UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN TELECOMUNICACIONES

Tema: PLATAFORMA DE SEGURIDAD PERIMETRAL PARA UN ISP (PROVEEDOR DE SERVICIOS DE INTERNET).

Trabajo de titulación previo a la obtención del Grado Académico de Magister en Telecomunicaciones

Modalidad de Titulación: Proyecto de Desarrollo

Autor: Ingeniera Gladys Cristina Yacchirema Lumbi.

Director: Ingeniero David Omar Guevara Aulestia, Mg.

Ambato-Ecuador

2021

APROBACIÓN DEL TRABAJO DE TITULACIÓN

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor de la defensa Trabajo de Titulación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia, Magíster, e integrado por los señores Ingeniero Rubén Eduardo Nogales Portero Magíster e Ingeniero Víctor Santiago Manzano Villafuerte Magíster, designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "PLATAFORMA DE SEGURIDAD PERIMETRAL PARA UN ISP (PROVEEDOR DE SERVICIOS DE INTERNET)", elaborado y presentado por la señorita Ingeniera Gladys Cristina Yacchirema Lumbi, para optar por el Grado Académico de Magíster en Telecomunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la Universidad Técnica de Ambato.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Elsa Pilar Urrutia Urrutia Mg.

Presidente y Miembro del Tribunal de Defensa

Firmado electrónicamente por:
RUBEN EDUARDO NOGALES PORTERO

Ing. Rubén Eduardo Nogales Portero, Mg.

Miembro del Tribunal de Defensa

Firmado electrónicamente por:
VICTOR SANTIAGO MANZANO VILLAFUERTE

Ing. Víctor Santiago Manzano Villafuerte, Mg.

Miembro del Tribunal de Defensa

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación con el tema: “PLATAFORMA DE SEGURIDAD PERIMETRAL PARA UN ISP (PROVEEDOR DE SERVICIOS DE INTERNET)”, le corresponde exclusivamente a la: Ingeniera Gladys Cristina Yacchirema Lumbi, Autor bajo la Dirección del Ingeniero David Omar Guevara Aulestia, Magister, Director del Trabajo de Titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Firmado electrónicamente por:
GLADYS CRISTINA YACCHIREMA LUMBI

Ing. Gladys Cristina Yacchirema Lumbi

AUTORA

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia, Mg.

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Firmado electrónicamente por:
GLADYS CRISTINA YACCHIREMA LUMBI

Ing. Gladys Cristina Yacchirema Lumbi

c.c. 0201886579

ÍNDICE GENERAL

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

En primer lugar, quiero agradecer a mi director de tesis, Ing. David Guevara, gracias a su guía y dedicación pudimos sacar adelante este proyecto para su pronta culminación.

Mis agradecimientos también van al Ing. Luis Estévez, Gerente Técnico de Simantec, por la apertura y estima que tuvo hacia mí durante la elaboración del proyecto de investigación, su colaboración e interés sumaron para poder hacer un proyecto de calidad y relevancia para la empresa.

Por último, quiero agradecer a dos grandes amigos y colegas, Franklin y Gonzalo, juntos compartimos no solo el pregrado sino también esta maestría y solo nosotros sabemos lo difícil pero gratificante que fue alcanzar este logro profesional. Gracias amigos por los gratos momentos y de los malos, pues aprendimos de ellos.

Cristina

DEDICATORIA

Cada logro alcanzado en mi vida ha sido gracias a tres mujeres especiales e increíbles para mí.

La primera de ellas es mi madre, Beatriz, una mujer luchadora y ejemplar que supo hacer de mí una mujer de bien, lo que soy es gracias a ella, con su amor y apoyo constante he podido superar cada obstáculo que se ha presentado en mi camino.

Mis hermanas Fernanda y Shirley son los mejores regalos que me dieron mis padres, ellas complementan y alegran mi vida con sus ocurrencias, risas y locura, hacen de cada momento único y llevadero. Gracias por ser incondicionales para mí.

También dedico este trabajo a una persona que por cosas del destino no está entre nosotras, mi padre Luis Enrique. Sé que estás tan orgulloso de mí y me dirías que siempre debo ser lo mejor de lo mejor y aunque pase el tiempo siempre te llevaré en mi mente y en mi corazón. Te extrañamos tanto pero mi madre supo hacer un buen trabajo.

Gracias por ayudarme a cumplir esta meta, sin ustedes nada de esto sería realidad. Las amo con mi vida.

Cristina

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
MAESTRÍA EN TELECOMUNICACIONES

TEMA:

PLATAFORMA DE SEGURIDAD PERIMETRAL PARA UN ISP (PROVEEDOR DE SERVICIOS DE INTERNET).

AUTOR: Ingeniera Gladys Cristina Yacchirema Lumbi.
DIRECTOR: Ingeniero David Omar Guevara Aulestia, Magister.
LÍNEA DE INVESTIGACIÓN: Tecnologías, Seguridad y Gestión de Redes de Comunicaciones.
FECHA: 28 de octubre de 2021

RESUMEN EJECUTIVO

Hoy en día la seguridad informática juega un rol importante en todos los sectores de la sociedad empezando por organismos gubernamentales, entidades educativas, financieras, casas de salud y por supuestos las empresas; el compromiso y la responsabilidad de cada una de ellas es salvaguardar sus datos e información de las personas lo que conlleva a emplear plataformas que permita gestionar de manera eficiente las amenazas que intentan vulnerar la seguridad en una red.

Este proyecto de investigación tiene como fin implementar una plataforma de seguridad perimetral para la empresa Simantec, debido al giro de negocio de la empresa y el flujo de información que maneja, un sistema de seguridad perimetral cubre las necesidades y requerimientos que demanda esta entidad, siendo la mayor prioridad la protección de todos los datos considerados el activo más importante de la entidad. La implementación de un UTM propietario (Gestor Unificado de Amenazas) en el límite de la salida a internet y la red LAN permitirá mitigar las amenazas a la cual se encuentran expuestos los datos, funciones como antivirus, anti-spyware, anti-spam, firewall de red, prevención y

detección de intrusiones y filtrado de contenido maximizará la seguridad de la información. Además, la creación de VPN para ingresar a la red interna desde cualquier lugar y acceder a los servicios que posee la empresa incrementará la seguridad. A la par se configurará otro equipo de defensa, un UTM software con las mismas funciones del UTM propietario, el objetivo es comparar los dos gestores de amenazas, analizar las ventajas y desventajas de cada uno para elegir la mejor opción considerando costo/beneficio, características, rendimiento, seguridad y sobre todo rentabilidad. Finalmente, se propone la elaboración de un plan de buenas prácticas de seguridad, con el objetivo de que los empleados incorporen como hábito determinados métodos que permitan prevenir los ataques realizados a través de actividades maliciosas por terceras personas.

Descriptores: Seguridad perimetral, gestión unificada de amenazas, vulnerabilidades, ataques informáticos, proveedor de servicios de internet, red empresarial, UTM propietario, UTM software, buenas prácticas de seguridad informática, protección de datos.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN TELECOMUNICACIONES

THEME:

PERIMETER SECURITY PLATFORM FOR AN ISP (INTERNET SERVICE PROVIDER).

AUTHOR: Ingeniera Gladys Cristina Yacchirema Lumbi.

DIRECTED BY: Ingeniero David Omar Guevara Aulestia, Mg**.**

LINE OF RESEARCH: Technologies, Security and Management of Communications Networks.

DATE: October 28th, 2021

EXECUTIVE SUMMARY

Today computer security plays an important role in all sectors of society starting with government agencies, educational institutions, financial institutions, health centers and of course companies; the commitment and responsibility of each of them is to safeguard their data and information of people which leads to use platforms to efficiently manage the threats that try to breach the security of a network.

This research project aims to implement a perimeter security platform for the company Simantec, due to the business line of the company and the flow of information it handles, a perimeter security system covers the needs and requirements demanded by this entity, being the highest priority the protection of all data considered the most important asset of the entity. The implementation of a proprietary UTM (Unified Threat Manager) at the boundary of the Internet and LAN will mitigate the threats to which the data is exposed, functions such as antivirus, anti-spyware, anti-spam, network firewall, intrusion prevention and detection, and content filtering will maximize the security of the information. In addition, the creation of VPN to access the internal network from

anywhere and access the company's services will increase security. At the same time, another defense equipment will be configured, a software UTM with the same functions of the proprietary UTM. The objective is to compare the two threat managers, analyze the advantages and disadvantages of each one in order to choose the best option considering cost/benefit, features, performance, security and above all profitability. Finally, we propose the development of a plan of good security practices, with the aim that employees incorporate as a habit certain methods to prevent attacks carried out through malicious activities by third persons.

Keywords: Perimeter security, unified threat management, vulnerabilities, computer attacks, internet service provider, enterprise network, proprietary UTM, software UTM, good computer security practices, data protection.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

La seguridad de la información es una pieza fundamental dentro de una organización para que pueda desarrollar sus actividades sin asumir demasiados riesgos, a sabiendas de que los datos son esenciales para que un negocio siga realizando sus operaciones. Según la Organización de Naciones Unidas (ONU) las pequeñas y medianas empresas también conocidas como Pymes representan el 50 % del PIB a nivel mundial, generan entre el 60 % y el 70 % del empleo en un país y son consideradas como "la espina dorsal de la mayoría de las economías del mundo" [1]. Estas empresas generan ingresos importantes, fuentes de empleo, contribuyen a la reducción de la pobreza y fomentan el desarrollo especialmente de los sectores más vulnerables de la sociedad. Las Pymes han demostrado la capacidad de adaptación a los cambios que se vive en el mundo de hoy, sin embargo, uno de las principales limitantes es la falta de financiamiento que impide que estas empresas inviertan en su infraestructura física y digital.

Al hablar de la estructura digital de una empresa, especialmente en el campo de la seguridad informática, Stefan Deutscher líder mundial de BCG en Ciberseguridad y consejero líder del Foro Económico Mundial (WEF), señaló que "Todas las industrias y sectores se han convertido en blanco de ataques y Latinoamérica no es la excepción. En los últimos cinco años instituciones estatales y grandes empresas han sido víctimas de ataques phishing y hackeos en países como Chile, Argentina, Colombia y Perú". El valor promedio por cada ciberataque a nivel mundial es de US$11 millones, y el 72 % de las infracciones son por fallas humanas. El ciberataque es el 2° mayor riesgo global no climático o migratorio por consiguiente las Pymes son altamente vulnerables [2].

En Ecuador las Mipymes representan el 99 % de negocios e independientemente del producto que ofrezcan la innovación en tecnología es el talón de Aquiles de muchas de ellas y no van acorde a los cambios tecnológicos, es ahí donde se enfrentan ante graves eventualidades [3]. En la actualidad las Pymes representan la mayor fuerza económica del país, los rápidos cambios en la tecnología representan retos para seguir creciendo y

asegurar su permanencia en el mercado por ende la responsabilidad de proteger su información digital se ha convertido en un aspecto de suma importancia. Las pequeñas y medianas empresas han tomado conciencia de que sus sistemas son vulnerables a ataques en cualquier momento ya sea desde el interior o fuera de sus instalaciones y se ha comprobado que los riesgos internos provienen de los mismos empleados que por desconocimiento o malicia ocasionan situaciones que llevan a la filtración de datos. Por ejemplo, la técnica más empleada por los ciberdelincuentes es el phishing, crean páginas web falsas para engañar al usuario y suplantar su identidad abriendo la puerta a ataques internos. Digital Guardian asegura que el 97 % de los ataques informáticos no aprovechan una falla en el software, sino que usan técnicas de ingeniería social para conseguir las credenciales necesarias y así vulnerar la seguridad informática [4].

El siguiente trabajo de investigación titulado "PLATAFORMA DE SEGURIDAD PERIMETRAL PARA UN ISP (PROVEEDOR DE SERVICIOS DE INTERNET)" fue llevado a cabo con la finalidad de solventar falencias que tenía la empresa en cuanto a seguridad informática. En los siguientes capítulos se resume el proceso empleado para implementar la plataforma de seguridad.

En el Capítulo I se muestra el problema de investigación y se señala a través de datos estadísticos los índices de inseguridad informática que tienen las medianas y pequeñas empresas a nivel mundial, regional y territorial. De esta manera se pone en contexto los motivos y las aspiraciones al ejecutar este trabajo de investigación en el ISP, priorizando en todo momento la seguridad de los datos que son el bien más importante de la empresa.

En el Capítulo II se presenta trabajos previos que guardan relación con el trabajo propuesto en esta investigación para adquirir los conocimientos necesarios y alcanzar los objetivos planteados.

En el Capítulo III se señala el enfoque, modalidad, tipo de investigación y se indica la población y muestra sobre la cual se va a trabajar. Además, se muestra como se hará la recolección de toda la información obtenida en el trabajo de investigación.

En el Capítulo IV se analiza e interpreta los datos obtenidos al implementar tanto el UTM propietario o software y se demuestran que plataforma de seguridad perimetral tiene más incidencia en la seguridad informática del ISP.

En el Capítulo V se detallan las conclusiones a las que se llegó al terminar el trabajo de investigación también se indica una serie de recomendaciones que se pueden considerar para mejorar trabajos futuros relacionados con este tema.

1.2. Justificación

Simantec es una empresa que brinda el servicio de Internet a sus abonados a través de tecnologías como Fibra Óptica y WiMax; a lo largo de los años se ha ido expandiendo y junto a ella también creció su infraestructura, servicios y sistemas, pero sobre todo su base de datos ha sufrido una serie de cambios como actualizaciones y mejoras en beneficio de la empresa, empleados y clientes. A principios del año 2019 la empresa sufrió un ataque cibernético en uno de sus servidores de facturación, ocasionando pérdida de información y retraso en el área contable. La información no pudo ser recuperada pero este suceso hizo plantearse el hecho de que la seguridad entre la red interna de la empresa y el mundo del Internet es un punto crítico en la arquitectura empresarial. Por tal motivo se debe tomar medidas correctivas y preventivas para evitar este tipo de inconvenientes y sobre todo se debe plantear políticas y estrategias de protección confiables y eficientes.

Ahí recae la importancia de implementar un sistema que brinde la protección y seguridad necesaria a los datos de la empresa, los ataques a una red empresarial no solo provocan la pérdida de información sino también de recursos económicos e implica invertir más tiempo, dinero y personal para solventar esta situación. Sin embargo, estas tecnologías suelen ser caras y complejas y muchos negocios no pueden plantearse la idea de implementar una infraestructura avanzada contra amenazas, la empresa requiere una solución fácil de probar y desplegar que garantice el control de accesos y protección de los datos para evitar la vulnerabilidad en la información. Las soluciones UTM permiten englobar las funciones tradicionales de un firewall en un único dispositivo sea físico o virtual brindando servicios como antivirus, anti-spam, VPN, filtro de contenidos, balanceo de carga, prevención de fuga de datos, panel de informes de seguridad, etc.

De continuar con una red poco protegida ante ataques informáticos los datos de la empresa tienen un alta probabilidad de ser vulnerados, situación que pone en riesgo el porvenir de la entidad. Otro aspecto relevante a considerar es hacer que los empleados tomen conciencia y responsabilidad sobre la importancia de tomar medidas de seguridad al momento de manipular la información, una de las principales puertas de entrada que tienen los delincuentes informáticos para vulnerar la seguridad es atacar a través de fallas o errores humanos. Es ahí en donde recae la importancia de adoptar medidas y protocolos de seguridad con el fin de salvaguardar el bien más importante de la organización, los datos.

Este trabajo propuesto busca brindar un aporte significativo a la protección de la red interna de la empresa reduciendo los ataques que vulnere la información, esta medida beneficiará a la empresa, así como a sus empleados y clientes. Actualmente la empresa no dispone de una plataforma de seguridad robusta y eficiente por lo que la implementación de este sistema representa un impacto positivo en cuanto al resguardo de la información de todas sus áreas. El proyecto es factible porque cuenta con el apoyo económico y logístico de Gerencia Administrativa y Gerencia Técnica además el investigador cuenta con las herramientas y conocimientos necesarios para alcanzar los objetivos planteados.

1.3. Objetivos

1.3.1. General

Implementar una plataforma de seguridad perimetral en la empresa de internet “Simantec”.

1.3.2. Específicos

- Realizar un análisis de riesgos a la seguridad informática de la empresa para evaluar las amenazas potenciales a la que está expuesta la red empresarial.
- Configurar un UTM propietario y OpenSource en la red empresarial para establecer el mejor acorde a las necesidades de la empresa.
- Realizar un estudio comparativo entre los dos sistemas UTM para determinar el mejor rendimiento, potencial y rentabilidad.

- Elaborar un plan de buenas prácticas de seguridad dentro de la empresa para que el personal técnico y administrativo de la empresa adopte mecanismos de prevención ante acciones maliciosas.

CAPÍTULO II

ANTECEDENTES INVESTIGATIVOS

2.1. Estado del arte

Encalada Carlos en [5] realizado en Cuenca, Ecuador, estudia nuevas herramientas orientadas a la seguridad informática con el objetivo de elaborar un plan de renovación tecnológico y políticas de seguridad para reducir o eliminar los riesgos a los que está expuesta la red de datos de la Unidad Académica de Ingeniería de Sistemas y Eléctrica. El análisis de vulnerabilidades y evaluación de riesgos son los aspectos valorados para plantear el rediseño de la red que se ajusten a los requerimientos de la Unidad Académica. El nuevo sistema de defensa contó políticas de seguridad para usuarios internos y externos, empleó herramientas como los sistemas IDS (Intrusion Detection System) y adoptó una topología de red tipo DMZ (Demilitarized Zone). Sin embargo, en la investigación no se especifica el tipo de solución empleada ya sea hardware y software, por ende la elección se debe hacer previo un estudio comparativo entre los dos sistemas.

Flórez etc al. en [6] realizado en Colombia, proponen implementar una solución de seguridad informática que permita integrar funcionalidades como firewall, antivirus y control de contenidos en un solo UTM (Unified Threat Management) con el objetivo de contrarrestar los diferentes tipos de ataques y amenazas. Para lo cual se analiza los riesgos más comunes a los que las empresas están expuestas como ataques de denegación de servicio, riesgos por control de acceso y ejecución de malware. UTM pfSense es el software empleado para potenciar la seguridad, la instalación es rápida y sencilla y posee módulos como asistente de instalación, servidor proxy, reglas de firewall, control de acceso, bloqueo de páginas y reportes con estadísticas. Un aspecto importante que no se menciona son las características físicas que debe tener el hardware que va a hospedar al UTM software, estas cualidades deben ser evaluadas por el administrador de redes para que el equipo instalado cubra a corto y largo plazo las necesidades de la empresa.

Moreno Yamil en [7] realizado en Colombia, analiza esta tecnología para brindar a los interesados información sobre la aplicación y funcionalidad de un UTM en el mundo de

la seguridad informática. Es así como en su artículo expone algunas características siendo el equilibrio de carga un servicio fundamental que permite a los administradores de redes utilizar todos los servicios ofrecidos por un UTM. Dentro de las soluciones UTM existe protección antivirus, troyanos, spyware, adware, ataques DoS (Denial of Service), spam, filtrado de paquetes, protección contra el día cero. En la actualidad los UTM permiten aplicar y otorgar niveles de seguridad por usuario, controlar amenazas en tiempo real, agilizar ciclos de auditoría o controlar la fuga de datos. Otro aspecto que no se menciona son las diferentes marcas existentes en el mercado que ofrecen soluciones tanto de hardware y software, así como los aspectos a considerar para elegir el equipo más adecuado según las necesidades de cliente.

Vinit Agham en [8] realizado en la India, muestra las ventajas de emplear un UTM, como su nombre lo indica gestiona las amenazas unificando en una solución de seguridad integral. Entre las ventajas se destaca la reducción de la complejidad, fácil instalación, gestión remota donde se requiere una baja interacción con el operador, fácil solución de problemas. Sin embargo, antes de adquirir una tecnología UTM se debe analizar la red actual para identificar que recursos se debe implementar ya sea cortafuegos, filtro anti spam, filtrado URL e IDS/IPS. En conclusión, la Gestión Unificada de Amenazas representa una nueva era dentro de la seguridad de TI, la capacidad de estas tecnologías de seguridad al ser integradas ha demostrado ser eficientes para asegurar las redes comerciales con la capacidad de ser extensibles, pero no se menciona que a mayor capacidad y número de paquetes de seguridad que contengan estos sistemas el costo es más elevado limitando la adquisición por las entidades interesadas, si a esto se suma la licencia anual que se debe pagar en el caso del UTM propietario.

Kumar, D. y Gupta, M. en [9] realizado en la India, analizan los problemas de seguridad de red y las amenazas que están aumentando día a día. Para resolver este problema se plantean como solución la implementación de cortafuegos e IDS usando el software de código abierto pfSense. Esta distribución luego de ser instalada muestra una interfaz web amigable para la configuración de todos los componentes y servicios sin la necesidad de tener conocimientos en UNIX, utilizar comandos o editar manualmente cualquier conjunto de reglas. PfSense es una plataforma emergente cuya instalación y configuración

es simple y rentable. Es recomendable para las pequeñas y medianas empresas, ya que ofrece una amplia lista de servicios, mantiene la integridad y la seguridad de la red a un bajo costo. Si bien señala que el costo de la implementación de este tipo de soluciones es sumamente bajo no menciona que para una red que transmite gran cantidad de información el equipo hardware que hospedará al software pfSense debe ser robusto con características superiores a un computador convencional.

2.2. Marco Teórico

2.2.1. Seguridad de la Información

La seguridad de la información busca proteger los datos o minimizar en lo posible los riesgos informáticos a los que están expuestos los activos de una empresa. En la actualidad los sistemas informáticos son vulnerables y pueden sufrir ataques, piratería, pérdida de datos o siniestros, es por ello, que las organizaciones deben definir y garantizar la seguridad de sus recursos informáticos. En [10] la seguridad de la información cubre cuatro objetivos principales:

- **Disponibilidad:** Garantiza a las personas autorizadas el acceso a la información cuando lo requieran para su debido tratamiento.
- **Integridad:** Es la certeza de que la información no ha sido modificada o alterada de esta manera se considera que los datos son confiables y exactos.
- **Confidencialidad:** Se refiere cuando la información solo es accesible por el personal autorizado, garantizando que no sea divulgada a terceros sin consentimiento.
- **Prueba:** Garantiza que el emisor está identificado, tiene derechos y accesos lógicos de la información a enviar y que el receptor identificado está autorizado para recibir y acceder a la información.

2.2.2. ¿Por qué proteger?

Es importante reconocer que nuestra vida es digital ya que diariamente hablamos por teléfonos móviles, enviamos mensajes a través de aplicaciones IP, hacemos compras,

estudiamos y trabajamos a través de Internet, entramos en contacto con las empresas para adquirir sus servicios a través de su página web inclusive las empresas cierran contratos de manera electrónica sin la necesidad de una firma en un papel. Sin duda, la era de la información es el presente y potencialmente el futuro de las civilizaciones por lo tanto la seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de la información digital. Por ejemplo, una empresa debe restringir el acceso a personas no autorizadas a las partes protegidas de su web para evitar que la información sea alterada.

La seguridad completa es imposible, pero se debe asumir el despliegue de la máxima seguridad con los recursos asignados y con la formación actual del personal encargado, sin olvidar que para un ataque aparte del componente informático el factor humano facilita la tarea del atacante dificultando la tarea del administrador de redes [11].

2.2.3. ¿Qué proteger?

En una empresa el activo más importante son los datos, pero el presupuesto es otro aspecto que influye para aplicar las medidas de seguridad en toda la organización. Identificar los activos que se deben proteger es la tarea fundamental porque un equipo dañado o perdido se puede remplazar por otro igual o de mejor características pero los datos de una empresa una vez perdidos son irrecuperables e irreemplazables salvo por las copias de seguridad previamente obtenidas. Dentro de los activos que se puede proteger se encuentran [11]:

- **Equipos:** La seguridad física de los equipos consiste en evitar la sustracción del equipo entero o alguna pieza del mismo. Así mismo evitar la introducción de equipos no autorizados.
- **Aplicaciones**: Los empleados de la empresa deben tener en sus computadores solo las aplicaciones necesarias para cada actividad asignada, ni más ni menos. Además, se debe evitar la instalación de software extra ya que puede tener vulnerabilidad que puede causar problemas en el sistema operativo.
- **Datos:** Los datos son el bien más preciado de la empresa, si desaparecen la organización no puede funcionar con normalidad y si llegan a manos de terceros el futuro de la misma estaría en riesgo. Por lo tanto, es de suma importancia que

estos activos estén protegidos de software malicioso, el almacenamiento debe ser redundante en el caso de ocurrir algún fallo con el dispositivo de los alberga y con cifrado de esta manera la información será inútil si llega a manos de terceros al no poder descifrarla.

- **Comunicaciones:** Los datos en muchas ocasiones deben ser transferidos a otros usuarios que lo requieran, ese proceso debe ser protegido por medio de canales cifrados. A parte de proteger las comunicaciones de datos también es indispensable controlar las conexiones de la organización especialmente cuando los trabajadores realizan teletrabajo o en la propia oficina, de modo no cualquier persona puede entrar a la red empresarial para introducir algún tipo de malware y perjudique los activos de la empresa.

2.2.4. Amenazas

En [11] se considera como amenaza todo elemento o acción que atente contra la seguridad de la información. Una amenaza parte de una vulnerabilidad que pueda ser explotada, sea que comprometa o no la seguridad de la información.

Amenazas contra la seguridad física

La seguridad física se refiere a todo lo concerniente a equipos informativos como computadores, portátiles, servidores y otros equipamientos de la red. Este tipo de amenazas pueden ser:

- **Desastres naturales** como terremotos, inundaciones, incendios o hundimientos.
- **Robo de equipos** que contiene información valiosa para una persona u organización.
- **Fallos de suministro eléctrico** para que lo equipos no funcionen y no se pueda acceder a la información almacenada.

Amenazas contra la seguridad lógica

Al hablar de seguridad lógica se hace referencia a las diferentes aplicaciones que se ejecutan en cada equipo informático. Las amenazas contra las seguridades lógicas son:

- **Malware** o software malicioso como virus o troyanos.

- **Pérdida de datos** debido a un defecto en el código fuente de una aplicación que ocasiona modificaciones inexplicables en la información almacenada
- **Ataques a las aplicaciones de los servidores** a través de la explotación de vulnerabilidades encontradas en el sistema operativo o aplicaciones que se ejecutan en una máquina.

2.2.5. Vulnerabilidades

En [11] se define como vulnerabilidad a un defecto encontrado en una aplicación, al ser detectado el atacante puede programar un malware para aprovechar esa vulnerabilidad y tomar el control de la máquina para realizar actividades no autorizadas.

Tipos de vulnerabilidad

Existen tres tipos de vulnerabilidades:

- Vulnerabilidades reconocidas por el proveedor de la aplicación para las cuales existe un parche que las corrige.
- Vulnerabilidades reconocidas por el proveedor de la aplicación para las cuales no existen ningún parche
- Vulnerabilidades no reconocidas por el proveedor, siendo el peor de los casos puesto que la exposición a ataques es potencialmente alta.

2.2.6. Malware

El malware (malicious software) es un programa malicioso que tiene como objetivo infectar la red o un conjunto de computadores dentro de la organización para dañar la información.

Tipos de malware

Los malware más comunes son:

- **Virus:** El término virus hace referencia a programas diseñados para corromper o destruir datos y dañar el funcionamiento de la máquina en donde residen. La propagación de los virus informáticos es a través de correo electrónico, descarga

peer to peer, dispositivos de almacenamiento, descarga de archivos infectados que se encuentran en Internet [12].

- **Gusanos:** Se caracterizarán por hacer el mayor número de copias de sí mismos para propagarse fácilmente a través correo electrónico, archivos falsos, mensajería instantánea, etc.
- **Troyanos:** Es un código malicioso que tiene la capacidad de habilitar puertas trasera o backdoor para la administración remota de un usuario no autorizado [13].
- **Spyware:** Es un malware que se añade sin consentimiento en la máquina del usuario para recopilar información como, por ejemplo; los hábitos personales de navegación aumentando la cantidad de publicidad al navegar por la web y que además ralentiza el procesamiento del computador [12].
- **Adware:** Los adware tienen como objetivo mostrar publicidad web no deseada al usuario en forma de ventanas emergentes o se instalan a manera de barras en el navegador.
- **Rootkits:** Este tipo de malware modifica el sistema operativo de un computador para evitar que el usuario detecte el proceso malicioso que se está ejecutando en el ordenador, estos programas maliciosos también tienen rutinas no solo para ocultarse sino para evitar ser borrados.
- **Hijackers:** Este malware se instala como complemento en los navegadores cambiando las configuraciones de la página de inicio de manera que direcciona al usuario a páginas web de dudoso contenido.
- **Ransomware:** Llamados secuestradores o criptovirus, impiden el normal acceso a los datos del computador o servidor y la única forma de recuperar la información es pagar un rescate para acceder nuevamente a los datos [14].

2.2.7. Ataques informáticos

Un ataque informático consiste en aprovechar alguna vulnerabilidad en el software, hardware y hasta en las personas que manejan los datos informáticos a fin de causar daños en los activos de una empresa.

Tipos de ataques

Los ataques más comunes que usan los ciberdelincuentes son:

- **Ingeniería social:** Consiste en obtener información confidencial del usuario como claves por medio de la manipulación y confianza que el atacante logra obtener del usuario legítimo para sacar beneficios económicos a través del robo de cuentas bancarias, venta de información o chantajes [13].
- **Phishing:** El phishing es una estafa informática y consiste robar datos personales de cuentas de la víctima como Twitter, eBay, Facebook, Paypal, etc empleando procedimientos de ingeniería social. La mayoría de ataques tipo phishing son enfocados a obtener claves de acceso a la banca online así los ciberdelincuentes pueden hacer transferencias de la cuenta de la víctima o pueden vender la contraseña en el mercado negro para que terceras personas la utilicen [15].
- **Keyloggers:** Son programas maliciosos creados para robar información como números de tarjetas de crédito o contraseñas de correos electrónicos. Cuando el usuario teclea las letras o números el programa guarda esta información para enviar al creador y este pueda hacer pagos fraudulentos o espiar las conversaciones [16].
- **Fuerza bruta:** Esta técnica consiste en generar todas las combinaciones posibles para obtener la clave de acceso algún servidor, servicio o equipo [13].
- **Spoofing:** Consiste en suplantar la identidad de una máquina alterando algún elemento, por ejemplo, enviar mensajes con la misma dirección de la máquina original.
- **Sniffing:** Es una técnica en donde el atacante consigue conectarse en el mismo tramo de red del equipo atacado de esta forma tiene acceso directo a todas las máquinas de la intranet.
- **DoS:** La denegación de servicio consiste en saturar los puertos con múltiples flujos de información haciendo que el servidor se sobrecargue y no pueda atender la gran cantidad de peticiones dejándolo fuera de servicio [16].
- **DDoS:** La denegación de servicio distribuida (Distributed Denial of Service) consiste en la misma técnica que el DoS pero los ataques provienen de varias

máquinas distribuidas por todo el planeta hacia un mismo destino generando falsas peticiones para provocar el colapso del sistema [16].

A fin de reducir el impacto negativo ocasionado por los ataques informáticos se debe comprender cuales son las vulnerabilidades más comunes que pueden ser explotadas y los riesgos asociados para aplicar estrategias de seguridad efectivas que contrarresten estas actividades delictivas.

2.2.8. Seguridad Perimetral

En una organización los ataques a servidores, routers y sistemas internos son latentes, pero aumentan cuando la red corporativa está interconectada a una red pública. La seguridad perimetral busca ser la primera línea de defensa entre las redes públicas y las redes corporativas o privadas. El perímetro de seguridad como se muestra en la figura 2.1, consiste en cercar la red desde "fuera" para proteger todos los datos sensibles de una empresa [13].

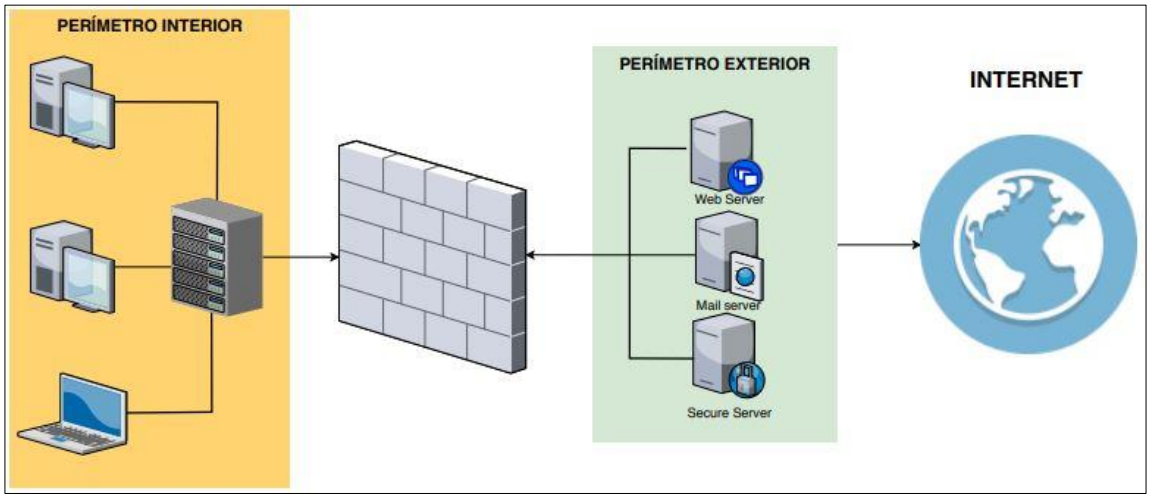


Figura 2.1 Seguridad Perimetral.
Fuente: Desarrollado por el investigador.

Entre las medidas de seguridad perimetral se encuentran los UTM que son prácticamente dispositivos que protegen la red otorgando todas las soluciones de seguridad que pueden ser configuradas y controladas. En la tabla 2.1 se muestra las ventajas y desventajas de un UTM.

Tabla 2.1. Ventajas y desventajas del UTM.

Ventajas	Desventajas
Flexibilidad	Único punto de falla
Bajo costo	Algunos servicios requiere suscripción
Integración Completa	Abierto a cualquier amenaza si se vulnera un UTM
Gestión desde una sola interfaz de administración	Puede tener problemas de rendimiento
Instalación ágil e intuitiva en hardware	La programación requiere más conocimiento en software

Fuente: [6]

2.2.9. UTM

La gestión unificada de amenazas o UTM fue usado por primera vez por Charles J. Kolodgy en 2004 y hace referencia a una única solución integrada de seguridad que combina funciones como firewall, detección de intrusos, anti-spam, anti-virus, VPN (virtual private network), spyware, filtrado de contenido, servidor de fugas entre otras funciones en un solo dispositivo. Este tipo de soluciones son creadas para brindar un blindaje total contra múltiples amenazas, también ofrecen balanceo de carga, enrutamiento remoto, traductor de direcciones NAT (Network Address Translation), compatibilidad con las VPN, prevención de fuga de datos, etc.

Es decir, un gestor unificado de amenazas simplifica equipos y tareas reduciendo y englobando todo en una sola tarea y producto, donde antes se ejecutaba y monitoreaba por separado cada tarea de seguridad hoy el administrador de redes puede controlar y tener centralizado desde un solo punto todas las medidas de seguridad. La ventaja de un UTM es controlar y mitigar varias amenazas en una sola acción, en la figura 2.2 se muestra algunas empresas a nivel mundial que proveen estos dispositivos sean licenciados u código abierto (OpenSource) [17].

Figura 2.2 Cuadrante de Gartner para UTM firewall 2021.
Fuente: [18]

Los Sistemas de Gestión Unificada de amenazas se encuentran en dos grupos hardware y software, ambos con características propias con alto nivel de protección además en este último tipo ofrece soluciones de código abierto (OpenSource).

2.2.10. Servicios de un UTM

Un Gestor Unificado de Amenazas es un equipo (hardware o software) complejo que reúne una serie de funciones como:

- **Firewall:** Se define como dispositivo hardware o software capaz de englobar funciones de seguridad como prevención de intrusos, filtrado de intrusos, protección contra malware, proxy, control de aplicaciones, sistemas de detección y prevención de intrusos.
- **Anti-virus:** Es la protección contra los virus informáticos.
- **Anti-spyware:** Es la protección contra software espías o spyware.

- **Anti-phishing:** Es la protección contra el phishing.
- **Anti-spam:** Es la protección contra el spam, el spam es correo basura y hace referencia a mensajes no solicitados o deseados, con remitente desconocido y de carácter masivo con un impacto perjudicial para el receptor. Para detectar si un correo electrónico es spam el Anti-spam inspecciona el contenido intentando averiguar la reputación del remitente, si detecta que es spam el correo se destruye, pero si hay dudas se coloca en una carpeta llamada correo no deseado para que el destinatario revise y decida qué hacer [19].
- **Sistema de Detección de Intrusos (IDS):** El IDS es un programa empleado para detectar accesos no autorizados a computadoras o redes, monitorizan el tráfico de la red y envían alertas cuando existen actividades sospechosas. Utiliza medidas correctivas o reactivas ante intrusiones analizando los paquetes entrantes para permitir o restringir el acceso y bloquear los paquetes. Para responder a un ataque el IDS necesita la asistencia de otros dispositivos de la red como routers o firewall [13] [20].
- **Sistema de Prevención de Intrusos (IPS):** El IPS es un dispositivo de repuesta rápida que restringe inmediatamente el tráfico malicioso, a diferencia del IDS todo el tráfico de entrada y salida pasan primero a través de él antes de que ingrese a la red para ser analizado y actuar rápidamente ante un problema. Ante una nueva vulnerabilidad detectada se crea un filtro específico y se añade al IPS para bloquear de manera automática cualquier intrusión maliciosa [13] [20].
- **Traducción de Direcciones de Red (NAT**): El sistema por el cual las redes privadas y redes públicas intercambian información se llama NAT y fue definida en el RFC 1631. Cuando una máquina de la red privada envía un paquete hacia la red pública la NAT permite que la máquina utilice una dirección no registrada y pueda conectarse a la red pública como por ejemplo Internet [21].
- **Red Privada Virtual (VPN):** Una VPN (Virtual Private Network) es una red virtual construida sobre redes físicas existentes para proveer comunicaciones seguras durante el intercambio de información sensible para el usuario sobre redes físicas inseguras. Una VPN representa una alternativa económica en

organizaciones que necesitan conectarse con sucursales remotas, es decir, permite que el usuario remoto acceda a la red corporativa (teletrabajo) [22].

- **Proxy:** Un proxy es un tipo de servidor que gestiona las peticiones de los clientes re direccionándolas a otros servidores, cuando recibe una petición del cliente se conecta con el servidor que cumple con las condiciones solicitadas. Además, el proxy almacena el servidor específico por si es utilizado posteriormente por el cliente para acelerar y optimizar el rendimiento de la red en futuras búsquedas [22].
- **Zona Desmilitarizada (DMZ):** La DMZ es una arquitectura segura utilizada para los servidores que deben ser accesibles desde Internet u otra red externa. El objetivo es colocar una subred (DMZ) entre las redes externa e interna para reducir los efectos de un ataque y pueda ser establecida entre dos routers como muestra la figura 2.3, un router interno conectado a la red protegida y un externo conectado a la red no protegida, además el uso de un firewall ubicado entre la red protegida y no protegida permite las conexiones requeridas de las redes externas no confiables a los servidores en la DMZ [20].

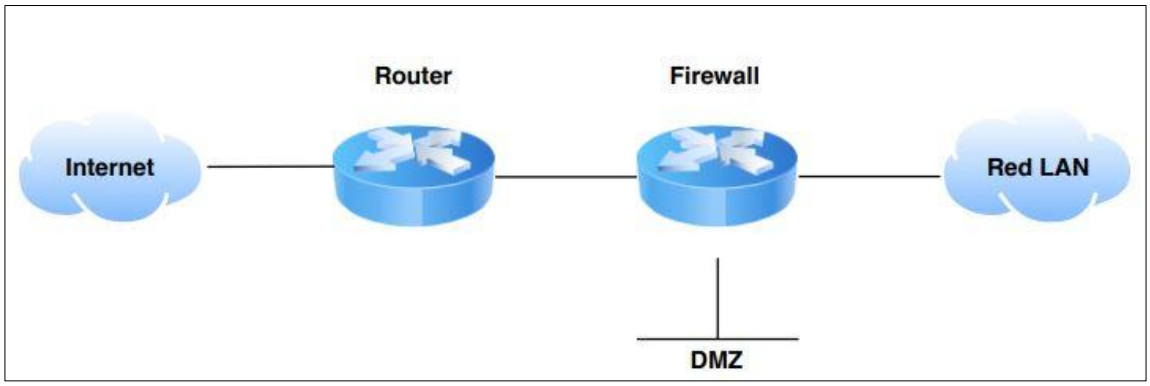


Figura 2.3 Enfoque DMZ.
Fuente: Desarrollado por el investigador.

2.2.11. Tipos de UTM

Los UTM pueden clasificarse en dos tipos específicos que son hardware y software.

- **UTM tipo hardware**

Los UTM tipo hardware son dispositivos que vienen con su propio Sistema Operativo, tienen una infraestructura lista para su respectiva conexión y configuración dentro de la red de la organización y no requieren de otro dispositivo para funcionar. Algunos fabricantes de este tipo de soluciones UTM son:

- ✓ Palo Alto Network
- ✓ Cisco
- ✓ Fortinet
- ✓ Sophos
- ✓ Check Point Software Technologies
- ✓ SonicWall
- ✓ Forcepoint
- ✓ Barracuda

- **UTM tipo software**

Los UTM tipo software son sistemas operativos listos para ser instalados y pueden ser licenciado de código abierto, este software necesariamente requiere de un hardware para poder funcionar, al hablar de hardware se hace referencia a dispositivos que pueden ir desde un simple computador hasta un potente servidor siempre y cuando cumplan con las características mínimas para soportar la instalación y el funcionamiento del software UTM. [23]

Dentro de este grupo existen versiones pagadas, gratis o código abierto, a continuación, se lista algunas soluciones UTM tipo software:

- ✓ Sophos
- ✓ Zentyal Gateway & UTM
- ✓ Endian Firewall
- ✓ pfSense
- ✓ OPNsense

2.2.12. Ethical Hacking

La terminología de hacking ético o ethical hacking hace referencia a conocimientos técnicos que poseen una persona para encontrar fallos o vulnerabilidades para luego prevenir, contraatacar y erradicar las vulnerabilidades encontradas en los sistemas informáticos. El objetivo principal del hacker ético es determinar el alcance que puede tener un intruso sobre los sistemas informáticos para luego tomar las medidas necesarias y así velar por la protección de la información.

2.2.13. Etapas del Ethical Hacking

Desde la perspectiva del hacking ético, el análisis de vulnerabilidades se realiza desde un enfoque constructivo e íntegro, a continuación, se lista las etapas de un hackeo real [24], [25], [26]:

- **Recolección de información**

  La recolección de información corresponde a la primera fase del Ethical Hacking, en esta etapa, el atacante define el objeto a atacar con el mayor detalle posible para obtener la mayor cantidad de información**.** Por ejemplo, si el objeto es una organización en un inicio el atacante no tiene mayor detalle que el nombre, entonces usa técnicas como: WhoIs, Ingeniería Social entre otras para encontrar información como direcciones IP, DNS y otros datos. La información recolectada proviene de fuentes públicas disponibles en Internet a todo tipo de público.
- **Escaneo**

  En la segunda etapa el atacante organiza toda la información obtenida para analizar como nombres de usuario, sistema operativo, software base instalado, direcciones IP, direcciones MAC, cuentas de usuario, etc con la finalidad de encontrar vulnerabilidades y en una fase posterior puedan ser explotadas para tener acceso al sistema. En esta fase se usa técnicas como NMAP.
- **Exploits de vulnerabilidades**

  Un exploit es un software que aprovecha las vulnerabilidades de un sistema para acceder a la información. Después de identificar las debilidades del sistema se procede a buscar un exploit para explotar las vulnerabilidades, escalar privilegios,

acceder a los sistemas y obtener así la mayor información. Una de las herramientas más utilizadas para explotar las vulnerabilidades de los equipos es MetaSploit

- **Mantener el acceso**

  Para mantener el acceso a un sistema se instala y ejecuta un software malicioso que permite mantener un canal abierto de conexión para ejecutar ataques o explotaciones a futuro.

