UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

INTEGRACIÓN DE SOLUCIONES DE CIBERSEGURIDAD EN SOFTWARE LIBRE COMO ALTERNATIVA ACCESIBLE PARA PYMES

AUTORES:

CRISTIAN BOLÍVAR BACUILIMA PULLA
WILLIAN ALFONSO PADILLA PINEDA

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2023

Autores:

Cristian Bolívar Bacuilima Pulla
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
cbaculima@ups.edu.ec

Willian Alfonso Padilla Pineda
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
wilypadilla@gmail.com

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de sistemas.
Máster en Redes de Comunicaciones.
jdominguez@ups.edu.ec

DEDICATORIA

“A mi Querida Esposa”

Ing. Cristian Bacuilima

DEDICATORIA

A Dios por darme la oportunidad de seguir mis objetivos y a mi familia por su apoyo constante, especialmente a mi esposa e hijo por ser el pilar fundamental en cualquier paso que doy.

Ing. Willian Padilla

AGRADECIMIENTO

"A Dios por sobre todas las cosas, a mi Esposa por su apoyo a mi familia a mi tutor de este proyecto"

Ing. Cristian Bacuilima

AGRADECIMIENTO

Agradezco principalmente a Dios por todo lo brindado, y a mi esposa Marcela por su apoyo durante todo este proceso, y de igual manera a mi hijo Gabriel por ser quienes me motivan a cumplir metas y seguir adelante.

Un agradecimiento especial a nuestro director de proyecto de graduación el Ing. Juan Carlos Domínguez, por su apoyo constante.

Ing. Willian Padilla

1. Tabla de contenido

Integración de soluciones de ciberseguridad en software libre como alternativa accesible para pymes

Autores:

CRISTIAN BOLIVAR BACUILIMA PULLA
WILLIAN ALFONSO PADILLA PINEDA

Resumen

El presente documento presenta una solución viable para la ciberseguridad de las pequeñas y medianas empresas, Pymes, utilizando herramientas de libre distribución, facilitando el acceso a este grupo de empresas que no cuenta con altos presupuestos para la inversión en infraestructura tecnológica.

La seguridad informática cada vez toma más importancia en el mundo de los negocios, empresas grandes, pequeñas, deben tener presente de los beneficios y riesgos de tener o no un plan de seguridad para casos de ser víctimas de un ataque cibernético. Por varias razones y una de las principales, la pandemia, obligaron a muchas empresas a migrar sus negocios a tiendas virtuales, existiendo un crecimiento del uso del Internet y consecuentemente mayor cantidad de vulnerabilidades donde la seguridad se vuelve imprescindible, y donde una solución basada en software libre con costos de inversión bajos es la alternativa idónea para las Pymes.

Es la propuesta que se brinda en el presente proyecto con el objetivo de dar seguridad a empresas pequeñas utilizando software libre como PFsense el cual actúa como escudo protector ante las amenazas externas e internas, levantando y configurando los servicios de Firewall, control de contenido, proxy, IDP IPS y control de ancho de banda.

Palabras Claves

Seguridad informática, plan de seguridad, ataque cibernético, tiendas virtuales, software libre, PFsense.

ABSTRACT

This document presents a viable solution for the cybersecurity of small and medium-sized companies, SMEs, using free distribution tools, facilitating their access to this large group of companies that don´t have high budgets for investment in technological infrastructure.

Computer security is becoming increasingly important in the business world, large and small companies must be aware of the benefits and risks of having or not having a security plan in case of being victims of a cyber-attack. For various reasons and one of the main ones, the pandemic, forced many companies to migrate their businesses to virtual stores, with a growth in the use of the Internet and consequently a greater number of vulnerabilities where security becomes essential, and where a solution based on free software with low investment costs is the ideal alternative for SMEs.

This is the proposal that is provided in this project with the aim of providing security to small companies using free software such as PFsense that acts as a protective shield against external and internal threats, raising and configuring Firewall services, content control, proxy, IDP IPS and bandwidth control.

Keywords

Computer security, security plan, cyber-attack, virtual stores, free Software, PFsense.

2. Introducción

La masificación del uso de internet ha llevado a las empresas a innovar su infraestructura tecnológica esto está pasando con las grandes corporaciones que están migrando a la nube o implementando propia infraestructura para brindar seguridad a sus clientes al momento de realizar compras por medio virtuales y demás beneficios que brinda la tecnología.

Las empresas pequeñas y medianas no están aisladas de este suceso y no deberían dejar pasar las oportunidades de involucrarse en el mundo de la tecnología. Es por ello por lo que la implementación de una solución de seguridad en software libre es la mejor alternativa para poder mitigar los problemas relacionados a ataques, intrusos, virus, control de navegación, esto será configurado e implementado usando PFsense como soluciones de Ciberseguridad.

Con esta solución el objetivo principal es proteger a las pequeñas empresas de los riesgos informáticos comunes, y consecuentemente brindar seguridad a los usuarios internos de cada empresa. Esto con un costo mínimo de implementación accesible al presupuesto de las Pymes.

Según el sitio web de la ISO, www.iso.org, Ecuador es uno de los países con los índices más bajos de certificaciones de seguridad en América Latina, es por ello por lo que los atacantes han visto en el país una gran oportunidad para buscar vulnerabilidades y atacarlas. (iso.org, 2021)

Últimamente han existido ataques hacia grandes instituciones como CNT, ANT, Banco Pichincha, todos estos casos de dominio público. A todo esto, se suma que existe poca legislación ante los ciberataques y no existen castigos claros y firmes por las leyes estatales, dejando un incentivo adicional para el atacante.

3. Determinación del Problema

Es de conocimiento mundial que las Tecnologías de la Información en la actualidad son el motor de muchas actividades y servicios en los diferentes campos: la educación, salud, gubernamental, empresarial, brinda acceso a múltiples servicios y facilidades para actividades profesionales, laborales o simplemente pasa tiempos.

Uno de los campos más amplios y donde más ha causado beneficios la tecnología es en el ámbito empresarial, las empresas para obtener crecimiento y surgir en un mercado competitivo deben actuar a la par con el desarrollo tecnológico o serán destinados a su desaparición o estancamiento empresarial.

Las empresas que tiene mayor posición competitiva en el mundo y consecuentemente obtienen recursos suficientes para invertir en áreas necesarias para mantener una buena posición, seguridad y desarrollo de su organización, no tienen mayor problema para cumplirlo, ya que tienen la capacidad de planificar y asignar grandes presupuestos a una parte fundamental como lo es la infraestructura tecnológica que busca la seguridad de la información de la empresa, conociendo la importancia que exige este aspecto. Es satisfactorio conocer que empresas que tiene capacidad de invertir en seguridad tecnológica para su protección lo ejecuten, sin embargo, es lamentable saber que empresas que tiene la posibilidad de implementar infraestructura para su seguridad y no lo hacen por desconocimiento de la importancia de la seguridad de la información de su empresa.

Desde otra perspectiva se observan empresas pequeñas y medianas que no tienen la liquides o ingresos necesarios para darse el “lujo” de adquirir infraestructura tecnológica para cubrir y proteger la seguridad informática de su empresa, exponiendo y dejando expuesta la seguridad local.

De cierta manera es justificable la decisión de que toma la parte directiva de las PYMES al no planificar y asignar un presupuesto fijo para la inversión en seguridad, por la alta inversión que esto requiere, hoy en día la infraestructura

necesaria para obtener un nivel satisfactorio de seguridad tiene costos demasiado altos para la gran mayoría de las PYMES, dejando con un alto riesgo a un grupo bastante representativo en el país y el mundo.

Es decir, el factor principal que afecta la seguridad informática en las PYMES es el económico, por lo que una alternativa que no tenga un alto costo se convertiría en una solución viable y accesible para cualquier pequeña y mediana empresa.

4. Marco teórico referencial

En el siglo XXI fue cuando despegó la importancia y dependencia de las tecnologías de la información de los gobiernos, fuerzas armadas, empresas privadas e individuos, lo cual permitía desarrollar tareas y servicios de una manera más práctica, sin embargo, esto también ponían en riesgo la información en cada uno de los campos mencionados anteriormente, todo esto invita al crecimiento potencial del campo de la seguridad para combatir o reducir las vulnerabilidades en cada área y poder seguir haciendo uso de la tecnología garantizando la protección de la información y el intercambio de la misma, por lo tanto el ciberespacio se ha convertido en un campo de batalla donde existe la constante competencia por mejorar las técnica de protección y la contraparte mejorar técnicas de ataque para encontrar nuevas vulnerabilidades. (Garcia, 2019)

CIBERSEGURIDAD

La ciberseguridad es la que se dedica a la protección eficaz de todo dato o información que se almacena en lo intangible del ciberespacio. (Garcia, 2019)

La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.

La ciberseguridad se dedica a la protección eficaz de todo dato o información que se almacenan en lo intangible del ciberespacio. (Garcia, 2019)

La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad

de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.

Teorías explicativas sobre ciberseguridad

Ataques

El ser humano siempre se ha valido del espionaje para muchos de sus intereses, conocer las actividades del otro se ha considerado como una ventaja para adelantar los siguientes pasos en beneficio propio, en tiempos de guerra este concepto se aplicaba con más insistencia, ya que se intentaba conocer las estrategias del enemigo para disuadirlas o atacar primero, por todo esto y debido a que hoy en día las tecnologías de la información están presentes en todo sentido, en muchas actividades cotidianas a nivel mundial. El avance del Internet se ha convertido en una gran red que brinda varios beneficios, sin embargo, al existir demasiadas personas conectadas entre sí, también se incrementa la superficie con vulnerabilidades a los ataques o espionajes y paralelamente evolucionan los métodos de defensa o protección de la información. Considerando los beneficios presentados en las tecnologías de la información sus funcionalidades se desplazan hacia diferentes empresas, entidades privadas y públicas, de tal modo que las instancias gubernamentales de los países de todo el mundo no se escapan de la mira de los atacantes informáticos, inclusive al ser entidades que contienen información crítica de los gobiernos se convierten en un objetivo muy apetecido por los ciberdelincuentes, al tener un mayor nivel de impacto al ser puntos vitales en un país, considerando aquellas que hacen funcionar infraestructuras y servicios esenciales. Entre las infraestructuras vitales de un país se encuentran los medios de telecomunicaciones, hoy en día fundamentales para trabajo, estudio, maquinarias, las redes de repartición de servicios básicos, los servicios de salud y emergencia, medios de transporte, los servicios gubernamentales y las Fuerzas Armadas que manejan información confidencial. (Puime Maroto, 2009)

Por la información que hay que proteger hoy en día y por las vulnerabilidades existentes al estar conectados en una red de millones de personas con buenas y malas intenciones, existe un gran riesgo al brindar o usar un servicio en la red, los atacantes siembren estarán buscando nuevas formas de atacar y vulnerar los principios de la información: confidencialidad, integridad y disponibilidad, ya sea para sacar beneficio económico o reconocimiento profesional.

Ingeniería Social

Se considera como un "arte" del engaño, ya que se refiere a toda acción mediante la cual se manipula a personas para evitar sistemas de seguridad, y obtener información de los usuarios por diferentes medios de comunicación o directamente, para obtener acceso a un sistema o netamente obtener información con diferentes objetivos. (Rodríguez Rincón, 2018)

En la actualidad se habla mucho sobre el hackeo de sistemas, de equipos, etc. así mismo se puede decir que la ingeniería social es el arte de hackear a la persona, es decir el ataque va netamente dirigido hacia quien es considerado como el eslabón más débil de la seguridad de una organización. La ingeniería social no es una técnica definida, la metodología de ataque depende de la creatividad e ingenio del atacante, aprovechando cualidades humanas como: la curiosidad, la atracción, el miedo o la empatía. (Camacho Nieto, 2016)

Phishing

Es un método de engaño mediante el cual se obtiene credenciales o información importante de la víctima, comúnmente se lo realiza mediante un correo electrónico, sin embargo, en la actualidad también se envía el ataque mediante mensajes de texto, redes sociales, etc., es uno de los métodos más utilizados en el mundo entero y uno de los más eficientes.

Ransomware

Software malicioso que se apodera de un sistema o de sus datos, y exige al usuario un pago de rescate para su liberación, uno de los métodos de ataque que ha tenido gran crecimiento en los últimos años, su metodología consiste en cifrar archivos con clave la misma que será entregada con el pago de la víctima (Trigo, y otros, 2017)

Desde el punto de vista legal, la modalidad delictiva del ransomware puede encuadrarse dentro del tipo penal básico de la extorsión, delito que según el COIP del Ecuador se castiga con una pena privativa de 5 a 7 años considerando ciertas circunstancias en el caso.

