías de Información*, n.º 27, pp. 553–565, 2020. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://www.researchgate.net/profile/Renato-Mauricio-Toasa-G/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad-perimetral-como-estrategia-de-seguridad-de-la-informacion.pdf

[9] L. A. Rivera Morla, "Red privada remota montada en raspberry PI para la gestión segura de los recursos informáticos entre las oficinas de builderecuador CIA.LTDA", Tesis de licenciatura, Universidad Ecotec, Samborondón, 2022. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repositorio.ecotec.edu.ec/bitstream/123456789/497/1/Rivera,%20Luis.pdf

[10] B. G. Borja Piñeiro, "Análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red para la comunicación segura sitio a sitio entre las PYMES", Tesis de licenciatura, Pontificia Universidad Católica del Ecuador, Esmeraldas, 2021. Accedido el 14 de febrero de 2023. [En línea]. Disponible: https://repositorio.pucese.edu.ec/bitstream/123456789/3314/1/Borja%20Piñeiro%20Brayan%20Guillermo.pdf

[11] Puerto Rico AREDN. Como configurar su teléfono Cisco SPA para SIP (PBX). (11 de diciembre de 2020). Accedido el 14 de febrero de 2023. [Video en línea]. Disponible: https://www.youtube.com/watch?v=3e6kE6BQpE4

[12] Jordi Baucells Rodríguez. Instalar Y Configurar Red VPN Con OpenVPN en Windows Server 2019. (12 de agosto de 2020). Accedido el 14 de febrero de 2023. [Video en línea]. Disponible: https://www.youtube.com/watch?v=Okhr9wGsyT4

[13] B. A. García Martínez, "Análisis de la implementación de listas de control de acceso (ACL), para mejorar la seguridad de la información en

la empresa Crawford Colombia LTDA", Trabajo de grado, Universidad Católica de Colombia, Bogotá, 2021. Accedido el 14 de febrero de 2023. [En línea].
Disponible: https://repository.ucatolica.edu.co/server/api/core/bitstreams/f208fdd1-3b01-4fa6-971e-84dd181edd24/content