- **Borrar huellas**

  La última etapa que un hacker debe ejecutar es limpiar cualquier evidencia como archivos de registro (log) o alarmas del sistema de detección de intrusos (IDS) para evitar ser detectado y así mantener puertas traseras para su uso.

2.2.14. Buenas prácticas

La seguridad informática de una empresa es una tarea ardua especialmente si existe gran cantidad de información que proteger y si existen múltiples puertas por donde se puede sufrir cualquier tipo de ataque. Como se indica en [11] la persona encargada de la seguridad debe:

- Localizar los activos de la organización que se debe proteger como datos, equipos, aplicaciones y comunicaciones.
- Revisar las copias de seguridad, es decir, qué, dónde y cuándo copiamos, dónde se guardan las copias y verificar su correcto funcionamiento.
- Redactar, revisar y aplicar los planes de actuación contra catástrofes de índole natural o intencionada.
- Instalar en los ordenadores de los empleados los programas estrictamente necesarios para el trabajo a desempeñar.
- Estar informado sobre los informes de seguridad o vulnerabilidades que día a día vayan apareciendo, para lo cual debe registrar los correos de los proveedores autorizados y así pueda recibir directamente las noticias.
- Activar las actualizaciones automáticas de las aplicaciones instaladas para resolver problemas con versiones anteriores.

- Plantear la opción de una auditoría externa que pueda detectar errores que el administrador haya pasado por alto.
- Revisar periódicamente los equipos conectados a la red y descartar que existan equipos no autorizados.
- Revisar los usuarios activos porque se puede dar el caso de que un ex empleado aun cuente con su usuario y privilegios habilitados.
- Capacitar a los usuarios sobre seguridad informática y sea una ayuda en sus labores diarias.

CAPÍTULO III

METODOLOGÍA

3.1. Ubicación

El presente trabajo de investigación se desarrolló en la empresa Simantec ubicada en la parroquia rural de Guayllabamba, cantón Quito provincia de Pichincha.

3.2. Equipos y materiales

Los equipos y materiales necesarios para el proceso de la investigación se detallan en la tabla 3.1.

Tabla 3.1 Equipos y materiales.

Equipo/Material	Cantidad
UTM Hardware: Sophos XG 115	1
Servidor HPE ProLiant MicroServer Gen10 Plus	1
Instalador pfSense	1
Computador	1
Patch Cord RJ45	5
Monitor	1
Teclado	1
Mouse	1
Direcciones IP públicas	2

Fuente: Desarrollado por el investigador.

3.3. Tipo de investigación

3.3.1. Investigación Cuantitativa

Según Packer, la investigación cuantitativa es objetiva, estudia las causas y provee de explicaciones además puede poner a prueba las hipótesis mientras que la investigación cualitativa es subjetiva, estudia las experiencias, proporciona solo descripciones y tan solo puede generar hipótesis, pero nunca probarlas por lo que no da explicaciones [27].

El presente proyecto de investigación es cuantitativo porque a través de datos medibles se pretende determinar el UTM que brinde mejor rendimiento y rentabilidad, los resultados obtenidos determinarán el alcance del proyecto y brindará el soporte necesario para llegar a las conclusiones generales de la investigación.

3.3.2. Investigación Cualitativa

La investigación es cualitativa porque el plan de buenas prácticas de seguridad fomentará el buen uso y cuidado de la información que maneja cada colaborador.

3.3.3. Investigación Experimental

La investigación es de tipo experimental ya que las pruebas se harán sobre el objeto de estudio en condiciones controladas y bajo parámetros requeridos por la empresa a fin de observar y obtener los resultados esperados.

3.3.4. Investigación Aplicada

La investigación es aplicada porque busca encontrar las vulnerabilidades a la que está expuesta la información de la empresa y pretende mejorar o minimizar en lo posible los ataques que se puedan suscitar en la red de Simantec.

3.4. Población y muestra

La población está conformada por todos los colaboradores de la empresa siendo el objeto de estudio la cantidad de información que transmiten por determinado ancho de banda asignado por el investigador. La muestra seleccionada fue la misma población debido a que la cantidad de datos es pequeña y se puede procesar.

3.5. Recolección de la información

El plan para recolectar la información contempla los siguientes pasos:

- Para determinar las vulnerabilidades a las que está expuesta la empresa se utilizó herramientas de Pentesting como Kali Linux y Shodan, estas herramientas en conjunto dieron paso para encontrar las vulnerabilidades de la empresa como

puertos abiertos, servicios activos y geo localización de los equipos conectados a internet.

- Una vez planificada la estructura de la plataforma de seguridad que requiere la empresa se procede con la configuración de los sistemas UTM tanto propietario como Open Source. En este proceso se experimenta con la configuración en cada equipo UTM para alcanzar los requerimientos que exige la empresa.
- Finalmente la toma de resultados se hace a través de los dashboard de cada sistema UTM, logs y la consola terminal de MikroTik, la interface web de Shodan y las gráficas y datos arrojados de Jperf, que es nada más que un software para evaluar el rendimiento de una red.

3.6.Procesamiento de la información y análisis estadístico

Como se menciona en apartados anteriores, esta investigación es de tipo experimental y con el fin de procesar la información recopilada se ha establecido los siguientes pasos:

- Configuración inicial del UTM propietario y UTM Open Source.
- Implementación de servicios como túnel IPsec (Internet Protocol security), VPN, servicios RDP, control web, limitación de ancho de banda e IPS en el UTM propietario y UTM Open Source.
- Descripción paso a paso de la configuración y puesta en marcha de cada servicio implementado en los dos sistemas UTM.
- Pruebas de funcionamiento de cada servicio.
- Uso de tablas comparativas para describir de forma breve y concisa los resultados obtenidos durante la configuración de cada servicio, una vez terminada las configuraciones se compara los dos sistemas UTM para determinar el sistema más adecuado para la empresa.

Análisis estadístico

Dentro del análisis estadístico se señala dos aspectos importantes, el número total de colaboradores de la empresa y la demanda de ancho de banda. Actualmente la matriz

cuenta con dos edificaciones, cada una está conformada por diferentes departamentos cuya distribución se muestra en la tabla 3.2.

Tabla 3.2 Total de usuarios matriz.

Edificio	Departamento	Número de usuarios
Edificio 1-Planta baja	Caja	2
Edificio 1-Planta baja	Cobranzas	6
Edificio 1-Planta baja	Comercialización	3
Edificio 1-Planta 1	Logística	3
Edificio 1-Planta 1	Recursos Humanos	1
Edificio 1-Planta 1	Contabilidad	1
Edificio 1-Planta 1	Gerencia administrativa	1
Edificio 1-Planta 2	Área Técnica	10
Edificio 1-Planta 2	Gerencia Técnica	1
Edificio 2-Planta 1	Bodega	5
Edificio 2-Planta 1	Médico Ocupacional	1
Total		34

Fuente: Desarrollado por el investigador.

La sucursal cuenta con dos edificaciones, los usuarios y equipos finales están distribuidos como muestra la tabla 3.3.

Tabla 3.3 Total de usuarios sucursal.

Edificio	Departamento	Número de usuarios
Edificio 1-Planta baja	Caja	2
Edificio 1-Planta baja	Bodega	1
Edificio 1-Planta baja	Área Técnica	1
Edificio 2-Planta 1	Área Técnica	2
Edificio 2-Planta 1	Cobranzas	1
Total		7

Fuente: Desarrollado por el investigador.

El total de usuarios en la empresa es de 41 colaboradores quienes requieren el acceso las horas 8 laborables a todos los servicios empresariales para desarrollar sus actividades diarias. En [28] se indica la fórmula para calcular el tamaño de la muestra para una población finita determinada por la ecuación 3.1:

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2} \tag{3.1}$$

Donde:

N = Tamaño de la población.

$\sigma =$ Desviación estándar de la población, generalmente cuando no se tiene su valor, se emplea un valor constante de 0,5.

Z = Valor obtenido de la distribución normal. Si no se tiene su valor, se considera en relación al 95% de confianza que equivale a 1,96 (como más usual) o en relación al 99% de confianza que equivale a 2,58, el valor que queda a criterio del investigador.

e = Límite aceptable de error muestral, generalmente cuando no se tiene su valor, se emplea un valor que varía entre el 1% (0,01) y 9% (0,09), el valor queda a criterio del encuestador.

n = Tamaño de la muestra.

$$n = \frac{41 * (0{,}5)^2 * (2{,}58)^2}{(41-1) * (0{,}01)^2 + (0{,}5)^2 * (2{,}58)^2}$$

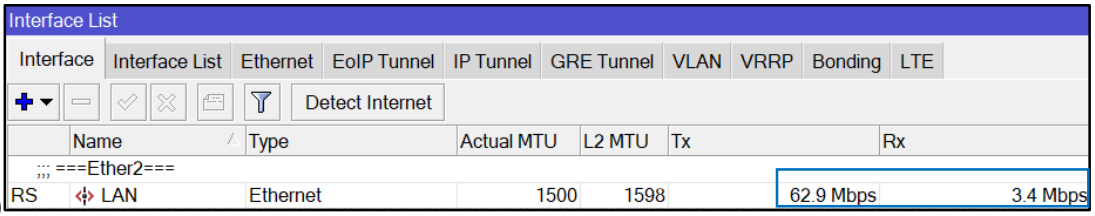
$$n = 40{,}901 \approx 41 \text{ usuarios}$$

El tamaño de la muestra de una población de 41 elementos con un nivel de confianza de 99% y un margen de error de 1% es de 41 usuarios.

El ancho de banda que los usuarios consumen es un dato tomado de los equipos MikroTik de la matriz y sucursal. Como muestra la figura 3.1 la interface LAN muestra la cantidad de tráfico que se transmite en horas pico por los empleados, considerando estas horas entre

las 12:00 y 15:00 de la tarde donde existe mayor afluencia de clientes y llamadas telefónicas.

a)



b)

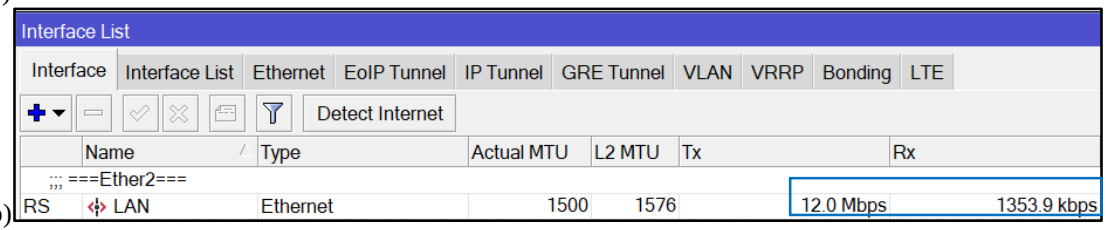


Figura 3.1 Tráfico total. a) Matriz. b) Sucursal.
Fuente: Desarrollado por el investigador.

Para calcular el ancho de banda por usuario se divide el tráfico total de la matriz y sucursal para el número de usuarios de cada sitio, entonces se tiene:

$$Ancho\_Banda_{usuario\_matriz} = Tráfico\_Matriz \div Usuarios\_matriz$$

$$Ancho\_Banda_{usuario\_matriz} = 62{,}9\ Mbps \div 34\ usuarios$$

$$Ancho\_Banda_{usuario\_matriz} = 1{,}85\ Mbps \approx 2\ Mbps$$

$$Ancho\_Banda_{usuario\_sucursal} = Tráfico\_Sucursal \div Usuarios\_sucursal$$

$$Ancho\_Banda_{usuario\_sucursal} = 12{,}0\ Mbps \div 7\ usuarios$$

$$Ancho\_Banda_{usuario\_sucursal} = 1{,}71\ Mbps \approx 2\ Mbps$$

Por lo tanto, cada empleado requiere un ancho de banda aproximadamente de 2 Mbps para desarrollar sus actividades. Existen departamentos en donde la demanda de ancho de banda es baja debido al número de usuarios como el caso de Recursos Humanos que solo cuenta con un colaborar. Sin embargo, el área técnica es el departamento que más ancho

de banda requiere para acceder a los distintos servidores, conexiones remotas, equipos finales de clientes, capacitaciones y servicios empresariales, con un total de 10 de colaboradores el departamento requiere 20 Mbps como ancho de banda.

3.7.Variables respuesta o resultados alcanzados

Dentro de los resultados se pretende:

- Alcanzar los objetivos propuestos en el Capítulo I para implementar una plataforma de seguridad perimetral en la empresa de internet “Simantec”.
- Recopilar información bibliografía relacionada con la investigación para abordar temas desconocidos y así desarrollar el proyecto planteado.
- Emplear la metodología propuesta en el Capítulo III para elaborar el trabajo de investigación acorde a los procedimientos propuestos.
- Implementar los servicios requeridos por la empresa en los dos sistemas UTM para elegir de acuerdo a su rendimiento, rentabilidad y en base a los resultados obtenidos Capítulo IV el sistema más idóneo para la empresa.
- Finalmente, obtener conclusiones y recomendaciones del trabajo elaborado acorde a los resultados esperados por el investigador.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Información General de Simantec

Simantec es una empresa ubicada en la parroquia de Guayllabamba perteneciente al cantón Quito y provee el servicio de Internet desde el año 2010 a más de 10000 usuarios. El modelo comercial se basa en brindar Internet a sus abonados a través de redes inalámbricas y ópticas según sus necesidades y presupuesto. El suministro de banda ancha es ilimitado para casa, negocios y pequeñas empresas con amplia cobertura en la zonas urbanas y rurales de los cantones Quito, Pedro Moncayo, Cayambe en la provincia de Pichincha y Otavalo en Imbabura.

Figura 4.1 Matriz Guayllabamba.
Fuente: Desarrollado por el investigador.

Figura 4.2 Sucursal Cayambe.
Fuente: Desarrollado por el investigador.

4.2. Levantamiento de la información

4.2.1. Topología física de la red

La red física actual de Simantec se basa en equipos de la marca Cisco y Mikrotik, su modelo jerárquico concentra en la capa de núcleo equipos que proveen altas tasas de transferencia con latencias bajas, mientas que los equipos de la capa de distribución proveen las funciones de ruteo sobre las diferentes redes para dividir dominios de broadcast y en la capa de acceso se tiene los equipos finales de los colaboradores tanto en la matriz Guayllabamba y sucursal Cayambe.

La capa de núcleo consta de equipos Cisco que se limita solo al reenvío de paquetes conmutándolos lo más rápido posible e interconecta varios equipos de la empresa. En la capa de distribución se tiene equipos de la marca MikroTik, específicamente Router de la serie 1036 o 1009. Estos dispositivos se encuentran entre la capa de núcleo y acceso, la función principal es de enrutamiento, filtrado y acceso a la WAN. Los dispositivos de esta capa envían la solicitud de los usuarios al núcleo para proporcionar acceso a los servicios

corporativos solicitados por los colaboradores de los diferentes departamentos de la matriz o sucursal. Finalmente, la capa de acceso consta de equipos como Switch de la marca TP-Link y MikroTik encargados de controlar que dispositivos se conectan o no a la red empresarial.

La figura 4.3 muestra la topología física que se maneja en la matriz y sucursal, el router de borde es del proveedor y está conectado a un MikroTik 1036 seguido de un Switch que administra los distintos servidores, así como los distintos puntos de acceso de los usuarios.

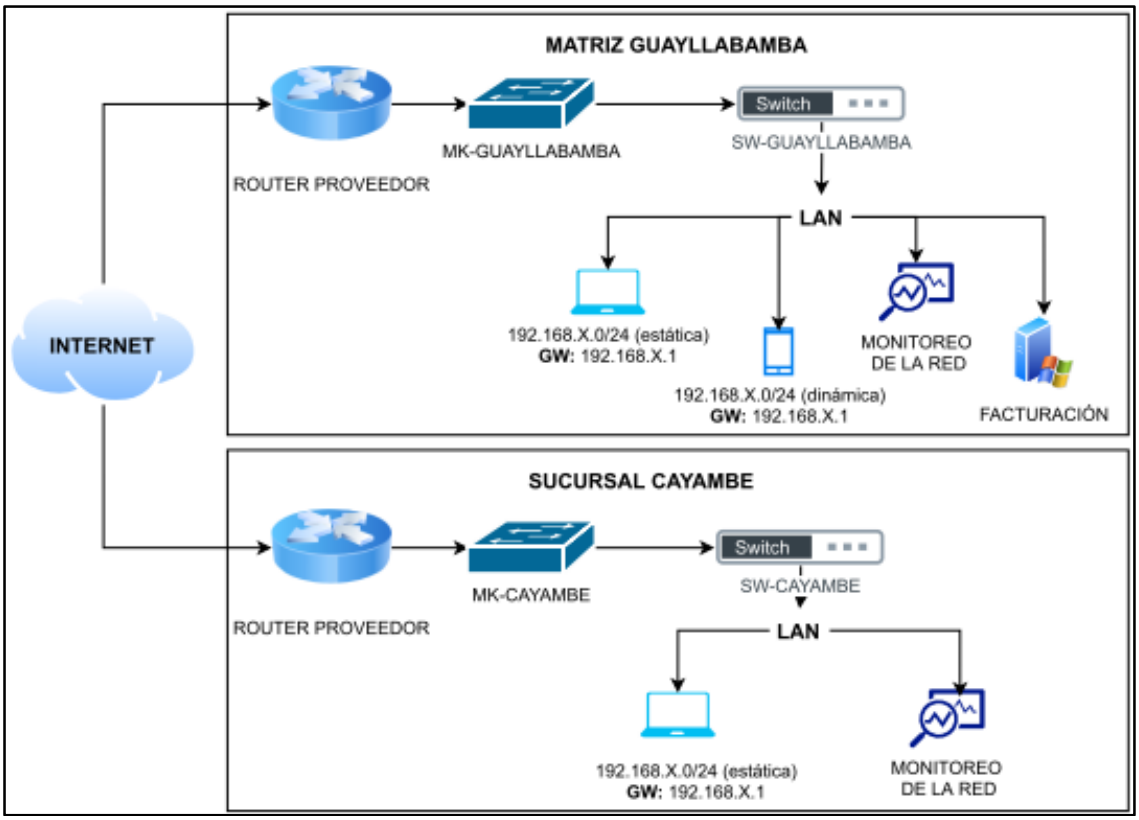


Figura 4.3 Topología física de la red.
Fuente: Desarrollado por el investigador.

Como se puede constatar, en primera instancia no hay equipos de frontera entre la red de Internet y los servidores de la empresa que pueda protegerlos de ataques que van desde los más comunes hasta avanzados por lo tanto están expuestos a un sin número de vulnerabilidades. Sin embargo, existe seguridades a nivel de sistema operativo levantados en los servidores y los equipos MikroTik que cumplen el papel de mitigar ataques o intrusión en los servidores, pero lo ideal es instalar un equipo entre Internet y los

servidores para reforzar la seguridad y optimizar el rendimiento de los mismos. Como caso práctico para este tema de investigación el perímetro de seguridad se aplicará entre los usuarios y la capa de distribución.

4.2.2. Direccionamiento lógico de la red

Los departamentos de la empresa están organizados bajo un esquema de direccionamiento IPv4, distribuida como muestra la tabla 4.1.

Tabla 4.1 Distribución de equipos finales matriz y sucursal.

Departamento	Red	Gateway
Gerencia General	192.168.X.X/24	192.168.X.X
Área Técnica Matriz	192.168.X.X/24	
Área Técnica Sucursal	192.168.X.X/24	
Bodega Matriz	192.168.X.X/24	
Bodega Sucursal	192.168.X.X/24	
Cajas Matriz	192.168.X.X/24	
Cajas Sucursal	192.168.X.X/24	
Logística	192.168.X.X/24	
Comercialización	192.168.X.X/24	
Cobranzas	192.168.X.X/24	
Parqueadero	192.168.X.X/24	
Dispensario Médico	192.168.X.X/24	
Seguridad y Salud Ocupacional	192.168.X.X/24	

Fuente: Desarrollado por el investigador.

4.3. Requerimientos

La empresa posee en sus instalaciones una serie de servidores para diferentes servicios como facturación, monitoreo del tráfico de la red empresarial, monitoreo de clientes con tecnología WiMax y fibra óptica entre otros. Para fines prácticos la propuesta de crear una plataforma de seguridad perimetral se aplicará desde y hacia los usuarios, además los servicios que la empresa necesita implementar a través de la plataforma de seguridad hacia los dispositivos finales de los usuarios son:

- Conexiones VPN.
- Limitación de ancho de banda a los usuarios por grupos.
- Control web.
- Protección contra malware.
- Prevención de intrusión.
- Filtrado antispam.
- Accesos al sistema interno.

A parte de estos servicios también es indispensable hacer un análisis de los riesgos a los cuales está expuesta la red empresarial en cuestión de seguridad informática.

4.4. Análisis de riesgos informáticos

El análisis de riesgos a la seguridad informática permite detectar las vulnerabilidades de la red empresarial y que al ser explotadas por un atacante pone en riesgo a toda la organización. Para hacer el análisis de riesgos se empleó virtual box que es una aplicación de virtualización de uso doméstico y empresarial disponible de forma gratuita. Se puede ejecutar en Windows, Linux, Macintosh y Solaris para crear servidores, computadores de escritorio y uso integrado. Las características que presenta este producto son: portabilidad, virtualización en 3D, carpetas compartidas, soporte de hardware, visualización remota de la máquina, soporte para dispositivos USB, compatibilidad de hardware, multiprocesamiento de invitados [29].

El análisis de riesgos cuenta con las siguientes fases: recolección de información, escaneo de vulnerabilidades, análisis de vulnerabilidades y reporte.

4.4.1. Recolección de información

En el mercado existen numerosas herramientas para el análisis de vulnerabilidades, en este proyecto se emplea Kali Linux 2020.2. Esta distro de hacking ético es la segunda actualización de 2020 y está basada Debian, contiene una serie de aplicaciones para realizar pruebas de seguridad en un entorno sencillo y seguro para el usuario. Este sistema operativo se instaló como máquina virtual en el software Oracle VM VirtualBox con una memoria base de 1024 MB, a partir de la cual se recolectará la información para escanear

y analizar las vulnerabilidades encontradas y poder interpretar todos los fallos encontrados dando una solución a estas falencias.

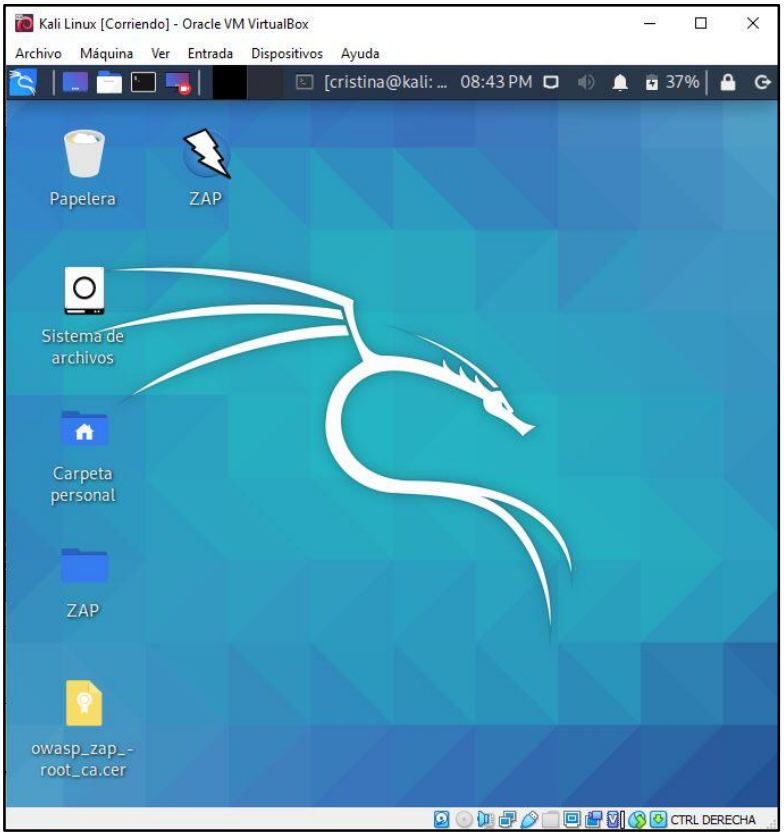


Figura 4.4 Kali Linux.
Fuente: Desarrollado por el investigador.

Uno de los comandos básicos para recolectar información es nslookup (Name Server Lookup) y permite obtener el registro de dirección de un dominio o consultar el sistema de nombres de dominio (DNS) de una IP determinada. Empelando Kali Linux y otras herramientas de Pentesting se analizará la página web de la empresa como muestra la figura 4.5.

Figura 4.5 Página Web.
Fuente: Desarrollado por el investigador.

En Kali Linux la sintaxis es nslookup [opción], la respuesta al dominio Simantec (www.simantec.ec) es 186.X.X.X como se muestra en la figura 4.6.

```
root@kali:/home/cristina# nslookup www.simantec.ec
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.simantec.ec
Address: 186.
root@kali:/home/cristina#
```

Figura 4.6 Comando nslookup.
Fuente: Desarrollado por el investigador.

Whois es otro comando que proporciona información acerca de un dominio, desde la consola de Kali Linux se usó el comando whois 186.X.X.X como muestra la figura 4.7 para obtener más información como el nombre del propietario, ID del propietario, responsable, dirección, país, teléfono, correo electrónico, etc

Figura 4.7 Comando whois.
Fuente: Desarrollado por el investigador.

Netcraft es otro sitio web que proporciona información acerca de un dominio, incluye la detección del tipo de servidor web y sistema operativo.

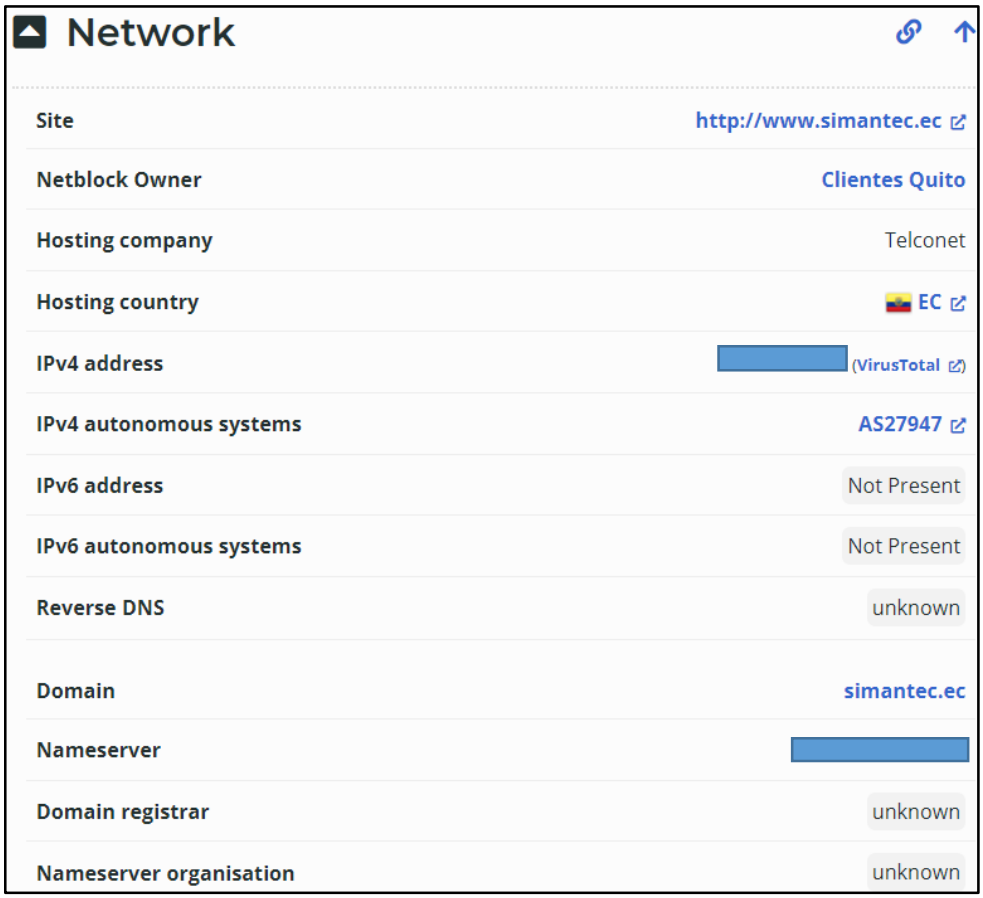


Figura 4.8 Información de Simantec a través de Netcraft.
Fuente: Desarrollado por el investigador.

Como se puede observar la IPv4 del dominio Simantec.ec es 186.X.X.X proporcionada por Telconet y no posee IPv6. La figura 4.9, en cambio muestra el hospedaje, sistema operativo y web server del dominio. Siendo este último Ngix, un servidor web de código abierto diseñado para ofrecer bajo uso de memoria y alta concurrencia, una de las características más destacadas es el soporte IPv6.

Figura 4.9 Historial de hospedaje.
Fuente: Desarrollado por el investigador.

Además, en la figura 4.10 se muestra que a través de la página web https://www.iplocation.net se obtuvo la geolocalización del dominio, por medio de IP2Location se identificó la ubicación geográfica de Clientes Quito y Telconet SA.

Figura 4.10 Ubicación geográfica del dominio.
Fuente: Desarrollado por el investigador.

4.4.2. Escaneo de vulnerabilidades

El método de caja blanca o WhiteBox actúa como usuario legítimo con privilegios dentro la red y busca de alguna manera realizar acciones adicionales en bases a esos privilegios otorgados mientras que el método de caja negra o BlackBox consiste en otorgar al analista

algo de información como una sola IP o el nombre de la empresa para que a partir de ahí empiece con la búsqueda de datos sensibles de la organización. Cabe mencionar que existe una gran diferencia entre análisis de vulnerabilidades y pentesting; el primero solo detecta y documenta las vulnerabilidades, pero el segundo busca explotar las vulnerabilidades encontradas. Este trabajo se rige bajo un acuerdo de confidencialidad en donde se menciona solo la detección de vulnerabilidades más no su explotación por protección a los activos de la empresa.

Una herramienta completa y compleja para el escaneo de vulnerabilidades es nmap y está orientada al reconocimiento de redes y puertos, como indica la figura 4.11 la ejecución de este comando sin parámetros realiza un escaneo sencillo a los 1000 puertos más comunes con peticiones TCP, UDP, ICMP, SCTP, entre otros.

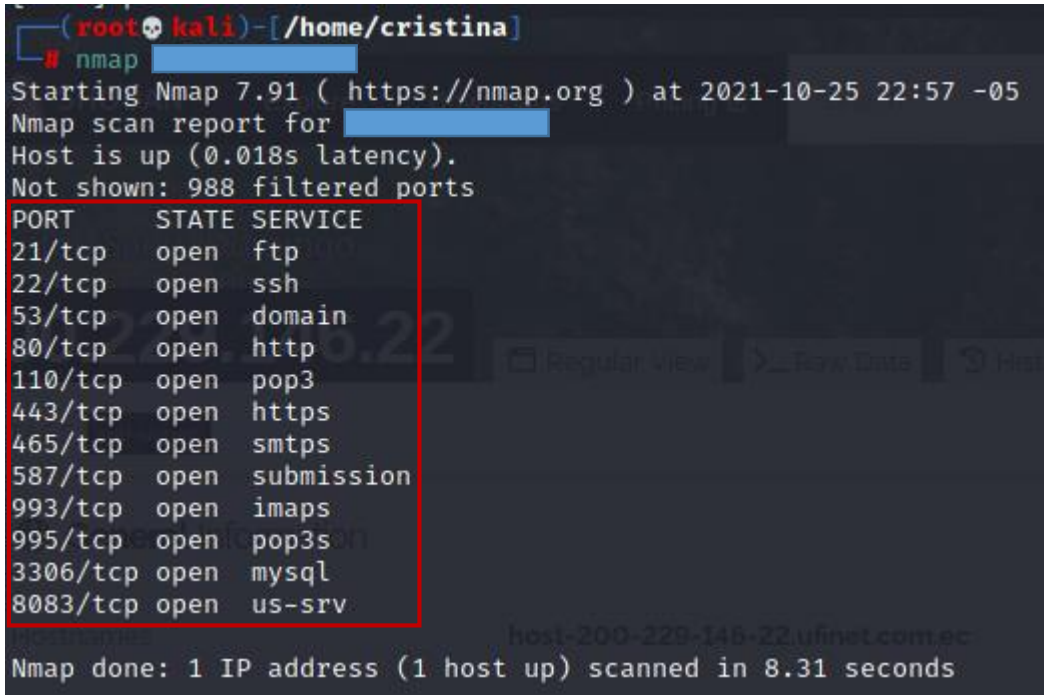


Figura 4.11 Escaneo con nmap.
Fuente: Desarrollado por el investigador.

Los puertos abiertos comprometen la seguridad de la red volviéndola más vulnerable a intrusos que aprovechan esta falencia para acceder y robar información. Todos los puertos abiertos tienen protocolo TCP, es decir, orientados a la conexión en el caso que ocurra

algún tipo de problema realiza retransmisiones para garantizar que todos los segmentos lleguen a su destino.

4.4.3. Análisis de vulnerabilidades

Para el análisis de vulnerabilidades se utilizó Shodan, la información que entrega la IP localizada va desde la geolocalización, país de origen, el tipo de servicio y puertos abiertos y las vulnerabilidades al que está expuesta. Bajo este criterio y como muestra la figura 4.12 se encontró dos vulnerabilidades para la IP 186.X.X.X.

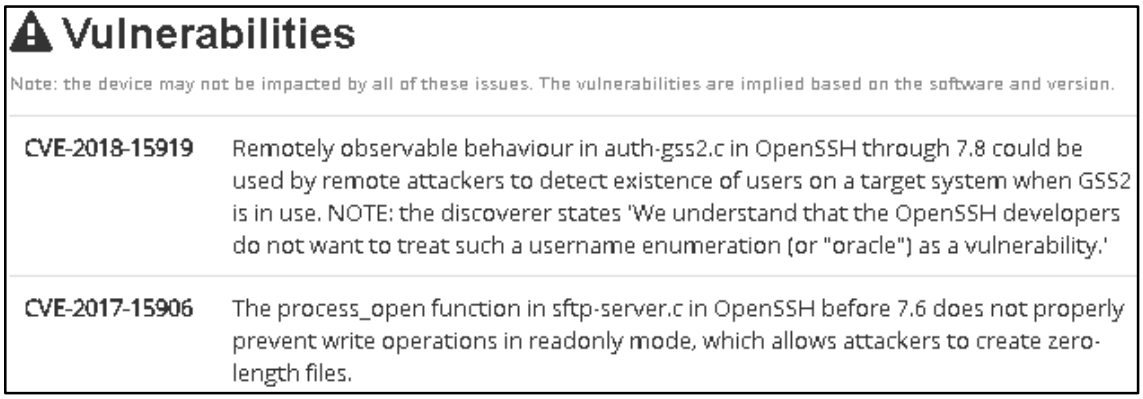


Figura 4.12 Análisis de vulnerabilidades con Shodan.
Fuente: Desarrollado por el investigador.

- **CVE-2018-15919:** Es una vulnerabilidad encontrada en OpenSSH hasta la versión 7.8 de clase error de validación de acceso. A través de la explotación de esta vulnerabilidad un intruso puede aprovechar para recopilar cuentas de usuarios válidas aumentando la probabilidad de ataques de fuerza bruta. La solución para esta vulnerabilidad es la actualización a la versión más actual de la aplicación.

- **CVE-2017-15906:** Es una vulnerabilidad encontrada en versiones anteriores a Open SSH 7.6, considerada como un error de diseño, deja a OpenSSH propenso a una vulnerabilidad de omisión de seguridad remota. La solución para esta vulnerabilidad es la actualización a la versión más actual de OpenSSH.

Una herramienta que permite buscar exploits para romper la seguridad a través de la vulnerabilidad encontrada es exploit database (exploit-db.com), sin embargo, y como

muestra la figura 4.13 las vulnerabilidades citadas anteriormente no disponen de exploits para explotar y ganar el acceso al servidor web.

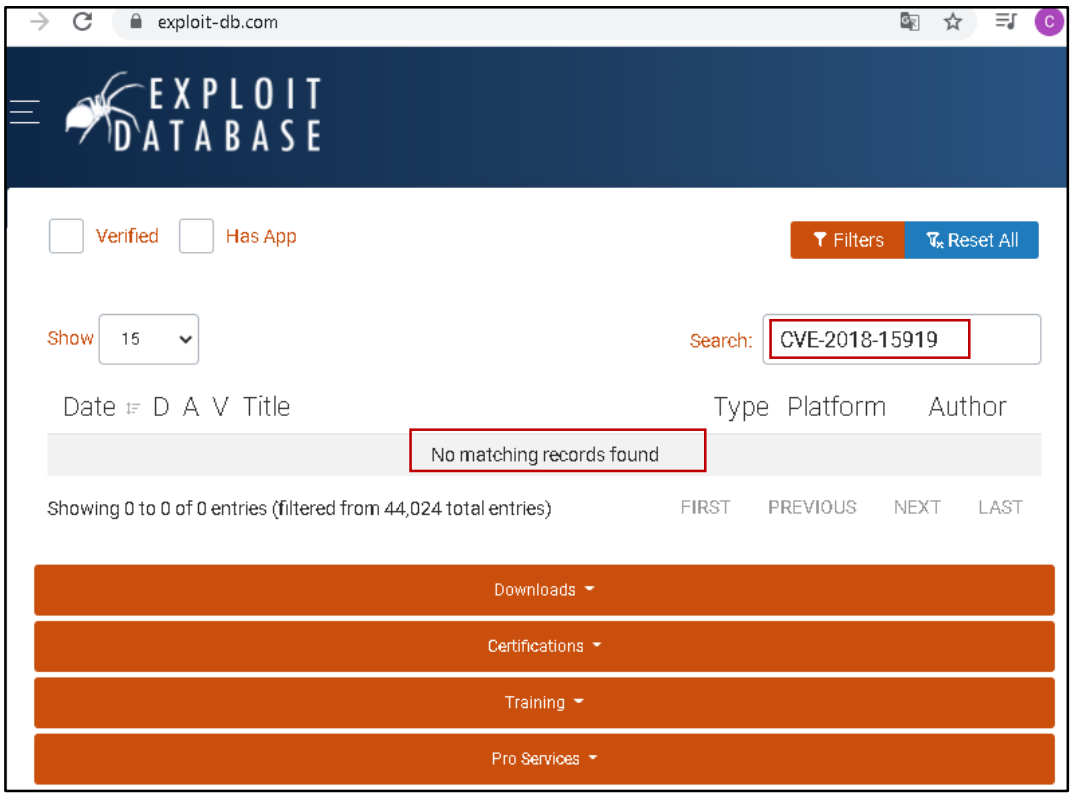


Figura 4.13 Buscador de exploit
Fuente: Desarrollado por el investigador.

4.4.4. Análisis de riesgos encontrados en la red empresarial.

La herramienta Shodan también arrojó información más relevante de la empresa, usando la sintaxis *hostname:.[nombre de la página]*se encontró 53 puertos abiertos entre ellos constan 443, 80, 21, 22, 23, etc. Los puertos 443 y 80 son puertos que se usan para la navegación web segura (https) y no segura (http), el puerto 21 se usa para conexión a servidores ftp, el puerto 22 para conexiones seguras SSH y SFTP y el puerto 23 para conexiones remotas a otro equipo vía Telnet.

Entre los servicios activos se encontró: ngnix, OPenSSH, acceso a cámaras de seguridad, equipos Mikrotik, escritorios remotos y sistemas operativos.

Zimbra

La figura 4.14 muestra la página de acceso a un servidor Zimbra, esta herramienta open source permite la gestión de correo electrónico, soporta accesos POP e IMAP, incluye protección anti-spam y antivirus. Para ganar el acceso a este servidor se puede hacer a través de ataque por diccionario o ataques por fuera bruta con las claves más comunes para servidores y obtener el usuario o contraseña de acceso.

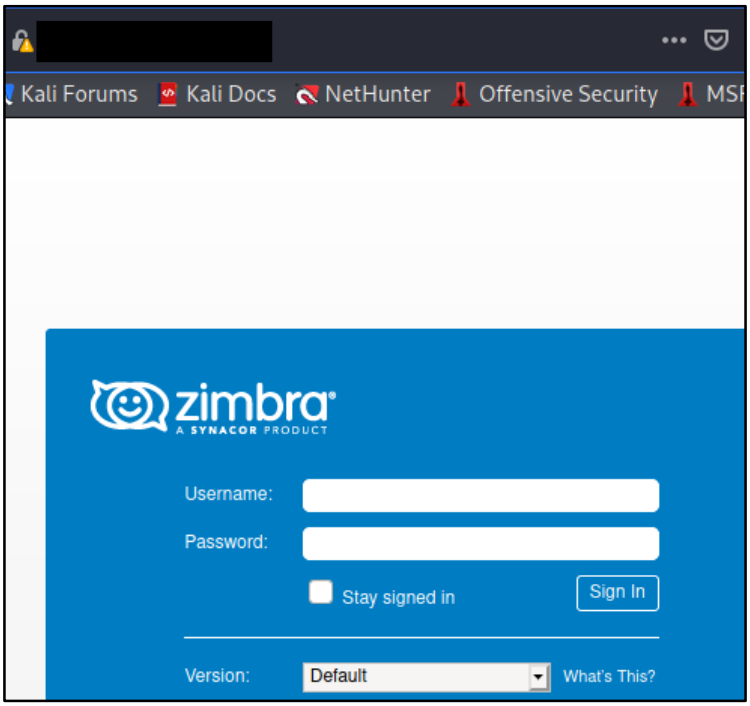


Figura 4.14 Ventana de acceso a Zimbra.
Fuente: Desarrollado por el investigador.

Cámaras de seguridad

La figura 4.15 muestra la consola de inicio con el logotipo de la marca Hikvision, por defecto el usuario y contraseña es admin aunque este no es el caso, entonces para ingresar a la interface de las cámaras se debe conseguir el usuario y contraseña mediante alguna técnica de cracking.