HERRAMIENTAS DE SEGURIDAD

FIREWALL

Uno de los elementos más conocidos o nombrados cuando se habla de seguridad informática en una organización es el FIREWALL o Cortafuegos en español, es un elemento de hardware o software ubicado entre la red interna de la organización o red local y la red externa o Internet, de tal manera que se controla y protege los accesos no autorizados desde el exterior hacia la red interna que puede traer propósitos dañinos para la organización y su información.

RESTRICCIONES EN FIREWALL

El objetivo principal del Firewall es permitir o bloquear ciertos servicios, los mismos que se configuran según las necesidades de los distintos usuarios y su ubicación:

- Usuarios locales con acceso a servicios restringidos externos: en este estado se permite agregar una configuración con direcciones validadas a la que se tendrá acceso, es decir solo tendrán acceso a los servicios externos definidos.

- Usuarios externos con permiso de acceso desde el exterior: este es el estado más crítico a monitorear, comúnmente se trata de usuarios externos que deben

tener acceso a la red local para desempeñar funciones fijas o temporales, por lo que se recomienda respetar los tiempos establecidos que durarán los accesos (Callegari, 2008).

Existen casos donde temporalmente un usuario interno se encuentra en otra ubicación física, ciudad o país, pero de igual manera debe seguir cumpliendo sus tareas con accesos a sistemas e información localizada en la red interna de la organización.

ANTIVIRUS

Un virus es un software informático malicioso que contiene una secuencia de código malicioso en algún tipo de lenguaje de programación, creado intencionalmente con el objetivo de: robar información, bloquear la red, dañar equipos, bromas, que se adhieren a un equipo informático sin el consentimiento del usuario (Arantón Areosa, 2008).

Existen diferentes tipos de virus entre los cuales podemos mencionar los siguientes:

Troyanos, se trata de una aplicación disfrazada que contine internamente un código malicioso que se ejecuta cuando el usuario abra el archivo y lo ejecute, y de este modo conseguir acceso remoto mediante accesos encontrados y vulnerados, recopilar o eliminar información. Los gusanos, son programas camuflados en correos electrónicos que se replican y reenvían automáticamente según la agenda existente del usuario y también existen los virus comunes que se ocultan en archivos ejecutables con el objetivo de dañar archivos del equipo o al equipo, o lanzar bromas que causan molestias, comúnmente es sencilla su eliminación (Arantón Areosa, 2008).

Un antivirus es un software que nos permite combatir este tipo de amenazas, de igual manera existen en el mercado muchos de licencia pagada y libre, es un programa que contiene opciones como monitoreo automático o manual de archivos sospechosos, cada uno tiene una nube de información donde

almacenan la base de datos de amenazas registradas, por esto es importante siempre mantener actualizados la base de datos de virus del antivirus.

GESTIÓN DE ANCHO DE BANDA

Es necesario una gestión de ancho de banda dentro de una organización, ya que mediante un análisis de estadísticas se puede concluir donde se consume mayor ancho de banda y donde menos, según estos resultados se pueden tomar decisiones a futuro, aplicando modificaciones, control de ancho de banda para no provocar lentitud por saturación de ciertos servicios

SOFTWARE LIBRE

Cuando se adquiere un software privativo, un Microsoft Office por ejemplo (no-libre) Microsoft vende el código máquina que es un código de ceros y unos (1000010111). Al contrario, cuando se usa software libre, se dispone también del código fuente en el que está escrito el programa, es por este motivo que se dice que el programa es de código abierto, se tiene acceso a su código y con los conocimientos necesarios se puede modificar el mismo para corregir errores o añadir nuevas funcionalidades y de esta manera ayudar o contribuir a toda una comunidad.

Figura 1-Beneficios Software Libre.

Es por este motivo básico de contribución que ha hecho al Software Libre, robusto y confiable porque los errores y cambios se hacen mucho más rápido que en un software privativo, es por este motivo y lo gratuito que se ha difundido y utilizado. Las soluciones de ciberseguridad no son la excepción en una pequeña empresa no importa si es software libre o no lo que más importa es el Precio que exigirá a la empresa acoplado a su realidad.

Tipos de software libre

Existe gran variedad de Software Libre que puede ser utilizado con cualquier objetivo, dependiendo la necesidad del usuario y que se adapten a ella:

- Linux Sistema Operativos.
    - Centos.
    - RedHat.
    - Alma Linux.
    - Ubuntu.
    - Fedora.
    - Debian.
    - Kali Linux.
- Utilitarios como Ares y Mozilla Firefox.
- Open Office, se trata de un análogo a los programas de Microsoft Office.
- Gimp como editor de imágenes.
- VLC o reproductor multimedia.
- jQuery se trata de una librería que facilita la programación el lenguaje JavaScript.

Esta idea de Software libre cada vez toma más adeptos dada la dinámica del mercado, lo económico, lo social, lo cultural. Ya que mucho de ello es producto de la capacidad intelectual de cada individuo que decidió contribuir con mejorar cada vez más este tipo de software de manera voluntaria y gratuita.

Es por ello por lo que esta forma de contribución a calado en la transferencia de conocimiento en disciplinas como biotecnología, genética contribuyendo en el desarrollo de economías emergentes como la nuestra apoyando así en el tema social y económico.

TIPOS DE LICENCIAMIENTO

En cuanto a los licenciamientos podemos decir que existe varias formas de licenciamiento libre que permite acceso, modificación y redistribución que serán descrita a breves rasgos.

- Licencia BSD (Berkely Software Distribution).
- Licencia GNU GPL (Licencia publica General de GNU).
- Licencia GNU LGPL (Licencia Publica General Menor de GNU).
- Licencia de Copyleft.
- Licencias Creative Commons.

Licencias BSD. - no restringe el acceso al código fuente contempla la redistribución y las modificaciones en otras palabras un acceso Total.

Licencias GNU GPL. - Es la más común y utilizado en el software libre, originalmente usada por la FSF (Free Software Fundación) de Richard Stallman en el proyecto GNU que crearon Linux, un sistema operativo totalmente libre creado en base a UNIX.

Licencias GNU LGPL. - Básicamente es menos restrictiva permitiendo la integración de cualquier otro software sin limitaciones.

Licencias Copyleft. - La antítesis del Copyright que básicamente define las licencias de Propietario tenemos las licencias Copyleft transformando los derechos de los propietarios en libertades permitiendo así la modificación y redistribución del código. Aplicando a la documentación de carácter Técnico o didáctico del software libre.

Licencias Creative Commons. - Aplicable básicamente a herramientas de software

Existen algunas opciones de software libre para la ciberseguridad, cual es la mejor opción para cierta empresa, es una pregunta sin respuesta, ya que dependería de las necesidades del usuario o la empresa de cual herramienta o solución implementar, considerando que cada una de las herramientas tienen sus características que pueden ser adaptables o no, según detalles de la organización.

FIREWALLS

El FIREWALL más conocido como cortafuegos es el responsable de la seguridad entre la red privada y la red WAN es el responsable quien da el acceso a todos los dispositivos de red ya sean servidores, servicios, cámaras entre otros. (Figura 2)

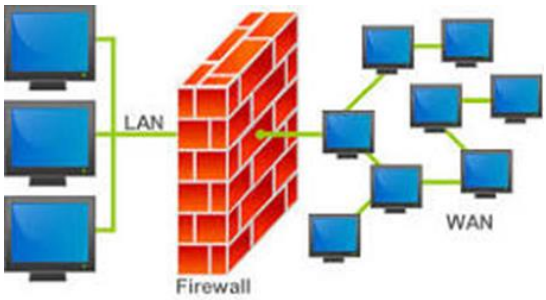


Figura 2-Estructura Firewall.

El nivel de seguridad también depende de cómo este configurado el firewall, una mala configuración podría ser perjudicial para la empresa, por lo que se ha tomado la decisión de elaborar este proyecto con una configuración optima en el firewall de PFsense el cual actuará como solución de ciberseguridad para las PYMES.

FILTRADO URL

Una de las soluciones de PFsense es el Filtrado URL esto es posible gracias a la configuración de SQUID Proxy en modo transparente que es una solución que está disponible para PFsense, que permitirá restringir URL específicas según políticas o requerimientos de la empresa.

PROXYS

Es básicamente un intermediario entre usuario y aplicación web o servicio, no cifra la conexión ni el contenido, oculta únicamente la dirección IP de origen.

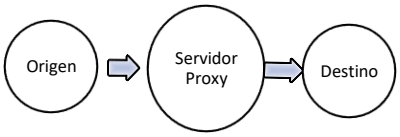


Figura 3- Servidor Proxy.

En otras palabras, es un puente entre el usuario y todo el internet. Mientras una persona navega en internet es la dirección IP del proxy la que se refleja en el sitio web brindando así seguridad en la navegación, existen varios proxys gratuitos que ocultan la IP del usuario para que pueda navegar de forma anónima, también es muy utilizado por hackers para ocultarse.

IPS (Sistemas de Prevención de Intrusos)

Son sistemas de prevención de intrusos (Instruction Prevention System) el objetivo es encontrar accesos no autorizados ya sea a la red o un ordenador. Trabaja de forma preventiva, analiza las conexiones y los protocolos en tiempo real para determinar si se está produciendo o se va a producir un ataque según los patrones, anomalías o tráfico sospechoso, además de permitir el control de acceso a la red. (INCIBE, 2020)

IDS (Sistemas de Detección de Intrusos)

Los sistemas de Detección de Intrusos (IDS) son usadas para detectar los accesos no autorizados en una red, monitorizan el tráfico entrante y lo compara con una base de datos actualizada de firmas de ataques conocidas. Si detectan alguna anomalía envían

alertas al administrador del sistema quien tomará las respectivas medidas de seguridad aplicables al problema presentado. (INCIBE, 2020)

CONTROL DE ANCHO DE BANDA

Existe una variedad de programas para el control de ancho de banda, uno de ellos es Bandwidth, su interfaz no es amigable, pero cumple la función de visualizar el consumo de ancho de banda en cada interfaz física o lógica del firewall. Otra opción es IPerf que cumple la función de medición de ancho como complemento de PFsense que es capaz de gestionar el ancho de banda entre redes virtuales VLAN.

PYMES EN ECUADOR

En el Ecuador este tipo de empresas son las consideradas pequeñas y medianas, de acuerdo con el número de empleados, volumen de ventas, activos pasivos, años en el mercado y sus niveles de producción.

Según el Banco Pichincha (https://www.pichincha.com/portal/blog/post/que-es-una-pyme) – Ecuador, catalogó como pymes de acuerdo con el siguiente gráfico. Figura_4

	Colaboradores	Valor bruto de ventas anuales	Activos
Pequeña empresa	10 a 49 personas	$100.001,00 a $1.000.000,00	$100.001,00 a $750.000,00
Mediana empresa	50 a 199 personas	$1.000.000,00 a $5.000.000,00	$750.001,00 a $399.000,00

Figura 4- Clasificación de Empresas Según sus Ingresos www.pichincha.com.

Las PYMES son una gran realidad en nuestro país, contempla empresas que quizá no deberían estar en este segmento, pero por razón de tributación prestamos etc. siguen perteneciendo a este segmento. En Ecuador pertenecen a este segmento casi el 95% de empresas, según datos del INEC.

ESTADÍSTICAS SOBRE LAS PYMES

En estos últimos años de pandemia se desconoce a ciencia cierta cuál es el número real de las empresas ya que ha habido gran número cierres de empresas pequeñas que no pudieron sobrellevar el gran impacto de la pandemia y la nula ayuda del régimen actual.

Según la CEPAL los altos costos de préstamos ya sea desde canales públicos o privados ha entorpecido el crecimiento que venía teniendo desde hace una década este tipo de segmento de empresas más o menos. https://repositorio.cepal.org/handle/11362/40726, es vedad también que la Banca privada ha sido su principal impulsor.

ANÁLISIS DEL MERCADO

Las pymes representan la mayor cantidad de empresas en el País estas son negocios familiares comúnmente, por ende, poseen poca cultura en lo que a tecnología se refiere y lamentablemente con un quemeimportismo en cuanto a inversión en esta área.

Es duro intentar cambiar estos patrones, pero hoy en día la dinámica del mercado ha obligado a muchas empresas a volcarse a la tecnología como medio para ventas online, muchas empresas supermercados, tiendas de víveres, restaurantes etc. por esta pandemia se ha visto obligados a invertir para poder subsistir en el mercado.

Como profesionales de TI siempre se debe recomendar la inversión y preocupación por la ciberseguridad a las empresas, optimizando todo según el tamaño de la empresa.

5. MATERIALES Y METODOLOGÍA

Metodología

De acuerdo a los requerimientos de nuestro proyecto se ha visto la necesidad de aplicar la metodología de investigación mixta, es decir aplicar lo necesario tanto de la metodología cuantitativa y de la cualitativa, considerando que se trata de procesos de recolección, análisis e integración para encontrar cumplir con los objetivos planteados.