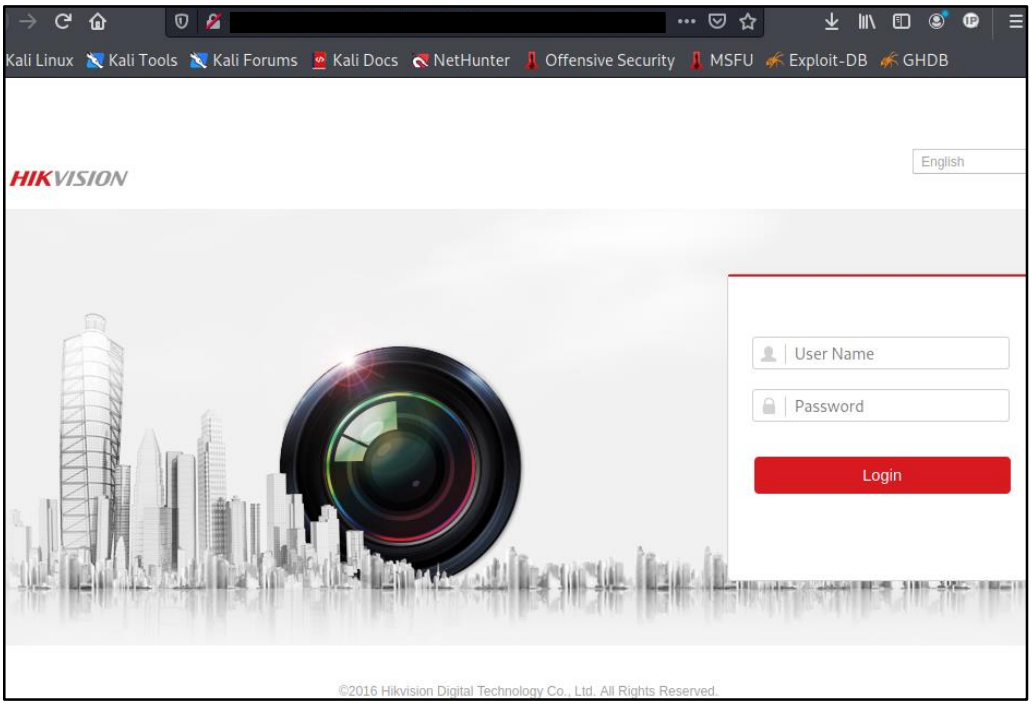


Figura 4.15 Ventana de acceso a las cámaras de seguridad.
Fuente: Desarrollado por el investigador.

Escritorio Remoto

La figura 4.16 muestra la ventana de acceso a un escritorio remoto de Windows o RDP (Remote Desktop Protocol), el puerto por defecto es 3389 pero lo más recomendable es cambiar el puerto, definir usuarios solo autorizados para el acceso y usar contraseñas robustas. Los RDP son vulnerables a ataques de fuerza bruta, estos ataques intentan adivinar el nombre de usuario y contraseña para acceder a la cuenta de usuario de escritorio remoto, en este caso es recomendable limitar el número de intentos fallidos de inicio de sesión para los usuarios y así para evitar el acceso no autorizado.

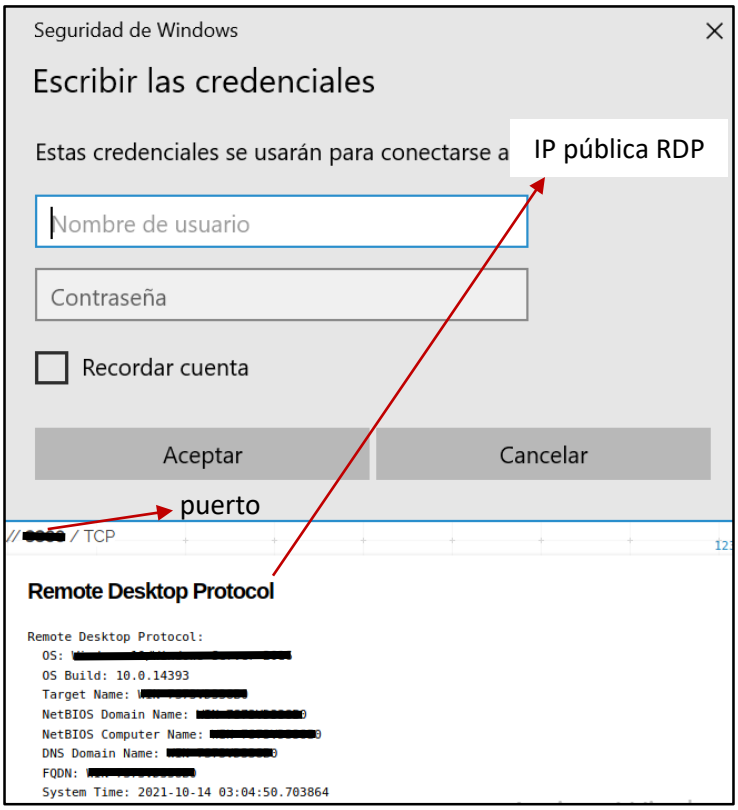


Figura 4.16 Ventana de acceso a escritorio remoto.
Fuente: Desarrollado por el investigador.

En [5] los riesgos se deben clasificar por el nivel de importancia y la gravedad de la pérdida, considerando que el costo económico para proteger la información no sea más alto de lo que realmente representa para la empresa. Para el análisis de riesgos hay que determinar los siguientes factores:

- Estimación del riesgo de perder el recurso (Ri).
- Estimación de la importancia del recurso (Wi).

Se entiende por recurso los servicios, servidores y equipos de la empresa. Para cuantificar el riesgo se puede asignar al riesgo de perder el recurso un valor numérico de 0 a 10, donde 0 representa que no hay riesgo y 10 presenta el riesgo más alto. Del mismo modo a la importancia del recurso se le asigna un valor de 0 a 10 donde 0 representa que no tiene importancia y 10 indica la máxima importancia. Esta relación se describe en la ecuación 4.1:

$$WRi = Ri * Wi \quad (4.1)$$

Donde WRi representa el riesgo evaluado del recurso "i".

En la tabla 4.2 se puede determinar que el servidor zimbra, cámaras de vigilancia, escritorio remoto y servidores MikroTik tienen un nivel de riesgo elevado ya que al vulnerar cualquiera de estos recursos se puede extraer información confidencial y frágil de la empresa, colaboradores y clientes. Cualquier tipo de información que salga del perímetro de red local empresarial pone en riesgo los datos y el personal por ende la continuidad de las actividades económicas de Simantec.

Tabla 4.2 Análisis de riesgos de los recursos de la empresa.

Recurso		**Riegos de pérdida (Ri)**	**Importancia (Wi)**	**Riesgo evaluado (WRi)**
Nº	**Nombre**			
1	Servidor Zimbra	10	10	100
2	Cámaras de vigilancia	10	10	100
3	Escritorio remoto	10	10	100
4	Servidores MikroTik	10	10	100

Fuente: Desarrollado por el investigador.

4.5. Sistema de Seguridad propuesto para la empresa

En este apartado se detalla soluciones UTM tanto en hardware como software escogidos por presentar características relevantes en comparación a otras marcas comerciales.

4.5.1. UTM Hardware

Para la selección del UTM tipo hardware se consideró costo, tiempo de entrega, soporte, facilidad de interacción con la marca y personal técnico además de las características, por lo tanto, de todas las soluciones existentes en el mercado se escogió dos marcas Check Point y Sophos.

Check Point: Los equipos UTM de la marca Check Point soluciones tanto hardware y software para mantener los niveles de seguridad en estructuras informáticas de pequeñas y grandes empresas y ofrece servicios de IPS, firewalls, antivirus, anti-spyware, filtrado

web, gestión e informes, networking, entro otros. En la figura 4.17 se muestra la arquitectura física descritas en la tabla 4.3.

Figura 4.17 Equipo Check Point 1530.
Fuente: [30]

Las interfaces físicas que presenta este equipo son:

Tabla 4.3 Interfaces equipo Check Point.

1	802.11 n/ac Wi-Fi (opcional)	5	Power button
2	USB port	6	USB-C Console port
3	5x 1GbE LAN switch	7	12V power connector
4	1x 1GbE WAN interface		

Fuente: [30]

Sophos: Dispone de productos empresariales para empresas en crecimiento, los UTM de escritorio permiten todas las funciones de seguridad que dispositivos de gran tamaño, pero con diseño compacto y a menor precio. El equipo XG 115 es una solución de seguridad integral y flexible que mitiga amenazas informáticas por medio de funciones de seguridad y red como firewall, VPN, IPS, control de aplicaciones, antivirus, anti-spam, filtrado de contenidos web. QoS, traffic shaping, entre otros. En la figura 4.18 se muestra la arquitectura física descritas también en la tabla 4.6.

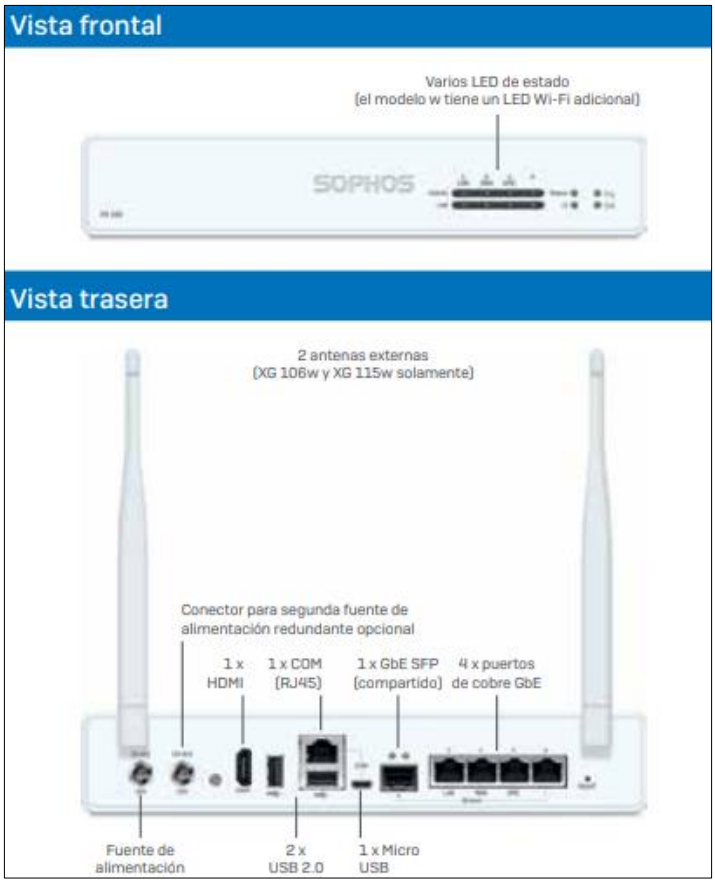


Figura 4.18 Equipo Sophos XG 115.
Fuente: [31]

La tabla 4.4 muestra las interfaces físicas del equipo Sophos XG 115:

Tabla 4.4 Interfaces equipo Sophos XG 115.

Interfaces físicas	**Características**
Nº de antenas	2 externas
Funciones MIMO	2 x 2:2
Interfaz inalámbrica	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)
Almacenamiento	SSD integrado
Interfaces Ethernet (fijas)	4 GbE cobre 1 GbE SFP (compartido)*
Módulos de conectividad	Módulo DSL SFP (VDSL2) Transceptores SFP
Puertos de E/S (trasero)	2 x USB 2.0 1 x Micro-USB 1 x COM (RJ45) 1 x HDMI

Interfaces físicas	Características
Fuente de alimentación	Alcance automático externo de DC: 12 V, 100-240 VCA, 36 W@50-60 Hz Fuente de alimentación redundante opcional (externa)

Fuente: [31]

La tabla 4.5 presenta un cuadro comparativo entre las soluciones UTM Check Point y Sophos de la serie XG, estos productos son aptos para una organización de 50 a 100 usuarios y en escenarios comunes del día a día.

Tabla 4.5 Sophos vs Check Point.

Parámetros	Sophos XG 115	Check Point 1530
Rendimiento del Firewall (Mbps)	4.000	2.000
Rendimiento del IPS (Mbps)	950	670
Rendimiento del NGFW (Mbps)	1.000	600
Rendimiento de la protección contra amenazas (Mbps)	375	340
Conexiones simultáneas	1.570.000	500.000
Conexiones nuevas/seg.	19.400	10.500
Conexiones usuarios VPN	80	100
Rendimiento de VPN IPsec (Mbps)	560	970
Precio incl. IVA (USD)	1.385,44	1.456,00
Tiempo de entrega (días)	25	45
Soporte 24x7, 5 horas (USD)	150	200
Facilidad de interacción con la marca	Fácil	Medio

Fuente: [32]

Ambas soluciones muestran ventajas y desventajas una sobre la otra sin embargo los parámetros más relevantes para elegir la mejor solución para la empresa son rendimiento de firewall, conexiones VPN, tiempo de entrega y precio, por lo tanto, el UTM de la marca Sophos fue elegido para la implementación de la plataforma de seguridad.

4.5.2. UTM Software

Entre las aplicaciones UTM de pago se encuentra Sophos y en las OpenSource se tiene Pfsense, OPNsense, Endian Firewall entre otras. La tabla 4.6 es un cuadro comparativo entre las 3 aplicaciones UTM de código abierto y presenta las siguientes características.

Tabla 4.6 Comparación aplicaciones UTM OpenSource.

Características	**Pfsense**	**OPNsense**	**Endian Firewall**
Firewall	Si	Si	Si
Fecha de creación	2004	2015	2005
Interfaz gráfica basada en web	Si	Si	Si
Asistente de configuración	Si	Si	Si
Soporte IPv4 e IPv6	Si	Si	Si
OpenVPN	Si	Si	Si
IPSec	Si	Si	Si
L2TP	Si (through package)	Si (tramite plugin)	Si
Monitoreo de la red en tiempo real	Si	Si	Si
IPS	Si (basado en Snort)	Si (basado en Suricata)	Si
Soporte	Si (Netgate Global Support)	Si (foros, comunidad, documentación, mail)	Opcional (Endian)
Actualización de seguridad	Si, con lanzamientos de parches	Si, semanalmente	Si, a la última versión

Fuente: [33] [34]

El UTM ha ser empleado por sus características será PfSense ya que se ajusta a las necesidades de la empresa. Este proyecto es una distribución de firewall gratuito basado en FreeBSD e incluye una interfaz web para la configuración y administración bajo la licencia Apache 2.0. Entre las aplicaciones que ofrece se encuentran: servidor VPN, balanceo de carga, modelado de tráfico, portal cautivo, dispositivo UTM, firewall, IDS/IPS, proxy, filtrado de contenido web y más [35].

A continuación, se nombran algunas características de PfSense:

- **Firewall y enrutador:** Inspección completa de paquetes (SPI), anti-spoofing, DNS dinámico, proxy inverso, portal cautivo, admite IPv4 e IPV6 simultáneamente, mapeo NAT, servidor DHCP entre otras.
- **VPN:** Dentro de las redes privadas virtuales se puede configurar parámetros como IPsec, OpenVPN, soporte VPN site to site y remote access, cifrado SSL, soporte NAT, enrutamiento y autenticación de usuarios.
- **IPS:** Para la prevención de intrusos el análisis de paquetes está basado en snort, inclusive se dispone de paquetes opcionales de código abierto para el bloqueo de aplicaciones.
- **Fiabilidad empresarial:** Dispone de un asistente de modelado de tráfico que permite reservar o restringir el ancho de banda según la prioridad del tráfico.
- **Autenticación de usuario:** Administración de base de datos de usuarios para otorgar privilegios basados en las necesidades de la organización y bloqueo automático después de varios intentos de ingreso.
- **Proxy y filtrado de paquetes:** Permite aplicar proxy HTTP y HTPPS, filtrado de URL, an-tivirus y contenido, también muestra la lista negra de nombres de dominio e informes de uso diario, mensuales, etc.
- **Administración/Configuración:** La configuración de Pfsense está basada en entorno web, la configuración inicial va acompañada de un asistente de instalación, actualizaciones simples, soporte multilingue y permite realizar copias de seguridad automática.
- **Sistema de seguridad:** Permite el acceso SSH basado en claves y aplica una estricta seguridad de transporte HTTP.

- **Informes y seguimiento:** Presenta un panel de widgets configurables, gráficos de monitoreo local, gráficos de tráfico en tiempo real, notificaciones a través de la interfaz web y el registro de acceso del administrador puede ser local o remoto.

4.6. Implementación del sistema de defensa hardware

4.6.1. Topología de la red con el equipo Sophos XG 115

Para la inserción del nuevo equipo UTM en la red de la empresa se ha modificado la estructura de tal manera que el firewall quede entre la red LAN de Guayllabamba y la salida a internet. La conexión entre el equipo Sophos XG 115 y la red LAN de la matriz se hará a través de un túnel IPsec y de igual manera para comunicar la matriz con la sucursal se empleará otro túnel IPsec entre el Sophos y el MikroTik de Cayambe.

La tecnología escogida para establecer la comunicación entre la red local (matriz) y la red remota (sucursal) es IPsec como se muestra en la figura 4.19, al actuar en la capa 3 o red se convierte en un protocolo completamente seguro garantizando total confidencialidad pues cifra los paquetes de datos enviados a través de una red IP haciéndolos inaccesibles e invisibles para terceros.

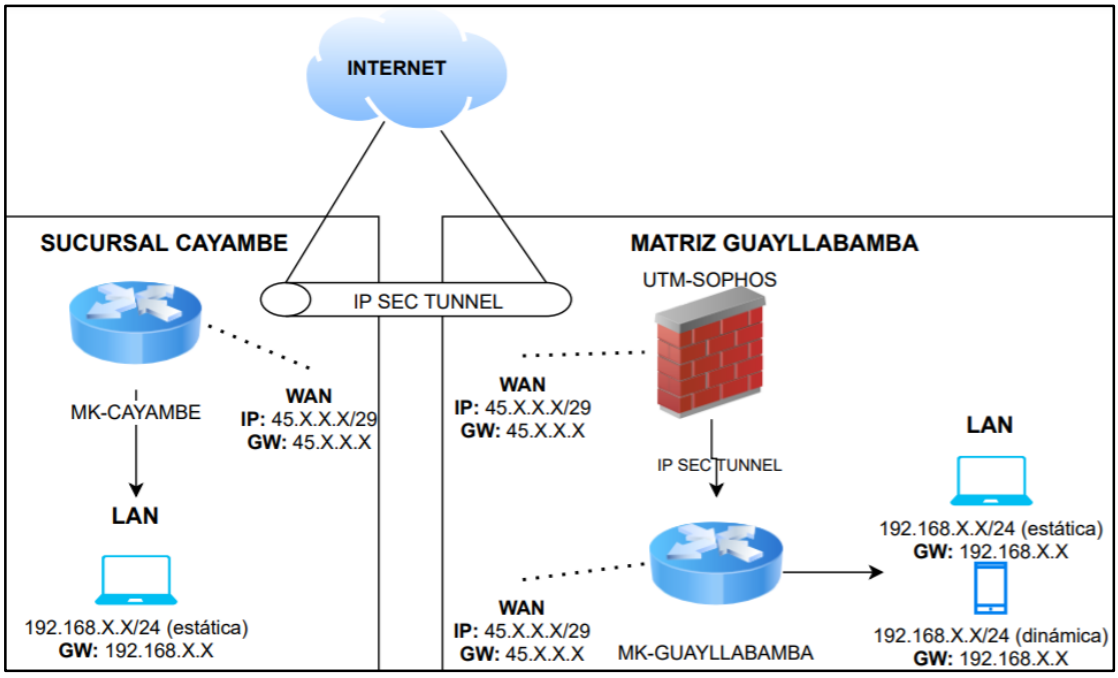


Figura 4.19 Topología física de la red con el equipo UTM.
Fuente: Desarrollado por el investigador.

4.6.2. Configuración Sophos XG 115

Para establecer la comunicación entre los dos equipos UTM y MikroTik se ha especificado una serie de pasos, a continuación se muestra la configuración en el Sophos XG 115.

- **Configurar la política IPsec:** Ir a VPN, IPsec policie, configurar los parámetros que muestra la figura 4.20 y clic en guardar. El protocolo de intercambio de claves por red versión 2 o IKEv2 brinda en el protocolo IPsec un canal de comunicación seguro para el intercambio de información entre sedes a través de Internet ya que el tráfico es cifrado, autenticado y sometido a una prueba de integridad de datos. En la fase 1 el grupo de Diffie-Hellman (DH) elegido es el Grupo 14 (2048 bits) porque a mayor número de bits la clave es más difícil de romper entre los pares autenticados sin dejar un lado que este proceso requiere mayor procesamiento de CPU. La encriptación es AES 256 (Advanced Encryption Standard) siendo la más segura ante atraques de fuerza bruta ya que para romper el cifrado se necesita de un ordenador que procese tantas combinaciones posibles que exceden su capacidad de cómputo. Por último, el algoritmo de autenticación para verificar la integridad y autenticidad de los datos fue usado fue SHA2 256

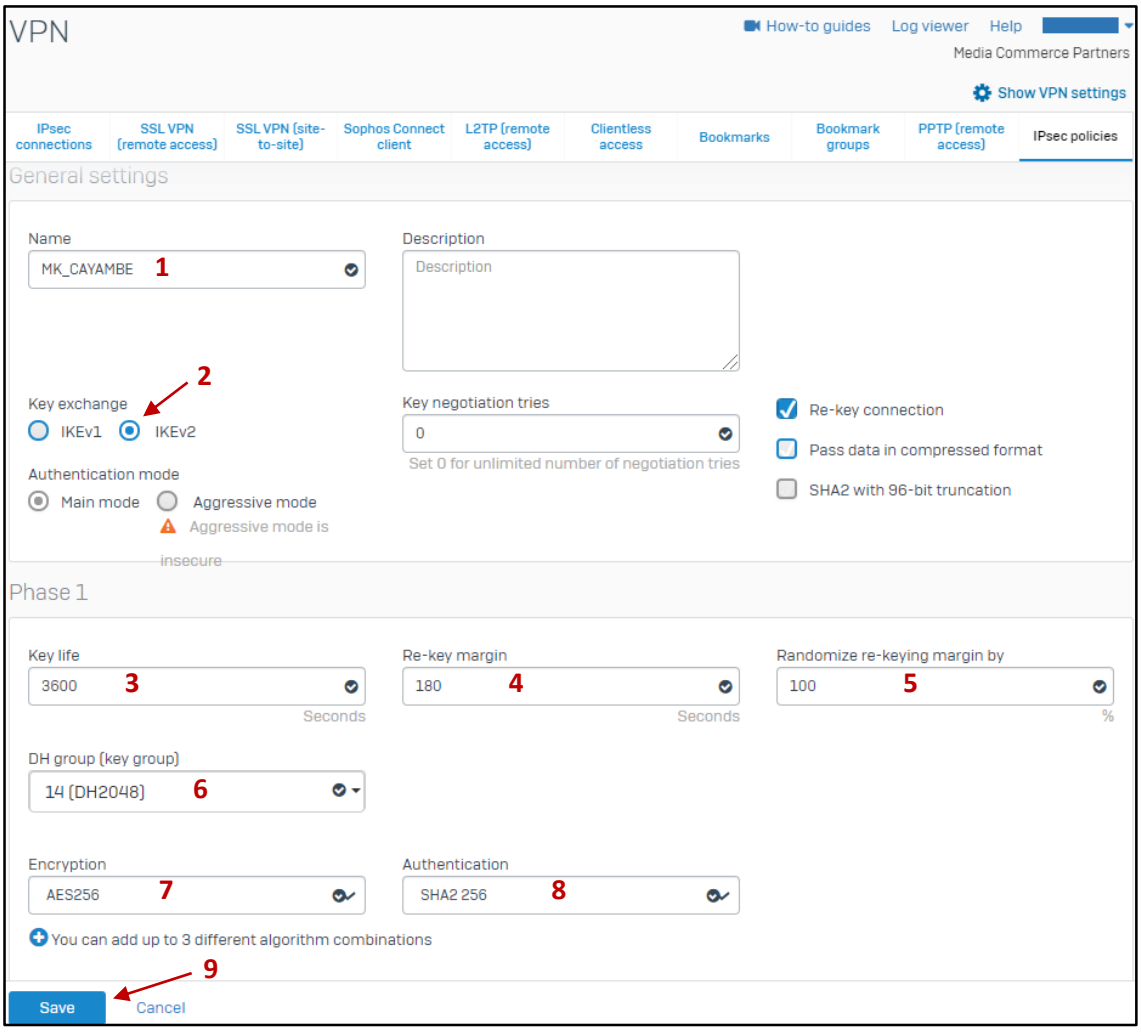


Figura 4.20 Configuración de la política IPsec en el equipo UTM.
Fuente: Desarrollado por el investigador.

La política IPsec presenta dos fases para configurar la seguridad durante la autenticación de los pares que intercambiaran información, en este caso la fase 2 (phase 2) contiene los mismos parámetros de la fase 1.

- **Configurar la conexión IPsec:** Ir a VPN, IPsec connections, configurar los parámetros que muestra la figura 4.21 y clic en guardar. La clave configurada en el Sophos debe ser la misma clave que se va a configurar el Mikrotik para que se cree una pasarela de seguridad y se establezca la comunicación entre las dos sedes.

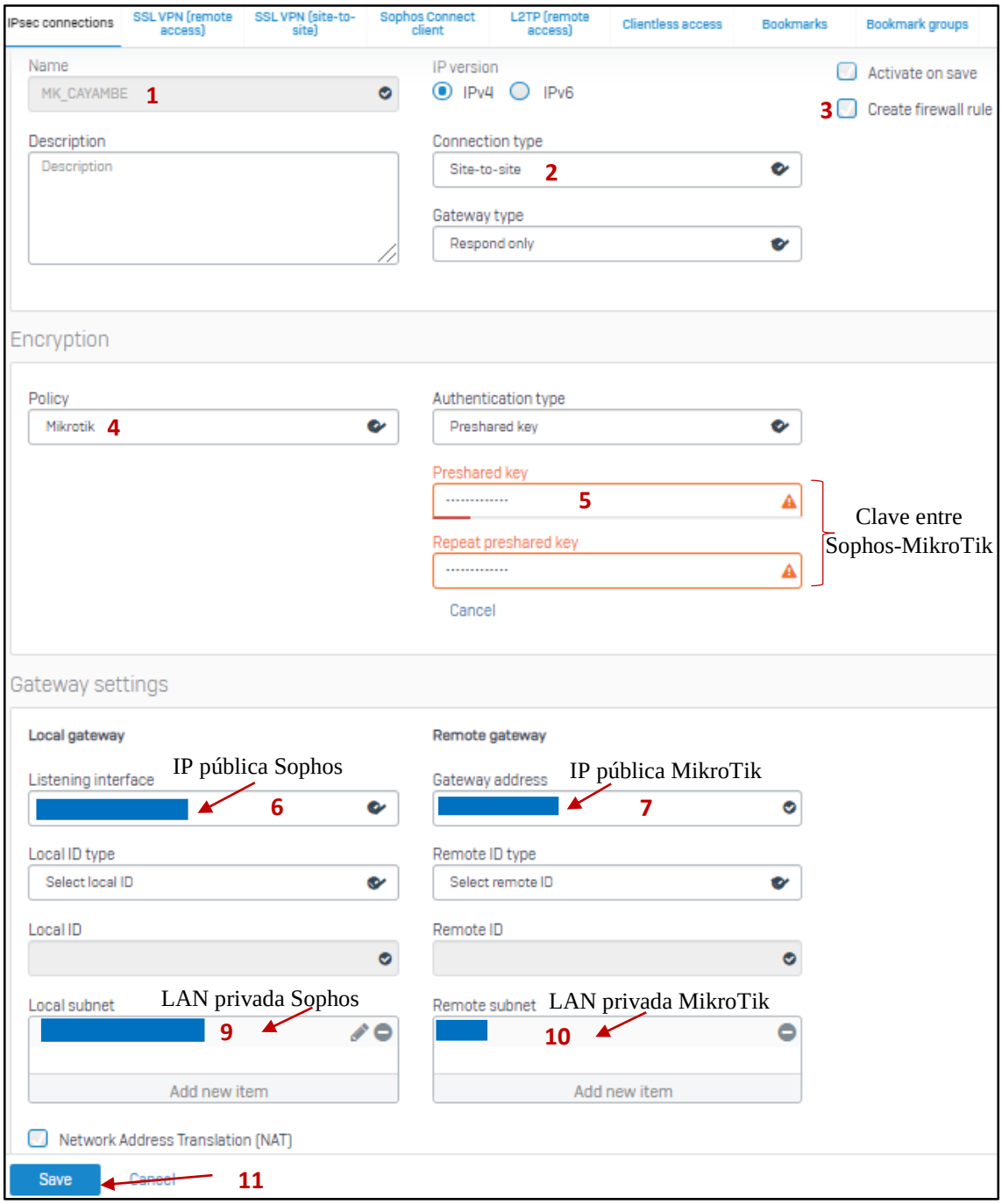


Figura 4.21 Configuración de la conexión IPSec.
Fuente: Desarrollado por el investigador.

- **Revisión de la regla en el firewall**: Ir a firewall, automatic VPN rule, IPSec prueba y revisar los parámetros que muestra la figura 4.22.

Figura 4.22 Regla de firewall creada para el túnel IPSec.
Fuente: Desarrollado por el investigador.

Finalmente, la figura 4.23 muestra el estado del túnel IPSec, en este caso está inactivo y sin conexión hasta configurar el protocolo IPSec en el MikroTik.

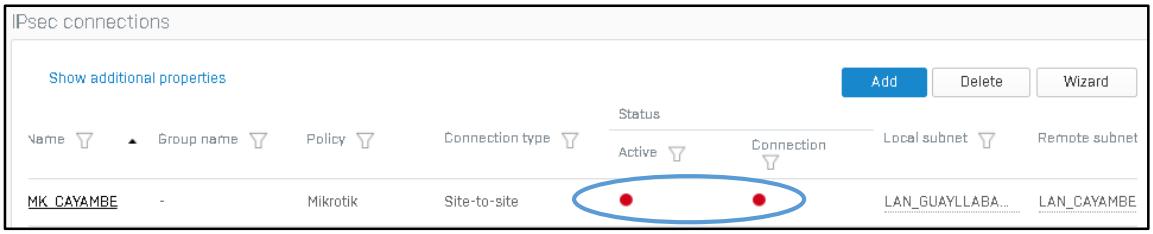


Figura 4.23 Estado de la conexión.
Fuente: Desarrollado por el investigador.

4.6.3. Configuración MikroTik

Para concretar la comunicación entre la matriz y la sucursal se debe crear el túnel IPSec en el MikroTik siguiendo estos pasos:

- **Configuración del perfil:** Ir a IP, IPsec y configurar el profile bajo los parámetros que se muestra en la figura 4.24, el algoritmo empleado para generar un hash de datos es SHA256, el algoritmo de encriptación de datos es a través de AES256 y el grupo de Diffie Hellman (DH) es modp2048; siendo estos tres compatibles entre sí.

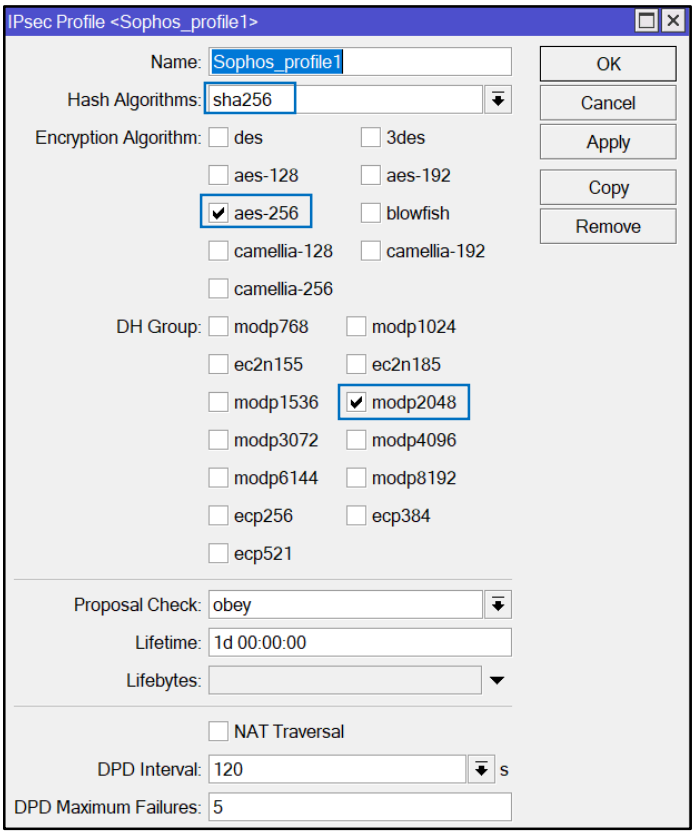


Figura 4.24 Configuración del perfil.
Fuente: Desarrollado por el investigador.

- **Configuración del emparejamiento o peer:** Ir a IP, IPsec, clic en IPsec peer y configurar los parámetros que se muestra en la figura 4.25. El modo de intercambio de claves de Internet es IKE2, protocolo de tunelización basado en IPSec.

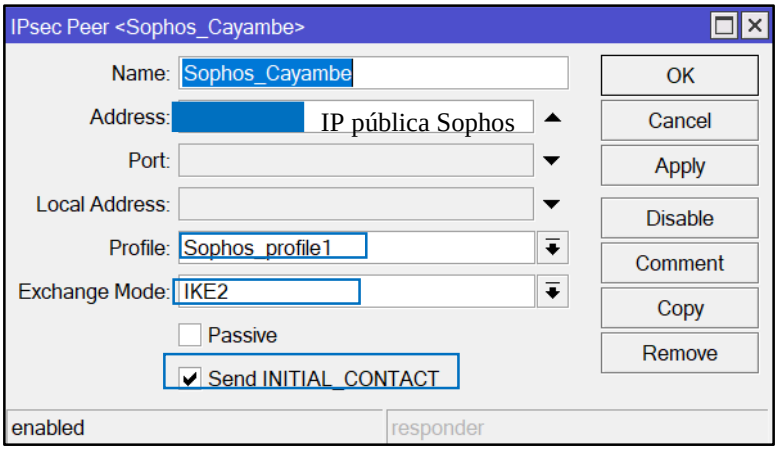


Figura 4.25 Configuración del IPsec Peer.
Fuente: Desarrollado por el investigador.

- **Configuración de la identidad:** Ir a IP, IPsec, clic en IPsec Identity y configurar los parámetros que se muestra en la figura 4.26.

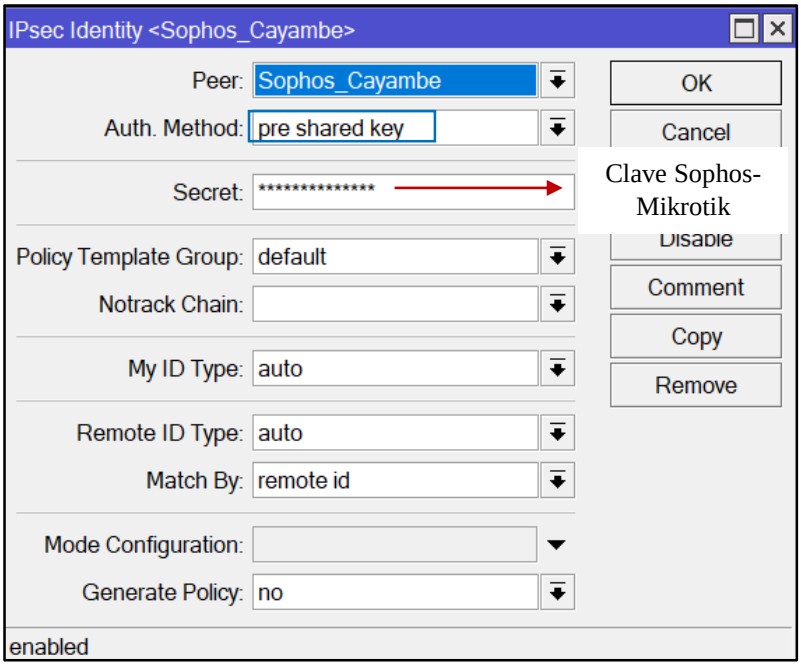


Figura 4.26 Configuración del IPsec Identity.
Fuente: Desarrollado por el investigador.

- **Configuración de la propuesta:** Ir a IP, IPsec, clic en IPsec Proporsal y configurar los parámetros que se muestra en la figura 4.27. Los algoritmos de encriptación empleados son AES256-cbc, AES256-ctr y AES256-gcm siendo los dos primeros protocolos antiguos y el último un algoritmo que proporciona mayor seguridad, sin embargo, en esta configuración se selecciona los tres protocolos con fines de compatibilidad en la configuración del túnel IPSec. El grupo de Perfect Forward Secrecy (PFS) es modp2048 para volver las claves más seguras y no necesariamente debe coincidir con el grupo DH.

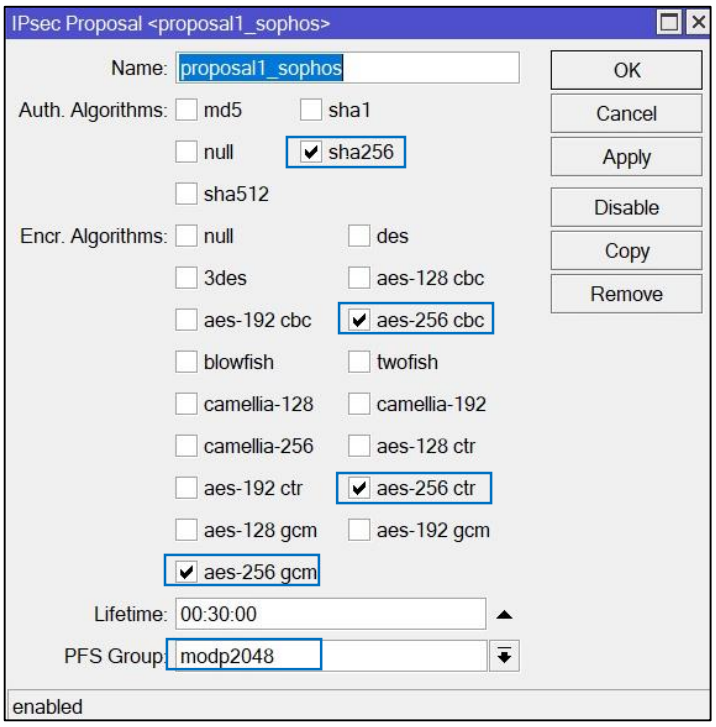
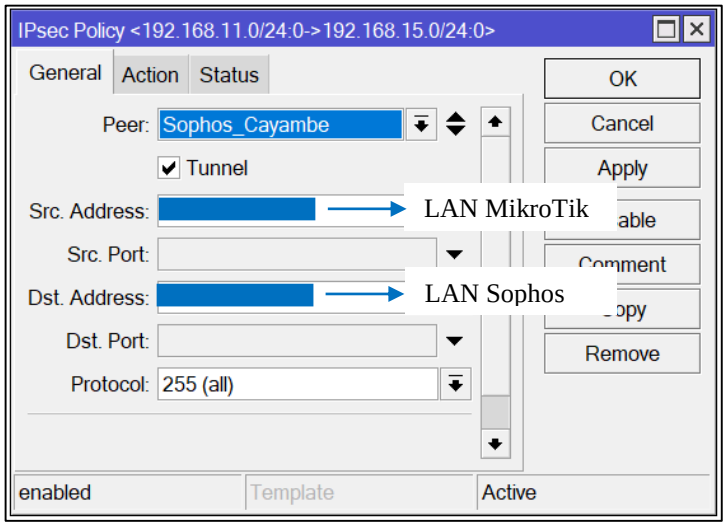


Figura 4.27 Configuración del IPsec Proposal.
Fuente: Desarrollado por el investigador.

- **Configuración de la política IPsec:** Ir a IP, IPsec, clic en IPsec Policy y configurar los parámetros que se muestra en la figura 4.28.

a)



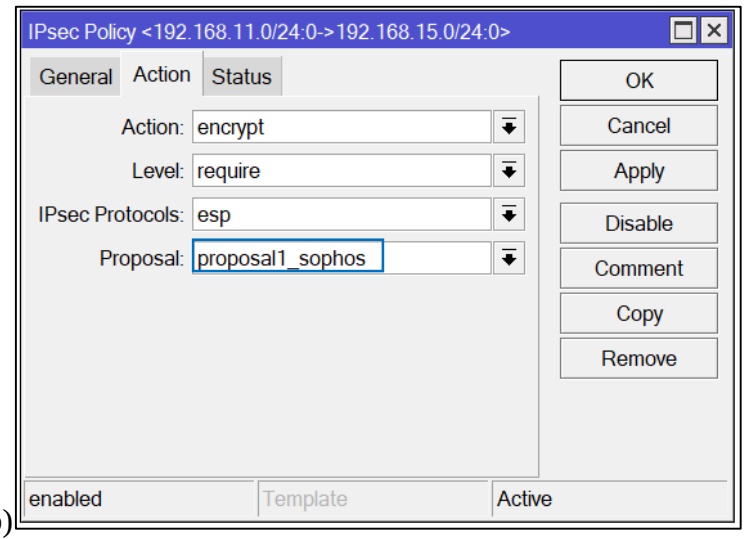
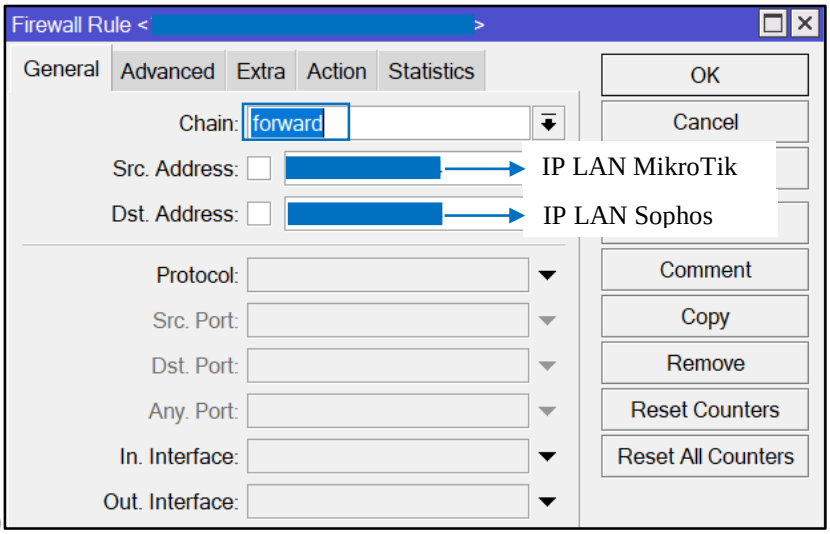
b)


Figura 4.28 Configuración del IPsec Policy. a) Configuración general. b) Configuración de acción.
Fuente: Desarrollado por el investigador.

- **Configuración de las reglas de filtrado:** Ir a IP, Firewall, clic en Filter Rules y agregar una nueva regla, esta regla debe ser creada de ida y vuelta, es decir, una regla con la dirección de origen desde la IP-MikroTik y la IP de destino la del equipo Sophos y otra regla con origen y destino contrario, en action se debe escoger la opción *accept* para permitir el tráfico entre las dos redes como muestra la figura 4.29.

a)


b)

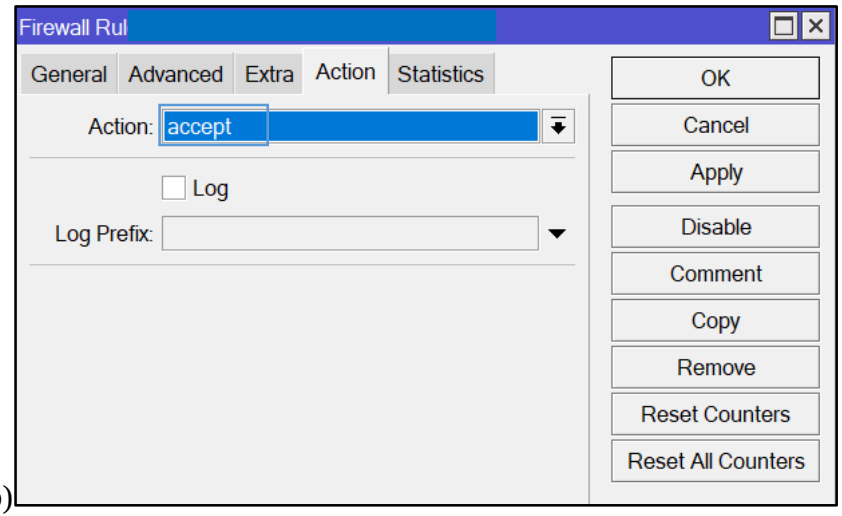


Figura 4.29 Creación de Firewall Rule. a) Configuración general. b) Configuración de acción.
Fuente: Desarrollado por el investigador.