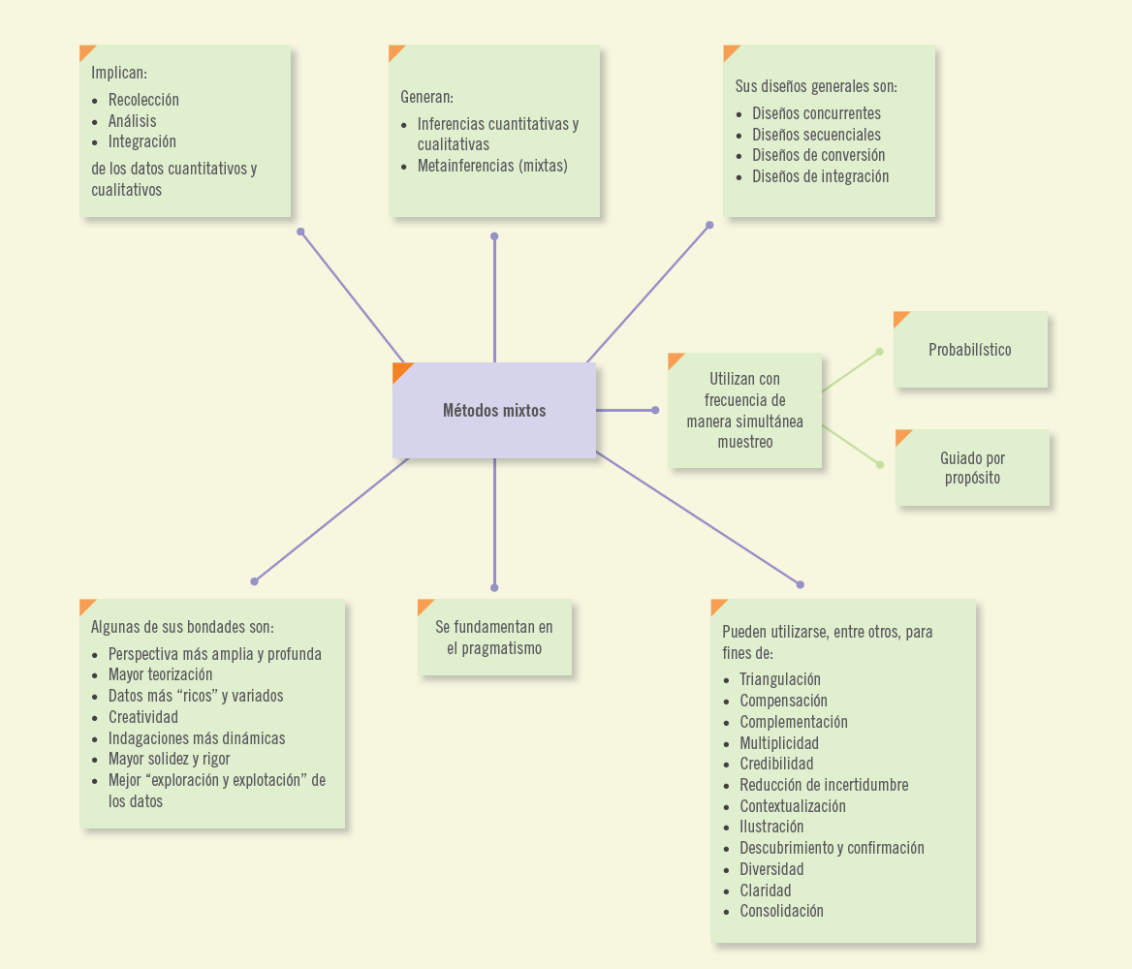


Figura 5- Mapa Conceptual Investigación Mixta (Hernandez, Fernandez, & Baptista, 2010).

a) Instrumentos empleados para recolectar datos cuantitativos y cualitativos

Cualitativo

Levantamiento de información detallada de fuentes de información online oficiales sobre las herramientas y conceptos necesarios para cumplir los objetivos específicos, y en base a la información recolectada, posteriormente realizar análisis de las mejores herramientas para una integración definitiva.

Cuantitativo

Se utiliza recolección de datos estadísticos de empresas Pymes de páginas oficiales indicadas en las referencias, como estadística histórica que indica un problema existente en un grupo específico, analizando la persistencia del problema al pasar de los tiempos y peor aún su incremento, entonces se puede decir que no se trata de un proceso lineal al pasar de los años si no un problema en crecimiento.

Para monitoreo de las soluciones implementadas y elección de las mejores herramientas en primera instancia se recolectará información diaria mediante las mismas herramientas durante una semana para verificar la efectividad de estas y de acuerdo con esto integrar las mejores herramientas.

b) Las prioridades de los datos cuantitativos y cualitativos

No existen prioridades entre el uno y el otro tanto los datos cualitativos como los cuantitativos son necesarios y fundamentales para este proyecto, todo dependerá de lo que se quiere demostrar en el momento.

La investigación cuantitativa se ocupará de demostrar los datos numéricos, los datos estadísticos, mientras que en la investigación cualitativa se emplean las palabras y los significados para entender de mejor manera conceptos y definiciones,

datos históricos de funcionamiento, efectividad documentada y experiencias recomendadas, en base a una implementación en un escenario real.

c) Secuencia en la recolección y análisis de los datos cuantitativos y cualitativos.

En primer lugar, usaremos datos cualitativos ya que nuestra recolección de información incluye entrevistas, para ser usados posteriormente en el enfoque cuantitativo, es decir se recolecta la información y luego se analizan los datos.

d) La forma como vamos a transformar, asociar y/o combinar diferentes tipos de datos.

El enfoque cualitativo busca principalmente "dispersión o expansión" de los datos e información, mientras que el enfoque cuantitativo pretende intencionalmente medir con precisión las variables del estudio, focalizar los datos.

e) Presentación de resultados

Tablas y gráficos dinámicos para tabular y medir la efectividad de las herramientas seleccionadas.

f) Unidad de análisis

A más de la información estadística obtenida sobre la situación real de las Pymes en cuanto a ciberseguridad al pasar del tiempo en nuestra región, se realiza el análisis de una empresa llamada Centro de Bordados Cuenca, a la misma que se realizan entrevistas y encuestas para considerar el nivel de seguridad que disponen y la infraestructura que manejan.

6. Resultados y discusión

SITUACIÓN ACTUAL DE LAS PYMES

Las Pymes en la actualidad poseen un modelo de seguridad de la información muy por debajo de lo recomendable para una organización con el objetivo claro de proteger la información interna de su empresa, e inclusive muchas veces ni siquiera disponen de infraestructura tecnológica para su seguridad.

Todas las empresas incluyen dentro de sus procesos la informática o herramientas tecnológicas con conexiones locales y externas, con acceso a internet.

En las empresas todos los días se almacena y trabaja con información sensible e importante, ya sea con dispositivos de almacenamiento informático como computadores, discos duros, dispositivos de almacenamiento USB, o información almacenada en la nube dentro de algún servicio externo. Las empresas al tener como sus principales procesos el de compra y venta, utilizan facturas físicas, proformas, cuentas bancarias, y mucha información almacenada en documentos físicos o tangibles, todo esto involucra información a proteger dentro de la organización sin distinción alguna, proteger de amenazas reales y existentes en el mundo informático, de ciberdelincuentes dispuestos a invertir tiempo en vulnerar la seguridad de la empresa y más aún si la empresa víctima no tiene mecanismos de protección, se convertirá en un objetivo demasiado fácil.

Puede ser un solo computador o varios, pocos o muchos documentos, esa será la información para proteger para la organización y uno de sus activos más importantes.

Para definir una línea de partida a más de definir la decadencia o ausencia de infraestructura para la ciberseguridad en las Pymes, es importante también analizar la situación del personal involucrado en los procesos de la empresa, se conoce que

el eslabón más débil de una infraestructura de ciberseguridad son los usuarios internos de la empresa, siendo netamente necesario definir un proceso de capacitación al usuario sobre la importancia de la seguridad informática que empieza desde su puesto de trabajo hasta la organización en general, todo esto va de la mano de una infraestructura básica de ciberseguridad, reduciendo el riesgo de un ataque significativamente.

Según el informe anual de Kaspersky 2021 revela que en Ecuador existe un crecimiento del 75% en ataques informáticos, es decir, existen alrededor de 89 ataques por minuto, esto no solo afecta a las grandes empresas o entidades financieras, como ha sido costumbre, cada vez los atacantes también colocan su interés en la información de pequeñas y medianas empresas, según Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky para América Latina, el alto índice de programas piratas comúnmente utilizados, es una de las causas principales para abrir muchas puertas para las ciberamenazas, motivo por el cual ha existido un crecimiento de los ataques informáticos en el país. (Diazgranados, latam Kaspersky, 2021)

Principales amenazas en ciberseguridad en las empresas

La transformación digital avanza a pasos agigantados y consecuentemente las amenazas, una de las principales amenazas que bien en crecimiento es el RANSOMWARE, y que preocupa mucho a las empresas por la razón de que a más de significar una pérdida económica también afecta al prestigio y la confianza que reflejará la empresa entre sus clientes y el mercado en general, según ESET existen 5 tipo de amenazas más comunes a nivel corporativo adicional al RANSOMWARE:

1. **Filtración o exposición de datos**

Esto ocurre de diferentes maneras, según la creatividad del atacante, una de las más conocidas es el Phishing, método muy utilizado por los atacantes dentro de la región a nivel empresarial, así como también se puede producir la exposición de datos por errores humanos, envíos erróneos o confusiones.

2. **Ataques de fuerza bruta**

Son ataques que tienen el objetivo de descifrar credenciales utilizando fuerza bruta con diferentes métodos y herramientas existentes en el internet, para acceder a sistemas internos de una organización. Por este motivo es importante colocar contraseñas robustas, sin embargo, en nuestro entorno esto no es común, los usuarios frecuentemente colocan contraseñas vulnerables y fáciles de descubrir para los atacantes, por la razón de que colocan una contraseña sencilla para no olvidarla, o en otros casos anotan sus credenciales en algún lugar visible, cuadernos, notas, archivos de texto, etc. colocando en riesgo la información, por todo esto es necesario capacitar al usuario sobre estos riesgos.

3. **Ataques a la cadena de suministro**

Son ataques destinados a proveedores de algún tipo de servicio a la organización, pudiendo con un solo ataque afectar a todos los clientes de este proveedor, por lo que es necesario tener proveedor con un nivel de seguridad aceptable.

4. **RAT Troyanos de acceso remoto**

Tipo de malware para espiar y robar información, se distribuyen mediante engaños, instaladores falsos, Phishing, enlaces maliciosos, con los que roban información almacenada en navegadores, mensajería, etc.

5. **Ingeniería social**

Quizás el más utilizado, es un conjunto de técnicas que utilizan los ciberdelincuentes para engañar a la gente y que les envíen datos confidenciales.

Según estos datos se ha buscado una empresa Pyme para realizar un análisis dentro de su infraestructura, esta empresa no cuenta con un método de ciberseguridad definido, el Centro de Bordados Cuenca es un ejemplo claro de muchas de las empresas de nuestra región, se dedican netamente a la actividad principal de su empresa descuidando cualquier situación ajena, como la ciberseguridad.

Considerando la situación actual de la mayoría de las pymes, se ha elegido una empresa como caso de estudio y para la posterior implementación de la solución integrada de ciberseguridad seleccionada.

Datos y actividades de la empresa:

RUC: 0190149897001.
Teléfono +593-7-2860060, cproarte@etapanet.net.
Proveedor de internet: ETAPA.
Personas de contacto: Sra. Angelita Viñansaca.
Dirección: Parque Industrial Lote 605 Estado Cuenca Ecuador.
Actividad: Importación y elaboración de tarjetas, vestimenta, sombreros de paja toquilla, tejidos, confeccionadas y bordadas a mano.
Dirección Web: www.centrodebordadoscuenca.com

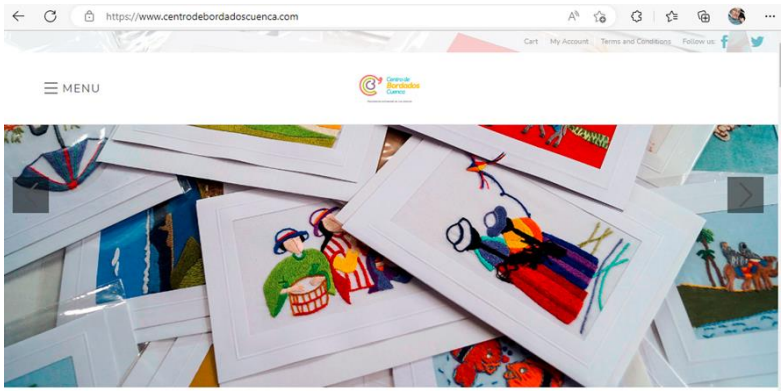


Figura 6- Sitio web de la empresa como caso de estudio.

Recursos tecnológicos que la empresa dispone:

- Router inalámbrico Huawei Etapa.
- 1 pc P4 windows xp (Sistema Antiguo BD).
- 1 pc Core i5 8Gb RAM (Administrador).
- 1 pc Dell Inspiron i3, 4Gb RAM, 500GB HDD (Taller).
- 1 laptop Dell Inspiron (Gerente).
- 1 impresora Epson L220.
- Impresora Epson FX 1300.

El objetivo es brindar una solución de ciberseguridad a esta pequeña empresa con un modelo estándar aplicable a Pymes.

Esta empresa reporta los siguientes problemas y requerimientos:

- Requiere compartir archivos (Router inalámbrico).
- Se requiere unir el pc Windows XP a la red, para compartir archivos y acceso a la base de datos interna (se requiere actualizar sistemas operativos).
- Brindar servicios adicionales mediante la red wifi.
- Según reporta se dispone de una cuenta institucional (cproarte@etapanet.net) que se encuentra hackeada y no se recuperado el su acceso.
- El proveedor de servicios de internet ha notificado que de la cuenta de correo asignada está enviando SPAM y por eso se encuentra bloqueada, esta cuenta se encuentra registrada en las entidades reguladores de funcionamiento, razón por la cual es importante su recuperación.

Se puede apreciar la falta de control de virus y spam en la red interna, así como también un control de acceso a sitios web (URL) de acuerdo con políticas internas de la empresa, siendo necesario evitar accesos a enlaces maliciosos, considerando este como uno de los riesgos principales que existen en la empresa.

Un software malicioso se considera de alto riesgo, debido a que un virus o un malware una vez infiltrado en la red o en cualquier de los equipos internos puede afectar a toda la red local, denegando servicios, robo o pérdida de información valiosa.

La empresa tiene necesidades para servicios que requieren utilizar, así como también la necesidad urgente de aplicar medidas de ciberseguridad en la red interna de la organización, en este ejemplo las necesidades serían cubiertas en su totalidad con solución propuesta. Es por ello por lo que se han planteado los requerimientos para poder implementar la solución integral, para casos como este que son muy comunes dentro de nuestro medio en las Pymes.

Adicionalmente para la implementación de la solución de ciberseguridad se necesitaría:

1 pc (Intel P4, Dual Core, Core2Duo, Core i3, 4G RAM, 2 interfaces de red, 80GB HHDD) Pfsence. (otra opción también es un Raspberry 4 que cumpliría la misma función), para la instalación de la solución integrada.

Figura 7- Raspberry Pi4, alternativa para instalación de solución de ciberseguridad.

Un switch básico mínimo de 8 puertos para distribuir la red local, LAN, para la distribución de la red en caso de necesitarlo.

Figura 8-Switch TPLink 8p.

Se dispone de un PC. DualCore 3 GB RAM disco de 300Gb y 2 interfaces de red, en el cual se implementará la solución inicial.

Esquema de red promedio de una Pyme, a continuación, se indica el esquema de red que comúnmente tiene una Pyme, por lo que se trabajará sobre este como punto de partida, viendo las necesidades de seguridad que requiere de acuerdo con este escenario.

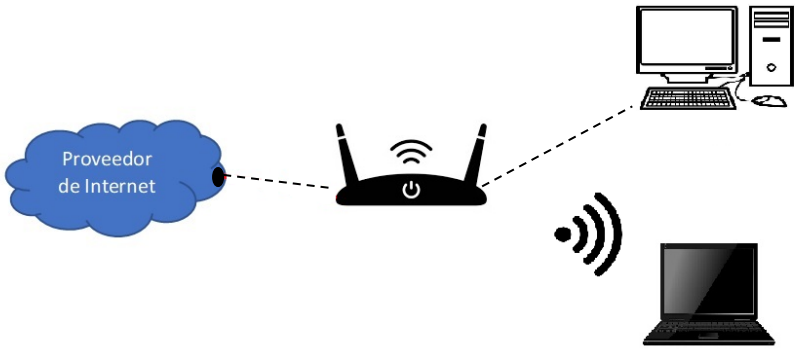


Figura 9-Esquema de red promedio de una pyme.

Esquema con solución de ciberseguridad, este es el esquema de red integrando las soluciones planificadas bajo el mismo escenario, de acuerdo a las necesidades de cada empresa se modificarán pequeños detalles, pero la estructura principal será la misma.

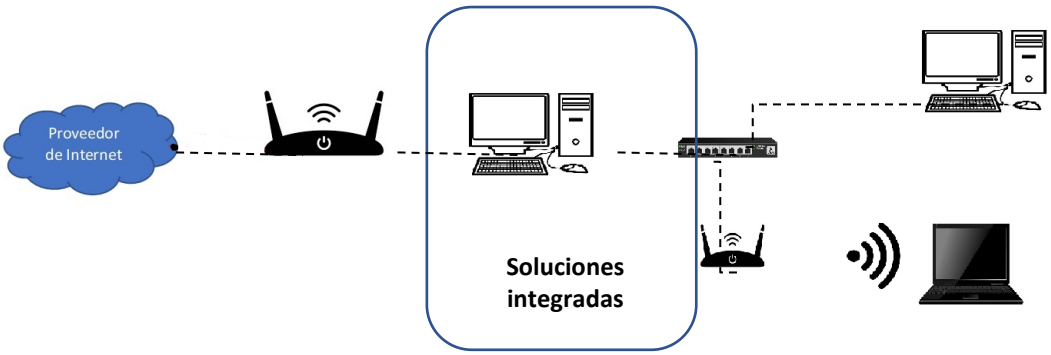


Figura 10- Esquema de red con solución integrada de ciberseguridad.

ANÁLISIS COMPARATIVO DE HERRAMIENTAS

Análisis de herramientas Firewall

	TIPO	CARACTERÍSTICAS	COMPATIBILIDAD
IPFire	Gratuita	* Construido sobre Netfilter * Gestión fácil, interfaz gráfica amigable * Permite agregar funciones * Usa IPTables para control de tráfico	Linux
OPNSense	* Gratuita * Código abierto	* Bifurcación de PFSense y m0n0wall * Posee características de firewalls comerciales * Posee interfaz gráfica amigable	Linux, MacOS X, Windows, FreeBSD, OpenBSD
PFSENSE	Distribución libre	* Basado en FreeBSD * Firewall líder a nivel comercial * Integrable y compatible con otras funcionalidades	Propio
SmoothWall	Distribución GNU/Linux	* Administrable mediante interfaz web * Soportar variedad de dispositivos de red * Soporte para módems ADSL y conexiones PPPoE.	Linux
UFW	Distribución GNU/Linux	* Fácil uso * Usa IPTables mediante consola * Desarrollado en Python * Usa la interfaz gráfica Gufw	Linux

Tabla 1-Comparativa de Herramientas Firewall.

Análisis de herramientas para Filtrado Url

	TIPO	CARACTERÍSTICAS	COMPATIBILIDAD
FlashStart	* Privativo * Demo	*La funcionalidad se llama: **internet content blocker** *Usa listas personalizadas *Permite programar bloques por intervalos de tiempo	Windows
RawStream	* Privativo * Demo de 15 días	*Con el filtrado de contenido protege de ransomware, malware, sitios de phishing *Utiliza lista de bloqueo y políticas flexibles	Windows
PFSENSE	* Sistema operativo propio * Distribución Libre	*Los servicios que se encargan del filtrado son squid y squidguard proxy *Permite trabajar con ACLs *Integrable y compatible con otras funcionalidades	Propio
Untangle	Basada en el sistema operativo Debian	*Ofrece varios servicios gratuitos y pagados *Ofrece filtrado url además de otras funcionalidades como IPS, Spam Blocker, Phish blocker, Firewall, Antivirus, Reportes.	Sistema operativo propio, basado en Linux

Tabla 2- Comparativa de Herramientas Filtrado Url.

Análisis de herramientas Antivirus

	TIPO	CARACTERÍSTICAS	COMPATIBILIDAD
VirusTotal	Gratuito	*Ofrece propuestas mas avanzadas pero son de pago *Antivirus online gratuito que permite analizar sitios web, archivos directamente desde su sitio web. *Rapidez y fiabilidad	Online
Kaspersky Security Cloud Free	Gratuito	*Fiabilidad *Análisis en tiempo real *Actualizaciones constantes de la base de datos de virus	Windows, Android
PFSENSE	Distribución Libre	*Squid proxy entrega la funcionalidad de antivirus *Funcionalidad agregada *Integrable y compatible con otras funcionalidades	Propio
ZoneAlarm	Gratuito	*Protegen de amenazas como robo de identidad *Firewall para red inalámbrica *Base de datos se actualiza constantemente *Requisitos de equipo mínimos	Windows

Tabla 3- Comparativa de Herramientas Antivirus.

	TIPO	CARACTERÍSTICAS	COMPATIBILIDAD
NETWORX	Privativo	*Monitoreo y supervisión de la red *Identifica actividades sospechosas *Monitoreo de aplicaciones en la red	Windows, MacOS
ZABBIX	- Monitoreo de ancho de banda gratuita - Código abierto	* Interfaz gráfica de administración robusta *Tráfico cifrado de red entre Zabbix y equipos	Compatibilidad con Linux
PFSENSE	Distribución Libre	*Integrable y compatible con otras funcionalidades *Dentro de la funcionalidad de Reportes y monitoreo se encuentra el manejo de tráfico y ancho de banda. *Escalabilidad, dispone de PFSense Plus +, para grandes empresas (servicio pagado)	Propio
SITE 24X7	Presenta información a nivel de equipos y conectividad Software Licenciado	* La consola está basada en la nube y se puede acceder desde cualquier lugar * Informes gráficos detallados *Monitorea latencia y la caída de paquetes	Windows
LIBRE NMS	Dispone de aplicaciones nativas de iPhone y Android para el monitoreo	*Dispone de un sistema flexible de alertas. *Notificaciones a través de Slack, IRC o correos electrónicos *Integración con otras herramientas como: NfSen, SmokePing, collectd, RANCID y Oxidized	Linux, complementos para Android y Apple
BIT METER OS	Software gratuito y de código abierto	* Interfaz gráfica amigable *Informes exportables en formato CSV	Linux, Windows

Tabla 4- Comparativa de Herramientas Gestor Ancho de Banda.

INTEGRACIÓN DE HERRAMIENTAS SELECCIONADAS

En base al análisis de herramientas realizado se ha decidido trabajar con PfSense, herramienta de libre distribución que ofrece los parámetros de seguridad que se busca en una Pyme, parámetros de seguridad como la de firewall donde se controla accesos como filtrado URL, control de ancho de banda de acuerdo a la red local (LAN) de la empresa y también un control antivirus, son las principales características de seguridad que debe tener una Pyme, considerando que no tiene costo el software por lo que la implementación para una empresa se reducirían los costos únicamente al hardware, convirtiéndose en una solución al alcance de muchas Pymes.

Pfsense también tiene características de mucha utilidad, como el control de logs, gráficos estadísticos o agregar widgets permitiendo un monitoreo constante por parte del administrador de seguridad de cada empresa. También contiene módulos

de configuración adicionales sin embargo en este proyecto se centrará en cubrir las necesidades de los parámetros explicados anteriormente.

Una vez instalado Pfsense se puede ingresar vía web con la dirección IP asignada en la interfaz LAN e ingresar con las credenciales de administrador.

La pantalla inicial de Pfsense tiene varias pestañas para configuración y monitoreo, se puede agregar widgets según las necesidades de cada administrador, donde se podrán visualizar parámetros como tráfico, accesos, bloqueos, etc. como se muestra en la siguiente Figura:

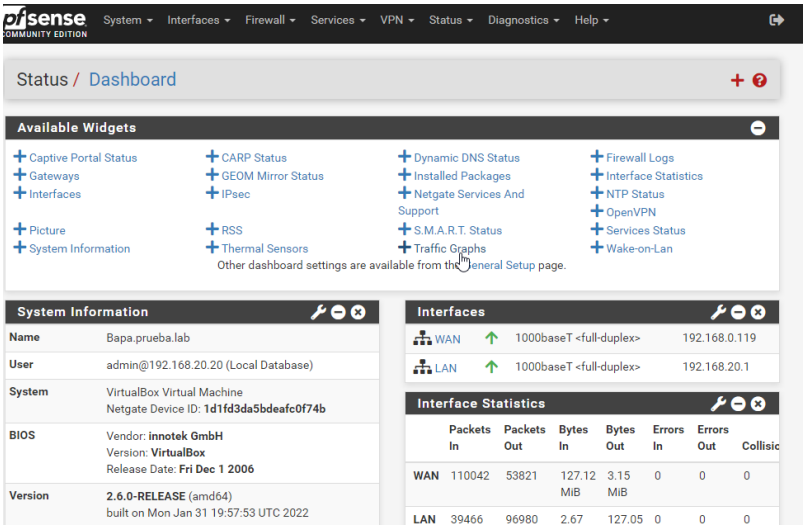


Figura 11. Interfaz Inicial de Pfsense.