- **Configuración Firewall-NAP:** Ir a IP, Firewall, clic en NAP y agregar el direccionamiento NAP como muestra la figura 4.30, además en action se debe escoger la opción *accept* para permitir el tráfico entre las dos redes. Para fines prácticos la red local que manejará el Sophos es la dirección IP 192.168.15.0/24.

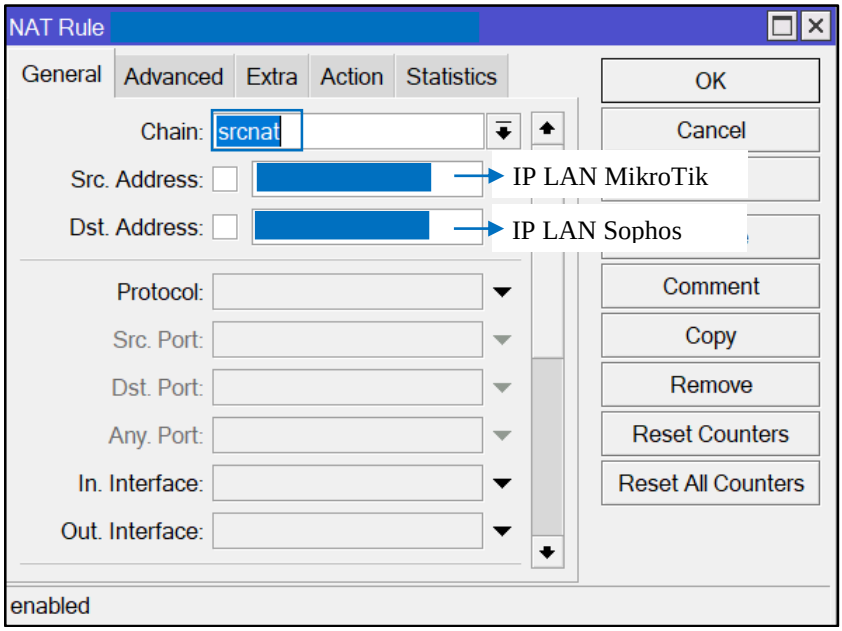


Figura 4.30 Direccionamiento NAP.
Fuente: Desarrollado por el investigador.

- **Configuración de la ruta:** Ir a IP, IPsec, clic en IPsec Proporsal y configurar los parámetros que se muestra en la figura 4.31, un parámetro importante es escoger siempre como Gateway la interface que este en modo bridge o la LAN de la red en la cual se configure el túnel IPsec.

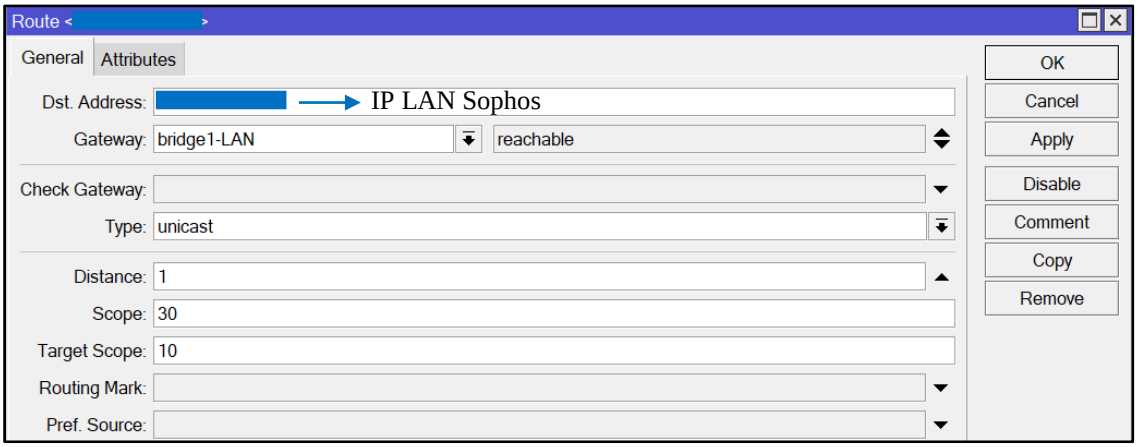


Figura 4.31 Agregar la ruta.
Fuente: Desarrollado por el investigador.

- **Estado de conexión:** Ir a IP, IPsec, clic en Active Peers y comprobar si el estado cambio a *established* como muestra la figura 4.32.

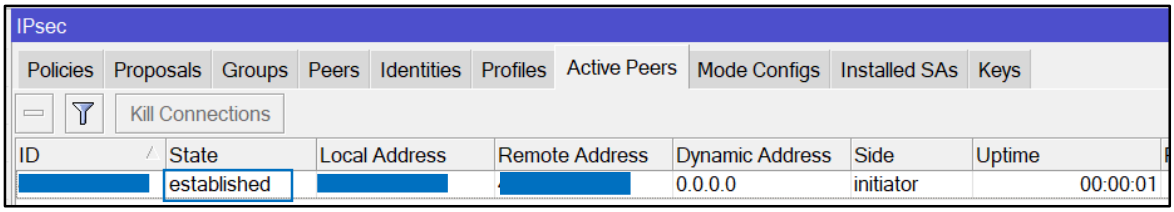


Figura 4.32 Conexión estable entre el MikroTik y Sophos.
Fuente: Desarrollado por el investigador.

Una vez establecida la conexión en el equipo Mikrotik como muestra la figura 4.33 se debe revisar el estado de la conexión en el Sophos, en Status la comunicación pasa de rojo a verde indicando si se entablo la conexión IPsec.

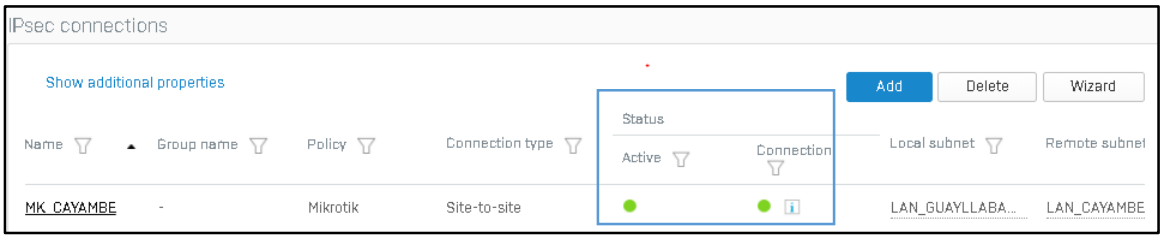


Figura 4.33 Conexión estable entre el MikroTik y Sophos.
Fuente: Desarrollado por el investigador.

4.6.4. Pruebas de conectividad

Para confirmar que la conexión está establecida se procede a hacer ping desde el terminal del MikroTik ubicado en Cayambe hasta alcanzar el Gateway de la red LAN configurada en el equipo Sophos ubicado en la matriz Guayllabamba como indica la figura 4.34.

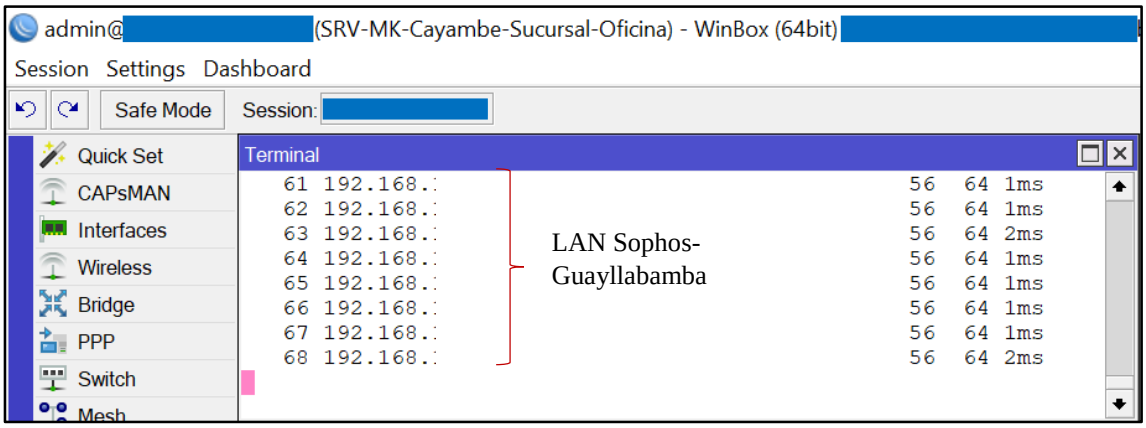


Figura 4.34 Ping exitoso desde MikroTik Cayambe hasta LAN Sophos en la matriz.
Fuente: Desarrollado por el investigador.

Ahora se hace la misma prueba de conectividad desde una PC configurada con una IP de la red LAN del equipo Sophos, en este caso la IP obtenida por DHCP es la 192.168.15.175/24, como muestra la figura 4.35, a través del cmd se hace un ping al Gateway de la red LAN configurada en el MikroTik en Cayambe

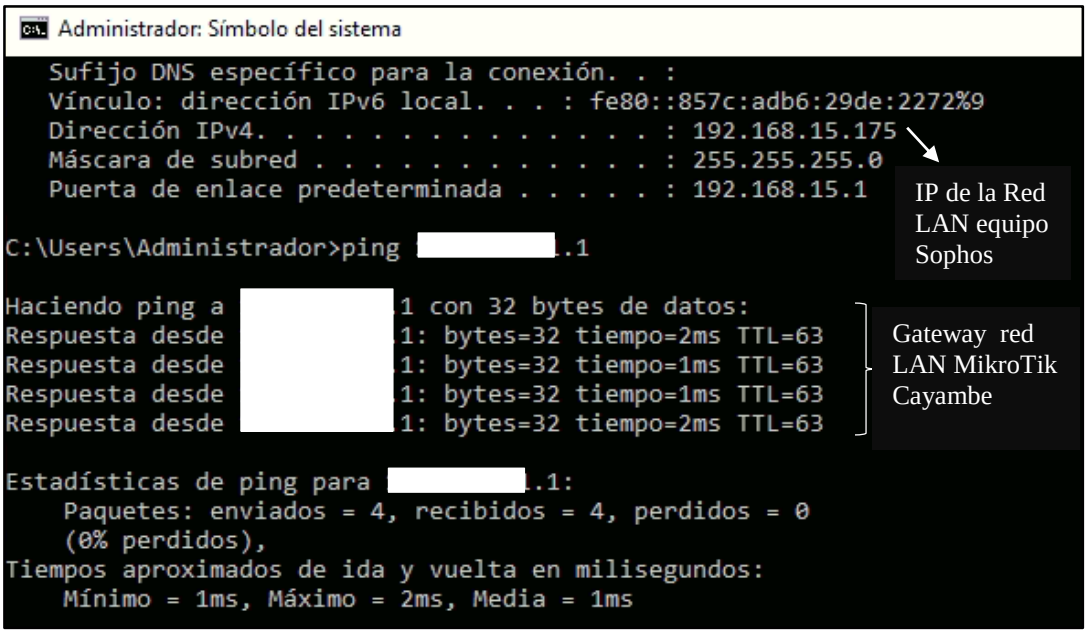


Figura 4.35 Ping exitoso desde LAN Sophos en la matriz hasta Mikrotik Cayambe.
Fuente: Desarrollado por el investigador.

4.6.5. Configuración de VPN

Una VPN es una tecnología empleada para conectar computadoras a una red privada por medio de internet. Uno de los protocolos que se utiliza en una VPN es IPsec para mejorar la seguridad a través de algoritmos de cifrado estables y un sistema de autentificación más íntegro. Para crear una VPN en el equipo Sophos XG 115 se debe configurar los siguientes parámetros:

- **Creación de un certificado:** Para crear una VPN primero se debe configurar un certificado para luego ser asociado a la SSL VPN o red privada virtual con certificado SSL (Secure Sockets Layer). Para ello se debe abrir la interface de Sophos, ir a certificados y añadir uno nuevo como se muestra en la figura 4.36.

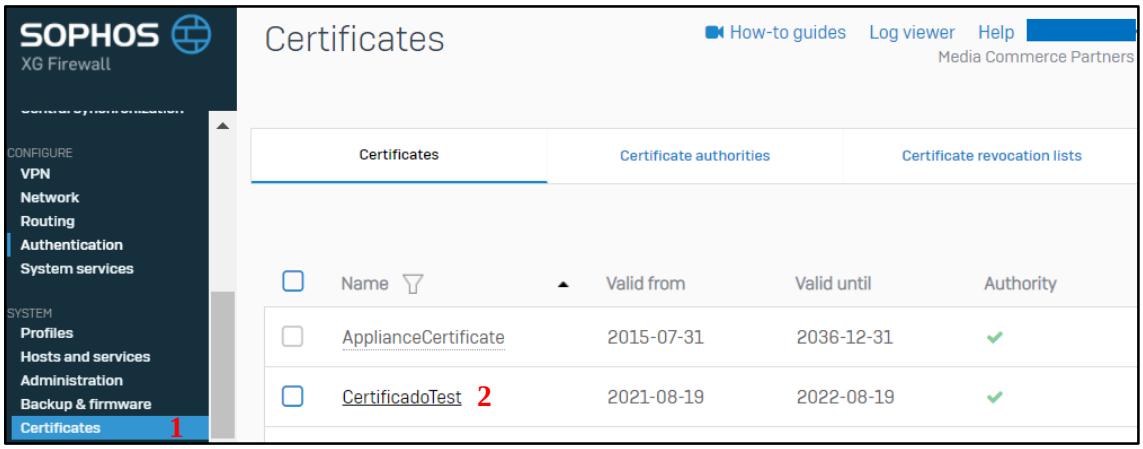


Figura 4.36 Creación del certificado.
Fuente: Desarrollado por el investigador.

- **Creación de usuarios:** La figura 4.37 indica cómo crear los usuarios para ello dar clic en configuración, autenticación, usuarios y agregar, considerando que cada nombre será el equivalente de un usuario VPN.

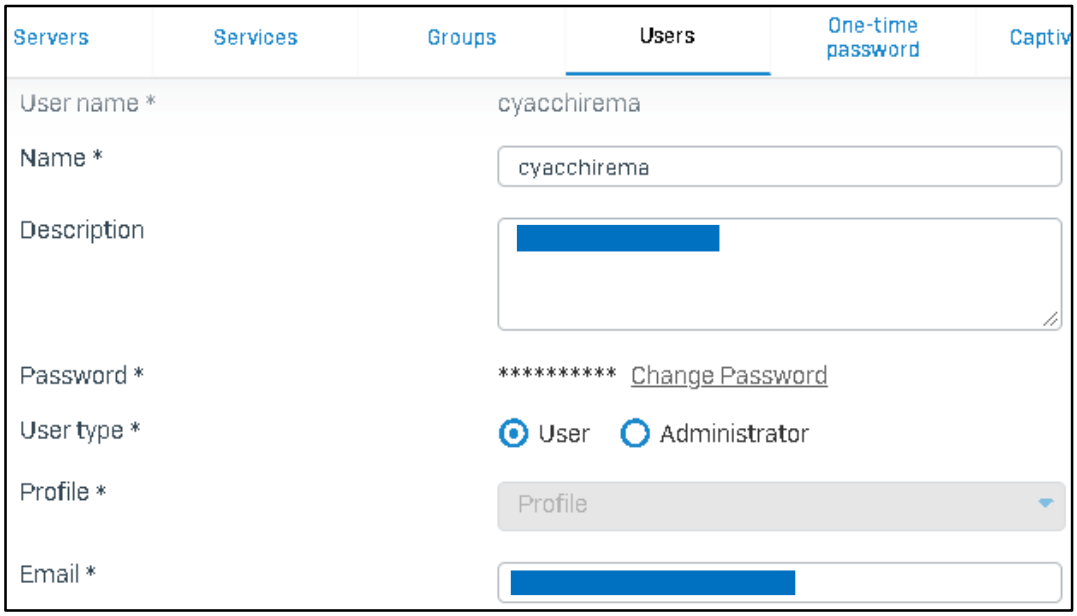


Figura 4.37 Creación de usuarios.
Fuente: Desarrollado por el investigador.

- Un aspecto importante que se debe tener en consideración es la elección del acceso remoto de la VPN, es este caso se debe crear la política SSL VPN que va a proporcionar acceso remoto a través de un portal web y acceso a nivel de red a

través de un túnel seguro SSL entre usuario y la red de la empresa. Para ello ir a configuración, clic en VPN, SSL VPN luego en agregar y aparecerá una ventana como se muestra en la figura 4.38, entonces se debe configurar los siguientes parámetros.

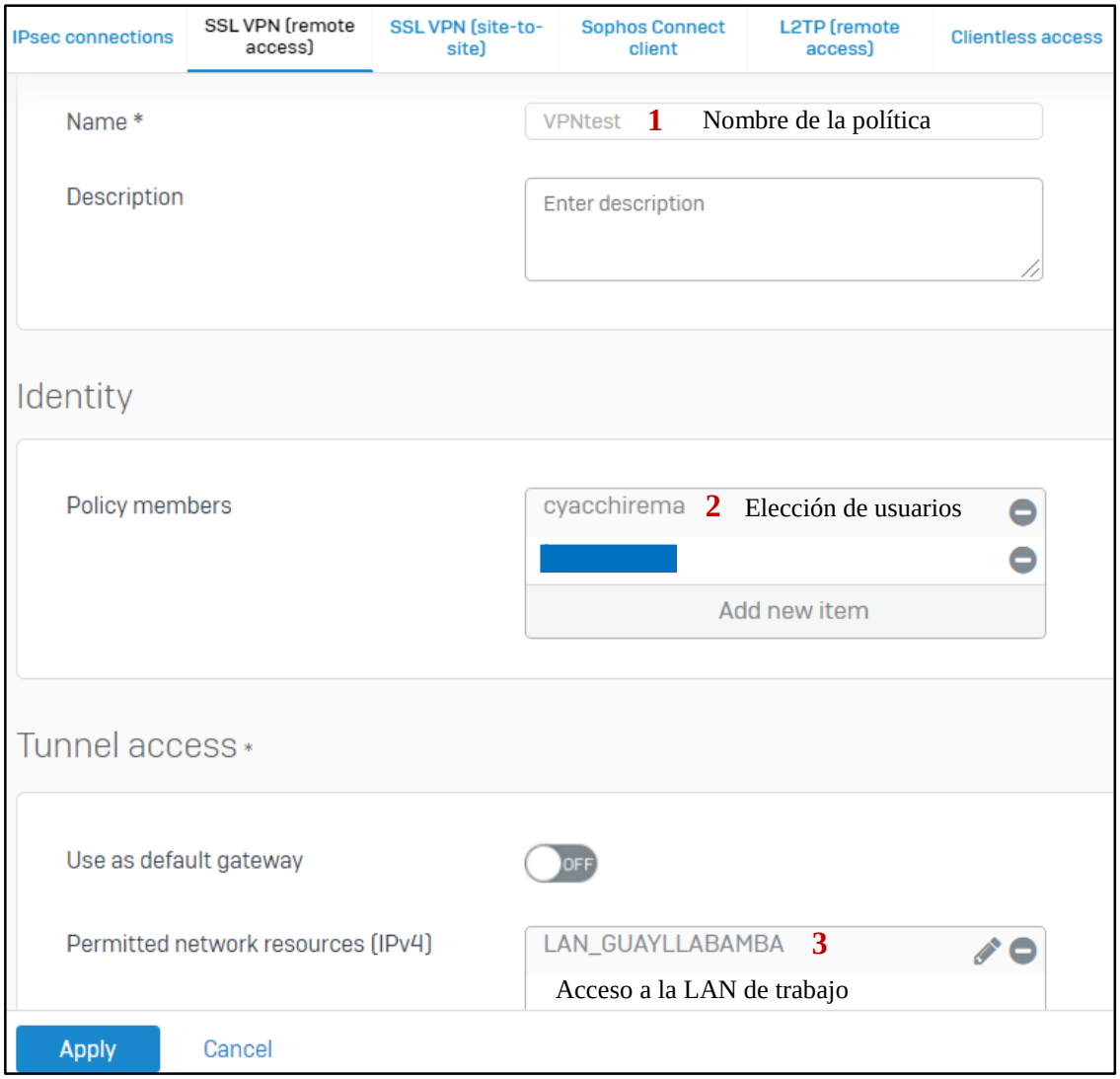


Figura 4.38 Creación de la política SSL VPN.
Fuente: Desarrollado por el investigador.

- Para culminar la configuración de los usuarios se debe configurar la política creada anteriormente y guardar como indica la figura 4.39.

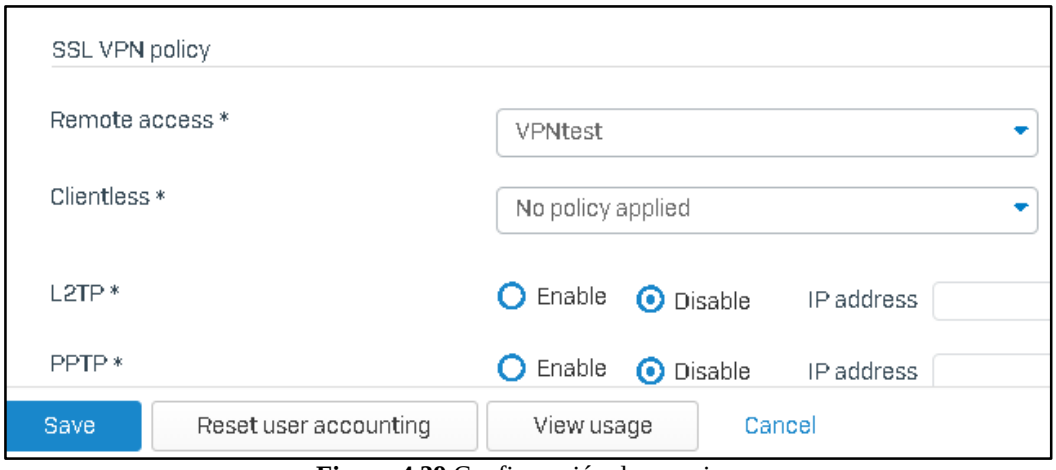


Figura 4.39 Configuración de usuarios.
Fuente: Desarrollado por el investigador.

- La figura 4.40 indica la interface web para ingresar al portal de usuario y acceder a los servicios que este portal ofrece.

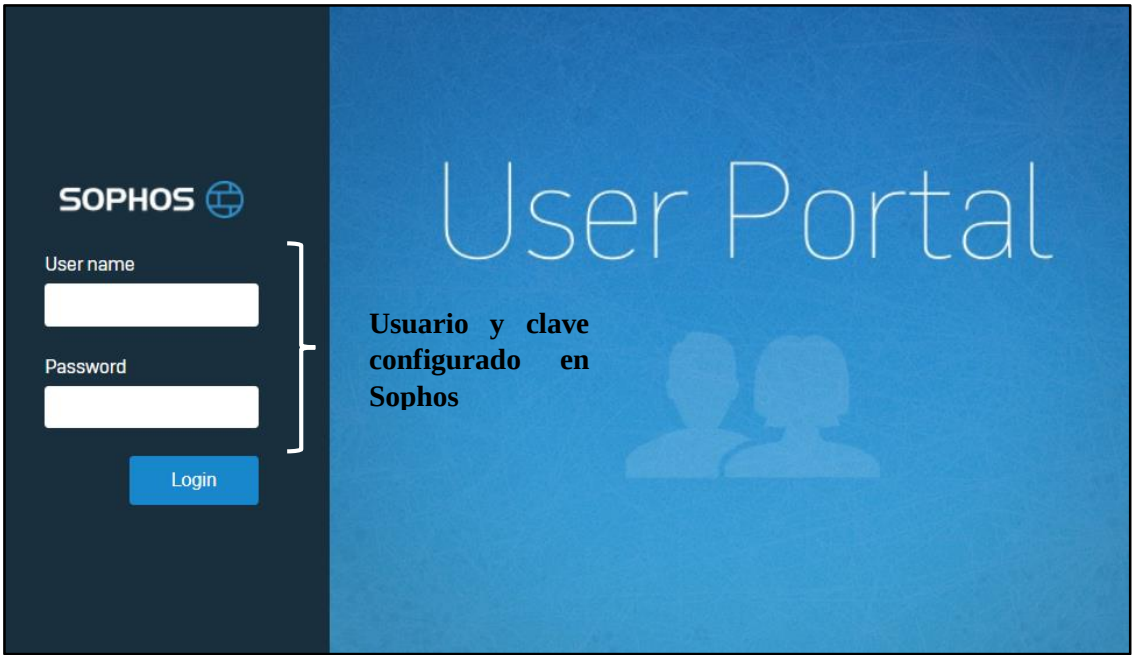


Figura 4.40 Portal de usuario.
Fuente: Desarrollado por el investigador.

- Una vez dentro de la interface de usuario se debe descargar e instalar la aplicación para Windows u otro sistema operativo como muestra la figura 4.41.

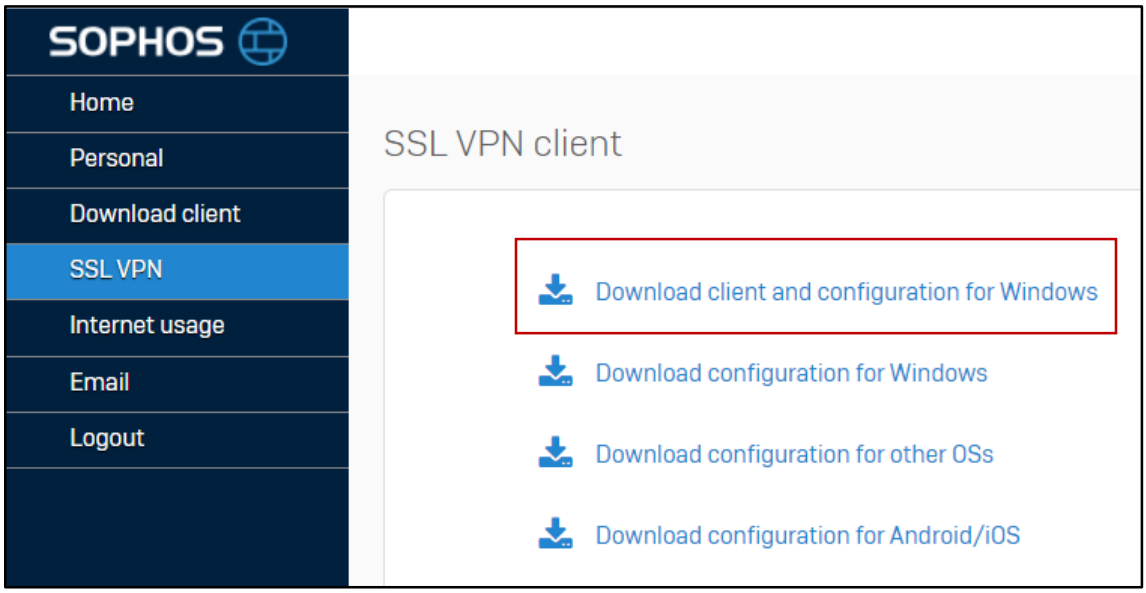
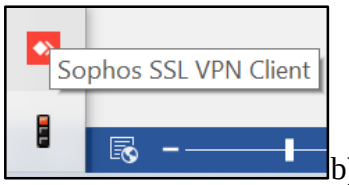


Figura 4.41 Aplicación VPN para Windows.
Fuente: Desarrollado por el investigador.

- Una vez instalada la VPN como indica la figura 4.42, la aplicación para cliente aparecerá en la parte inferior derecha del escritorio en forma de semáforo en donde el color rojo significa que no está activa, para activar damos clic derecho y conectar.

a) 

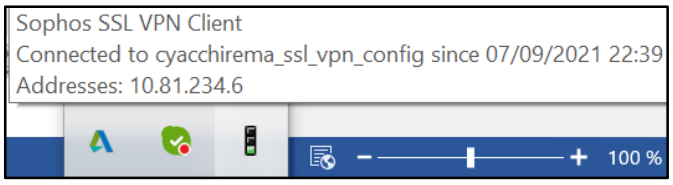
b) 

Figura 4.42 a) Cliente VPN inactivo. b) Cliente VPN activo.
Fuente: Desarrollado por el investigador.

- **Pruebas de conexión:** La figura 4.43 indica las pruebas de conexión mediante un ping desde la PC del cliente o usuario (lugar remoto en Quito) a la red local de la oficina en Guayllabamba.

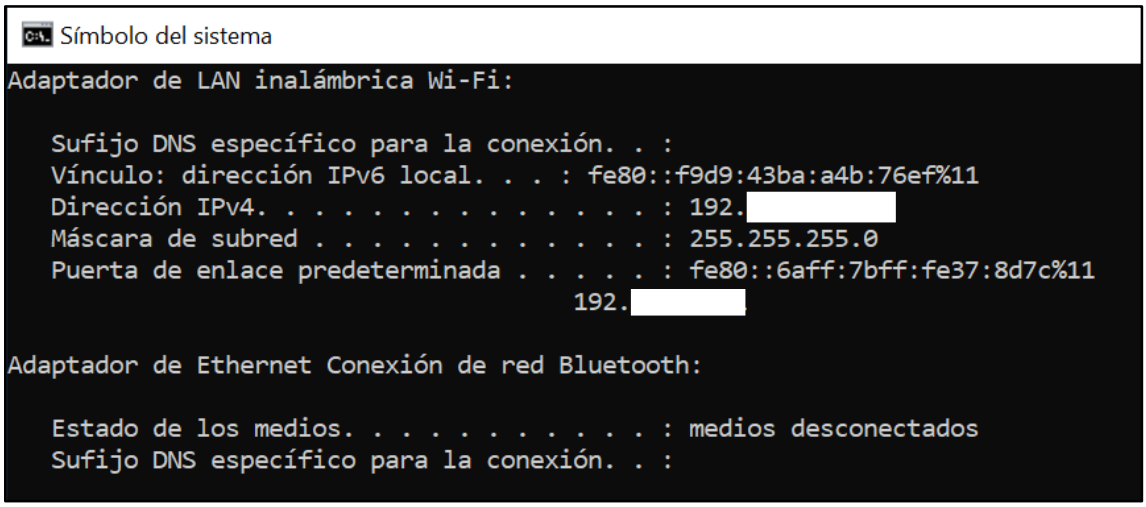


Figura 4.43 Dirección IP de la PC del usuario en Quito.
Fuente: Desarrollado por el investigador.

- Una vez activa, la VPN asigna una IP a través de la ethernet 2 a la PC del cliente remoto, este rango de IPs está configurada en el equipo Sophos como indica la figura 4.44.

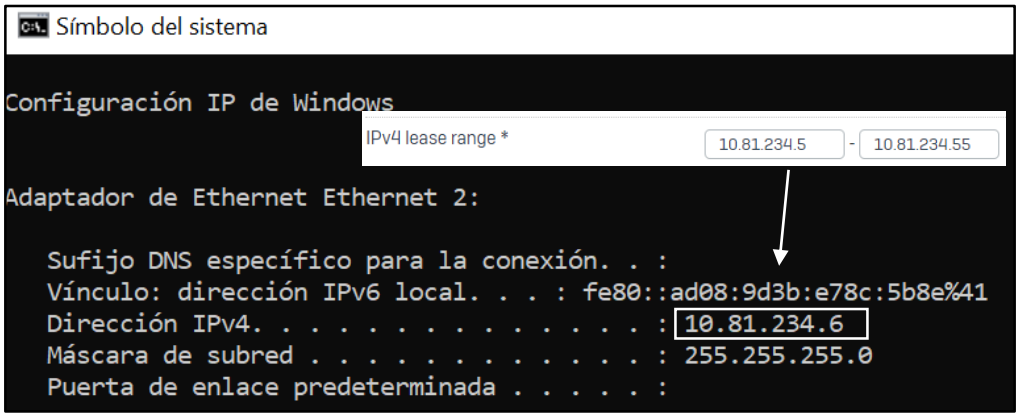


Figura 4.44 Dirección IP de la PC del usuario asignada por la VPN.
Fuente: Desarrollado por el investigador.

- En la figura 4.45 se muestra las pruebas de conectividad a través de la VPN desde una PC ubicada en Quito hacia el Gateway de la red LAN ubicada en Cayambe.

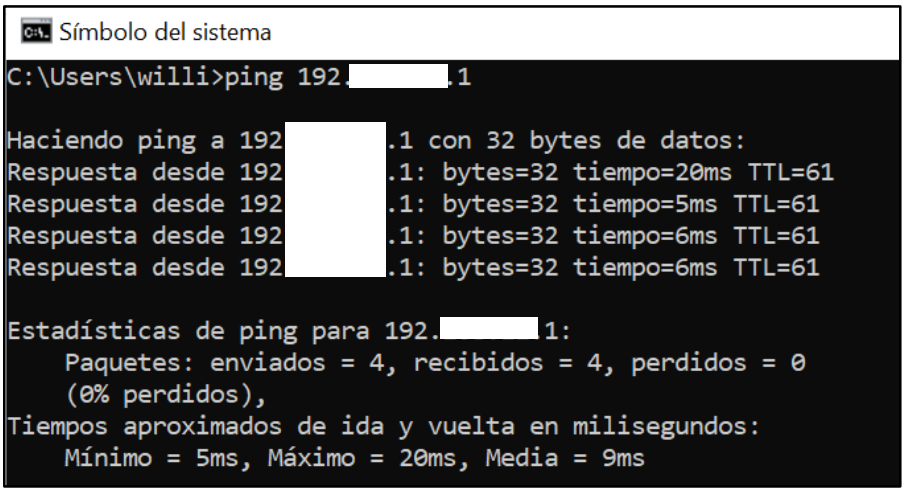


Figura 4.45 Ping exitoso desde un lugar remoto a la sucursal Cayambe a través de la VPN.
Fuente: Desarrollado por el investigador.

4.6.6. Configuración de Protocolo de Escritorio Remoto o RDP (Remote Desktop Protocol)

Actualmente la empresa utiliza escritorios remotos para acceder a los recursos corporativos el momento de realizar teletrabajo. El acceso remoto maneja un modelo lógico cliente-servidor en donde, el equipo al que queremos acceder es el servidor y los dispositivos que se conectan a él son los clientes. Cuando se entabla la comunicación se abre en el servidor un puerto comúnmente el 3389 que es la vía de entrada y salida de información, si el puerto no es correcto la petición es denegada sin embargo al utilizar una VPN no es necesario configurar puertos.

Entre los riesgos de utilizar un escritorio remoto son: el robo de información y datos confidenciales por ciberdelincuentes, cifrado de información para pedir un rescate, infecciones para convertir al equipo en un zombi y formar parte de un botnet, entre otros.

El uso de una VPN elimina o minimiza los riesgos antes mencionados, en el caso de que los ciberdelincuentes logren acceder al servidor VPN aún deben conseguir el acceso al escritorio remoto. A continuación se muestra la configuración de servicio RDP en el equipo Sophos.

- Ir a configuración, VPN, bookmarks y establecer los parámetros mostrados en la figura 4.46.

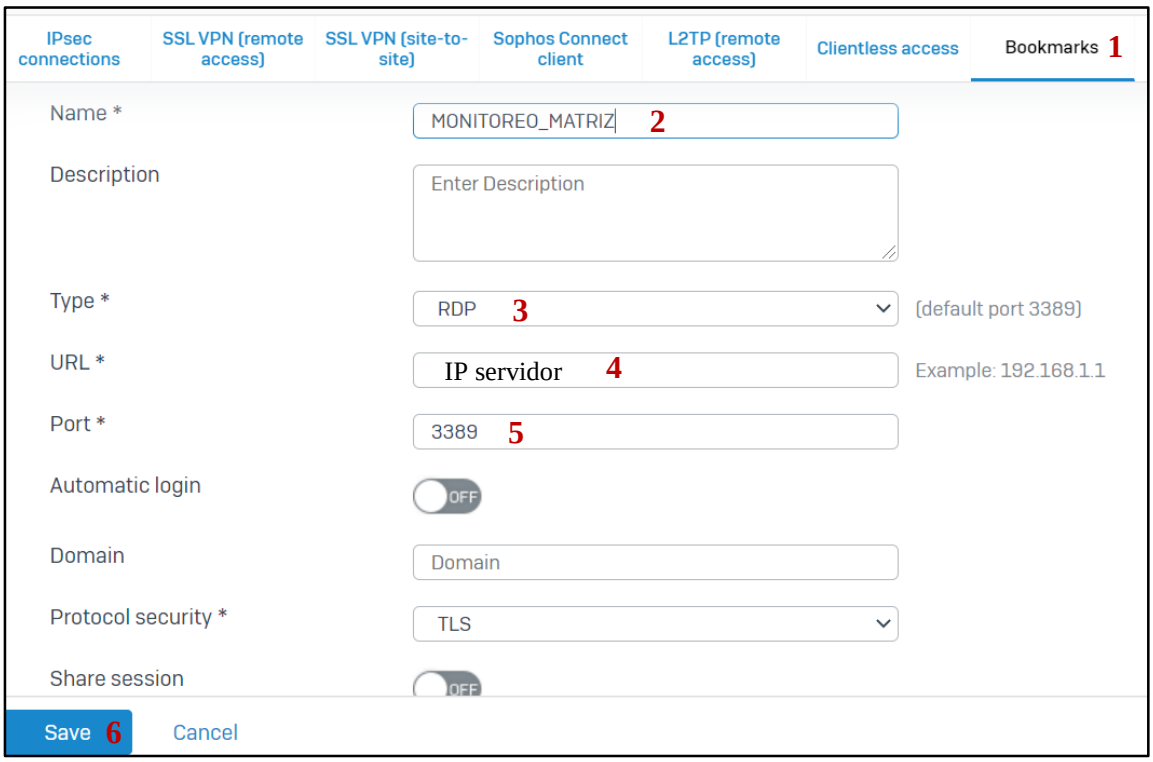


Figura 4.46 Configuración RDP.
Fuente: Desarrollado por el investigador.

- Para configurar que usuarios pueden acceder a los diferentes servicios se debe ir a configuration, VNP, clientless access y establecer los parámetros mostrados en la figura 4.47.

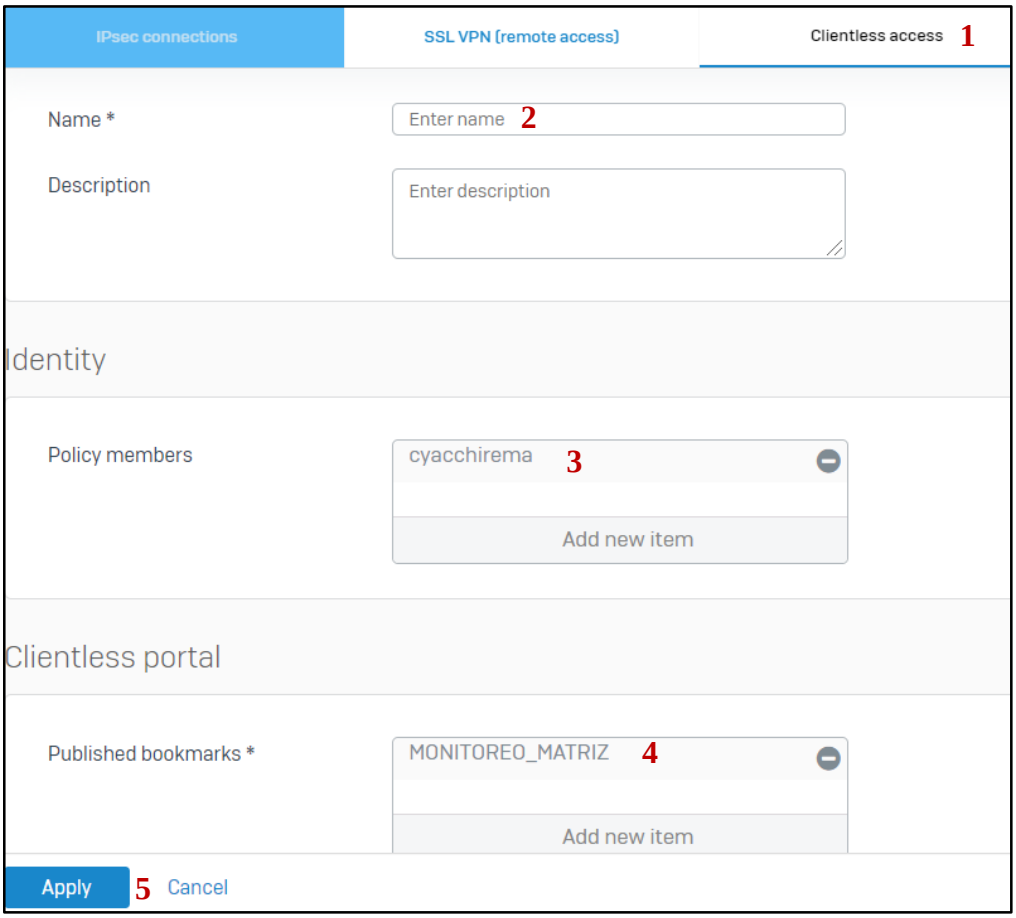


Figura 4.47 Configuración de acceso al servicio RDP.
Fuente: Desarrollado por el investigador.

- Para acceder a los servicios RDP ir al portal de usuario, ingresar usuario y contraseña, clic en la pestaña SSL VPN y escoger el servicio al cual se desea acceder como muestra la figura 4.48.

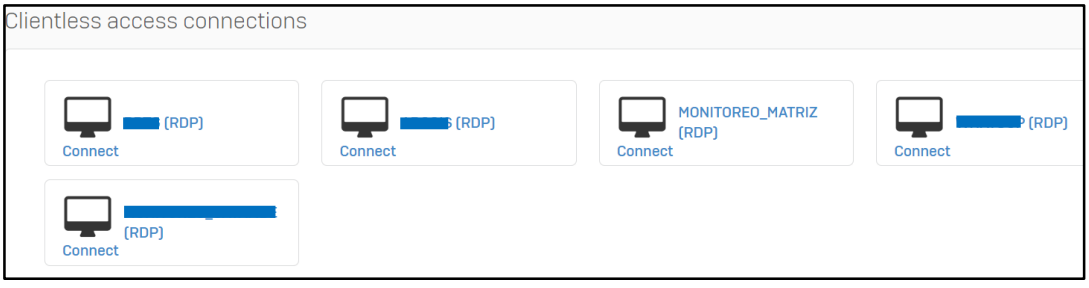


Figura 4.48 Lista de servidores.
Fuente: Desarrollado por el investigador.

- La figura 4.49 muestra la interface de acceso al servidor MONITOREO_MATRIZ a través del equipo Sophos.

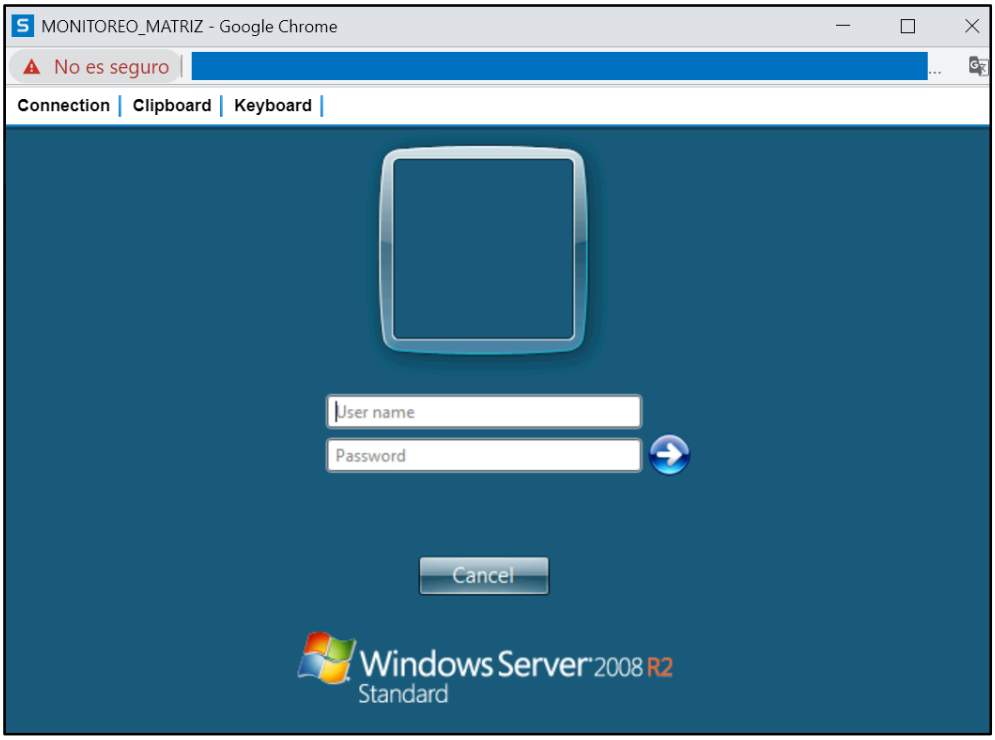


Figura 4.49 Servidor Monitoreo_Matriz.
Fuente: Desarrollado por el investigador.

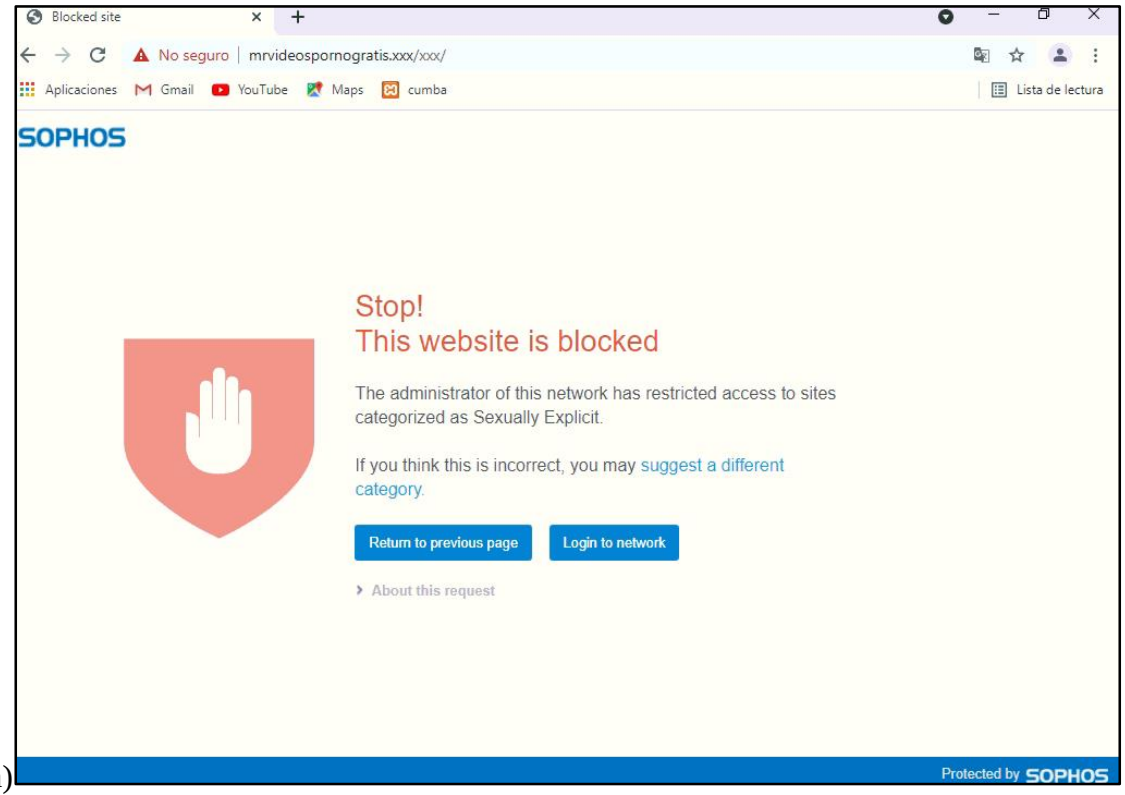
4.6.7. Control web

El control web es otro requerimiento de la empresa para crear una política en cuanto al acceso a Internet y su correcto uso en el horario laboral de todos sus colaboradores, entre las ventajas que proporcionada el control web completo son:

- Crear políticas en base a un horario específico.
- Acceso y restricciones por usuario o grupos.
- Aplicación de políticas a los usuarios dentro y fuera de la red de la empresa.
- Informes y registro de usuarios detallados.

La figura 4.50 muestra una de las restricciones aplicadas en la red LAN de la empresa.

a)



b)

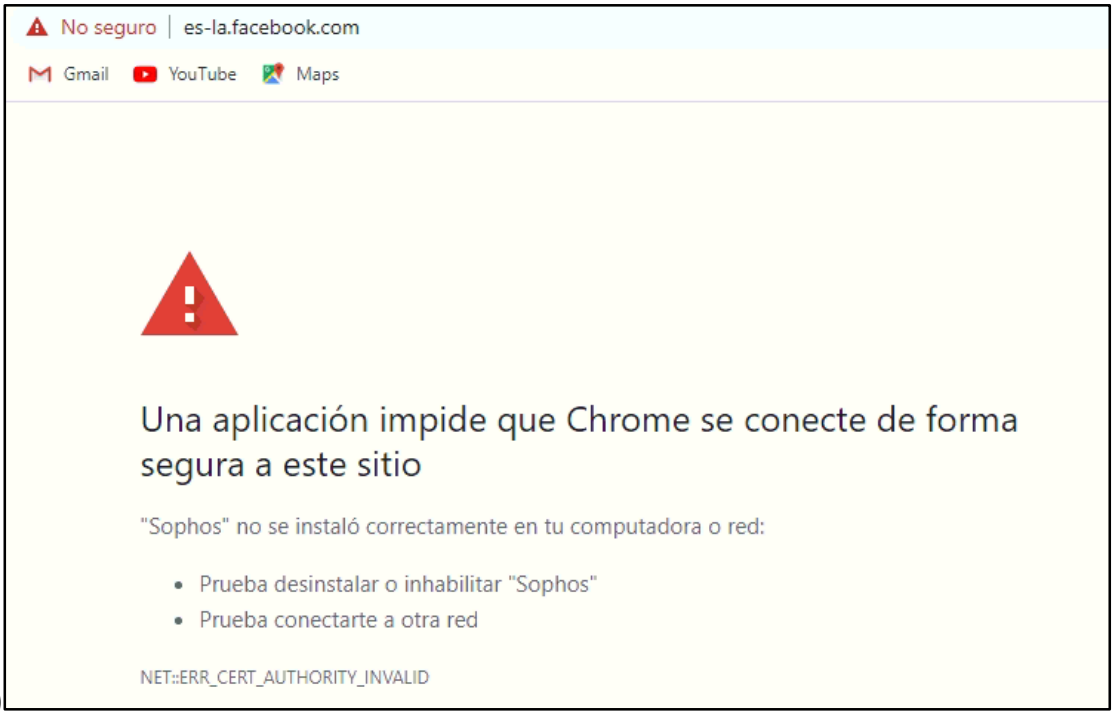


Figura 4.50 a) Bloqueo de páginas pornográficas. b) Bloqueo de redes sociales.
Fuente: Desarrollado por el investigador.

4.6.8. Limitación de ancho de banda a los usuarios por grupos

Para aplicar una regla que limite el ancho de banda primero se debe crear la lista de usuarios y encasillarlos en un grupo específico, esta opción se encuentra en autenticación, grupos, nuevo y se debe configurar los parámetros indicados en la figura 4.51.

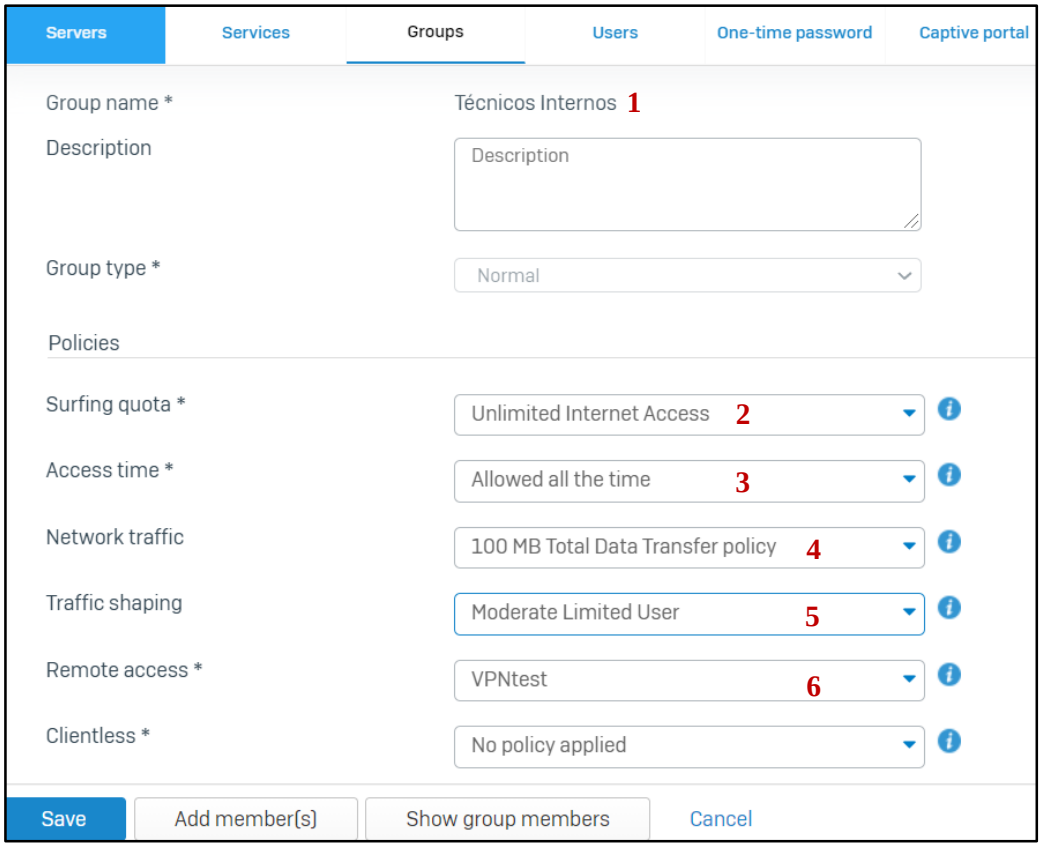


Figura 4.51 Control de ancho de banda por grupo de usuarios.
Fuente: Desarrollado por el investigador.

Los usuarios que tengan el perfil de Técnicos Internos tendrán los mayores privilegios en la empresa a diferencia de los usuarios de otros departamentos, es así como se ha configurado que la navegación y acceso a internet sea ilimitado y este permitido en todo tiempo, el tráfico permito será 20 MB aplicando una técnica de control de tráfico moderado para optimizar y garantizar de la red.

4.6.9. Prevención de intrusión

El sistema de prevención de intrusos o IPS toma decisiones de control de acceso basado en el tráfico y no en direcciones IP o puerto, la característica fundamental es el análisis en tiempo real de los paquetes de datos de tráfico buscando algún tipo de ataque o riesgo.

Sophos posee un apartado dedicado a la configuración de prevención de intrusos, mediante políticas se definen reglas especificando la acción a realizar cuando el tráfico no coincide con los criterios permitidos. Para agregar una nueva política se debe configurar los parámetros indicados en la figura 4.52:

- Ir a prevención de intrusos, políticas IPS, agregar nueva política, en este caso la política está dirigida para prevenir todo tipo de ataques DoS y la acción a tomar en caso que recibir ese tipo de ataque será de descartar los paquetes.

Figura 4.52 Configuración de política contra ataques DoS.
Fuente: Desarrollado por el investigador.

- Una vez creada la política como muestra la figura 4.53 debe ser asignada a una regla de Firewall, en este caso será aplica en todo el tráfico desde internet.

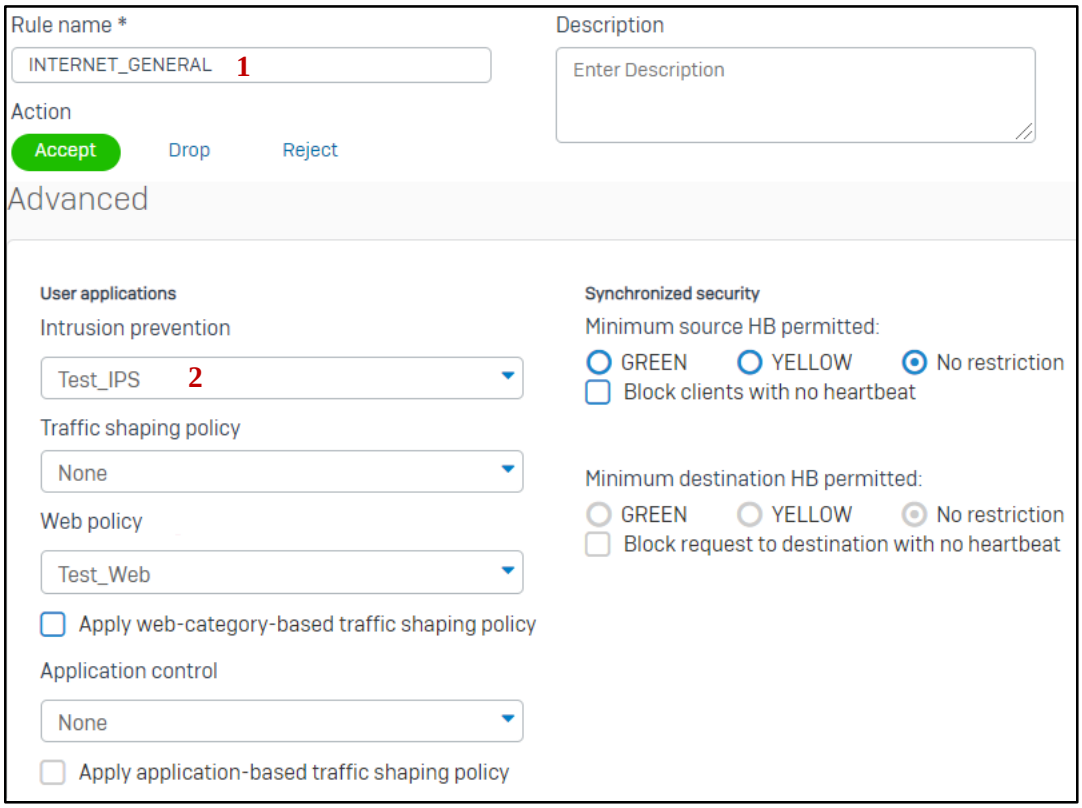


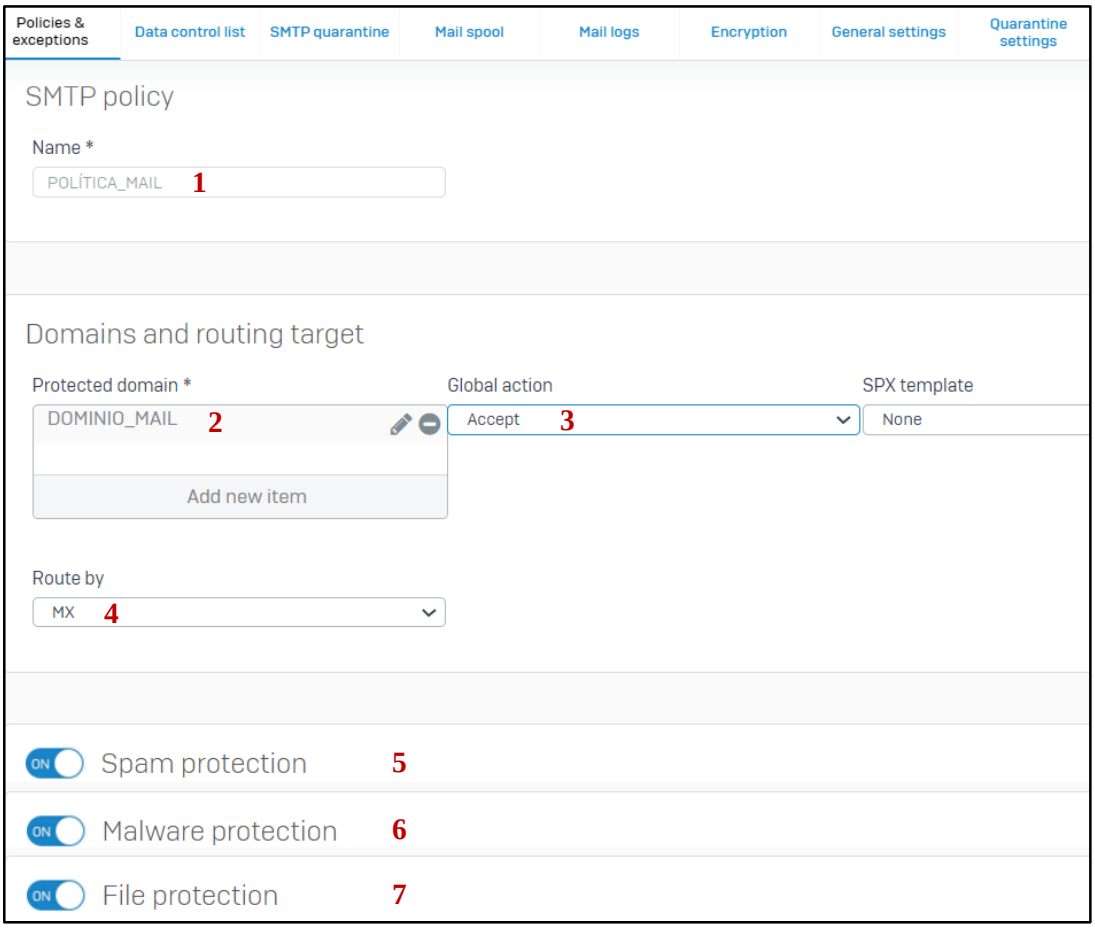
Figura 4.53 Configuración de política contra ataques DoS.
Fuente: Desarrollado por el investigador.

4.6.10. Filtrado antispam

El correo electrónico es una herramienta corporativa que la empresa emplea con suma frecuencia entre colaboradores y hacia personal externo, sin embargo el spam o correo basura amenaza la seguridad de los datos existentes en las computadoras de cada colaborador. Sophos también dispone de un apartado dedicado a la protección de correos electrónicos, para configurar esta opción se debe seguir los siguientes pasos:

- Ir a protect, email y agregar una nueva política configurando los parámetros indicados en la figura 4.54, el dominio a proteger para este caso de estudio es simantec.ec. Adicional, en la misma política se deben activar protecciones de spam, malware y archivos para elevar el nivel de protección.

a)



b)

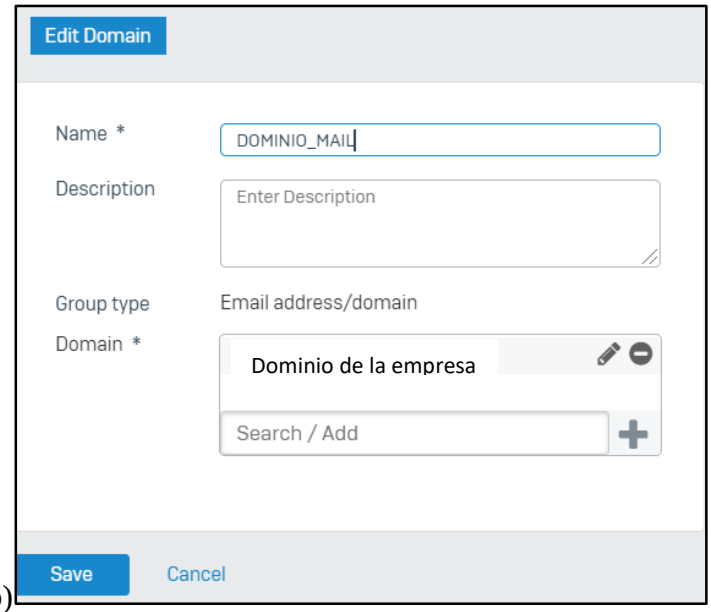


Figura 4.54 a) Configuración anti-spam. b) Configuración del dominio mail.
Fuente: Desarrollado por el investigador.

4.6.11. Acceso al sistema interno

El requerimiento más importante de la empresa es tener acceso al sistema interno, parte de la migración a la plataforma de seguridad es tener conexión con los recursos que los colabores necesitan en su trabajo diario. La figura 4.55 muestra el acceso al sistema interno a través de la VPN hasta llegar a la red LAN en donde se encuentra alojado.

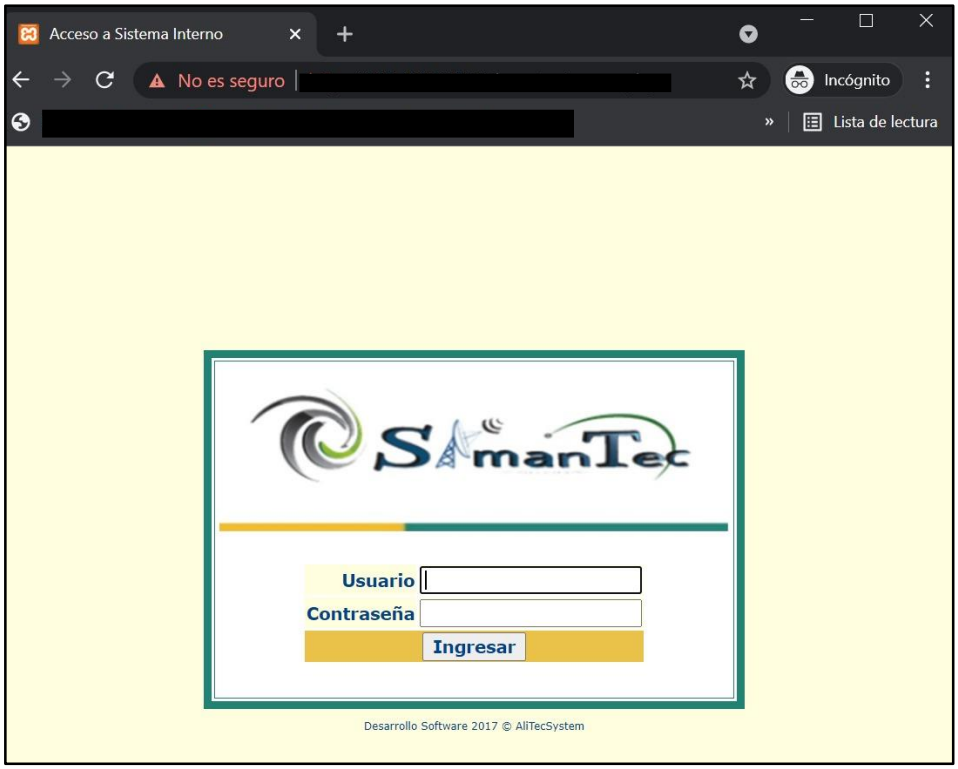


Figura 4.55 Ingreso sistema interno.
Fuente: Desarrollado por el investigador.

4.7. Implementación del sistema de defensa software

Pfsense es un firewall de código abierto, presenta una interface gráfica intuitiva y amigable con el usuario que puede instalarse de forma física en una computadora o en una máquina virtual dentro de un sistema físico eliminando la necesidad de un ordenador más en la red. Este sistema operativo puede instalarse en cualquier ordenador pero el rendimiento depende del hardware y la configuración del propio firewall. Un aspecto importante es la configuración y reconocimiento de las tarjetas de red, una destinada para la WAN y otro para la LAN.

4.7.1. Elección del servidor

Durante la elección del servidor se debe dimensionar para soportar la red que se va a proteger, aspectos como cantidad de usuarios simultáneos, servicios levantados como VPN, proxy, captive portal, DMZ entre otras funciones demandaran más recursos de la máquina física. Bajo este concepto se optó por el Servidor HPE ProLiant MicroServer Gen10 Plus, cuyas características se muestran en la tabla 4.7.

Tabla 4.7 Características servidor Servidor HPE ProLiant MicroServer Gen10 Plus.

Servidor HPE ProLiant MicroServer Gen10 Plus	**Características**
Vista frontal  Vista trasera 	Tipo de procesador: Intel
	Nombre del procesador: Intel Xeon E-2224.
	Núcleo de procesador disponible: 4 núcleos.
	RAM: 32GB
	Disco Duro: 8 TB
	Caché de procesador: 8 MB L3
	Número del procesador: 1
	Velocidad del procesador: 3,4 GHz
	Tipo de memoria: Memoria estándar HPE DDR4
	Memoria, estándar: 16 GB (1 x 16 GB) UDIMM
	Número de ranuras: 2
	Velocidad: 2666 MT/s
	Controlador de red: 4

Fuente: [36]

4.7.2. Instalación Pfsense

Una vez escogido el sistema físico como es el servidor Servidor HPE ProLiant MicroServer Gen10 Plus, PfSense será implementado en una máquina virtual, existen algunos software de virtualización como VirtualBox, VM Ware, KVM para este caso se escogió VirtualBox por ser de fácil manejo y amigable con el usuario. La instalación del software se hace a través de estos sencillos pasos:

- Descargar la ISO en la página web www.pfsense.org/download como indica la figura 4.56, aparecerá una ventana para elegir la arquitectura del procesador y la plataforma ISO para montar en la máquina virtual.

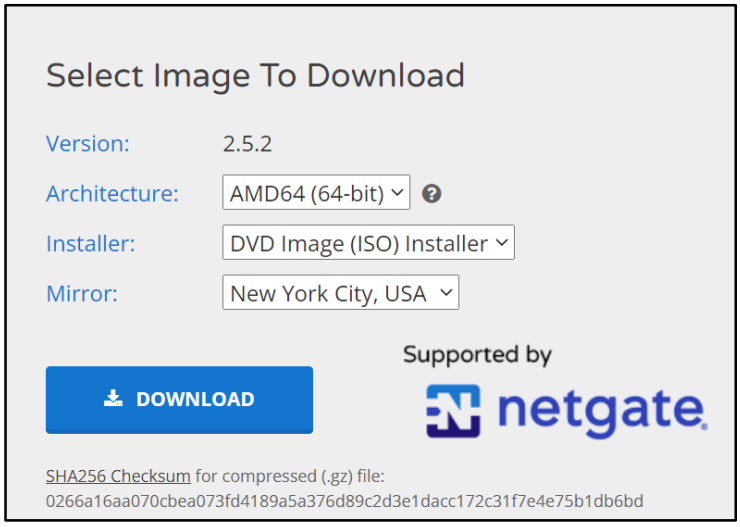


Figura 4.56 Descarga imagen ISO de pfSense.
Fuente: Desarrollado por el investigador.

- Luego de descargar la ISO se crea la máquina virtual seleccionando el sistema operativo y la versión, para este caso de estudio el sistema operativo elegido es FreeBSD para 64-bit como se indica en la figura 4.57.

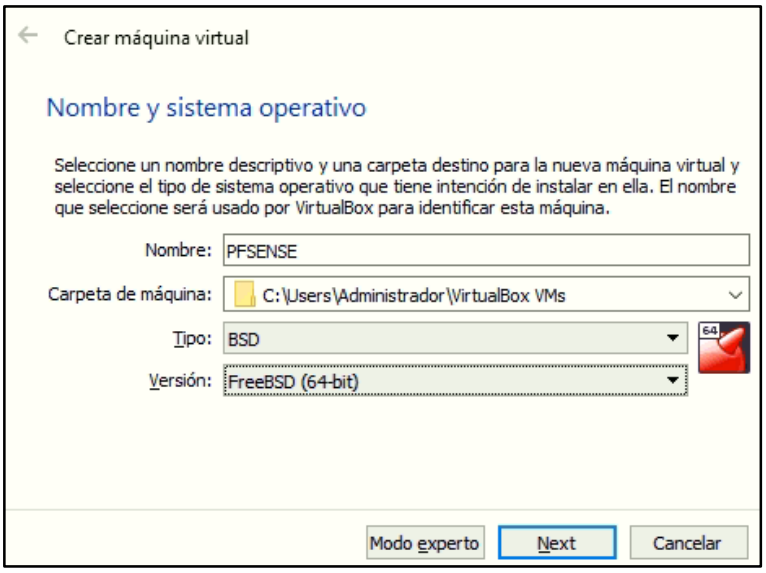


Figura 4.57 Creación máquina virtual.
Fuente: Desarrollado por el investigador.

- El siguiente paso es seleccionar el tamaño de memoria, como pfSense no usa interface gráfica con 4096 MB de RAM es suficiente. Luego se debe crear el disco duro virtual seleccionando VDI (VirtualBox Disk Image) y elegir el tamaño del disco virtual para este caso práctico se utilizará 128 GB. Una vez realizadas las configuraciones se debe iniciar la máquina para instalar pfSense, la instalación de este software consiste en aceptar los parámetros de configuración para avanzar en el proceso.
- Dos aspectos fundamentales dentro de la configuración de pfSense son la asignación de direcciones IP a la LAN y WAN, la WAN tendrá la dirección 200.X.X.X/29 y la LAN tendrá la dirección 192.168.16.0/24 asignada por el usuario.
- Finalmente aparecerá la consola de pfSense como muestra la figura 4.58 lista para usar y configurar según las necesidades del administrador de la red.

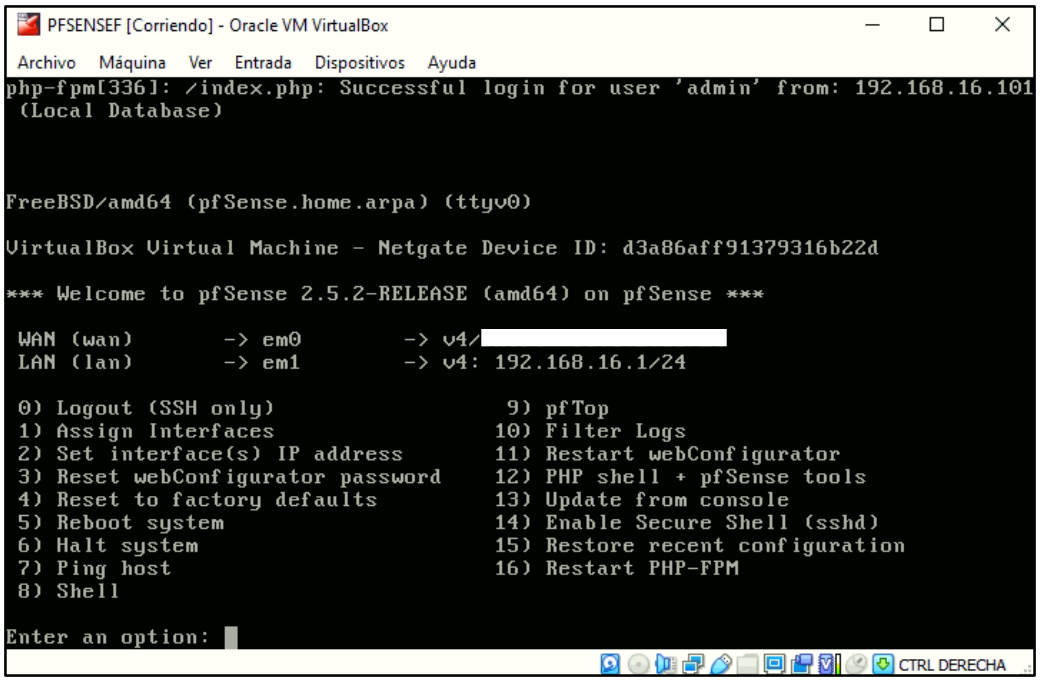
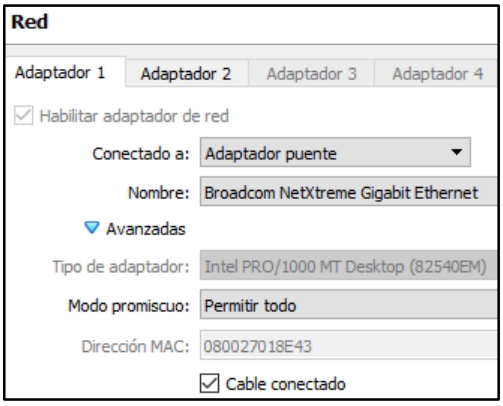


Figura 4.58 Consola pfSense.
Fuente: Desarrollado por el investigador.

4.7.3. Configuración física y lógica pfSense

La configuración física del software pfSense se realizó estableciendo conexión entre el Adaptador 1 de la máquina virtual conectado en modo puente al puerto Ethernet 1 del servidor donde está configurada la IP pública con salida a internet. El Adoptador 2 configurado con la IP 192.168.16.0 máscara 255.255.255.0 de la máquina virtual está conectado al puerto físico Ethernet 2 del servidor para otorgar direcciones IP por DHCP a los dispositivos que se encuentren dentro de la red local como muestra la figura 4.59.

a)


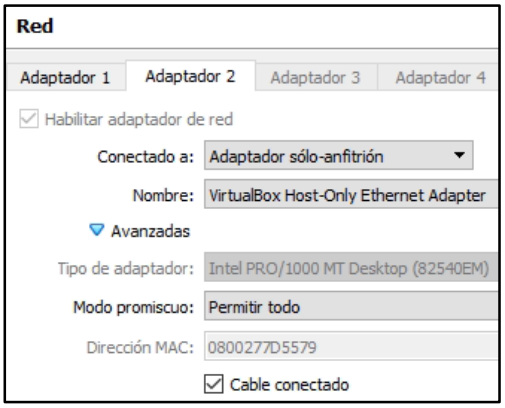
b)


Figura 4.59 Configuración de red. a) Adaptador 1_WAN. b) Adaptador 2_LAN.
Fuente: Desarrollado por el investigador.

La figura 4.60 muestra la conexión física entre el servidor y la máquina virtual, el servidor dispone de 4 puertos Ethernet, en la Eth1 está configurado la IP pública con salida a Internet y en la Eth2 está configurada la red local además se dispone de dos puertos libres para configurar más servicios o redes locales.

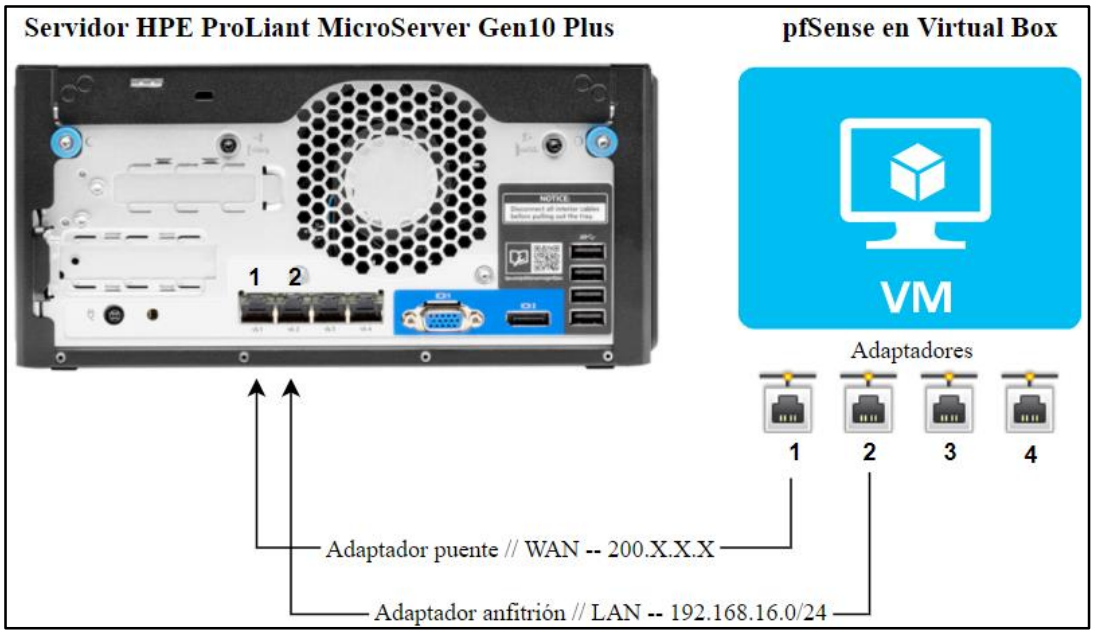


Figura 4.60 Servidor pfSense.
Fuente: Desarrollado por el investigador.

4.7.4. Configuración IPsec

La configuración IPsec entre la sucursal Cayambe y pfSense tiene la topología que se muestra en la figura 4.61, el túnel IPsec será el medio para comunicar las redes LAN de matriz con la sucursal, entiéndase también todos los recursos que las dos sedes deben compartir para el desarrollo de las actividades diarias de los colaboradores. Los dos sitios se conectarán a través de sus direcciones públicas configuradas en el servidor que aloja al software UTM y en el MikroTik ubicado en la matriz, una vez que se establezca la comunicación las redes locales se podrá acceder de manera bidireccional a los recursos de la empresa.

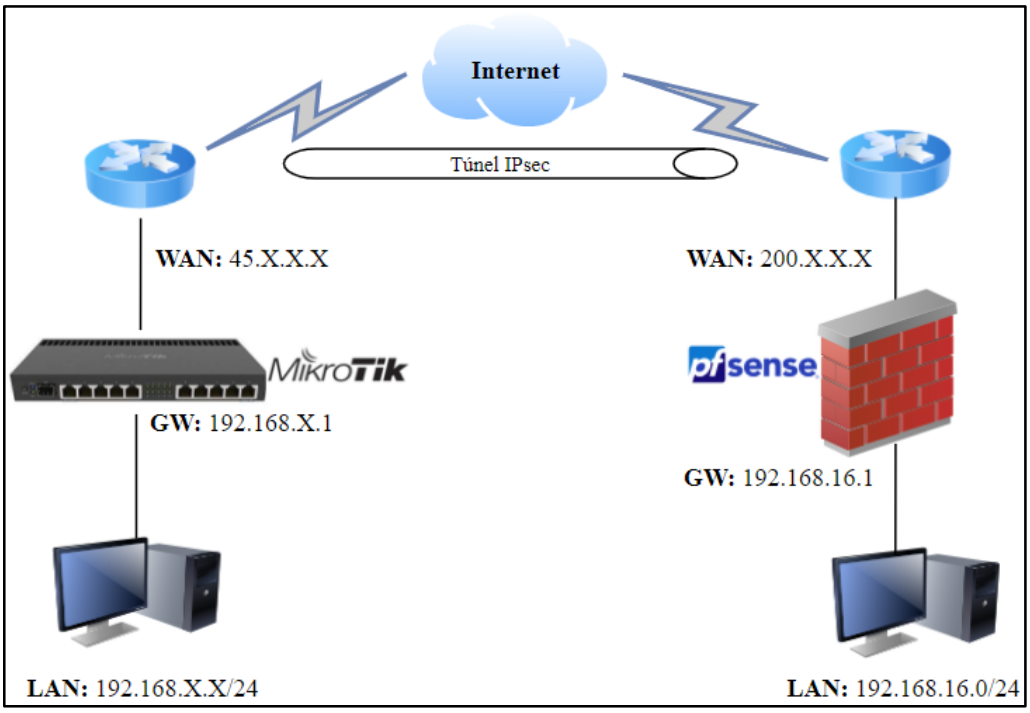


Figura 4.61 Configuración IPsec entre MikroTik Cayambe y pfSense Guayllabamba.
Fuente: Desarrollado por el investigador.

Para configurar el túnel IPsec en el pfSense se debe seguir los pasos indicados en la figura 4.62:

- Ir a VPN, IPsec, añadir un nuevo túnel y configurar la fase 1 de tal manera que los campos tengan estos parámetros.
  - ✓ Key Exchange version: IKEv2
  - ✓ Internet Protocol: IPv4
  - ✓ Interface: WAN
  - ✓ Remote gateway: IP pública MikroTik
  - ✓ Authentication Method: Mutual PSK
  - ✓ My identifier: My IP address
  - ✓ Peer identifier: Peer IP address
  - ✓ Pre-Shared Key: Contraseña MiktoTik-pfSense
  - ✓ Encryption Algorithm: AES
  - ✓ Algorithm: 128 bits
  - ✓ Key length: SHA256

- ✓ Hash: 14 (2048 bit)
- ✓ Los demás parámetros se mantienen con los valores predeterminados.
- ✓ Enable DPD: Habilitar
- ✓ Guardar

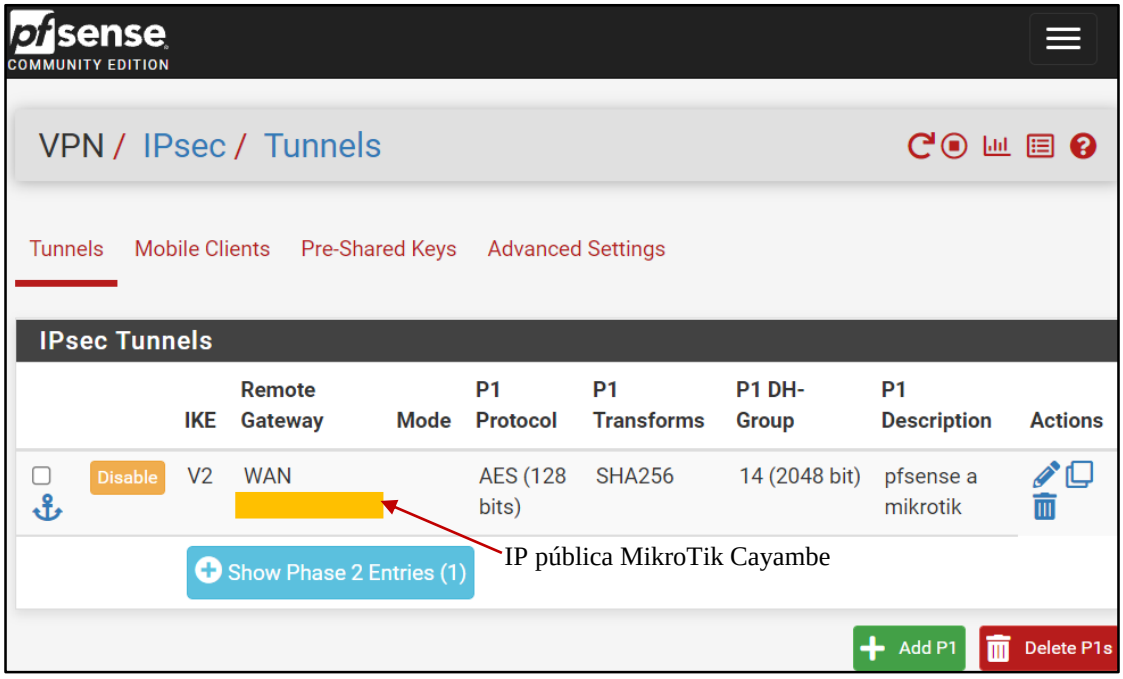


Figura 4.62 Configuración IPsec fase 1.
Fuente: Desarrollado por el investigador.