FIREWALL

CONTROL Y GESTIÓN DE ACCESOS URL

Pfsense brinda la opción de controlar los accesos a Internet, permitir o bloquear el acceso a direcciones web según las políticas de cada empresa, característica de mucha utilidad en una infraestructura de ciberseguridad.

En el mundo laboral es importante no brindar un acceso 100% libre a la web porque esto puede generar puertas hacia amenazas de seguridad, considerando la existencia de sitios inseguros, y tomando en cuenta que el usuario estándar no conoce de los riesgos que puede tener un sitio web o las malas intenciones que pueden estar ocultas tras anuncios, publicidad, programas o archivos descargados, razón por la cual es necesario implementar un control de accesos a ciertas direcciones web que puedan ser consideradas como riesgosas.

También la empresa puede incluir dentro de sus políticas el bloqueo a ciertos sitios de ocio como, por ejemplo: redes sociales, juegos, streaming, videos, música, etc., que no necesariamente serían de utilidad para las tareas organizacionales, que de

cierta manera también podría incluir algún tipo de riesgo de seguridad, sin embargo, estos ya son casos particulares de cada organización.

CREACIÓN DE ALIAS

El primer paso para restringir una dirección URL es crear un Alias, el alias es un objeto que contiene una dirección IP que corresponde al sitio que se desea bloquear o restringir el acceso, es decir si yo deseo restringir el acceso a la página www.facebook.com se debe conocer cuál es la dirección IP pública de este sitio para agregarla como alias.

Para conocer cuál es la dirección IP publica de un sitio se lo puede realizar de la siguiente manera:

Figura 12. Comando para Obtención de Dirección IP de un Sitio Web.

Una vez obtenido este dato se procede a crear un alias, ingresar en la opción Firewall Aliases, el proceso se inicia con el botón “Import”.

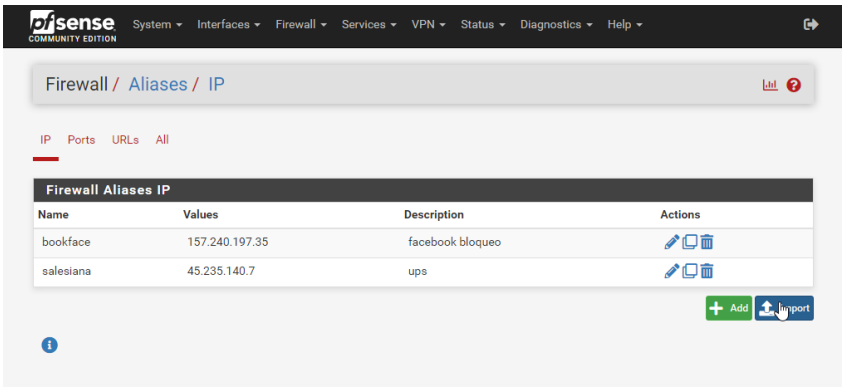


Figura 13. Pfsense Creación de Alias por Dirección IP.

Posteriormente se pedirá ingresar los siguientes datos:

Alias Name: Un nombre para identificar el alias.

Description: Una breve descripción para información.

Aliases to import: este es el campo más importante ya que contendrá la dirección IP del sitio web en cuestión, obtenida anteriormente.

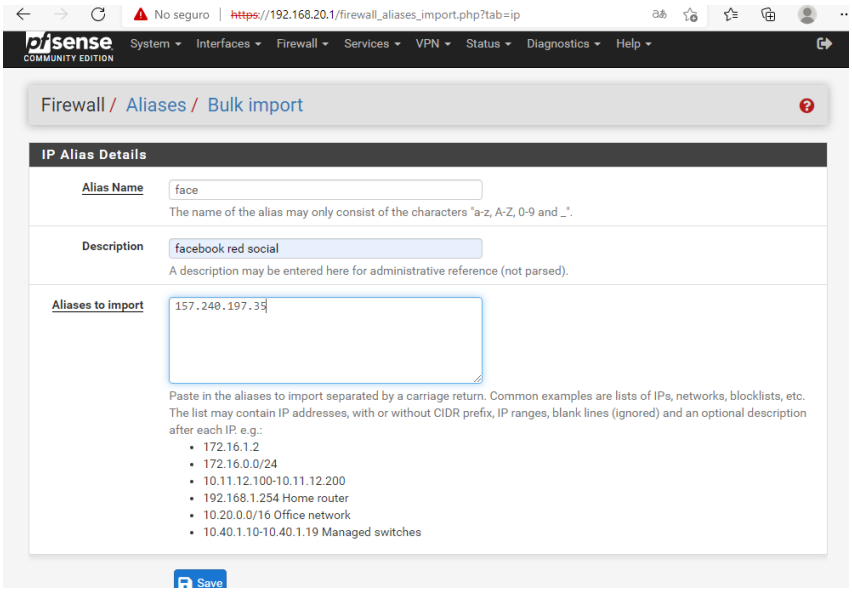


Figura 14. Pfsense Agregar IP para Bloqueo.

Una vez creado el alias se procede a crear la regla, dentro de Firewall/Rules y luego en la pestaña de LAN, en este caso se indicarán los parámetros para bloquear el alias que fue creado anteriormente.

Action: La acción que se desea realizar en esta regla, en este caso se desea bloquear un acceso por lo que se elige la opción “Block”.

Disable: Habilitar en caso de que se desea mantener inactiva esta regla.

Interface: La interfaz sobre la cual se ejecutará esta regla, en este caso sobre toda la LAN.

Adress Family: Protocolo de internet considerado, se trabaja con IPv4.

Protocolo: Todo el tráfico TCP.

Source: Se elige any ya que se desea controlar todo el tráfico saliente de la interfaz LAN.

Destination: seleccionar “single host or alias” ya que se trabaja con el alias creado y se elige el nombre de alias creado en este caso “face”.

Creación de regla

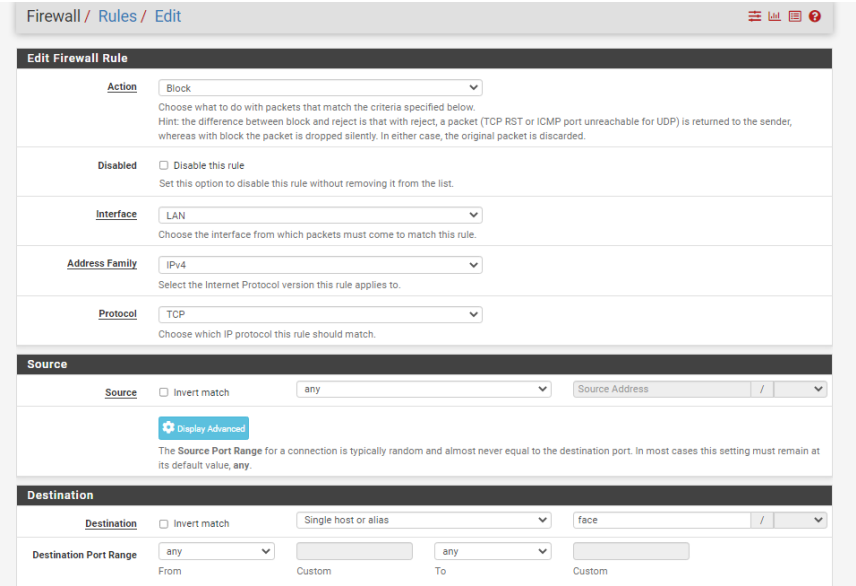


Figura 15. Creación de Regla en Firewall Pfsense.

Adicionalmente se puede habilitar la opción Log, para que permita monitorear cuando esta regla se ejecute durante el tráfico.

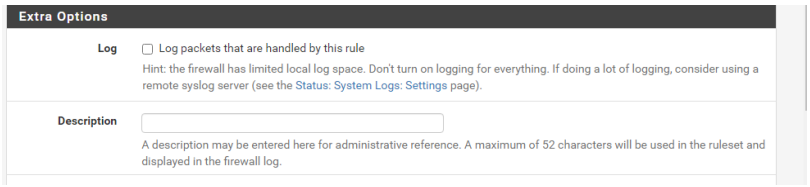


Figura 16. Activar Logs en una Regla del Firewall Pfsense.

Control de ancho de banda sobre la LAN

Realizar un control de ancho de banda dentro del tráfico que genera la red local es un método que puede reducir el riesgo en gran medida, ya que se podrá controlar o limitar el consumo de ancho de banda de equipos o Vlans específicas de acuerdo con los requerimientos y políticas de la empresa.

Es importante también para evitar un consumo excesivo de ciertos equipos, produciendo saturación o lentitud en la red.

Creación de limitadores

En primera instancia se necesita crear los límites que serán los valores de ancho de banda tanto de subida como de bajada, es decir por cada valor definido se deberá crear un límite de subida y bajada, por ejemplo, si quiero controlar un ancho de banda de 10 Megas a cierto equipo o a cierta subred se debe crear 2 limitadores, uno de subida y otro de bajada, dentro de: *Firewall/Traffic shaper/ Limiters.*

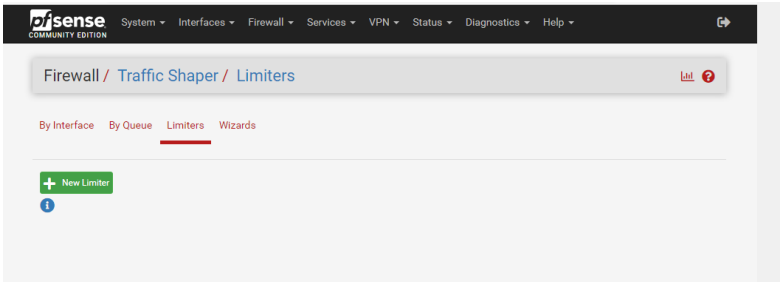


Figura 17. Agregar Limitadores para Ancho de Banda.

Con el botón "*New Limiter*", pedirá los siguientes parámetros:

Activar la opción *Enable limiter and its children* para activar el limitador.

Bandwith: Valor limitante de ancho de banda y la unidad de medida en el que se encuentra el valor.

Mask: valor a seleccionar *Source addresses* si es valor de subida y *Destination addresses* si es limitador de bajada.

Limitador de subida

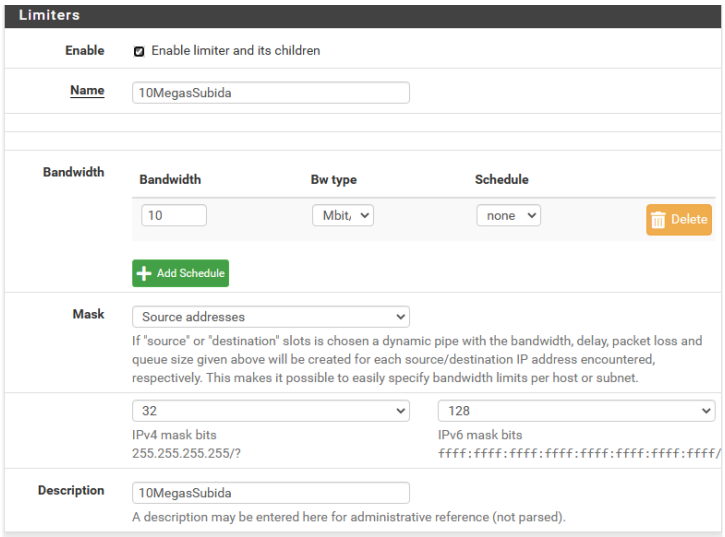


Figura 18. Limitador de Subida Ancho de Banda.

Limitador de bajada

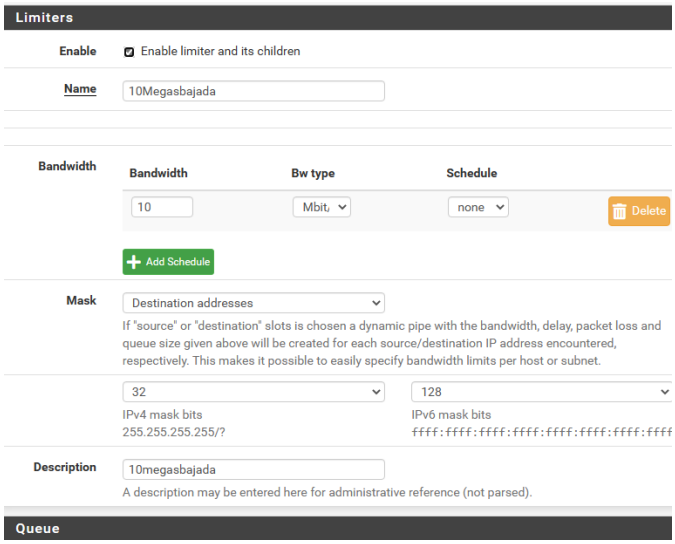


Figura 19. Limitador de Bajada Ancho de Banda.

Creación de alias

Es importante la creación de un alias para identificar el equipo o la red a la que será aplicado el control de ancho de banda, en este caso es únicamente a una dirección IP dentro de la red local.

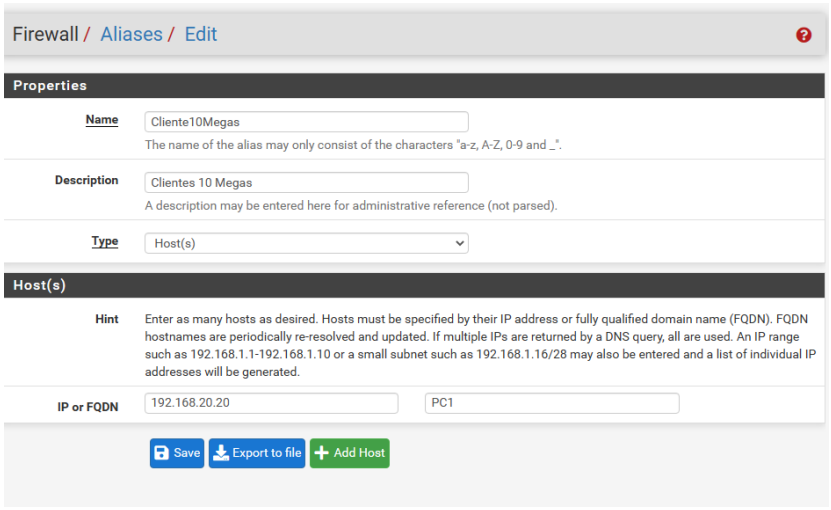
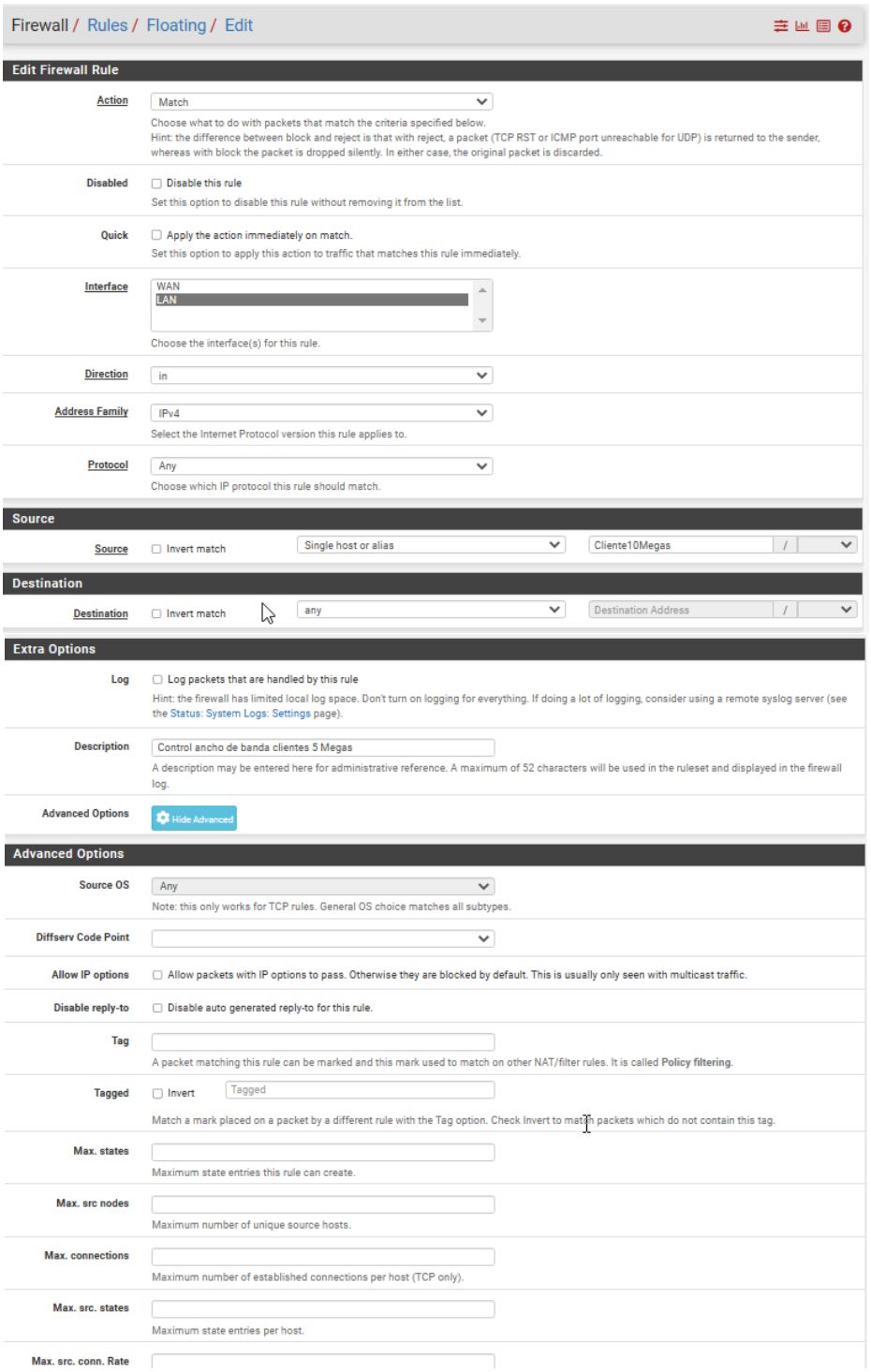


Figura 20. Creación de Alias para Gestión Ancho de Banda.

Y finalmente se crea una regla para emparejar los valores creados, tanto el alias como el limitador. Dentro de Firewall/Rules/Floating con la opción Add se agrega una nueva regla con la acción de Match para emparejar el alias creado con el limitador correspondiente.


Firewall / Rules / Floating / Edit
Edit Firewall Rule
Action
Match
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Quick
Apply the action immediately on match.
Set this option to apply this action to traffic that matches this rule immediately.
Interface
WAN
LAN
Choose the interface(s) for this rule.
Direction
in
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
Single host or alias
Cliente10Megas
Destination
Destination
Invert match
any
Destination Address
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
Control ancho de banda clientes 5 Megas
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Hide Advanced
Advanced Options
Source OS
Any
Note: this only works for TCP rules. General OS choice matches all subtypes.
Diffserv Code Point
Allow IP options
Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.
Disable reply-to
Disable auto generated reply-to for this rule.
Tag
A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called Policy filtering.
Tagged
Invert
Tagged
Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.
Max. states
Maximum state entries this rule can create.
Max. src nodes
Maximum number of unique source hosts.
Max. connections
Maximum number of established connections per host (TCP only).
Max. src. states
Maximum state entries per host.
Max. src. conn. Rate

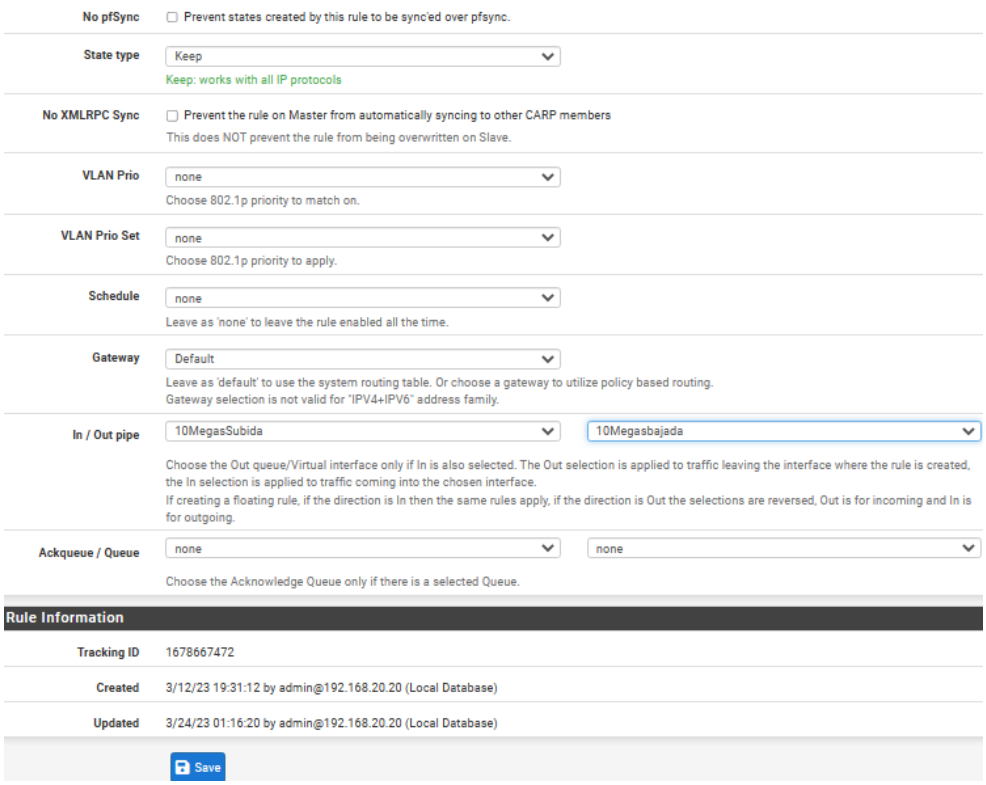


Figura 21. Reglas Flotantes para Gestión de Ancho de Banda.

La regla se encuentra creada y se visualizará de la siguiente manera, recordando también que con las opciones de "Actions" permite Editar, copiar, deshabilitar y eliminar la regla:

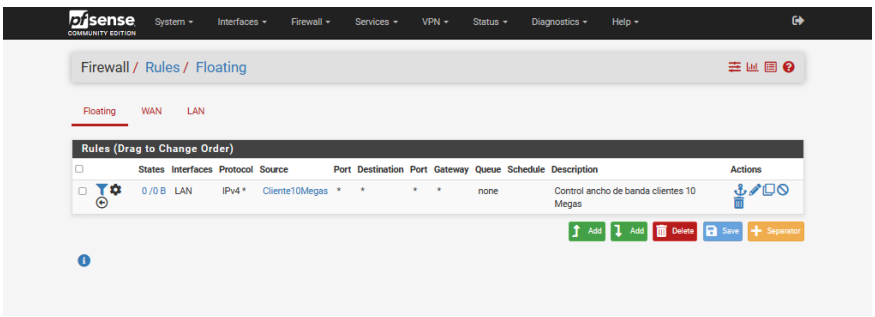


Figura 22. Regla Flotante Creada.

Aplicar cambios para concluir y distribuir las configuraciones realizadas.

CERTIFICADOS

Ahora para los siguientes servicios de Pfsense vamos a necesitar un certificado el cual ayudará en la efectividad de tareas del Squid.

Por este motivo se genera 3 certificados.

1. CA_Tesis (Autoridad de Certificación Interna).
2. CA_Tesis_INTER (Autoridad de Certificación Intermedia).
3. SSL_Tesis (Certificado Interno).

Estos certificados serán utilizados en las configuraciones del Squid Proxy Server.

SQUID PROXY

Uno de los servicios más importantes para el control de acceso o filtro URL es sin duda el Squid Proxy Server, este servicio no está preinstalado en el pfsense, lo que debemos hacer es ingresar al administrador de paquetes y buscarlos en los paquetes disponibles del Pfsense.

Para ello ingresar en las siguientes opciones de menú. System/Package Manager como muestra la siguiente figura:

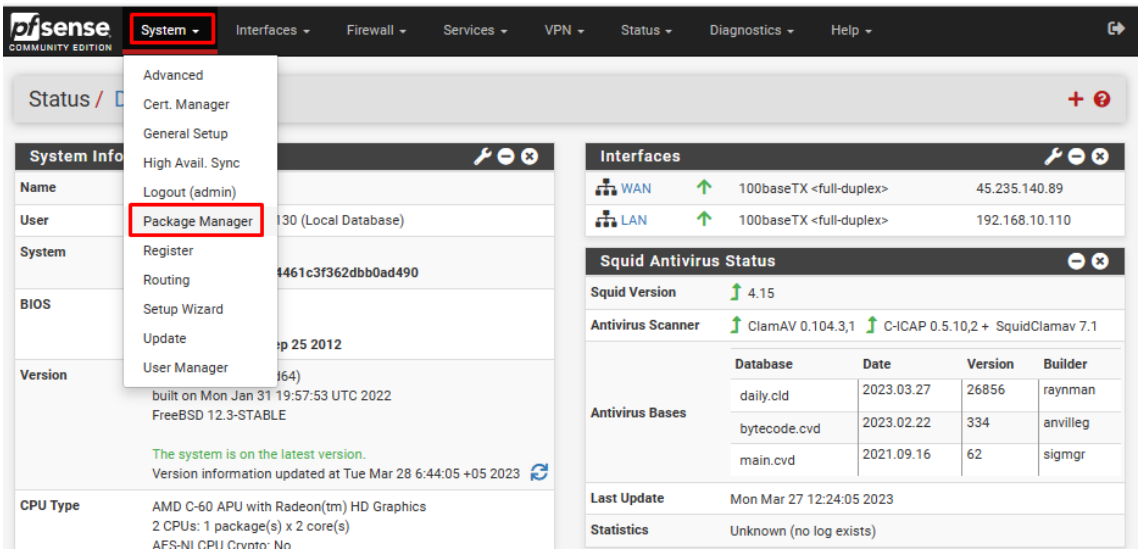


Figura 23. Instalación de Paquetes Squid Proxy.