- Clic en show phase 2 entries y configurar la fase 2 de tal manera que los campos tengan los parámetros mostrados en la figura 4.63.
  - ✓ Mode: Tunnel IPv4
  - ✓ Local Network: LAN subnet
  - ✓ Remote Network: IP LAN MikroTik
  - ✓ Phase 2 proporsal-Protocol: ESP
  - ✓ Encryption Algorithms: AES (128 bits)
  - ✓ Encryption Algorithms: AES128-GCM (128 bits)
  - ✓ Hash Algorithms: SHA256
  - ✓ PFS key group: 14 (2048 bit)
  - ✓ Los demás parámetros se mantienen con los valores predeterminados
  - ✓ Guardar

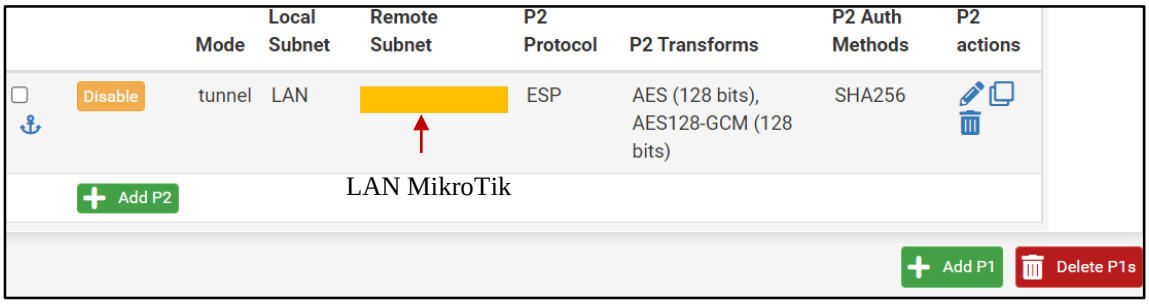


Figura 4.63 Configuración IPsec fase 2.
Fuente: Desarrollado por el investigador.

- Para configurar las reglas de firewall; ir a firewall, rules, IPsec y agregar una regla con los parámetros que se indica en la figura 4.64.
  - ✓ Action: Pass
  - ✓ Interface: OpenVPN
  - ✓ Adress Family: IPv4
  - ✓ Protocol: Any
  - ✓ Source: Any
  - ✓ Destination: Any
  - ✓ Guardar

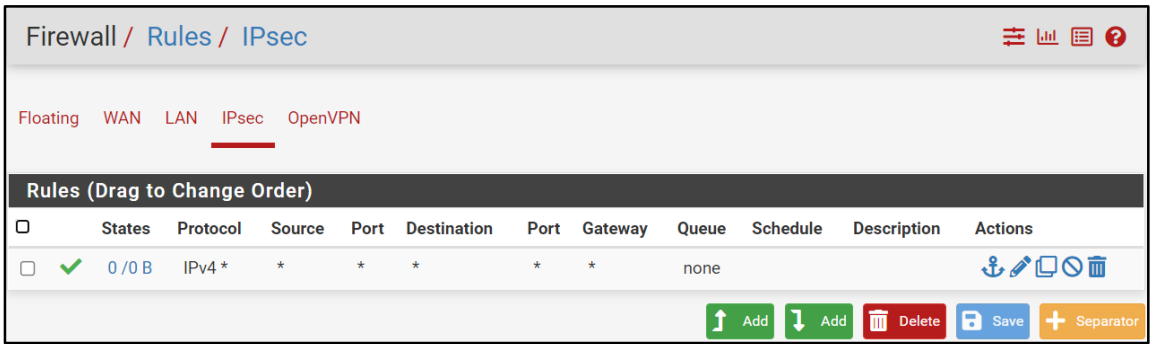


Figura 4.64 Configuración reglas de firewall
Fuente: Desarrollado por el investigador.

La configuración Ipsec en el Mikrotik tiene el mismo procedimiento presentado en el apartado 4.6.3, con la diferencia que se debe configurar con la IP pública (200.X.X.X) y red local (192.168.16.0/24) configurada en el pfSense. Una vez configurado todos los parámetros, en la pestaña Policies el estado de la fase 2 cambiará ha establecido como muestra la figura 4.65. Un aspecto muy importante es mantener en el MikroTik y el

pfSense el mismo tipo de contraseña, grupo Diffie-Hellman, la encriptación y autenticación para entablar la comunicación entre los dos sitios.

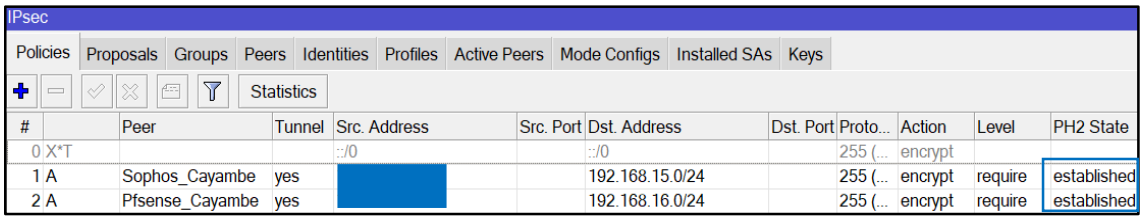


Figura 4.65 Conexión entre MikroTik sucursal y pfSense.
Fuente: Desarrollado por el investigador.

Situación similar presenta el pfSense, en la pestaña Status, IPsec el estado de la conexión cambiará ha conectado como muestra la figura 4.66.

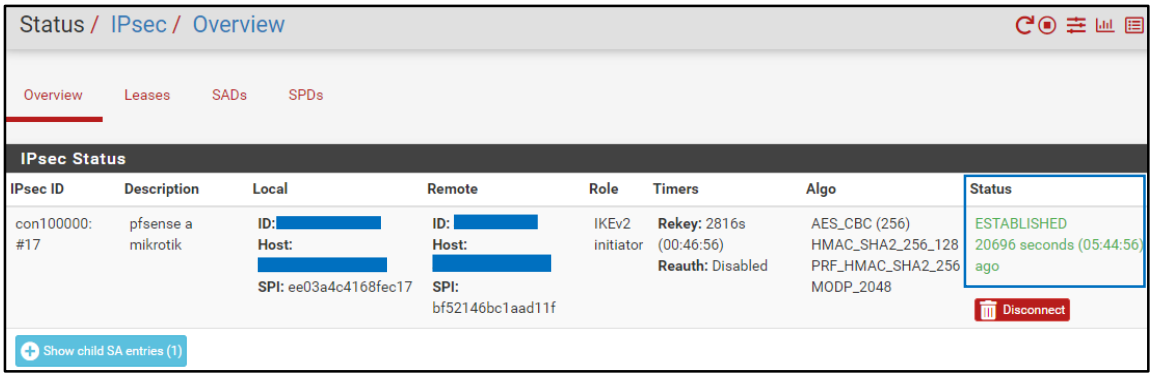


Figura 4.66 Conexión entre pfSense matriz y MikroTik sucursal.
Fuente: Desarrollado por el investigador.

4.7.5. Pruebas de conectividad

Las pruebas de conectividad se harán en ambos sentidos MikroTik-pfSense, desde el terminal del MikroTik se hace ping al Gateway de la red local configurada en el pfSense 192.168.16.1 y desde el pfSense se hace ping al Gateway de la red local configurada en el MikroTik 192.168.X.X. Las figuras 4.67 y 4.68 muestran que si existe conexión hacia las dos redes locales configuradas en los diferentes equipos de la matriz en el caso del Servidor_psSense y el MikroTik en el caso de la sucursal.

```
Terminal <18>
[admin@SRV-MK-Cayambe-Sucursal-Oficina] > ping 192.168.16.1 size=2000
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.16.1                             2000  64 4ms
    1 192.168.16.1                             2000  64 4ms
    2 192.168.16.1                             2000  64 4ms
    3 192.168.16.1                             2000  64 4ms
    4 192.168.16.1                             2000  64 4ms
    5 192.168.16.1                             2000  64 4ms
    6 192.168.16.1                             2000  64 5ms
    7 192.168.16.1                             2000  64 4ms
    sent=8 received=8 packet-loss=0% min-rtt=4ms avg-rtt=4ms
   max-rtt=5ms
```

Figura 4.67 Pruebas de conectividad MikroTik-pfSense.
Fuente: Desarrollado por el investigador.

La figura 4.68 muestra la consola de una máquina con la IP 192.168.16.105 de la red LAN del pfSense, desde ahí se hace un ping al Gateway de la red LAN configurada en el MikroTik_Cayambe demostrando que si existe conexión entre los dos sitios.

```
~
[NEW] | 1 |
root# ipconfig
bash: ipconfig: command not found
root# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:BA:B0
          inet addr:192.168.16.105  Bcast:192.168.16.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45055 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34635 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33143624 (31.6 MiB)  TX bytes:4391487 (4.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:624 (624.0 B)  TX bytes:624 (624.0 B)

root# ping 192.[redacted].1
PING 192.168[redacted]1): 56 data bytes
64 bytes from 192[redacted].1: seq=0 ttl=63 time=4.882 ms
64 bytes from 192[redacted].1: seq=1 ttl=63 time=4.135 ms
64 bytes from 192[redacted].1: seq=2 ttl=63 time=3.624 ms
64 bytes from 192[redacted].1: seq=3 ttl=63 time=4.105 ms
64 bytes from 192[redacted].1: seq=4 ttl=63 time=3.997 ms
```

Figura 4.68 Pruebas de conectividad pfSense matriz- MikroTik sucursal.
Fuente: Desarrollado por el investigador.

4.7.6. Configuración VPN

Para crear una VPN en pfSense se debe seguir los siguientes pasos:

- **Creación de certificados:** La configuración de una VPN va de la mano de la creación de una unidad certificadora como indica la figura 4.69, para ello ir a System, Certificate Manager, CAs, Add y configurar cada campo con los siguientes parámetros:
  - ✓ Descriptive name: Nombre_VPN
  - ✓ Method: Create an internal Certificate Authority
  - ✓ Key type, Digest Algorithm, Lifetime (days): Mantener parámetros por defecto
  - ✓ Common Name: Nombre_Certificado
  - ✓ Country Code: Ecuador
  - ✓ State or Province: Pichincha
  - ✓ City: Quito
  - ✓ Organization: Nombre_Empresa
  - ✓ Organizational Unit: Nombre_Departamento
  - ✓ Guardar

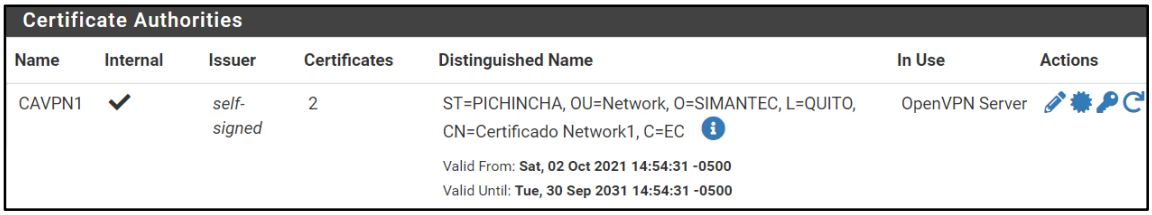
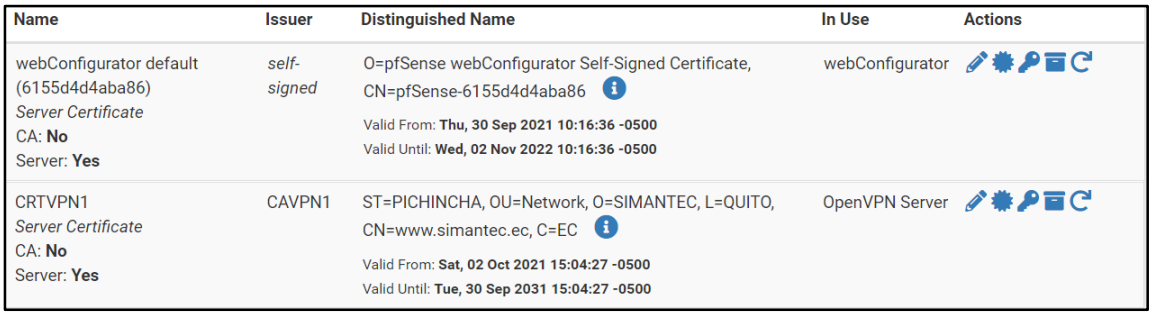


Figura 4.69 Creación Unidad Certificadora.
Fuente: Desarrollado por el investigador.

- **Creación de certificado tipo servidor:** Este tipo de certificado como muestra la figura 4.70 es necesario para el servidor VPN que estará del lado del servidor. Ir a System, Certificate Manager, Certificates, Add y configurar cada campo con los siguientes parámetros:
  - ✓ Method: Create an internal Certificate
  - ✓ Descriptive name: Nombre_Certificado

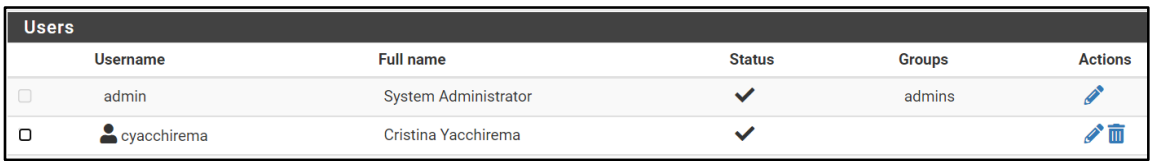
- ✓ Certificate authority: Nombre_Unidad Certificadora
- ✓ Key type, Digest Algorithm, Lifetime (days): Mantener parámetros por defecto
- ✓ Common Name: Dirección web empresa
- ✓ Certificate Type: Server Certificate
- ✓ Guardar



Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6155d4d4aba86) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6155d4d4aba86 Valid From: **Thu, 30 Sep 2021 10:16:36 -0500** Valid Until: **Wed, 02 Nov 2022 10:16:36 -0500**	webConfigurator	
CRTVPN1 *Server Certificate* CA: **No** Server: **Yes**	CAVPN1	ST=PICHINCHA, OU=Network, O=SIMANTEC, L=QUITO, CN=www.simantec.ec, C=EC Valid From: **Sat, 02 Oct 2021 15:04:27 -0500** Valid Until: **Tue, 30 Sep 2031 15:04:27 -0500**	OpenVPN Server	

Figura 4.70 Creación Certificado VPN Server.
Fuente: Desarrollado por el investigador.

- **Creación de usuarios:** Para crear los usuarios ir a System, User Manager y añadir para configurar los campo los parámetros indicados en la figura 4.71:
  - ✓ Username: Nombre_Usuario
  - ✓ Password: Clave_segura
  - ✓ Full name: Nombre_Apellido
  - ✓ Certificate: Marcar casillero para crear un certifico válido para el usuario
  - ✓ Description name: Nombre_Certificado
  - ✓ Certificate authority: Nombre Certificado creado (fig. 4.70)
  - ✓ Mantener los parámetros por defecto en los demás items
  - ✓ Guardar



Users

	Username	Full name	Status	Groups	Actions
☐	admin	System Administrator	✓	admins	
☐	cyacchirema	Cristina Yacchirema	✓		

Figura 4.71 Creación de usuario VPN.
Fuente: Desarrollado por el investigador.

- **Configuración VPN:** Ir a VPN, OpenVPN, Servers, añadir y configurar los campos indicados en la figura 4.72:
  - ✓ Server mode: Remote Access (SSL/TLS+User Auth)
  - ✓ Backend for authentication: Local Database
  - ✓ Protocol: UP Don IPv4 only
  - ✓ Device mode: tun-Layer 3 Tunnel Mode
  - ✓ Interface: WAN
  - ✓ Local Port: 1195
  - ✓ Description: Nombre_VPN
  - ✓ Use a TLS Key: Marcar casillero
  - ✓ Automatically generate a TLS Key.: Marcar casillero
  - ✓ Peer Certificate Authority: Nombre_Unidad_Certidicadora
  - ✓ Server certificate: Seleccionar cetificado creado previamente
  - ✓ DH Parameter Length: 2048 bit
  - ✓ Data Encryption Algorithms: AES-128-CBC, AES-256-CBC, AES-256-GCM
  - ✓ Fallback Data Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)
  - ✓ Auth digest algorithm: SHA256 (256-bit)
  - ✓ Hardware Crypto: No Hardware Crypto Acceleration
  - ✓ Strict User-CN Matching: Marcar casillero
  - ✓ IPv4 Tunnel Network: 192.168.100.0/24
  - ✓ IPv4 Tunnel Network: Marcar casillero
  - ✓ Dynamic IP: Marcar casillero
  - ✓ Redirect IPv4 Gateway: Marcar casillero
  - ✓ Gateway creation: IPv4 only
  - ✓ Verbosity level: 3 (recommended)
  - ✓ Mantener los parámetros por defecto en los demás items
  - ✓ Guardar

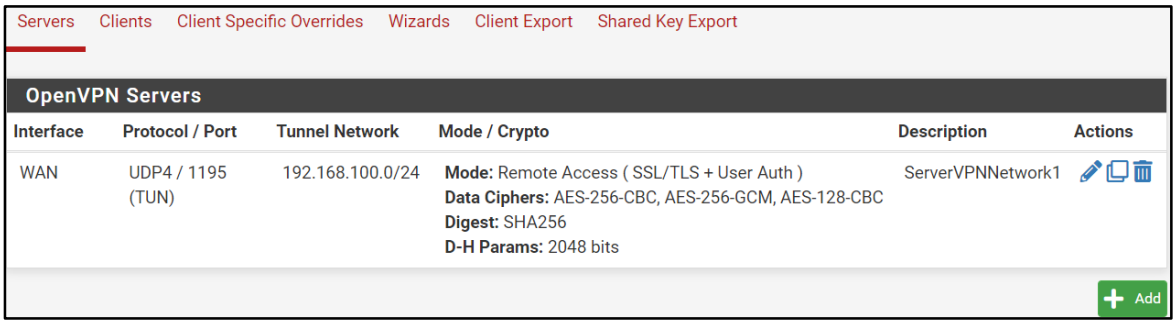


Figura 4.72 Creación ServerVPN.
Fuente: Desarrollado por el investigador.

- **Creación de reglas WAN:** La figura 4.73 muestra los parámetros para crear reglas WAN, ir a Firewall, Rules, Wan, añadir nueva regla y configurar los siguientes parámetros.
  - ✓ Action: Pass
  - ✓ Interface: WAN
  - ✓ Address Family: IPv4
  - ✓ Protocol: UDP
  - ✓ Source: Any
  - ✓ Destination: Any
  - ✓ Destination Port Range: 1195
  - ✓ Log: Marcar casillero
  - ✓ Description: Nombre_Regla
  - ✓ Guardar

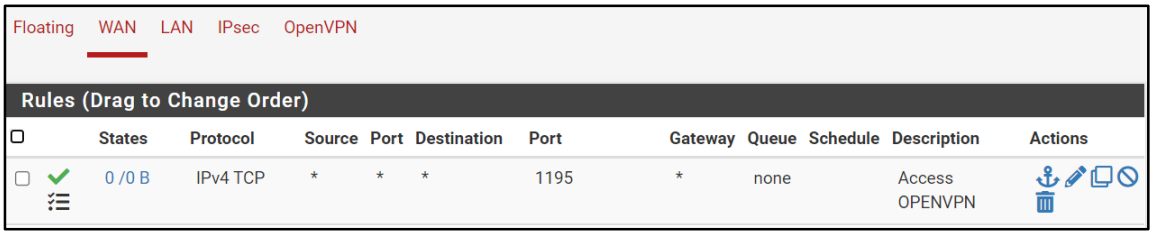


Figura 4.73 Creación regla WAN.
Fuente: Desarrollado por el investigador.

- **Creación de regla OpenVPN:** Ir a Firewall, Rules, OpenVPN, añadir nueva regla y configurar los parámetros mostrados en la figura 4.74.

- ✓ Action: Pass
- ✓ Interface: OpenVPN
- ✓ Address Family: IPv4
- ✓ Protocol: UDP
- ✓ Source: Any
- ✓ Destination: Any
- ✓ Log: Marcar casillero
- ✓ Description: Nombre_Regla
- ✓ Guardar

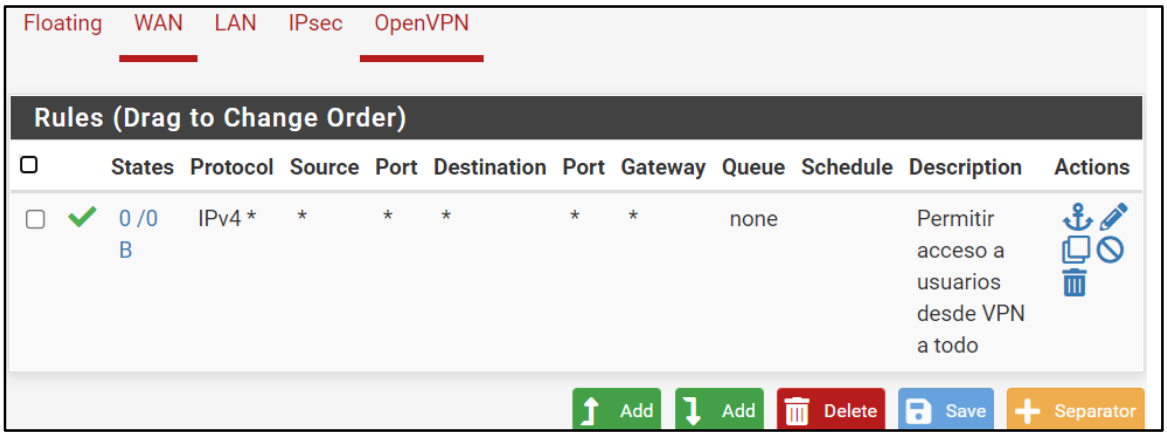


Figura 4.74 Creación regla WAN.
Fuente: Desarrollado por el investigador.

- **Instalar aplicación VPN:** Ir a System, Package Manager, seleccionar el paquete openvpn-client-export para instalar como indica la figura 4.75.

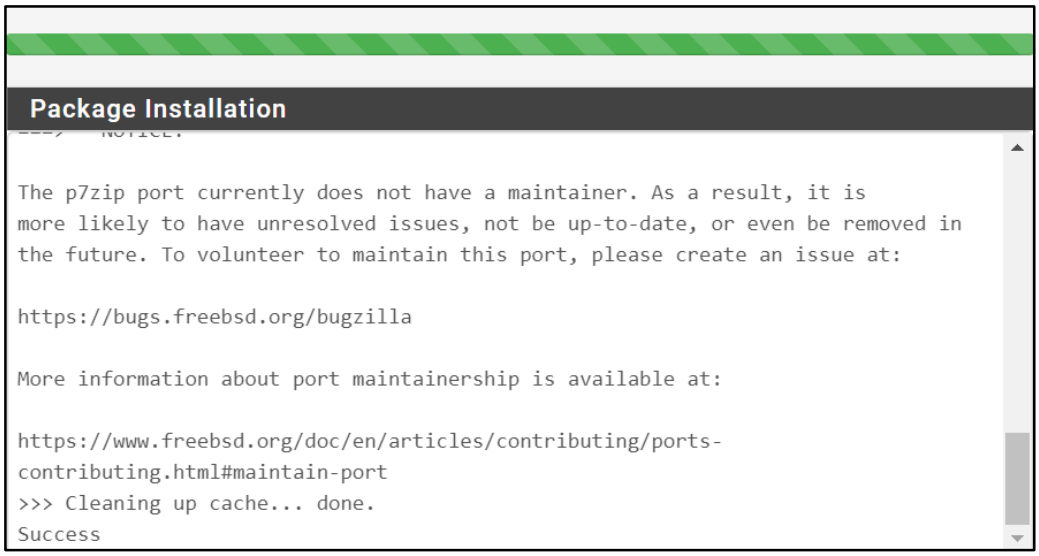


Figura 4.75 Instalación paquete VPN.
Fuente: Desarrollado por el investigador.

- Descargar aplicación VPN cliente como muestra la figura 4.76: Ir a VPN, Open VPN, Client Export y descargar la aplicación para el usuario creado previamente, una vez descarda la aplicación se debe instalar.

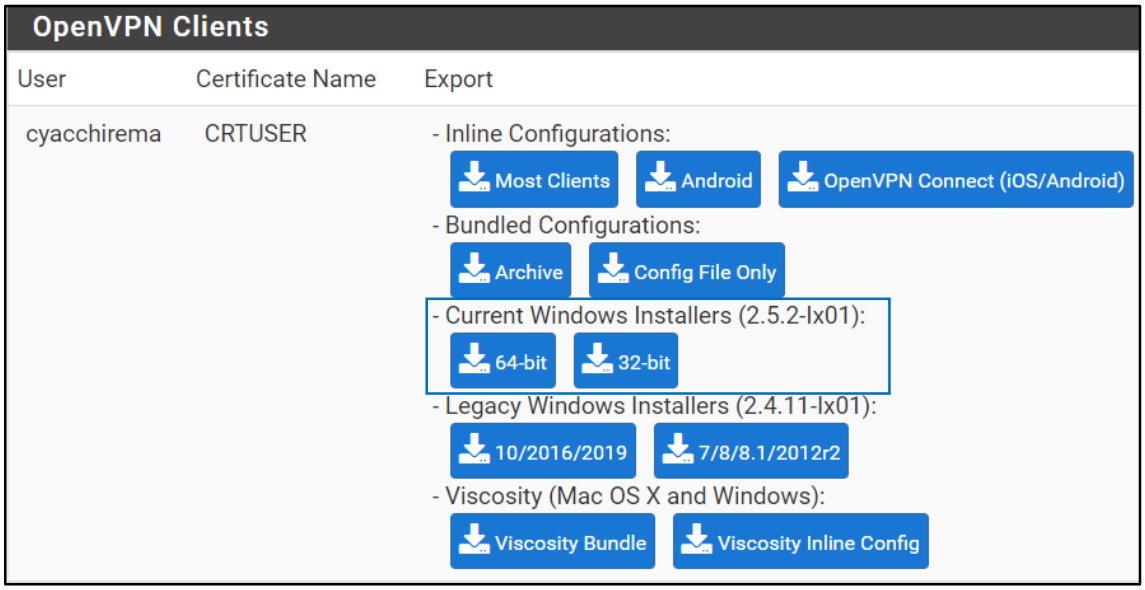


Figura 4.76 Aplicación VPN para cliente.
Fuente: Desarrollado por el investigador.

- **Pruebas de conexión:** Para verificar si la conexión VPN se estableció ir a Sattus, Systems Logs y Firewall, como se muestra en la figura 4.77 la conexión se estableció desde la IP del computador del usuario hasta la red local del pfSense a través del puerto 1194.

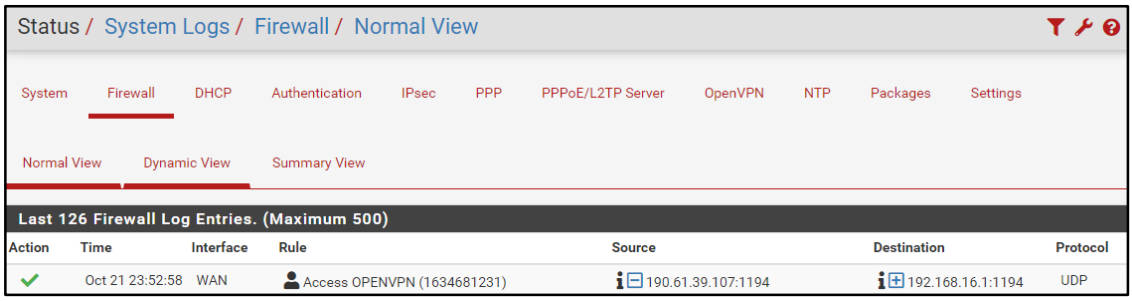


Figura 4.77 Estado de la conexión VPN.
Fuente: Desarrollado por el investigador.

- Una vez activa, la interface VPN empieza a marca el tráfico de paquetes que se transmite por el túnel entre la red local y la IP configurada para la VPN que para este caso práctico fue 10.100.0.0/24 como indica a figura 4.78.

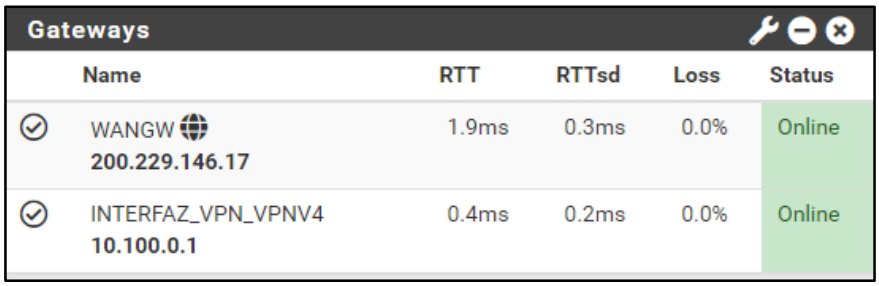


Figura 4.78 Interface VPN activa.
Fuente: Desarrollado por el investigador.

4.7.7. Control web

Para realizar un control web en pfSense se requiere una serie de configuraciones previas en el software, como muestra la figura 4.79:

- En primer lugar se debe instalar los paquetes squid y squidGuard, squid funciona como proxy transparente entre los ordenadores de la red LAN e internet para aceptar o denegar la peticiones mientras que squidGuard emplea un sistema de

filtrado por listas negras y permite crear las restricciones necesarias según los requerimientos de la empresa. Ir a System, Package Manager, Available Packages y descargar squid y squidGuard.

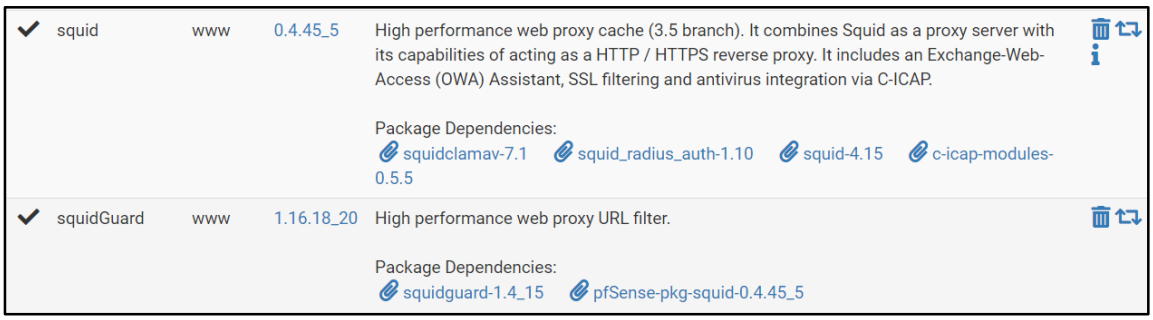


Figura 4.79 Instalación de paquetes para control web.
Fuente: Desarrollado por el investigador.

- Para configurar squidGuard ir a Services, SquidGuard Proxy Filter, clic en Blacklist. En este apartado se debe colocar la URL del sitio de donde se pretende descargar las lista negras, en este caso será de *http://www.shallalist.de/Downloads/shallalist.tar.gz* señalada en a figura 4.80.

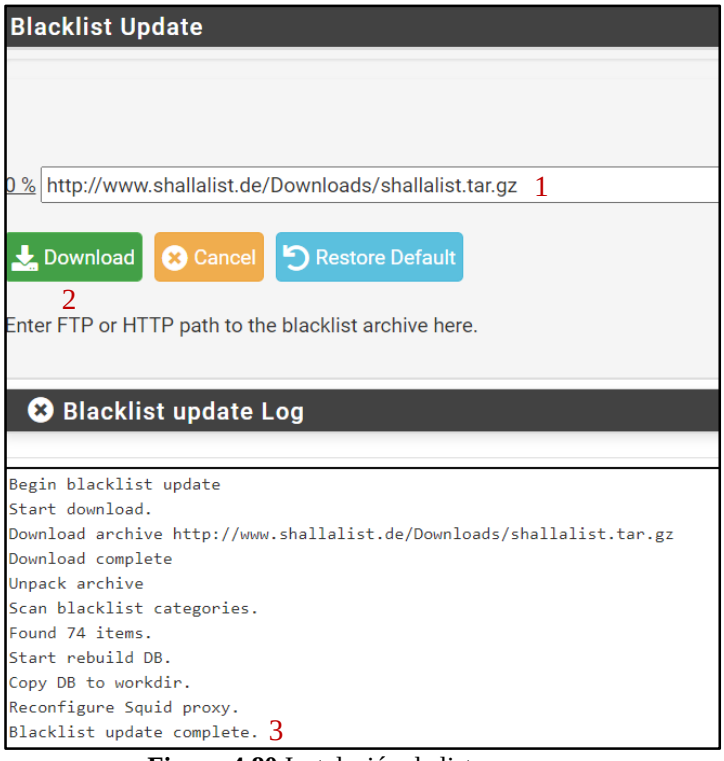


Figura 4.80 Instalación de listas negras.
Fuente: Desarrollado por el investigador.

- Una vez descargar las listas negras ir a Common ACL, clic en Targer Rules List para ver la lista de sitios bloqueados como indica la figura 4.81, por defecto todo está denegado pero se puede configurar el listado según los requerimientos de la organización.

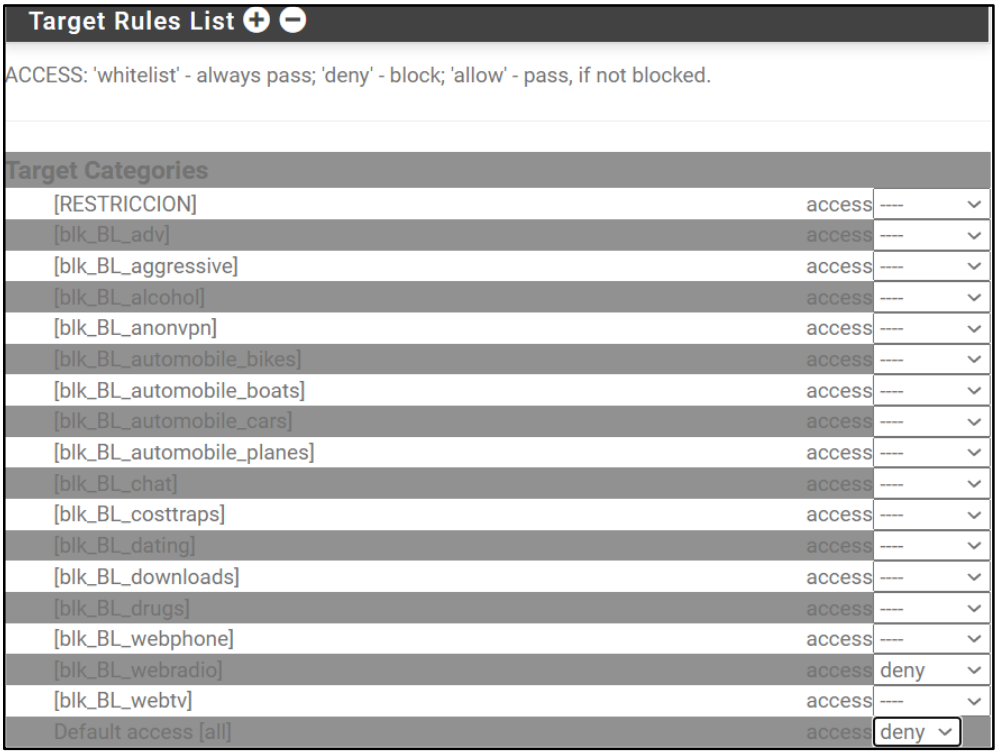


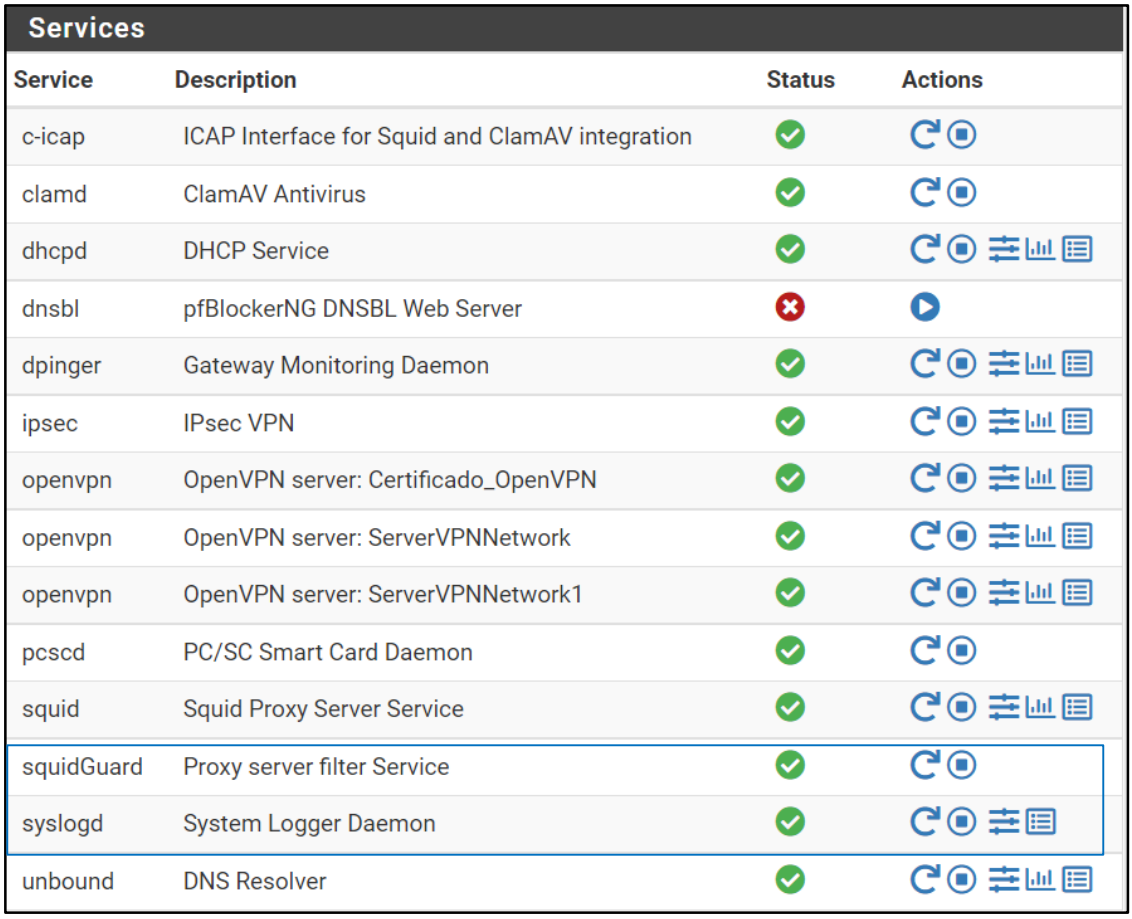
Figura 4.81 Listas negras.
Fuente: Desarrollado por el investigador.

Del listado de la figura 4.82 en Default Access se cambia el estado access: allow para permitir todo y solo se va restringir redes sociales, videos y páginas pornográficas. Finalmente ir a General settings y habilitar los siguientes parámetros:

- ✓ Enable
- ✓ Enable GUI log
- ✓ Enable log
- ✓ Enable log rotation
- ✓ Blacklist
- ✓ Blacklist URL: http://www.shallalist.de/Downloads/shallalist.tar.gz
- ✓ Apply
- ✓ Save

- Para configurar Squid ir a Services, Squid Proxy Server, General y habilitar los siguientes parámetros.
  - ✓ Enable Squid Proxy
  - ✓ Keep Settings/Data
  - ✓ Allow Users on Interface.
  - ✓ Transparent HTTP Proxy
  - ✓ HTTPS/SSL Interception
  - ✓ Enable Access Logging
  - ✓ Save

Una vez realizadas estas configuraciones ir a Status, Services y chequear si los dos servicios están activos para hacer las pruebas de bloqueo de páginas como señala la figura 4.82.



Services

Service	Description	Status	Actions
c-icap	ICAP Interface for Squid and ClamAV integration	✓	
clamd	ClamAV Antivirus	✓	
dhcpd	DHCP Service	✓	
dnsbl	pfBlockerNG DNSBL Web Server	✗	
dpinger	Gateway Monitoring Daemon	✓	
ipsec	IPsec VPN	✓	
openvpn	OpenVPN server: Certificado_OpenVPN	✓	
openvpn	OpenVPN server: ServerVPNNetwork	✓	
openvpn	OpenVPN server: ServerVPNNetwork1	✓	
pcscd	PC/SC Smart Card Daemon	✓	
squid	Squid Proxy Server Service	✓	
squidGuard	Proxy server filter Service	✓	
syslogd	System Logger Daemon	✓	
unbound	DNS Resolver	✓	

Figura 4.82 Revisión del estado de los servicios.
Fuente: Desarrollado por el investigador.

- La figura 4.83 muestra el bloqueo de una página pornográfica desde un computador que está dentro de la red local de pfSense.

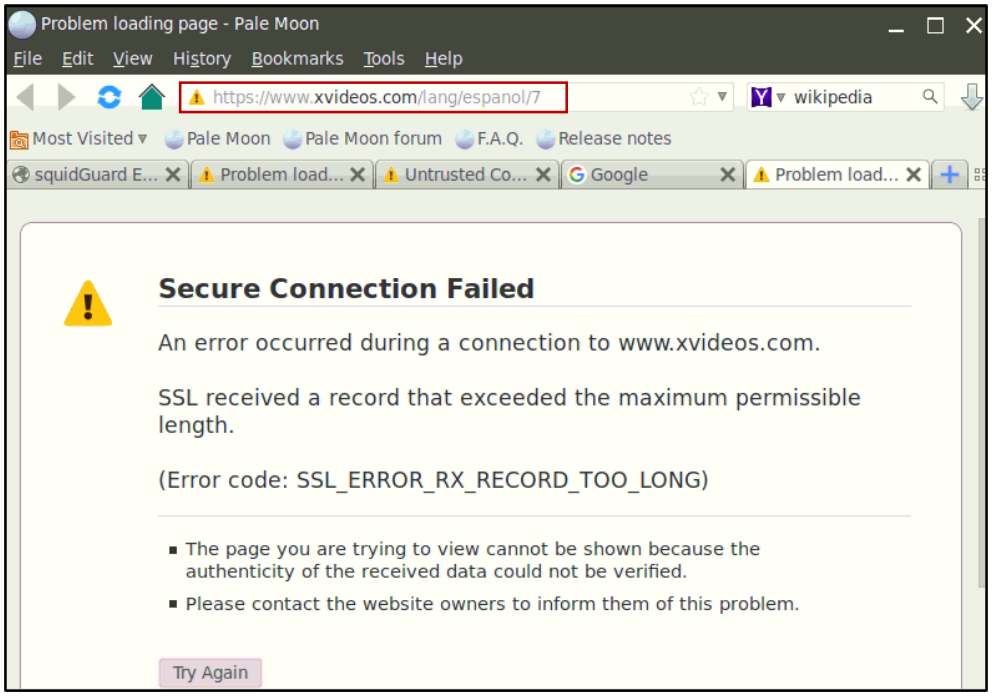


Figura 4.83 Bloqueo de páginas pornográficas.
Fuente: Desarrollado por el investigador.

- Si revisamos las conexiones en tiempo real mostrará la hora, el host con la dirección IP y las peticiones denegadas por las reglas aplicadas como muestra la figura 4.84.

SquidGuard Table

SquidGuard Logs

Date-Time	ACL	Address	Host	User
10.10.2021 09:26:00	Request(default/blk_BL_porn/-)	www.xvideos.com:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:26:00	Request(default/in-addr/-)	185.88.181.3:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:26:00	Request(default/blk_BL_porn/-)	www.xvideos.com:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:26:00	Request(default/in-addr/-)	185.88.181.3:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:25:48	Request(default/blk_BL_porn/-)	www.xnxx.com:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:25:48	Request(default/in-addr/-)	185.88.181.56:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:25:48	Request(default/blk_BL_porn/-)	www.xnxx.com:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:25:48	Request(default/in-addr/-)	185.88.181.56:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:24:21	Request(default/in-addr/-)	172.217.30.206:443	192.168.16.101/192.168.16.101	-
10.10.2021 09:23:41	Request(default/in-addr/-)	142.250.78.163:443	192.168.16.101/192.168.16.101	-

Figura 4.84 Logs de intento de acceso a páginas bloqueadas.
Fuente: Desarrollado por el investigador.