Dentro de esta opción se tienen dos opciones disponibles, paquetes instalados y paquetes disponibles.

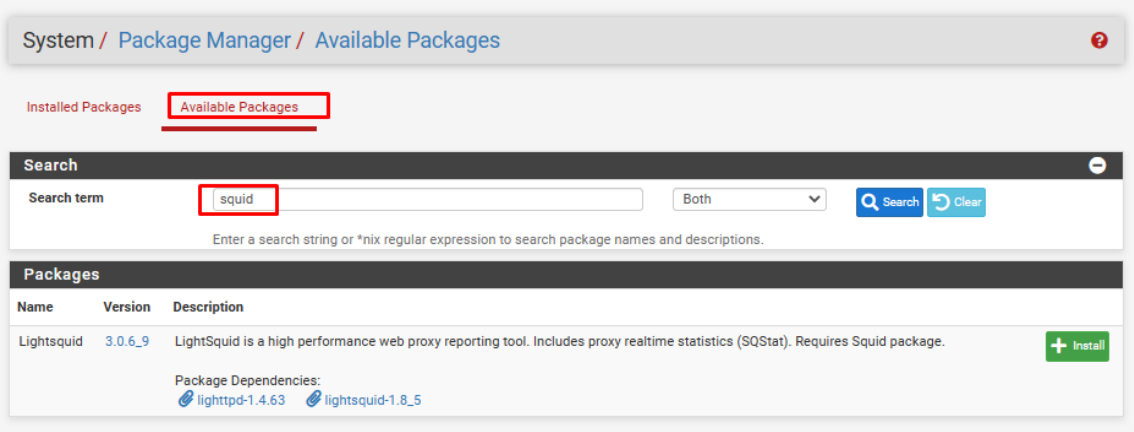


Figura 24. Paquetes Disponibles en Squid Proxy.

Se realiza una búsqueda de squid e instalamos las siguientes dos opciones:

1.-Squid Proxy Server.

2.- SquidGuard. Pinchamos en el botón de verde “Install”.

Se puede verificar dentro de la opción de “Paquetes Instalados” que se encuentra instalado las 2 opciones de Squid, Squid Proxy Server y Squid Guard, tal como muestra la siguiente figura:

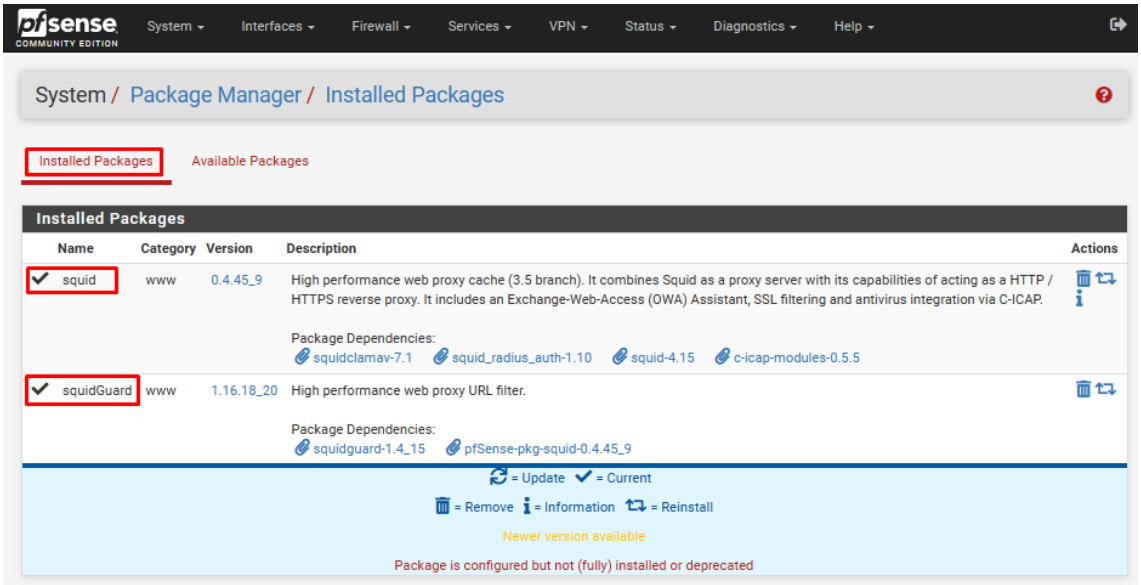


Figura 25. Paquetes Instalados Squid.

Una vez instalado los programas se activarán dentro del menú desplegable de servicios las siguientes opciones (Figura 26). En las cuales accederemos para configurar cada uno de los servicios requeridos.

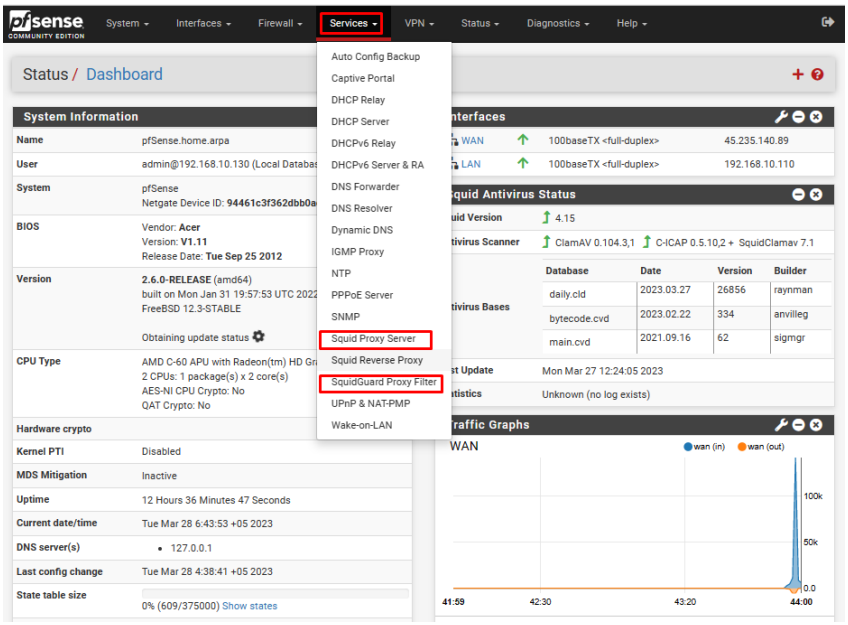
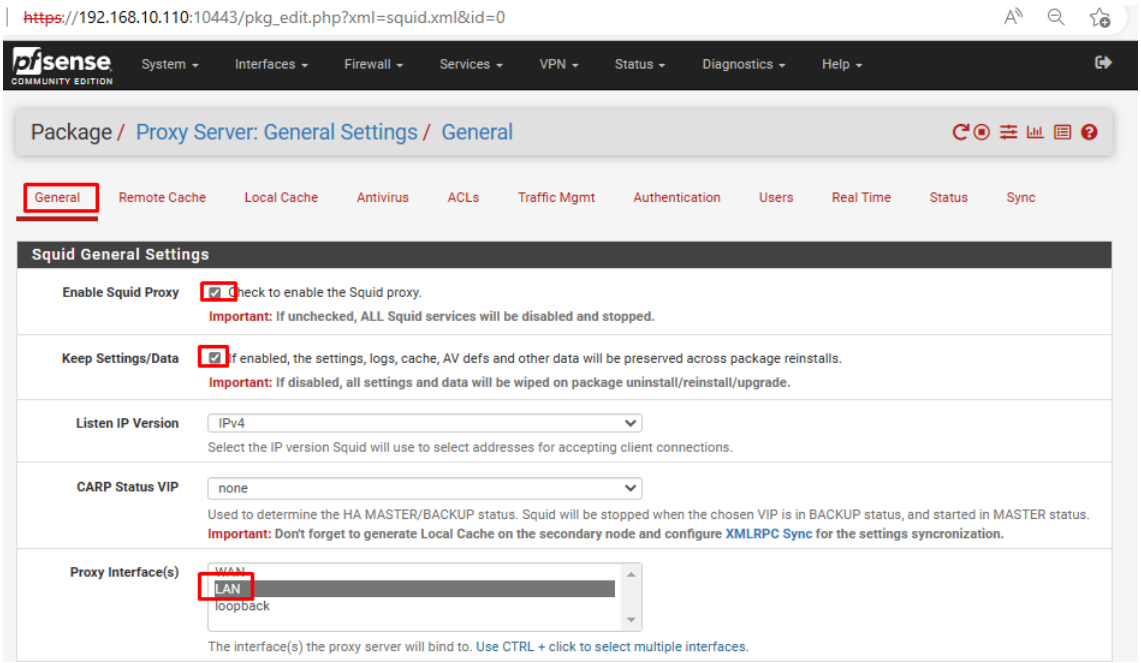
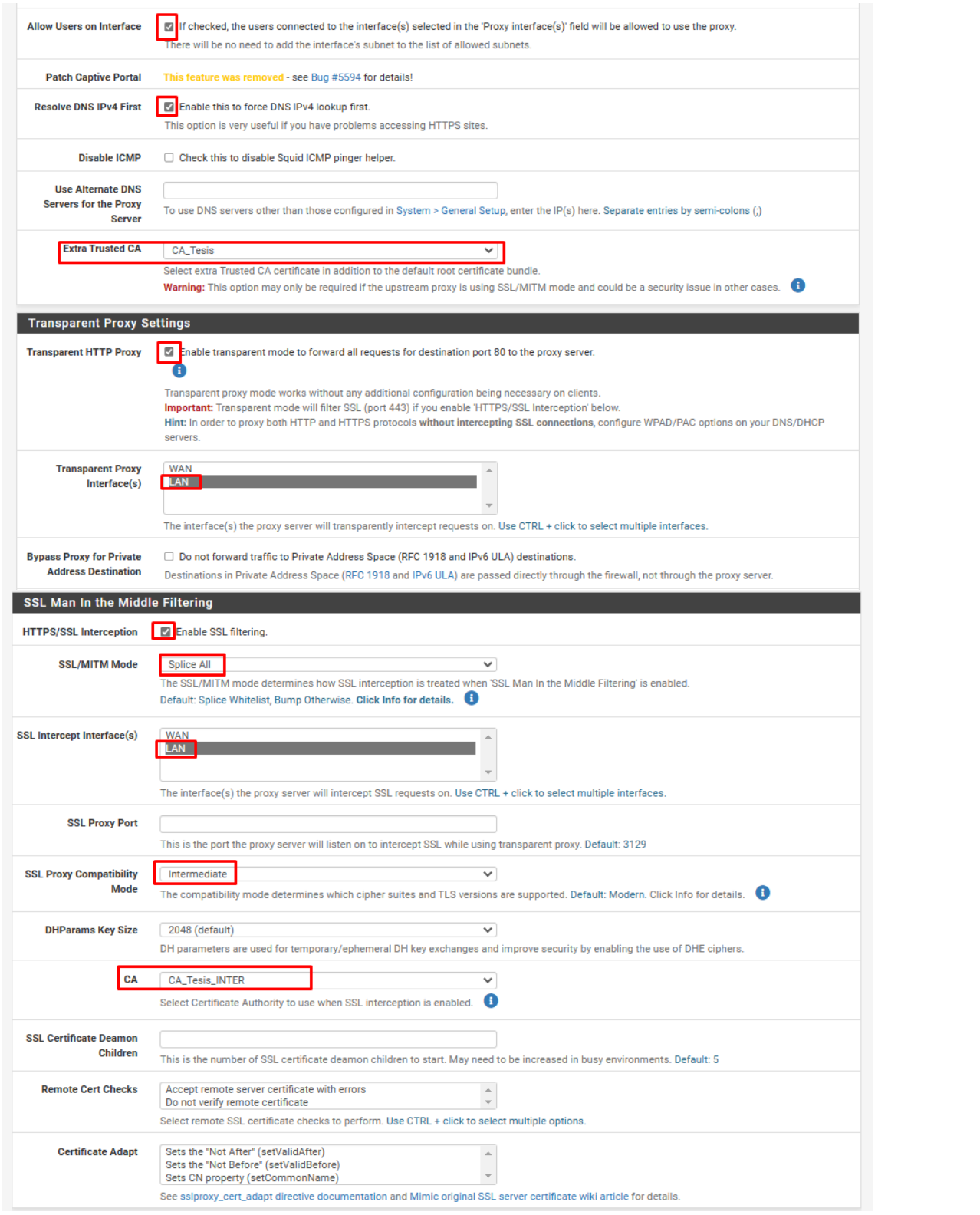


Figura 26. Servicios Squid Activos.