4.7.8. Limitación de ancho de banda

En pfSense existe la opción de Traffic Shaper, esta herramienta de gestión de ancho de banda prioriza la transmisión de datos aplicación por aplicación para lo cual marca los paquetes que deben tener mayor prioridad en la transmisión y los paquetes que no están marcados esperan su turno en una cola de tráfico para ser transmitidos. Para configurar esta opción ir a Firewall, Traffic Shaper, Wizard, clic en *traffic_shaper_wizard_multi_all.xml* y configurar los siguientes parámetros:

- pfSense Traffic Shaper
  - ✓ Enter number of WAN type connections: 1
  - ✓ Enter number of LAN type interfaces: 1
  - ✓ Next
- Shaper configuration
  - ✓ Interface & Scheduler LAN #1: LAN
  - ✓ Interface & Scheduler: PRIQ
  - ✓ Interface & Scheduler WAN#1: WAN
  - ✓ Interface & Scheduler: PRIQ
  - ✓ Upload: 20 Mbit/s
  - ✓ Download: 20 Mbit/s
  - ✓ Next
- Voice over IP
  - ✓ Parámetros por defecto
  - ✓ Next
- Penalty Box
  - ✓ Enable: Penalize IP or Alias
  - ✓ Address: 192.168.16.101
  - ✓ Next
- Peer to Peer networking
  - ✓ Enable: Lower priority of Peer-to-Peer traffic
  - ✓ p2pCatchAll: Enable
  - ✓ BitTorrent- Enable

- ✓ Next

- Network Games
  - ✓ Parámetros por defecto
  - ✓ Next
- Raise or lower other Applications
  - ✓ Enable: Other networking protocols
  - ✓ Otorgar el nivel de prioridad por aplicación
  - ✓ Next
- Finalizar la configuración

Una vez culminado las configuraciones ir a Status, Traffic Graph como indica la figura 4.85, en este caso se analizará el tráfico de la red local en donde un host con la dirección 192.168.16.101 presenta flujo de tráfico de descargada desde la WAN hacia la LAN. El grupo de usuarios de la red local tienen configurado un ancho de banda de baja de subida y bajada de 20 Mbps simétrico, sin embargo se puede asignar estos valores de acuerdo a la actividad de cada usuario dentro de la empresa.

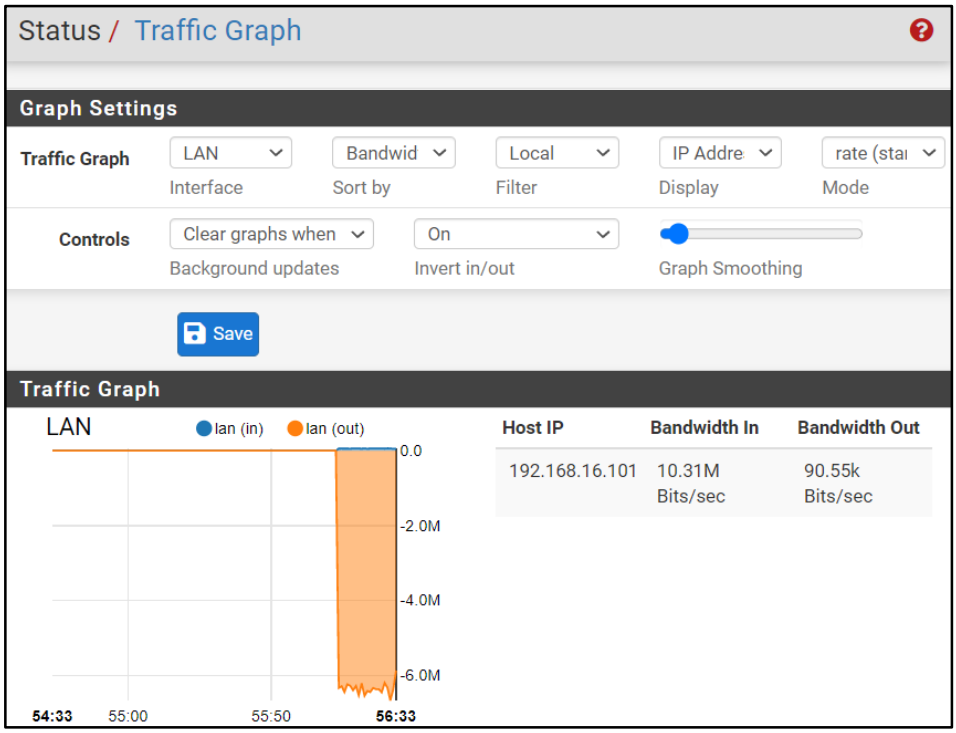


Figura 4.85 Control de tráfico por host.
Fuente: Desarrollado por el investigador.

4.7.9. Prevención de intrusos

Una herramienta que permite controlar todos los paquetes que atraviesan una red es Snort, este software de código abierto funciona como IPS, está integrado en pfSense y permite monitorizar el flujo de paquetes dentro de la red en tiempo real. Una vez que los paquetes son analizados a partir de las reglas previamente configuradas se puede alertar y responder ante alguna anomalía encontrada.

Para instalar y configurar este paquete se debe seguir los siguientes pasos:

- Reglas: Crear una cuenta en la página de Snort para acceder al código Oinkcode como indica la figura 4.86, este código es único y permitirá descargar las reglas IPS.

Figura 4.86 Código Oinkcode.
Fuente: Desarrollado por el investigador.

- Instalación: Ir a System, Package Manager, Available Packages y buscamos Snort para proceder con la instalación.
- Configuración global: Ir a Services, Snort, Global Setting y configurar los siguientes parámetros.
  - ✓ Enable Snort VRT
  - ✓ Snort Oinkmaster Code: 98e3b38a9c9e63a18dea96ec3c8396ff4c107912
  - ✓ Enable Snort GPLv2
  - ✓ Enable ET Open
  - ✓ Enable OpenAppID
  - ✓ Enable AppID Open Text Rules
  - ✓ Enable Hide Deprecated Rules Categories
  - ✓ Enable Keep Snort Settings After Deinstall
  - ✓ Save

- Descarga de reglas: Ir a updates y dar clic en Update Rules.

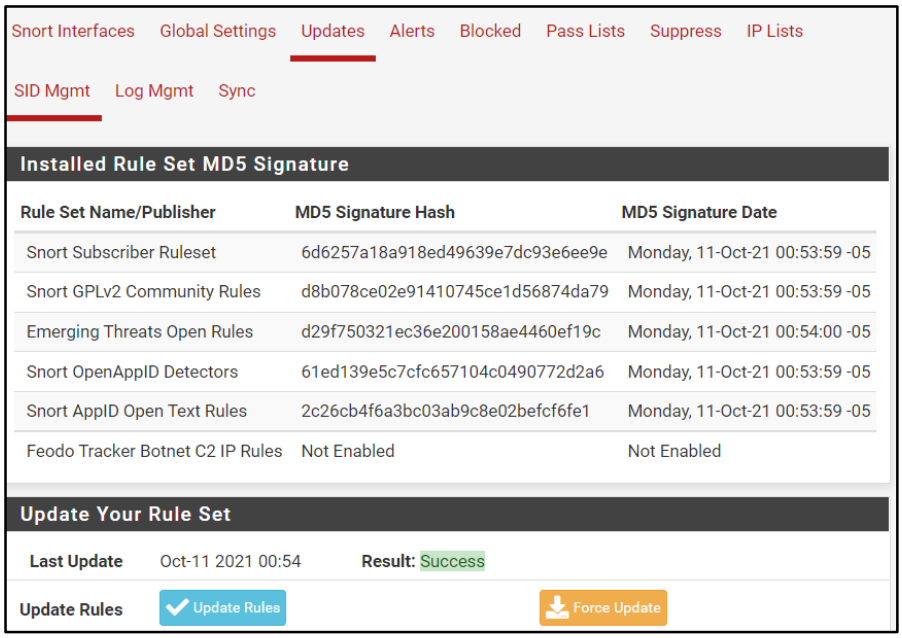


Figura 4.87 Reglas de Snort.
Fuente: Desarrollado por el investigador.

- **Configuración WAN:** Ir a Services, Snort, Snort Interfaces y dar clic en agregar para configurar los siguientes parámetros.
  - ✓ Enable interface
  - ✓ Interface: WAN (vtnet0)
  - ✓ Enable search optimization. Default is Not Checked.
  - ✓ Save
- **Configuración LAN:** Ir a Services, Snort, Snort Interfaces y dar clic en agregar para configurar los siguientes parámetros.
  - ✓ Enable interface
  - ✓ Interface: LAN (em0)
  - ✓ Enable search optimization. Default is Not Checked.
  - ✓ Save
- **Habitación reglas WAN:** Ir a Services, Snort, Snort Interfaces, dar clic en WAN-Categories para configurar los siguientes parámetros.
  - ✓ Enable: Use IPS Policy

- ✓ IPS Policy Selection: Connectivity
- ✓ Enable: Snort GPLv2 Community Rules (Talos certified)
- ✓ Select All
- ✓ Save
- ✓ Ir a WAN Preprocs y habilitar: Use OpenAppID to detect various applications. Default is Not Checked y guardar como muestra la figura 4.88.

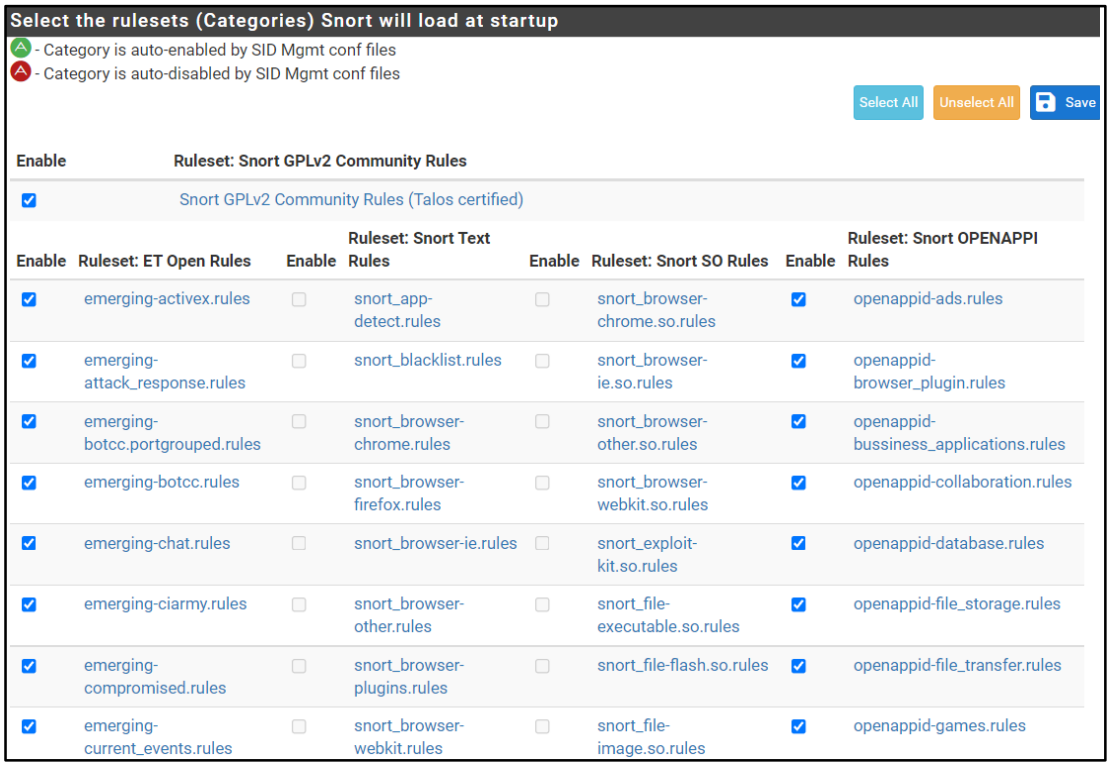


Figura 4.88 Habilitación de Reglas Snort.
Fuente: Desarrollado por el investigador.

- Habitación reglas LAN: Configurar los mismos parámetros indicados en la habilitación de reglas WAN.
- Encender las interfaces WAN y LAN como indica la figura 4.89.

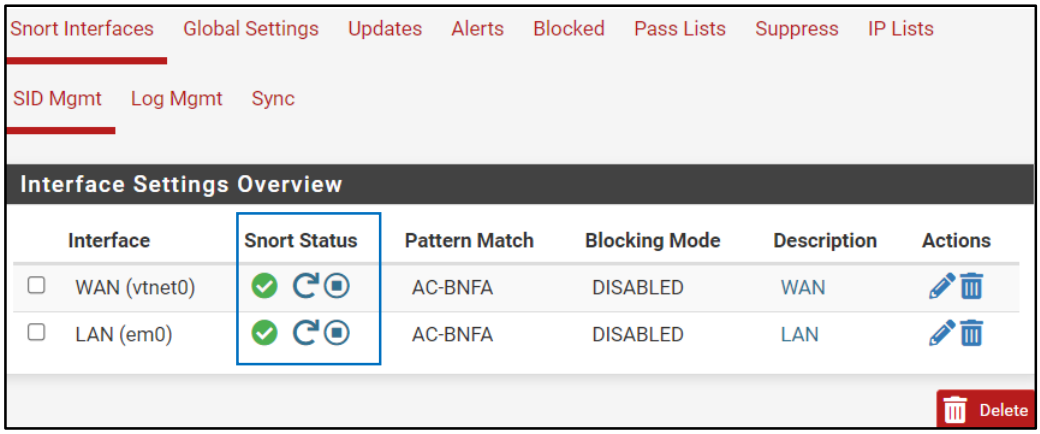


Figura 4.89 Configuración interface WAN/LAN modo alerta.
Fuente: Desarrollado por el investigador.

- **Revisión de las alertas:** La revisión de alertas se puede hacer tanto a la LAN o WAN. Para este caso se filtrará el tráfico generado por la red local como indica la figura 4.90, en el informe se pude ver cada alerta, la dirección IP de origen, IP destino, protocolo, puerto y la página a donde se quiere acceder, Snort identifica el tipo de tráfico y bloquea todo lo que está declarado en las reglas. Estas reglas puede ser configuradas por el administrador, inclusive se pueden deshabilitar por su SID o identificador. Al deshabilitar una regla se entiende que Snort no proporcionará ningún tipo de información sobre la misma, es decir, que alguna anomalía encontrada en cuanto a la regla deshabilitada no será informada al administrador.

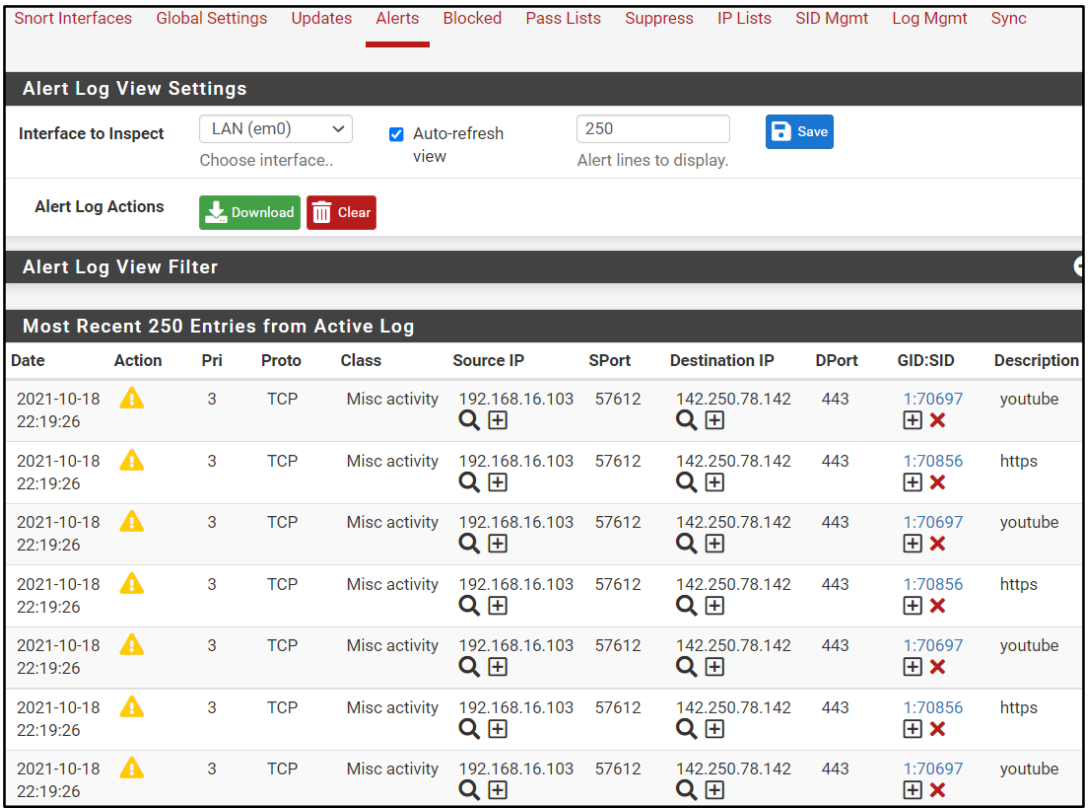


Figura 4.90 Revisión de alertas LAN.
Fuente: Desarrollado por el investigador.

4.8.Comparación entre los dos sistemas UTM

Una vez configuradas y realizadas las respectivas pruebas con los UTM hardware y software se hace una comparación de sus características más destacadas identificadas en el transcurso del proyecto.

4.8.1. Seguridad

Para evaluar este parámetro nuevamente se usó la herramienta Shodan, en este motor de búsqueda se revisó las direcciones IP de los dos equipos UTM arrojando los siguientes resultados:

- **UTM propietario Sophos XG 115**

  La información más destacada al investigar información de la IP configurada en el puerto WAN de este equipo fue el número de puertos abiertos en el Sophos, como muestra la figura 4.91 existe un total de 3 puertos abiertos. El puerto 500 hace referencia al servicio VPN configurado en el equipo mientras que el puerto

4443 hace referencia al portal de usuario del cliente VPN. Este mismo puerto muestra como información adicional la marca del equipo (Sophos) y el nombre del Partner donde fue adquirido. El último puerto abierto es el 8443, este puerto se utiliza cuando se ha asegurado la conexión mediante un certificado SSL entre el navegador y con el servidor web (Portal de Usuario Sophos, ver fig. 4.40)

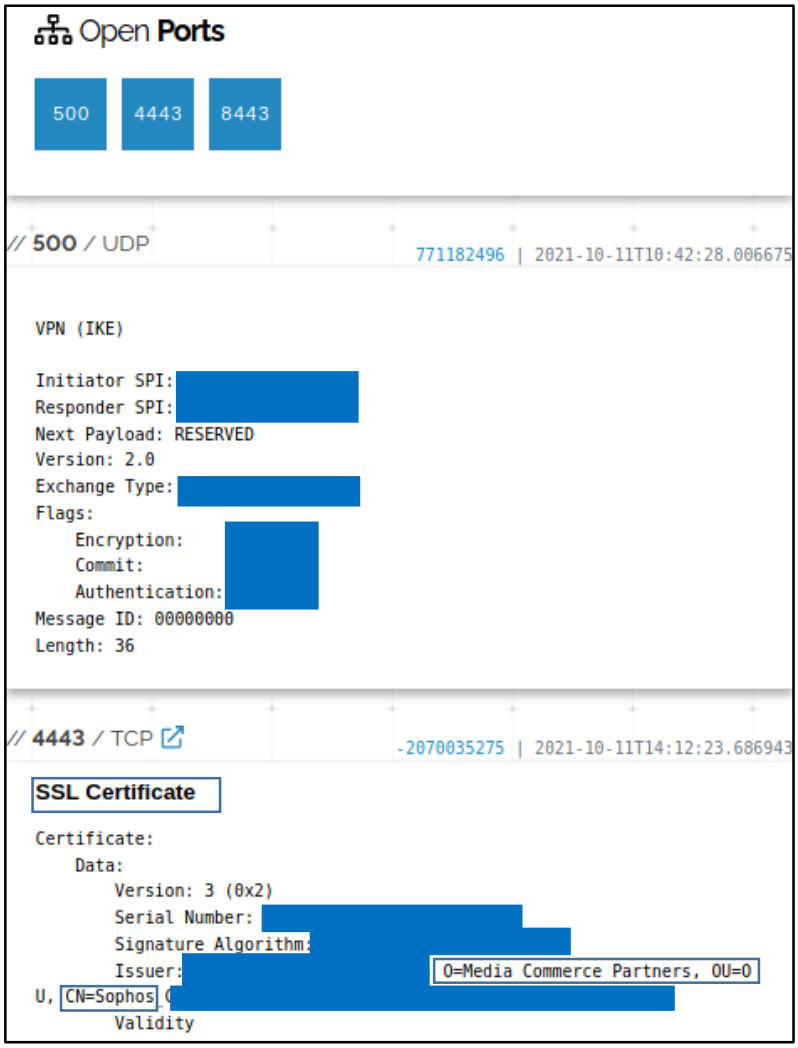


Figura 4.91 Puertos abiertos en el equipo Sophos.
Fuente: Desarrollado por el investigador.

- **UTM Open Sourse pfSense**

  Al investigar información de la IP configurada en la Eth1 o puerto WAN en el servidor pfSense se encontraron 8 puertos abiertos como muestra la figura 4.92. Los puertos 135, 137, 445, 5357 y 5985 son propios del sistema operativo en este caso el servidor cuenta con Windows Server 2016. El puerto 443 hace referencia al certificado SSL de pfSense mientras que el puerto 3389 es comúnmente utilizado para conexiones a escritorios remotos.

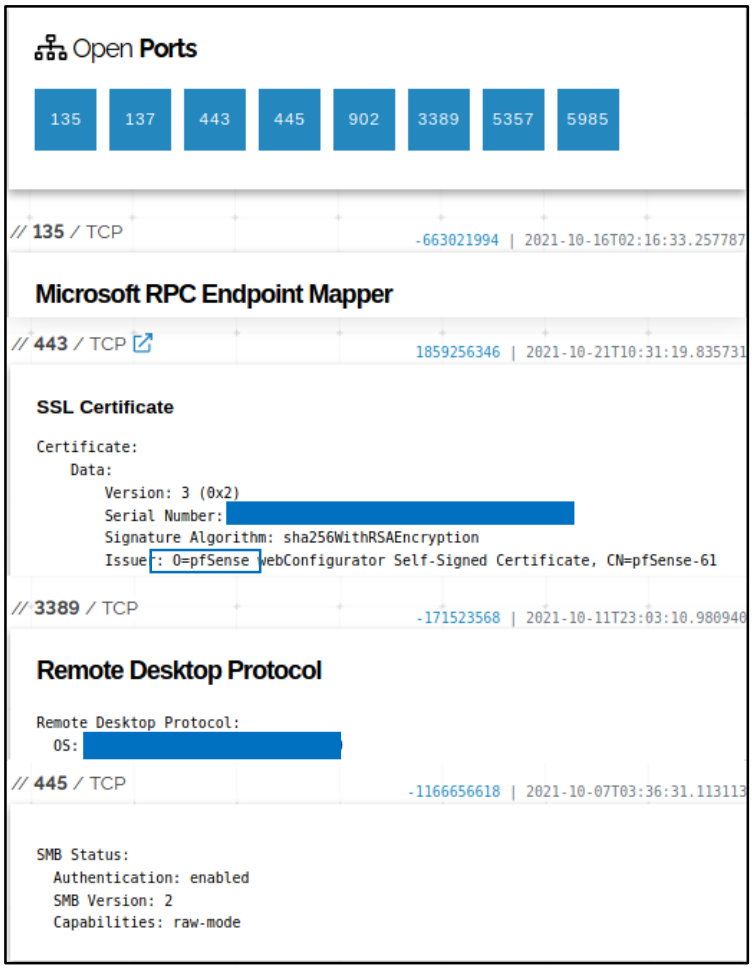


Figura 4.92 Puertos abiertos en el servidor_pfSense.
Fuente: Desarrollado por el investigador.

En tema seguridad se evidenció que el UTM propietario Sophos XG 115 presenta menos puerto abiertos que el UTM Open Sourse pfSense, esto se debe a la configuración de bookmarks en el equipo Sophos que facilita la conexión a escritorios remotos a través del

portal de usuario de este equipo sin acceder al servicio RDP que proporciona Windows de esta manera no es necesario la apertura de puertos en las reglas de firewall. Mientras que PfSense al no contar con la herramienta bookmarks fue necesario habilitar en el firewall los puertos necesarios para la conexión hacia los distintos RDP que tiene la empresa siendo el puerto por defecto el 3389 para este servicio.

4.8.2. Rendimiento

Las pruebas de rendimiento se realizaron sometiendo a los dos sistemas UTM a una conexión simultánea de 41 usuarios que corresponde al total del personal de la empresa. Los dos parámetros fundamentales que se evaluaron fueron ancho de banda y jitter por usuario.

- **UTM propietario Sophos XG 115**

La figura 4.93 muestra flujo de datos enviados también a través JPerf desde un cliente configurado con la IP 192.168.15.127 (red LAN Sophos) hasta un servidor configurado con la IP 192.168.15.128 para medir el máximo ancho de banda y jitter por usuario. Dentro de las características del equipo (ver tabla 4.5) menciona que el número máximo de usuarios es de 80, para esta prueba se configuró solo 41 clientes decir usa solo se usa la mitad de capacitad del equipo Sophos XG 115.

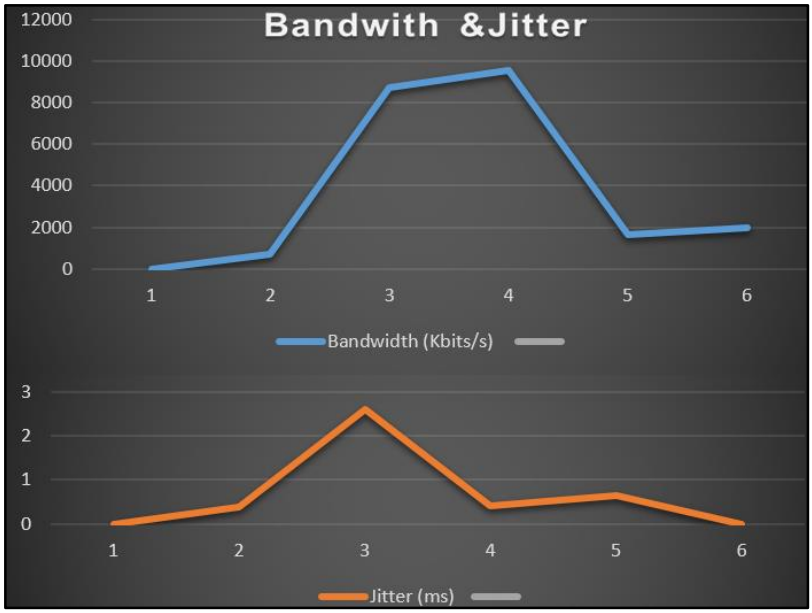
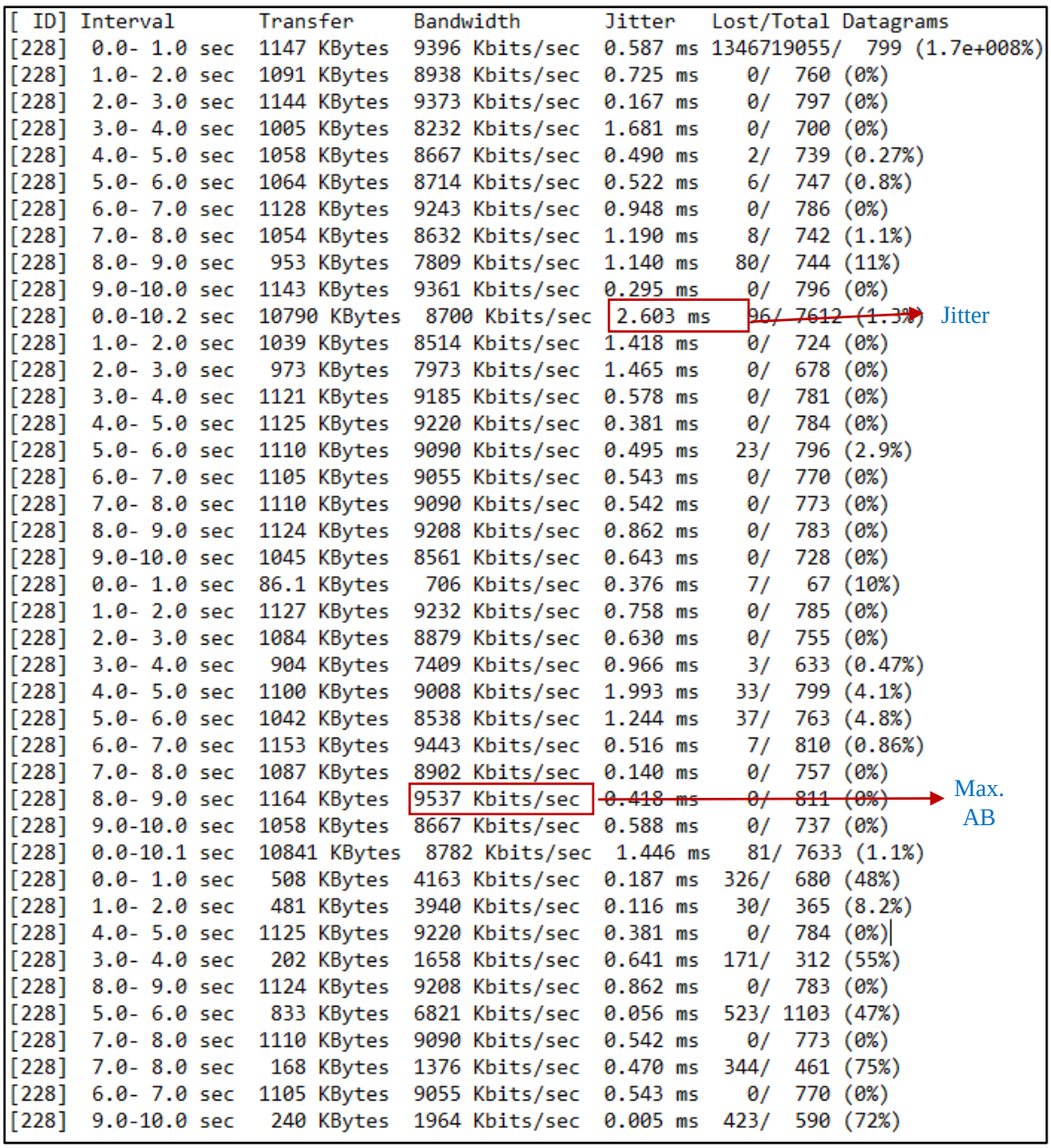


Figura 4.93 Máximo ancho de banda y jitter de los clientes de la red LAN Sophos.
Fuente: Desarrollado por el investigador.

Como se puede observar en la figura 4.94 el máximo ancho de banda que un usuario tendrá es de 9 Mbps configurado en el apartado 4.6.8 en donde se limita a todos los usuarios por grupo a un ancho de banda máximo de 20 Mbps. También se observa que el usuario con mayor fluctuación presenta un jitter mayor de 2.603 ms.



[ID]	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[228]	0.0- 1.0 sec	1147 KBytes	9396 Kbits/sec	0.587 ms	1346719055/ 799 (1.7e+008%)
[228]	1.0- 2.0 sec	1091 KBytes	8938 Kbits/sec	0.725 ms	0/ 760 (0%)
[228]	2.0- 3.0 sec	1144 KBytes	9373 Kbits/sec	0.167 ms	0/ 797 (0%)
[228]	3.0- 4.0 sec	1005 KBytes	8232 Kbits/sec	1.681 ms	0/ 700 (0%)
[228]	4.0- 5.0 sec	1058 KBytes	8667 Kbits/sec	0.490 ms	2/ 739 (0.27%)
[228]	5.0- 6.0 sec	1064 KBytes	8714 Kbits/sec	0.522 ms	6/ 747 (0.8%)
[228]	6.0- 7.0 sec	1128 KBytes	9243 Kbits/sec	0.948 ms	0/ 786 (0%)
[228]	7.0- 8.0 sec	1054 KBytes	8632 Kbits/sec	1.190 ms	8/ 742 (1.1%)
[228]	8.0- 9.0 sec	953 KBytes	7809 Kbits/sec	1.140 ms	80/ 744 (11%)
[228]	9.0-10.0 sec	1143 KBytes	9361 Kbits/sec	0.295 ms	0/ 796 (0%)
[228]	0.0-10.2 sec	10790 KBytes	8700 Kbits/sec	2.603 ms	96/ 7612 (1.3%)
[228]	1.0- 2.0 sec	1039 KBytes	8514 Kbits/sec	1.418 ms	0/ 724 (0%)
[228]	2.0- 3.0 sec	973 KBytes	7973 Kbits/sec	1.465 ms	0/ 678 (0%)
[228]	3.0- 4.0 sec	1121 KBytes	9185 Kbits/sec	0.578 ms	0/ 781 (0%)
[228]	4.0- 5.0 sec	1125 KBytes	9220 Kbits/sec	0.381 ms	0/ 784 (0%)
[228]	5.0- 6.0 sec	1110 KBytes	9090 Kbits/sec	0.495 ms	23/ 796 (2.9%)
[228]	6.0- 7.0 sec	1105 KBytes	9055 Kbits/sec	0.543 ms	0/ 770 (0%)
[228]	7.0- 8.0 sec	1110 KBytes	9090 Kbits/sec	0.542 ms	0/ 773 (0%)
[228]	8.0- 9.0 sec	1124 KBytes	9208 Kbits/sec	0.862 ms	0/ 783 (0%)
[228]	9.0-10.0 sec	1045 KBytes	8561 Kbits/sec	0.643 ms	0/ 728 (0%)
[228]	0.0- 1.0 sec	86.1 KBytes	706 Kbits/sec	0.376 ms	7/ 67 (10%)
[228]	1.0- 2.0 sec	1127 KBytes	9232 Kbits/sec	0.758 ms	0/ 785 (0%)
[228]	2.0- 3.0 sec	1084 KBytes	8879 Kbits/sec	0.630 ms	0/ 755 (0%)
[228]	3.0- 4.0 sec	904 KBytes	7409 Kbits/sec	0.966 ms	3/ 633 (0.47%)
[228]	4.0- 5.0 sec	1100 KBytes	9008 Kbits/sec	1.993 ms	33/ 799 (4.1%)
[228]	5.0- 6.0 sec	1042 KBytes	8538 Kbits/sec	1.244 ms	37/ 763 (4.8%)
[228]	6.0- 7.0 sec	1153 KBytes	9443 Kbits/sec	0.516 ms	7/ 810 (0.86%)
[228]	7.0- 8.0 sec	1087 KBytes	8902 Kbits/sec	0.140 ms	0/ 757 (0%)
[228]	8.0- 9.0 sec	1164 KBytes	9537 Kbits/sec	0.418 ms	0/ 811 (0%)
[228]	9.0-10.0 sec	1058 KBytes	8667 Kbits/sec	0.588 ms	0/ 737 (0%)
[228]	0.0-10.1 sec	10841 KBytes	8782 Kbits/sec	1.446 ms	81/ 7633 (1.1%)
[228]	0.0- 1.0 sec	508 KBytes	4163 Kbits/sec	0.187 ms	326/ 680 (48%)
[228]	1.0- 2.0 sec	481 KBytes	3940 Kbits/sec	0.116 ms	30/ 365 (8.2%)
[228]	4.0- 5.0 sec	1125 KBytes	9220 Kbits/sec	0.381 ms	0/ 784 (0%)
[228]	3.0- 4.0 sec	202 KBytes	1658 Kbits/sec	0.641 ms	171/ 312 (55%)
[228]	8.0- 9.0 sec	1124 KBytes	9208 Kbits/sec	0.862 ms	0/ 783 (0%)
[228]	5.0- 6.0 sec	833 KBytes	6821 Kbits/sec	0.056 ms	523/ 1103 (47%)
[228]	7.0- 8.0 sec	1110 KBytes	9090 Kbits/sec	0.542 ms	0/ 773 (0%)
[228]	7.0- 8.0 sec	168 KBytes	1376 Kbits/sec	0.470 ms	344/ 461 (75%)
[228]	6.0- 7.0 sec	1105 KBytes	9055 Kbits/sec	0.543 ms	0/ 770 (0%)
[228]	9.0-10.0 sec	240 KBytes	1964 Kbits/sec	0.005 ms	423/ 590 (72%)

Figura 4.94 Conexiones simultáneas de 41 clientes LAN en Sophos.
Fuente: Desarrollado por el investigador.

Una característica importante de resaltar del equipo Sophos es que asegura la comunicación de los 41 clientes conectados a la vez, la figura 4.94 también muestra que todos los paquetes enviados son recibidos sin pérdida alguna.

- **UTM Open Sourse pfSense**

La figura 4.95 muestra flujo de datos enviados a través JPerf desde un cliente configurado con la IP 192.168.16.109 (red LAN pfSense) hasta un servidor configurado con la IP 192.168.16.108 para medir el máximo ancho de banda y jitter por usuario.

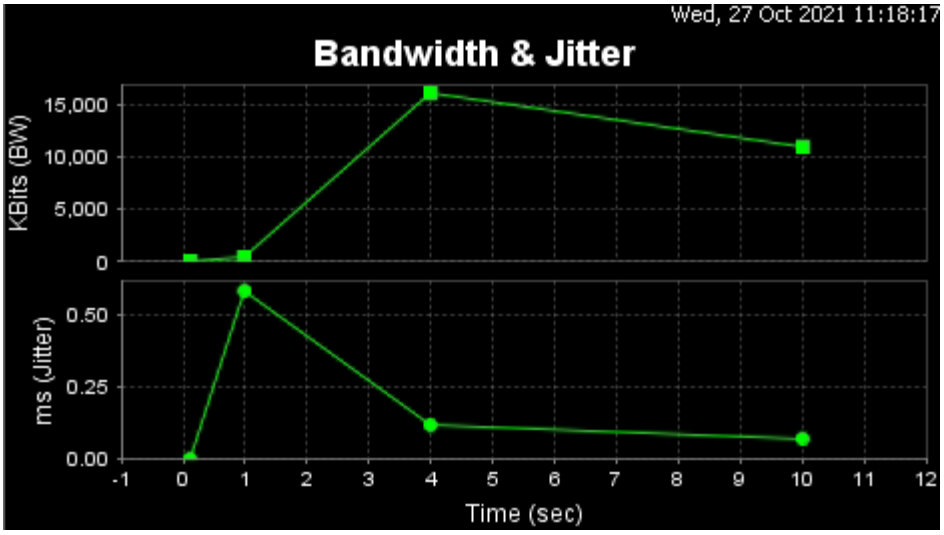


Figura 4.95 Máximo ancho de banda y jitter de los clientes de la red LAN pfSense.
Fuente: Desarrollado por el investigador.

Como se puede observar en la figura 4.96 el máximo ancho de banda que un usuario tendrá es de 15 Mbps configurado en el apartado 4.7.8 en donde se limita a todos los usuarios por grupo a un ancho de banda máximo de 20 Mbps. También se observa que el usuario con mayor fluctuación es el que presenta un jitter mayor de 2.692 ms, considerando que un jitter mayor a 30 ms produce un retraso en el envío recepción de datos o a su pérdida de información no siendo este el caso.

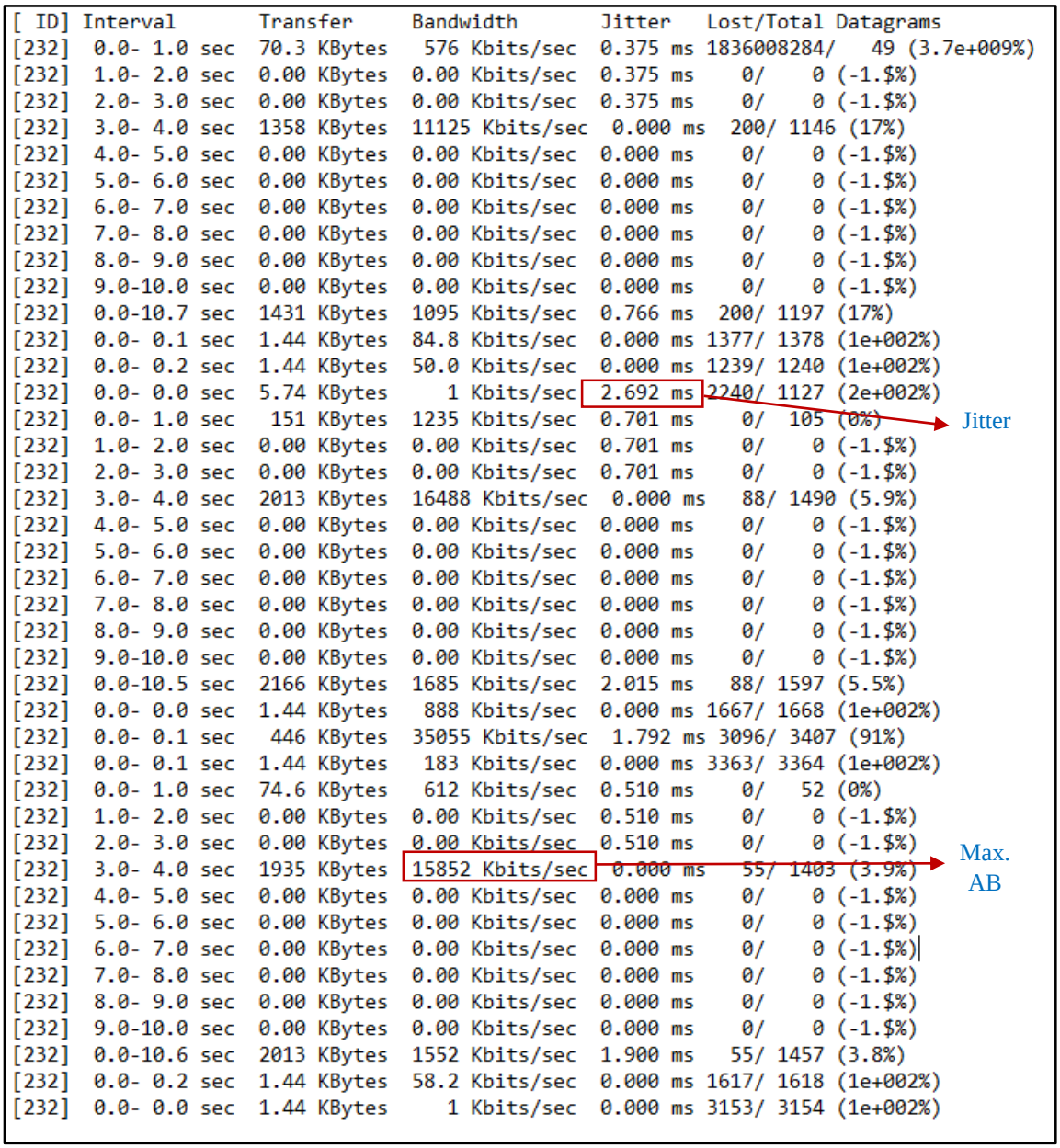


Figura 4.96 Conexiones simultáneas de 41 clientes_LAN en pfSense.
Fuente: Desarrollado por el investigador.

La figura 4.96 también muestra que no todos los paquetes enviados son recibidos, de un total de 41 clientes conectados 24 clientes son víctimas de pérdida de información. Si bien el ancho de banda es el óptimo para trabajar no compensa que la mitad de los colaboradores pierdan conexión a la red empresarial.

En resumen la tabla 4.8 muestra los resultados globales del análisis.

Tabla 4.8 Rendimiento Sophos vs pfSense.

Usuarios	**Ancho de Banda (Kbits/sec)**		**Jitter (ms)**	
	psSense	**Sophos**	**psSense**	**Sophos**
User X	1 (min)	706 (min)	0.375 (min)	0.05 (min)
User Y	15852 (max)	9443 (max)	2.692 (max)	2.603 (max)

Fuente: Desarrollado por el investigador.

Se deduce que el mejor rendimiento entre los dos sistemas UTM es del equipo Sophos, al brindar menor ancho de banda a los usuarios conectados evita que haya pérdida de paquetes de datos manteniendo un jitter bajo para asegurar las conexiones de cada cliente. A diferencia de pfSense que prioriza el ancho de banda dejando un lado la conexión de los clientes.

Rentabilidad

La tabla 4.9 muestra la inversión económica inicial así como el tiempo invertido por el investigador en cada uno de los sistemas implementados.

Tabla 4.9 Rentabilidad Sophos vs pfSense.

Características	**Sophos**	**pfSense**
Precio (incl. licencia)	$ 1.385,44	$ 0
Precio anual de la licencia	$ 438,44	$ 0
Equipo de alojamiento (servidor)	No (hardware y software en un solo equipo)	$ 999 (requiere de hardware para la instalación del software)
Interface web amigable con el usuario	Si	Si
Tiempo de configuración	1 mes	2 meses
Soporte técnico	Si	No (Community Support)

Características	Sophos	pfSense
Capacitación inicial	Si (incluye en la compra del equipo)	No (investigación)
Dificultad de instalación	No	Si
Dificultad de configuración	No	Si
Dificultad de configuración del equipo de alojamiento	No aplica	Si
Dificultad de adquisición	Si	No
Módulos de protección	Si (incluye todos)	No (instalación acorde a las necesidades del administrador)
Costo Total	$ 1.385,44	$ 999

Fuente: Desarrollado por el investigador.

Análisis de Resultados

Una vez concluidas las fases de pruebas de ambos sistemas y en base a la tabla 4.11 se muestra los siguientes resultados:

- La implementación del equipo Sophos tiene un costo inicial de $1.385,44 incluyendo la licencia. El segundo año y años posteriores de funcionamiento el costo de la licencia anual será aproximadamente de $ 438,44, este valor puede variar dependiendo de la versión de hardware y paquetes adicionales que se requiera instalar. Por otro lado pfSense es un software no licenciado pero requiere un equipo de alojamiento para instalar el sistema, este equipo puede ir desde un computador de escritorio hasta un servidor. Por lo tanto el costo inicial de implementar pfSense es de $ 999 debido al costo del servidor, en los años posteriores de funcionamiento no representará mayores gastos para la empresa salvo que el hardware (PC o servidor) presenten daños y se deba cambiar por otro equipo.

- Sophos al englobar en un solo equipo hardware y software requiere de una licencia anual para usar y habilitar cada paquete de protección mientras que pfSense al no ser licenciado depende del aporte de la comunidad para actualizar y mejorar el código fuente de cada paquete de protección.
- PfSense requiere de un host de alojamiento para instalar el software, a modo de prueba se puede utilizar un computador con características modestas para que el sistema arranque pero si la implementación es a nivel de empresas donde se maneja gran cantidad de información es necesario un servidor con recursos más robustos para soportar el flujo de tráfico al momento de configurar cada servicio o paquete de seguridad.
- Los dos sistemas UTM presentan una interface web intuitiva y amena con el usuario aunque en pfSense las configuraciones también se pueden hacer vía consola siempre y cuando se tenga el conocimiento necesario.
- La marca Sophos proporciona soporte técnico 24/7 por un costo adicional mientras que pfSense no dispone de soporte técnico, son los miembros de la comunidad quienes resuelven fallas y comparten su experiencia y soluciones en foros.
- Por la adquisición del equipo Sophos se obtuvo una capacitación inicial de configuración para dos miembros de la empresa, mientras que pfSense al ser un software Open Source pertenece a la comunidad y la configuración se basa en consultas y pruebas realizadas por el investigador.
- La adquisición del equipo Sophos duró algunas semanas debido al presupuesto y disponibilidad del producto por parte del Partner en Ecuador, mientras que pfSense está disponible 24/7 en su página web y con unos sencillos pasos se puede descargar para su pronta instalación.
- Si bien Sophos es un equipo propietario hardware y software que no necesita mayor configuración inicial aparte de las interfaces WAN y LAN, posterior a ello las configuraciones de los servicios de seguridad son de mediana dificultad. Esto no sucede con pfSense, en donde la configuración inicial de las interfaces WAN y LAN de la máquina virtual con las interfaces físicas de la máquina real requiere

de una investigación profunda del investigador siendo el mismo caso la configuración de los paquetes de seguridad.

4.9.Manual de buenas prácticas

El manual de buenas prácticas se muestra en el Anexo 1.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Las herramientas informáticas como Kali Linux, Netcraft y Shodan permitieron identificar información sensible de la empresa como direcciones IP, puertos abiertos, servicios disponibles y demás datos que se derivan en vulnerabilidades y que al ser explotadas por personas mal intencionadas ponen en riesgos los activos de la empresa. Las vulnerabilidades encontradas provenían en su mayoría de puertos abiertos y software sin actualizar, un puerto abierto es una ventana abierta para que un intruso vulnere la escasa seguridad, gane acceso y robe los datos, instale malware o incluso apague el sistema.
- La configuración de un gestor unificado de amenazas propietario como Sophos dentro de la red empresarial optimiza el tiempo y recursos que el administrador de redes debe invertir por ser fácil e intuitivo de gestionar puesto que todo el paquete de seguridad está concentrado en un solo dispositivo. Las políticas de firewall y servicios que se levante en el equipo depende del requerimiento de la empresa, mientras más políticas de seguridad se configure mayor será la integridad de los datos corporativos.
- La configuración de pfSense como gestor unificado de amenazas para proteger la red empresarial requiere de más tiempo y recursos por parte del administrador de redes, en primero lugar es necesario elegir el equipo de alojamiento con las características físicas y lógicas para instalar el software y soporte todas las configuraciones que demanda la empresa para proteger sus datos. Y por último, el administrador debe investigar cada problema que surja durante la configuración del sistema ya que al ser Open Source no dispone de soporte técnico, además cada paquete de seguridad debe ser descargado e instalado posterior a la configuración del software. Cada una de las configuraciones realizadas en pfSense crea por defecto reglas de firewall las mismas que limitan el acceso a otros servicios ya establecidos y es necesario revisar constantemente si hay bloqueos innecesarios que limiten o restrinjan servicios previamente levantados y verificados.

- Una de las características más destacadas de Sophos frente a pfSense es el acceso a un portal del usuario, en dicho portal los usuarios tienen acceso a diferentes servicios, por ejemplo, escritorios remotos. Desde el portal web de Sophos se puede acceder sin ser necesario ingresar por el escritorio remoto de Windows volviéndose innecesario el uso de puertos para el ingreso. Si a esto se le suma el uso de VPN como puerta de enlace entre el servidor RDP y el usuario se minimizará los riesgos de sufrir un incidente de seguridad. PfSense no constan con un portal de usuario para configurar el acceso vía web a escritorios remotos, si se requiere acceder a un RDP es necesario habilitar el puerto de acceso en las reglas de firewall.

- Al final del proyecto se llega a la conclusión que Sophos brinda mayor confianza y sencillez para implementar una solución efectiva contra amenazas que pfSense. Si bien pfSense es gratuito y no licenciado para ser implementado en una empresa mediana o grande su host de alojamiento debe tener características superiores a un ordenador común, por eso se habla de servidores con los recursos necesarios para instalar y poner en marcha este sistema. Sophos a diferencia de pfSense cuenta con asesoría y acompañamiento durante la configuración y puesta en marcha del equipo, claro que representa un valor económico adicional para la empresa pero se justifica con el hecho que sus activos estén protegidos.
- El manual buenas prácticas de seguridad está orientado al personal técnico y administrativo de la empresa para adoptar mecanismos de prevención ante acciones maliciosas ya que en la mayoría de ocasiones la pérdida o adulteración de la información ocurre por los propios empleados ya sea por desconocimiento o una acción premeditada lo que conlleva a una situación de peligro si no se tienen respaldos de los datos comprometidos. En el manual se detalla el proceso para resguardar la información más valiosa para cada usuario, también proporciona consejos para que el administrador de redes también adopte buenas prácticas para administrar toda la información de la empresa y sus colaboradores.

5.2. Recomendaciones

- En el manual de buenas prácticas se recomienda la creación de contraseñas seguras, que contengan al menos ocho letras, un número, letras mayúsculas y minúsculas y un carácter especial. En la actualidad existen programas que administran y generan claves seguras creadas a partir de las directrices que el administrador de la red defina. Una vez creadas las contraseñas se debe controlar que los usuarios no tengan anotadas en sus escritorios o bloc de notas siendo visible para terceras personas, ya que, por más robusta que sea una contraseña si está a la vista de todos sigue siendo vulnerable.
- La página web de la empresa carece de certificado SSL, es decir, no es segura por lo que cualquier tipo de información que los usuarios ingresen está propenso a ser interceptada por atacantes poniendo en peligro la información de la empresa y los clientes por lo que es necesario cifrar o encriptar las conexiones entre el navegador y servidor web así toda la información que se intercambia estará protegida generando confianza en los usuarios.
- La marca Sophos permite dos formas de gestionar el UTM XG 115, la primera es a través de su Partner y la segunda de manera independiente. Cabe mencionar que cada consulta al Partner tiene un valor económico por la hora de asesoría y si a esto se le suma la activación anual de la licencia representa gastos extras para la empresa. La opción más acertada es administrar el equipo de manera autónoma, es decir, invertir en capacitaciones para el personal de redes tenga el conocimiento necesario para administrar el equipo según los requerimientos de la empresa.
- Durante la configuración de pfSense verificar que el servidor en donde se va a instalar tenga habilitado en la BIOS la opción de virtualización. También es necesario que el servidor contenga más de tres puertos Ethernet de tal manera que si se pierde conexión y se bloquea el servicio por las reglas de firewall o proxy habilitadas se pueda ingresar por un puerto totalmente diferente de la red WAN y LAN del pfSense. Por último, aplicar la IP pública con acceso a internet directamente a la WAN del pfSense y conectar en modo puente al puerto Ethernet del servidor previamente configurado con los DNS en el caso de ser necesario.

- Cambiar los puertos de acceso a la interface de Sophos y portal de usuario, por defecto está configurado los puertos 445 y 443, el cambio deber ser por un par de puertos que soporte el protocolo https.
- Es recomendable implementar equipos de seguridad perimetral para redes en dispositivos netamente destinados a una función específica (Servidor como Firewall); sin embargo para circunstancias en las que no se cuente con un equipo destinado para una única función de red, la virtualización puede ser una solución efectiva únicamente si al equipo de propósito general se le ha dotado de interfaces, periféricos, procesadores, memoria y adicionalmente se configuran las interfaces de red como adaptadores puenteados con el afán de obtener el contacto directo con los dispositivos a controlar.

BIBLIOGRAFÍA

[1] 20minutos, «www.20minutos.es - Últimas Noticias.,» 01 Julio 2018. [En línea]. Available: https://www.20minutos.es/noticia/3382959/0/pymes-microempresas-onu-economia-empleo/?autoref=true. [Último acceso: 10 Marzo 2020].

[2] E&N, «www.estrategiaynegocios.net,» 26 Septiembre 2017. [En línea]. Available: https://www.estrategiaynegocios.net/centroamericaymundo/1111615-330/los-ciberataques-en-el-mundo-cuestan-us575000-m-anuales. [Último acceso: 12 Marzo 2020].

[3] El Universo, «www.eluniverso.com,» 27 Junio 2019. [En línea]. Available: https://www.eluniverso.com/noticias/2019/06/27/nota/7396308/mipymes-representan-99-negocios-pais. [Último acceso: 12 Marzo 2020].

[4] A. Hernández Dominguez y S. Storchak, «Sistema para la detección de ataques Phishing utilizando correo electrónico,» *Telemática,* vol. 17, nº 2, pp. 60-70, 28.

[5] C. Encalada, «Mejorar la Seguridad Perimetral de la red de datos de la Unidad Académica de Ingeniería de Sistemas Eléctrica y Electrónica de la Universidad Católica de Cuenca,» *ResearchGate,* pp. 1-11, 2012.

[6] W. Floréz R., C. A. Arboleda S. y J. F. Cadavid A., «Solución integral de seguridad para las pymes mediante un UTM,» *Ingenierías USBMed,* vol. 3, nº 1, pp. 35-42, 2012.

[7] Y. Casas Moreno, «UTM: Administración Unificada de Amenazas,» *Ventana Informática,* nº 22, pp. 173-185, 2010.

[8] V. Agham, «Unified Threat Management,» *International Research Journal of Engineering and Technology (IRJET),* vol. 03, nº 04, pp. 32-36, 2016.

[9] D. Kumar y M. Gupta, «Implementation of firewall & intrusion detection system using pfSense to enhance network security.,» *International Journal of Electrical Electronics & Computer Science Engineering, ICSCAAIT-2018,* pp. 131-137, 2016.

[10] J.-F. Carpentier, La seguridad informática en la PYME: Situacón actual y mejores prácticas, Barcelona : Ediciones ENI , 2016.

[11] J. F. Roa, Seguridad Informática, Madrid: McGraw-Hill/Interamericana de España, S. L, 2013.

[12] N. Nguyen, Essential Cyber Security Handbook In Spanish: Manual esencial de seguridad cibernética en español, 2018.

[13] J. Santos Costas , Seguridad y Alta Disponibilidad (GRADO SUPERIOR)., Madrid : Grupo Editorial RA-MA, 2014.

[14] Ó. A. Martín, UF0863 - Reparación y ampliación de equipos y componentes hardware microinformáticos, Elearning, 2015.

[15] P. Cervantes y O. Tauste, Internet Negro: El lado oscuro de la red, Grupo Planeta Spain, 2015.

[16] J. M. Ferro Veiga, Perito Judicial en Seguridad física y lógica de un sistema de información, 2020.

[17] G. F. Miguez Gomez, «Implementación de un sistema de gestión unificada de amenazas (UTM) para la empresa de créditos Palacio del Hogar,» 2017.

[18] TECNOZERO, «www.tecnozero.com/,» 14 Diciembre 2019. [En línea]. Available: https://www.tecnozero.com/firewall/cuadrante-de-gartner-para-utm-firewall-2018/. [Último acceso: 18 Abril 2020].

[19] J. Zubieta Moreno, Ciberdiccionario: Conceptos de ciberseguridad en lenguaje #Entendible, 2019.

[20] E. Ariganello, Redes CISCO. Guía de estudio para la certificación CCNA Security, Madrid : RA-MA, 2013.

[21] J. Íñigo Griera y J. M. Barceló Ordinas, Estructura de redes de computadores, Primera ed., Barcelona: UOC, 2009.

[22] M. Guerra Soto, Interconexión de Redes Privadas y Redes Publicas. (MF0956_2), Grupo Editorial RA-MA, 2016.

[23] SOPHOS, «www.sophos.com,» 2015. [En línea]. Available: Descripción general de Sophos UTM. [Último acceso: 29 Mayo 2020].

[24] A. Giannone, «Repositorio de la Universidad Tecnologica Nacional,» 2018. [En línea]. Available: https://ria.utn.edu.ar/bitstream/handle/20.500.12272/4068/Tesis%20Maestria%20GIANNONE%20Ariel%20.pdf?sequence=1&isAllowed=y. [Último acceso: 11 Marzo 2021].

[25] D. Galarza, «Repositorio Digital Escuela Politécnica Nacional,» 2020. [En línea]. Available:

https://bibdigital.epn.edu.ec/bitstream/15000/21377/1/CD%2010605.pdf. [Último acceso: 12 Marzo 2021].

[26] A. Mora, «Repositorio Institucional Universidad de Cuenca,» 2017. [En línea]. Available: http://dspace.ucuenca.edu.ec/bitstream/123456789/28552/1/Trabajo%20de%20titulaci%c3%b3n.pdf. [Último acceso: 11 Marzo 2021].

[27] M. Packer, La ciencia de la investigación cualitativa, Ediciones Uniandes-Universidad de los Andes, 2013.

[28] J. Cano, «Research Gate,» Septiembre 2015. [En línea]. Available: https://www.researchgate.net/figure/Figura-2-Calculo-del-tamano-de-la-muestra_fig2_282769507. [Último acceso: 13 Noviembre 2021].

[29] O. Corporation, «Oracle,» Oracle Corporation, 2021. [En línea]. Available: https://www.oracle.com/virtualization/virtualbox/. [Último acceso: 4 Marzo 2021].

[30] FORTINET, *FortiGate® 100D Series. Technical report,* 2017, pp. 1-6.

[31] SOPHOS, «www.sophos.com,» 2020. [En línea]. Available: https://www.sophos.com/es-es/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-brna.pdf. [Último acceso: 19 Abril 2020].

[32] MIERCOM, *Resultados de la prueba comparativa de rendimiento y límites de resistencia - Dispositivos UTM,* 2014.

[33] ENDIAN, «www.endian.com,» 2020. [En línea]. Available: https://www.endian.com/de/community/comparison/. [Último acceso: 18 Mayo 2020].

[34] «www.firewallhardware.it,» 2020. [En línea]. Available: https://www.firewallhardware.it/en/pfsense-vs-opnsense-technical-comparison/. [Último acceso: 18 Mayo 2020].

[35] NETGATE, «www.netgate.com,» 2020. [En línea]. Available: https://www.netgate.com/solutions/pfsense/features.html. [Último acceso: 22 Mayo 2020].

[36] Hewlett Packard , «Hewlett Packard Enterprise Development LP,» 2021. [En línea]. Available: https://www.hpe.com/es/es/about.html. [Último acceso: 28 Septiembre 2021].

ANEXOS

Anexo 1. Manual de buenas prácticas.

Manual de buenas prácticas

Guía de uso y aplicación para el personal administrativo y técnico de la empresa Simantec.

Elaborado por: Ing. Cristina Yacchirema
SIMANTEC

SimanTec
INTERNET sin límites...!

INDICE

1. ¿Qué son las buenas prácticas?

Se define como buenas prácticas a las pautas aconsejables que el usuario final debe seguir en el trabajo diario o al ejecutar un proceso concreto, el objetivo es resguardar la información que maneja y evitar o minimizar en lo posible el robo o pérdida de datos que son de vital importancia para una empresa. Las buenas prácticas deber ser sistematizadas de tal manera que se convierta en un proceso de retroalimentación, es decir, que se pueda aprender de las experiencias y aprendizajes para mejorar procesos anteriores.

Este manual de buenas prácticas tiene como objetivo ser una guía sobre los aspectos más básicos y fundamentales que el personal administrativo y técnico de Simantec debe conocer y considerar al momento de manejar datos sensibles de la organización. El activo más importante de una empresa son sus datos y el mayor riesgo al que están expuestos son a fallas humanas ya sean intencionales o no, es ahí en donde recae la importancia de capacitar al personal y concientizar sobre el uso adecuado de los datos empleando herramientas informáticas que ayuden a la protección, integridad, autenticidad y acceso a los mismos.

A continuación, se presenta una serie de buenas prácticas orientas a:

- Buenas prácticas ante catástrofes naturales y/o causados por el hombre.
- Buenas prácticas adaptables a la seguridad lógica y física.
- Buenas prácticas en la contratación y capacitación del personal.
- Buenas prácticas para el uso de internet.
- Buenas prácticas de seguridad en las comunicaciones.
- Buenas prácticas para la protección de datos de usuario.

Sin embargo, el primer paso es reconocer y localizar que activos se debe proteger, sin duda, los activos más importantes son datos contables, acceso a servidores y equipos a través de contraseñas que solo el personal autorizado posee.

2. Buenas prácticas ante catástrofes naturales y/o causados por el hombre

Hoy en día la mayor parte de las actividades de la empresa se desarrolla a través de un ambiente tecnológico, por lo tanto, es indispensables que esté preparada para afrontar algún evento inesperado como un desastre natural o causado por el hombre en donde la pérdida de datos sea mínima. La exposición a riesgos de la empresa es moderada razón por lo cual se debe tener un plan de recuperación en donde se plantee los posibles peligros y las políticas a seguir para asegurar la continuidad del negocio. A continuación, se expone los riesgos más comunes y recomendaciones para enfrentar cada panorama que se presente.

Tabla 1. Buenas prácticas ante catástrofes y/o causados por el hombre.

Riesgo	Recomendación
Robo	• Asegurar los equipos de la empresa. • Disponer de copias de seguridad en diferente locación para que no sufra también de robo.
Fallas humanas	• Capacitación continua a los empleados de la empresa sobre buenas prácticas de seguridad informática.
Fallas eléctricas	• Disponer de generadores de energía para no ininterrumpir el suministro eléctrico. • Conectar los equipos a un UPS. • Controlar el uso de extensiones eléctricas para evitar sobrecargas que causen cortocircuitos.
Terremotos	• Tener respaldos de la información en un lugar diferente al que ocurrió el evento adverso. • En lo posible tener asegurado los equipos ante desastres naturales.
Agua	• No ubicar los equipos cerca de fuentes de agua. • No ubicar los equipos al nivel del piso si existe riego de inundación. • Cerrar puertas y ventanas cuando exista presencia de lluvia. • Proteger las instalaciones eléctricas.

Riesgo	Recomendación
Fuego	• No ubicar los equipos informáticos como computadores, servidores o impresoras cerca de áreas inflamables. • Las paredes, pisos y techos deben ser construidos de materiales incombustibles y resistentes al fuego. • Las zonas cercanas al cuarto de equipos deben ser libre de humo con prohibición de fumar.

Elaborador por: Autor.

Fuente: [1]

3. Buenas prácticas adaptables la seguridad lógica y física

3.1. Seguridad Lógica

El activo más importante que tiene una empresa es la información por esta razón se debe implantar técnicas que van a más allá de la seguridad física, entonces se habla de una seguridad lógica. La seguridad lógica consiste en implementar barreras y procedimientos que resguarden el acceso a datos y permita el acceso solo al personal autorizado. Este tipo de seguridad se basa en la efectiva administración de permisos y control de acceso a los recursos informáticos a través de la identificación, autenticación y autorización. A continuación, se expone recomendaciones de seguridad a seguir:

3.1.1. Copias de seguridad

Las copias de seguridad son información de un sistema informático obtenidas con el fin de recuperar información robada, borrada, alterada, inaccesible por el fallo del sistema o porque sufrió algún otro daño. Hacer copias de seguridad es una tarea importante que se debe planificar y hacer periódicamente para resguardar los datos de la empresa. A continuación, se expone algunos consejos al momento de hacer copas de seguridad [2].

- Para evitar que el administrador olvide sacar respaldos de la información se aconseja automatizar la tarea de hacer copias de seguridad.
- En lo posible las copias de seguridad se deben almacenar en un lugar diferente de donde se encuentran los sistemas informáticos para evitar que sufran el mismo daño.
- Si la cantidad de información a respaldar es moderada es aconsejable hacer una copia completa, pero si la cantidad es muy alta es mejor realizar copias diferenciales o incrementales.
- Al momento de hacer copias de seguridad lo ideal es comprimir la copia para ocupar menos espacio de memoria.
- Las copias que ya no se utilicen deben ser borradas para que no puedan ser utilizadas y no ocupen memoria en el dispositivo o fichero de almacenamiento.
- Finalmente, otro aspecto a considerar es, qué información se debe guardar. La información de cada usuario es importante, pero se debe seleccionar los datos que

se van a respaldar en carpetas identificando el usuario para llevar un mejor control.

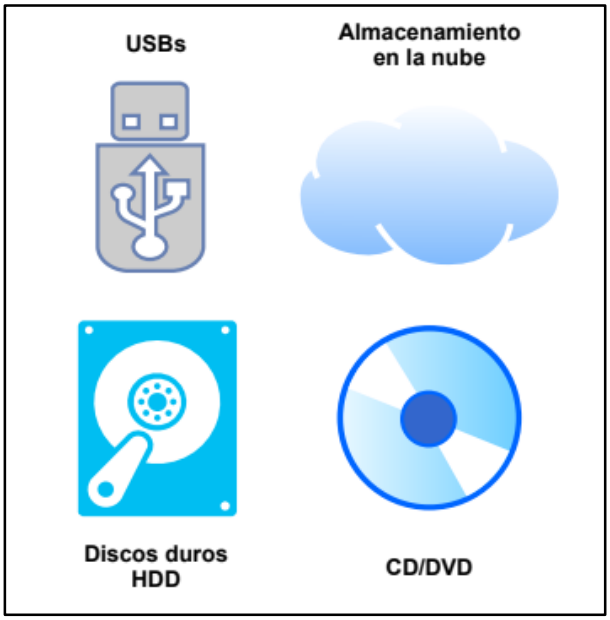


Figura 1. Soportes para realizar copias de seguridad.
Elaborado por: Autor.

3.1.2. Contraseñas

Las contraseñas son claves que se usan para acceder a información almacenada en un equipo, servidor, carpetas o acceder a aplicaciones como mail, redes sociales etc. Para que una contraseña sea segura se recomienda [3]:

- Una longitud mínima de 8 caracteres, pero lo ideal es 14 caracteres o más.
- Combinación de caracteres entre minúsculas, mayúsculas números y símbolos especiales, mientras más diversa sea la combinación más fuerte será la contraseña.
- No generar una contraseña con caracteres repetidos o su secuencia ejemplo: “12345678”, “22222222”, “abcdefg”.
- No emplear un nombre como inicio de sesión.
- No emplear la misma contraseña para varios entornos.
- No emplear la opción de contraseña en blanco.
- Cambiar regularmente las contraseñas.
- Evitar revelar las contraseñas a terceras personas.

- No escribir la contraseña en notas y dejar en la pantalla del monitor dejando a la vista del resto de personal.

3.1.3. Permisos de usuario

La creación de usuario, contraseña y asignación de determinado perfil con ciertos privilegios es una tarea fundamental que el administrador de redes debe realizar y conlleva 4 pasos:

- **Definir el puesto:** Consiste en otorgar los permisos mínimos requeridos para que el empleado desempeñe su función dentro de la organización.
- **Determinar la sensibilidad del puesto:** Determinar si el cargo del empleado implica permisos críticos con los cuales pueda acceder o alterar información confidencial.
- **Elegir el personal para cada puesto:** Consiste en escoger a la persona idónea con experiencia y conocimiento para el cargo encomendado.
- **Formación inicial y continua de usuarios:** Poner en conocimiento al personal nuevo las políticas de seguridad informática de la organización además de seguir reforzar y concientizando la importancia de proteger los recursos informáticos en los demás empleados.

Tabla 2. Perfiles de usuarios.

	Perfiles de usuario					
	Gerencia Administrativa	**Gerencia Técnica**	**Área técnica**	**RRHH**	**Bodega**	**Contabilidad**
Correo electrónico	✗	✓	✓	✗	✗	✗
Nómina	✓	✗	✗	✓	✗	✗
Facturación	✓	✗	✗	✗	✗	✓
Página web	✗	✓	✓	✗	✗	✗
Servidores	✗	✓	✓	✗	✗	✗
Stock de material	✓	✗	✗	✗	✓	✗

Elaborado por: Autor.

3.1.4. Cifrado de datos y comunicaciones

Los datos que están almacenados en dispositivos deben ser protegidos ante robos, manipulación, adulteración o la intersección de personas con malas intenciones, un método que permite la protección de datos es el cifrado de dispositivos. A continuación, se presenta como cifrar los siguientes dispositivos [4]:

- **Cifrado de memorias USB:** Se puede emplear el algoritmo AES para cifrar la contraseña de acceso al dispositivo e instalar utilidades para acceder a la memoria usando las claves cifradas.
- **Cifrado de discos duros externos:** Se puede cifrar solo las particiones o todo el disco duro y de la misma manera se debe instalar una aplicación para abrir el disco en otros equipos.
- **Cifrado de todo el equipo:** Al cifrar todo el equipo se incluye sistema operativo y todas las particiones. La información cifrada se almacena en otro dispositivo de almacenamiento que posteriormente se usará para realizar el proceso de descifrado.

El cifrado de cualquier dispositivo de almacenamiento impide que una persona no autorizada acceda a los datos, pero olvidar la clave implica que el usuario autorizado de ninguna manera tendrá acceso a los datos.

3.1.5. Software específico antimalware y antivirus

En [5] menciona que los programas antivirus tienen como objetivo la prevención e intentan evitar que un ordenador se infecte de virus, si de algún modo el computador está infectado intenta evitar que el virus se active. Por otro lado, un antimalware se emplea para extraer el malware de un equipo infectado en el caso de haya pasado por inadvertido en el escaneo del antivirus. Para eliminar un malware por completo es necesario varias comprobaciones de ubicación y técnicas de análisis antivirus.

En el mercado existen algunos programas gratuitos y de pago para eliminar malware como: Windows Defender, BullGuard, ESET, Panda, Bitdefender, Norton, etc.

Figura 2. Antivirus en el mercado.
Elaborado por: Autor.

Recomendaciones para evitar que un computador se infecte de virus.

- Utilizar un software de protección antivirus en el computador.
- Descargar programas o aplicaciones en sitios web de confianza.
- No hacer clic en enlaces de duda procedencia incluido enlaces de correos electrónicos, mensajes spam o páginas web, ya que al hacer clic automáticamente se descarga el malware afectando posteriormente al equipo.
- Mantener el sistema operativo del computador actualizado.
- No introducir memorias USB desconocidas en el computador.

Figura 3. Recomendaciones para evitar virus informáticos.
Elaborado por: Autor.

Recomendaciones si el equipo está infectado.

- Ejecutar el antivirus instalado en el computador.
- Una vez detectado el malware proceda a elimina el archivo o póngalo en cuarentena.
- Reiniciar el computador.
- Cambiar la contraseña del equipo.
- Actualizar el software, navegador y sistema operativo.
- Analizar nuevamente el equipo para comprobar si no existen más amenazas.

El ransomware se ha convertido en una ciberamenaza muy común y consiste en cifrar los archivos de un equipo en segundo plano sin que el usuario se dé cuenta, una vez que infecta todo el equipo envía un mensaje al usuario para que pueda recuperar la información a través de un rescate. En la mayoría de las situaciones y pese a pagar el rescate la información nunca es recuperada, bajo este contexto se expone algunas recomendaciones para evitar caer en esta situación.

- Hacer copias de seguridad periódicamente ya sea en la nube como Dropbox, Google Drive, etc. y en un ligar físico como discos duros, memorias USB, etc.
- Verificar que las copias de seguridad estén funcionales.
- No abrir archivos adjuntos de remitentes desconocidos ya que puede contener virus.
- Activar la opción *mostrar extensiones de archivos* (para Windows) con la finalidad de mantenerse alejado de extensiones como "exe", "vbs" y "scr". Los programas con este tipo de extensión pueden contener archivos maliciosos.
- Actualizar el sistema operativo, navegador, antivirus y otros programas así se tendrá las últimas versiones de los programas con mejores características y errores corregidos en cuanto a vulnerabilidades.
- Utilizar un antivirus fuerte que proteja el equipo del ransomware.
- Si se observa algún evento sospecho en un equipo se debe desconectar inmediatamente de Internet para evitar en lo posible el cifrado de todos los archivos.
- Si la máquina ha sido infectada es recomendable no pagar el rescate y contarse con un experto en ciberseguridad porque existe la posibilidad de restaurar los archivos cifrados.

3.2. Seguridad Física

La seguridad física consiste en aplicar barreras físicas y procesos de control como medidas de prevención ante amenazas a los activos de una empresa, la seguridad física muchas veces ha sido un aspecto poco considerado al momento del diseño de un sistema informático; sin embargo, los servidores, computadores, software o copias de seguridad

son elementos que están expuestos a robos, actos delictivos, sabotajes o destrozo por personas ajenas o propias a la empresa. A continuación, se presenta los posibles riesgos y soluciones para cada caso [1].

Tabla 3. Seguridad física.

Riesgo	Solución
Robo de equipos informativos.	• Uso de credenciales de identificación para controlar el ingreso y salida del personal en la empresa. • Uso de credenciales para la apertura o cerramiento de puertas. • Instalación de cámaras de vigilancia para el seguimiento si fuera necesario. • Disponer de armario o rack bajo llave. • Llevar un registro de visitantes. • Mantener un inventario de los equipos computacionales y tecnológicos de la empresa. • Contrar el ingreso y salida de los equipos de la empresa, donde conste responsables, destino y quien autoriza.
Robo de software o información almacenada en memorias USB o CD.	• Guardar información sensible como discos duros, memorias USB, CD bajo llave. • Retirar puertos USB y quemadores de CD.

Elaborado por: Autor.

4. Buenas prácticas en la contratación y desvinculación del personal en la empresa

Uno de los principales problemas de la seguridad informática es el factor humano, a diferencia de una máquina, las personas tienen la facultad de decidir *romper* las reglas de seguridad. Una organización puede tener el mejor sistema de seguridad, pero si un solo empleado incumple las normas establecidas puede abrir la puerta para que un ciberdelincuente robe la información [1].

Contratación de personal: Cuando en la empresa se contrate nuevo personal es recomendable firmar un acuerdo de confidencialidad especialmente si van a manejar información sensible de la organización, además es indispensable definir el perfil de usuario que va a tener y así otorgar solo los permisos y privilegios necesarios. En cuanto a la capacitación es necesario informar cuales son las responsabilidades y obligaciones en cuestión de seguridad de los datos que va a manejar dentro de la empresa.

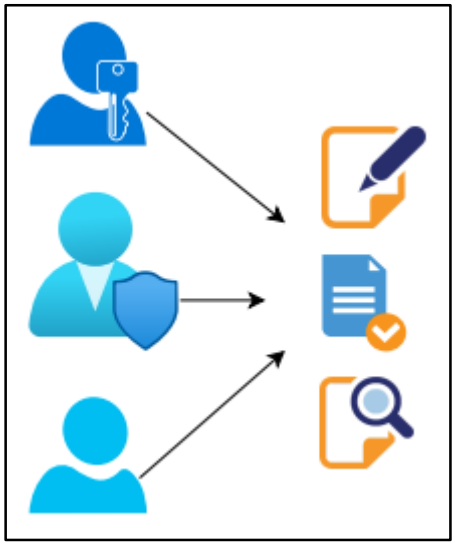


Figura 4. Permisos y privilegios por usuario.
Elaborado por: Autor.

Desvinculación de personal: Cuando un empleado se desvincula de la empresa es necesario dar de baja todas sus cuentas de usuario para invalidar permisos y privilegios asignados, también se debe hacer la devolución de equipos y otros dispositivos que estén a su cargo.

A continuación, se lista una serie de recomendaciones para el administrador de sistemas de la empresa:

- Dar a conocer a los usuarios desde que lugar y equipos pueden ingresar al sistema informático de la empresa, así como el nivel de acceso permitido, recursos, aplicaciones y operaciones al que tienen acceso.
- Impartir a los usuarios formación continua en cuanto al sistema informático de la empresa incluido cambios o mejoras y seguridad informática.
- Informar y preparar de forma adecuada al nuevo personal especialmente si va a trabajar en áreas con información sensible o aplicaciones significativas para el funcionamiento de la empresa.
- Otorgar en lo posible equipo nuevo al personal para conocer el uso que da a los equipos de la empresa.
- Proporcionar una nueva cuenta de correo corporativo para filtrar y controlar la información que comparte. Para poder auditar el correo electrónico se debe colocar una cláusula en el contrato de empleo.
- Notificar a los empleados que el uso del Internet está orientado solo a fines laborales.
- Informar al personal que solo debe emplear herramientas corporativas, la instalación de software adicional debe ser previamente autorizado.

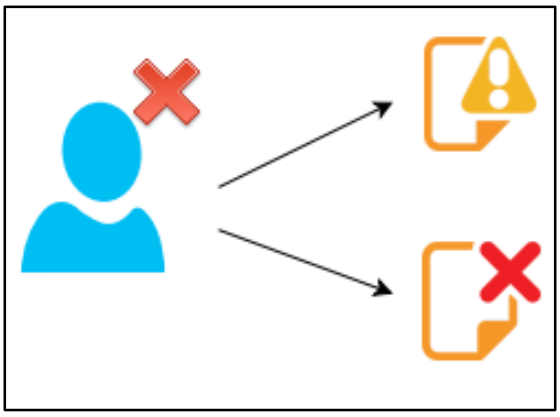


Figura 5. Denegación de permisos y privilegios.
Elaborado por: Autor.

5. Buenas prácticas para el uso de internet

Las herramientas de seguridad en cuanto al buen uso del internet en la empresa ayudan a mejorar la productividad de los empleados, descongestiona el ancho de banda y reduce el uso de memoria, limita la entrada de virus y minimiza el robo de información confidencial. Algunos consejos para que el internet tenga un buen uso dentro de la empresa son [6]:

- Limitar el acceso a redes sociales dentro de las horas de trabajo, según estudios realizados, el uso en horas laborables reduce la productividad y concentración de los empleados.
- Difundir que el acceso a los servicios de Internet y correo electrónico deben ser exclusivamente para actividades laborales.
- Restringir el acceso a ciertas páginas web como pornografía o con contenido ilícito o perjudicial para la empresa.
- Restringir el acceso a sitios e entretenimiento, videos, música, fotografías o correo electrónico personal.
- Consentir el ingreso a sitios de soporte técnico, aliados comerciales, entidades bancarias, páginas web del estado, sitio web del cliente.

Figura 6. Buen uso del internet.
Elaborado por: Autor.

5.1. Medidas de seguridad para el correo electrónico

El correcto uso del correo electrónico puede evitar la entrada de código malicioso en el computador además de impulsa el respeto a la privacidad de otras personas. Entre las buenas prácticas del uso de correo electrónico se tiene:

- **Prudencia antes de abrir archivos adjuntos:** Al recibir un correo con archivos adjuntos es conveniente configurar el correo para que el antivirus instalado analice los mensajes, sino se puede descargar y guardar el archivo el adjunto sin abrirlo para analizarlo con el antivirus. Aunque el emisor del correo sea conocido una foto, documento de texto o cualquier archivo puede contener código malicioso que infecte el ordenador.

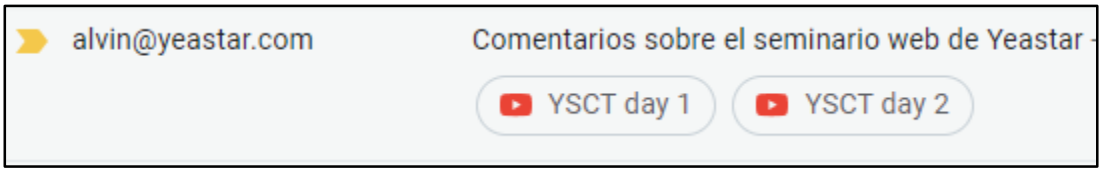


Figura 7. Archivos adjuntos en correos.
Elaborado por: Autor.

- **Usar la copia de seguridad para envíos o reenvíos masivos:** Los destinatarios del correo electrónico reciben una copia del correo, pero no visualizarán las otras direcciones de mail a las que ha sido enviado.

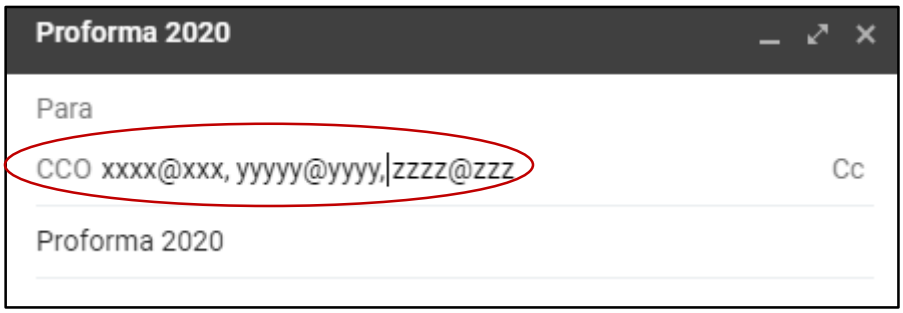


Figura 8. Copias de seguridad ante envíos masivos.
Elaborado por: Autor.

- **Borrar la lista de correos electrónicos antes de reenviarlo:** Si se reenvía un correo sin hacer el proceso anterior el remitente tendrá acceso a la lista de e-mails que también fueron destinarios de dicho correo.

- **Romper con las cadenas de correo hoax:** La finalidad de estos e-mails es acaparar direcciones electrónicas y saturar el tráfico en la red.

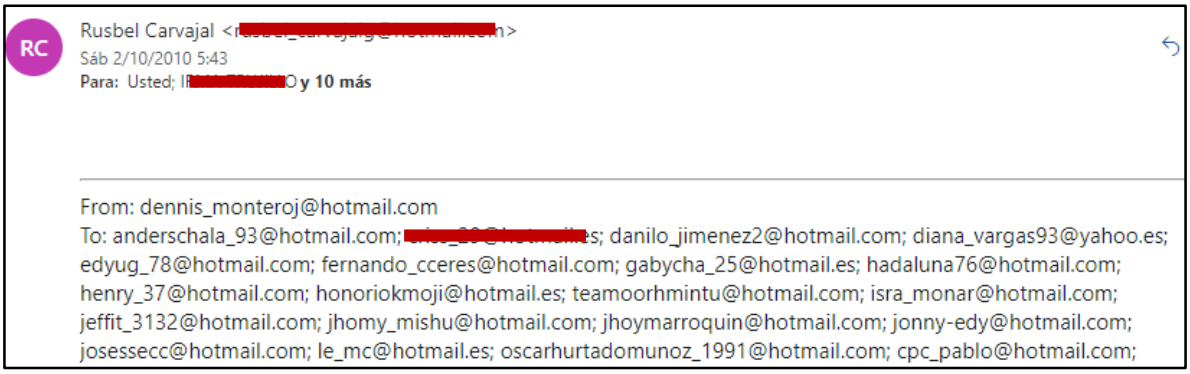


Figura 9. Cadenas de correo hoax.
Elaborado por: Autor.

- **No hacer clic en enlaces que aparezcan en un correo electrónico:** A no ser que sea de entera confianza puesto que puede ser una página web falsa para captar datos personales.
- **Denunciar el correo fraudulento:** Este proceso se puede realizar al propio ISP contratado o al titular del servicio de correo de dónde provino el mensaje.

6. Recomendaciones de seguridad

- Informar novedades y alertas de seguridad.
- Actualizar el equipo tanto sistema operativo, aplicaciones y antivirus puesto que la base de datos de malware se actualiza en base al nuevo malware conocido.
- Realizar copias de seguridad periódicamente, además deben ser guardadas en un lugar seguro para evitar la pérdida de información.
- Emplear software licenciado ya que proporciona garantía y soporte técnico.
- Utilizar contraseñas fuertes en todos los usuarios, aplicaciones y demás accesos para obstaculizar la suplantación de identidad.
- Realizar cronogramas de mantenimiento de los equipos para evitar su pronto deterioro.
- Bloquear sesiones de usuario cuando el empleado no este activo.
- Colocar contraseñas a los archivos o documentos que contienen información relevante para la empresa.

7. Referencias

[1] M. Rodriguez y C. John, «Universida Distrital Francisco José de Caldas,» 2001. [En línea]. Available: https://revistas.udistrital.edu.co/index.php/visele/article/view/3884. [Último acceso: 4 Octubre 2020].

[2] A. García y M. d. P. Alegre, Seguridad Informática, Madrid: Paraninfo, SA, 2011.

[3] J. Costas, Seguridad y Alta Disponibilidad, Ra-Ma, 2011.

[4] A. Palacios, Seguridad Informática, Madrid: Paraningo, 2020.

[5] Kaspersky, «Kaspersky,» Kaspersky, 2021. [En línea]. Available: https://latam.kaspersky.com/resource-center/preemptive-safety/malware-remover-vs-antivirus-software. [Último acceso: 21 Agosto 2020].

[6] S. Lourdes, G. Alma y F. Álvarez, «ResearchGate: El Impacto de las Redes Sociales en la Productividad de las Empresas.,» Enero 2016. [En línea]. Available: https://www.researchgate.net/publication/303444972_El_Impacto_de_las_Redes_Sociales_en_la_Productividad_de_las_Empresas. [Último acceso: 1 Septiembre 2020].