Seleccionar Squid Proxy Server. En este espacio se configura el servidor proxy, posicionarse en General y se desplegará todas las opciones posibles de las cuales seleccionar las que indica la siguiente figura:




Allow Users on Interface
If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal
This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First
Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP
Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server
To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)
Extra Trusted CA
CA_Tesis
Select extra Trusted CA certificate in addition to the default root certificate bundle.
Warning: This option may only be required if the upstream proxy is using SSL/MITM mode and could be a security issue in other cases.
Transparent Proxy Settings
Transparent HTTP Proxy
Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)
WAN
LAN
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.
Bypass Proxy for Private Address Destination
Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.
Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.
SSL Man In the Middle Filtering
HTTPS/SSL Interception
Enable SSL filtering.
SSL/MITM Mode
Splice All
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. Click Info for details.
SSL Intercept Interface(s)
WAN
LAN
The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.
SSL Proxy Port
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
SSL Proxy Compatibility Mode
Intermediate
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.
DHParams Key Size
2048 (default)
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
CA
CA_Tesis_INTER
Select Certificate Authority to use when SSL interception is enabled.
SSL Certificate Deamon Children
This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5
Remote Cert Checks
Accept remote server certificate with errors
Do not verify remote certificate
Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.
Certificate Adapt
Sets the "Not After" (setValidAfter)
Sets the "Not Before" (setValidBefore)
Sets CN property (setCommonName)
See sslproxy_cert_adapt directive documentation and Mimic original SSL server certificate wiki article for details.

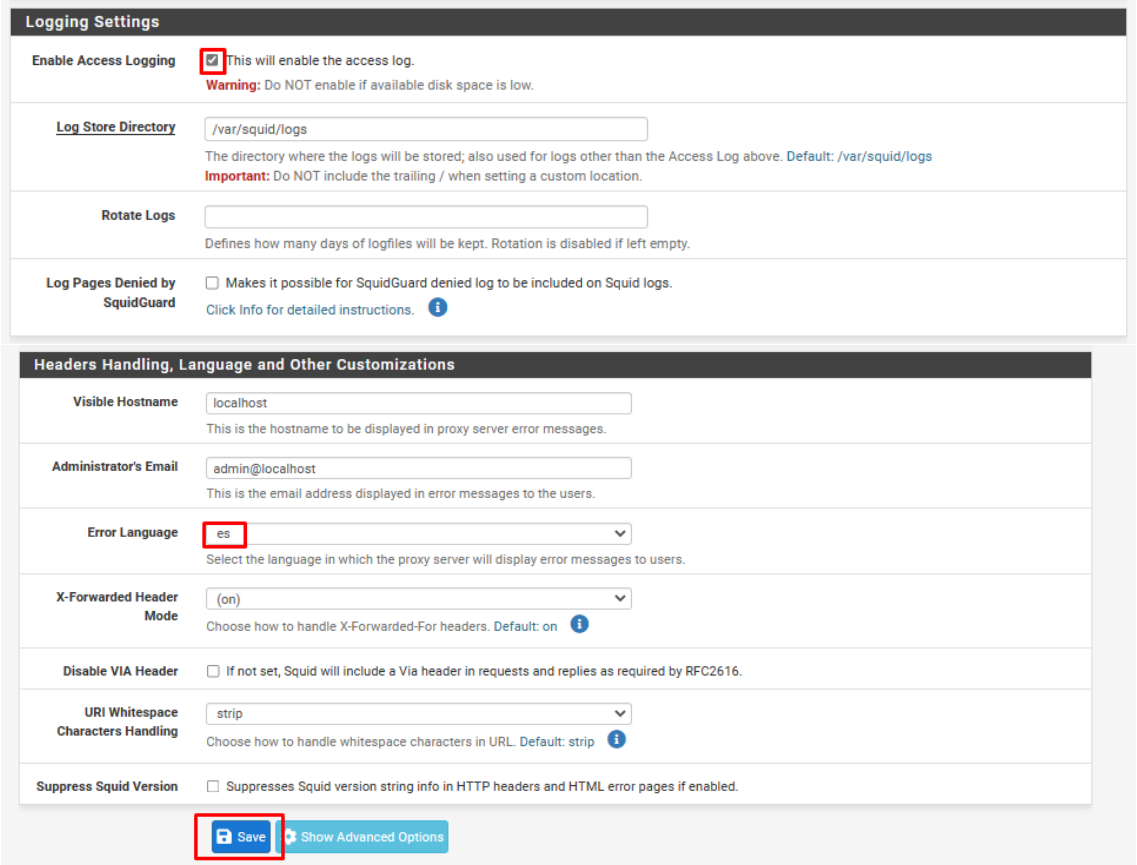


Figura 27. Configuraciones Squid.

Una vez seleccionadas las opciones necesarias para el funcionamiento del Squid Proxy Server, Grabar.

Squid Enable Proxy: Con esta opción se activa el servicio de Squid Proxy Server.

Keep Setting/Data: Esta opción sirve para guardar los logs,cache,etc.

Proxy Interface: por lo general ya viene seleccionado LAN.

Allow Users and Interface: Con esta opción se aplica el servicio a las interfaces.

Resolve DNS IPv4 First: Esta opción ya viene seleccionada por defecto.

Extra Trusted CA: En esta opción se selecciona el certificado raíz previamente creada.

Transparent HTTP Proxy: Para activar proxy transparente.

Transparent Proxy Interface: Por lo general ya viene seleccionado la LAN.

HTTPS/SSL Interception: Esta opción nos ayuda para el bloqueo de páginas https.

SSL/MITM Mode: En esta opción escoger Splice All. Método de intercepción SSL.

SSL Intercep Interface: Por lo general ya viene seleccionada la opción LAN.

SSL Proxy Compatibility Mode: Seleccionar Intermediate.

CA: Seleccionar el certificado Intermedio previamente creado.

Enable Access Loggin: Seleccionar esta opción para la generación de logs del dquid. Seleccionar solo si se dispone de espacio en el Disco Duro Interno.

Error Language: Seleccionar el idioma, para esta práctica, “es”.

SAVE: Guardar las configuraciones y probar.

A continuación, se configurará el cache local y dentro de la pestaña de Local Cache como indica la siguiente figura:

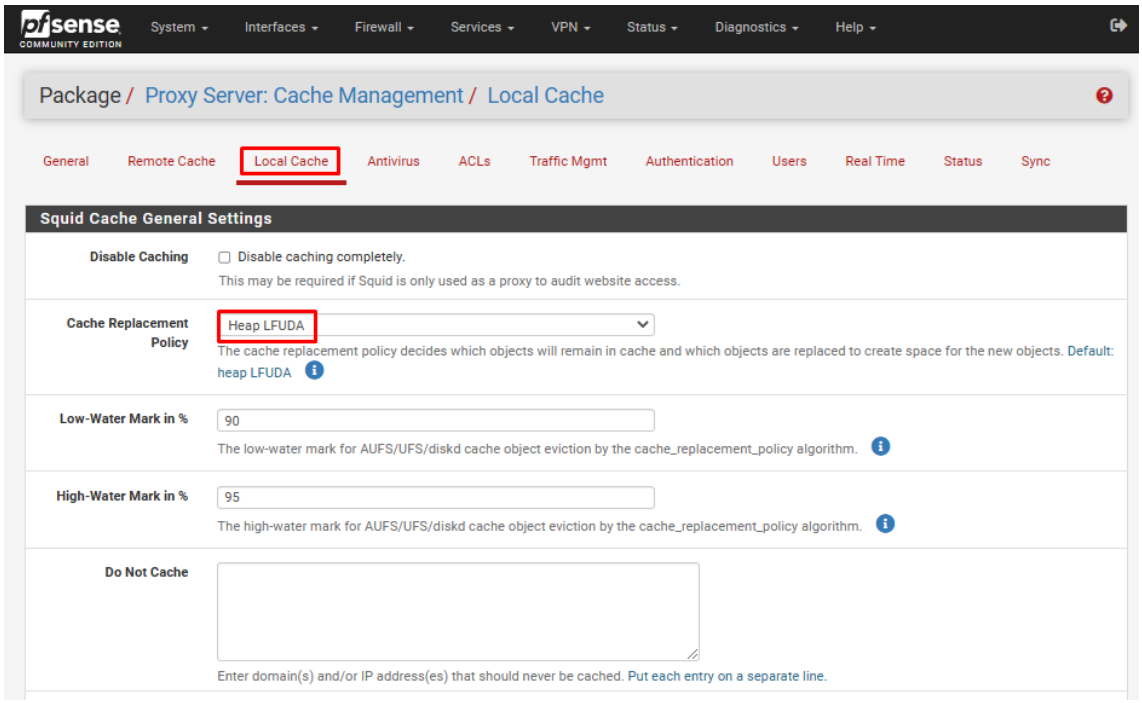


Figura 28. Configuración de Caché Local.

Sin realizar cambios, se guarda la configuración por defecto para que se genere el archivo de caché.

Ahora se crea la ACL, para ello dentro de la pestaña ACLs, se agregan las páginas a ser bloqueadas en la sección de Blacklist, como muestra la siguiente figura:

Figura 29. Creación de Blacklist.

Para realizar la prueba virtualizamos una máquina con Windows 10 en este caso VMware Workstation, lo más importante de esta configuración es esta máquina virtual debe estar dentro de la misma red LAN del Pfsense, ya que simulará un cliente, para ello se configura la interfaz de red de la VM como tipo puente.

Prendemos nuestra VM y procedemos con las pruebas del bloqueo desde el navegador EDGE de Windows 10.

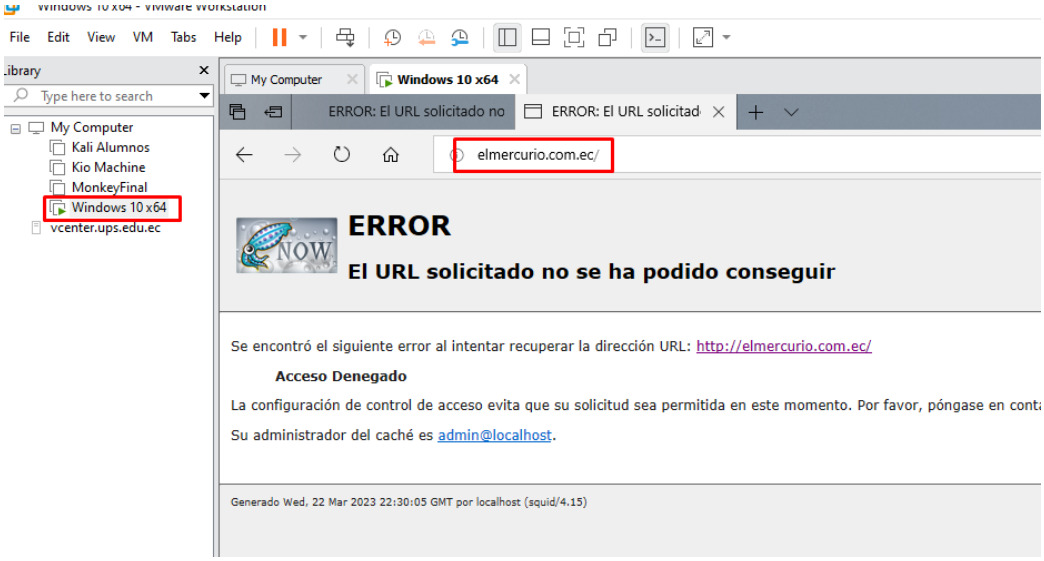


Figura 30. Bloqueo de Sitio Web.

Dentro de las configuraciones del squid proxy server se indica que se guarden los logs.

Ahora, para acceder al archivo de logs se realiza lo siguiente:

En la página principal del pfsense ya sea en físico o virtual, existe la opción número **14 habilitar sshd** la cual habilita el acceso desde un putty o mRemoteNG, en este caso se utiliza esta última**.**

Para acceder a los archivos físicos de log se selecciona la opción **8, Shell,** del menú principal del Pfsense, de esta manera gana un acceso a shell y se tendrá acceso a los archivos físicos donde se guardan los logs, se podría usar el comando: tail –f /var/squid/logs/access.log, y ver el contenido del archivo access.log como se muestra en la siguiente figura:

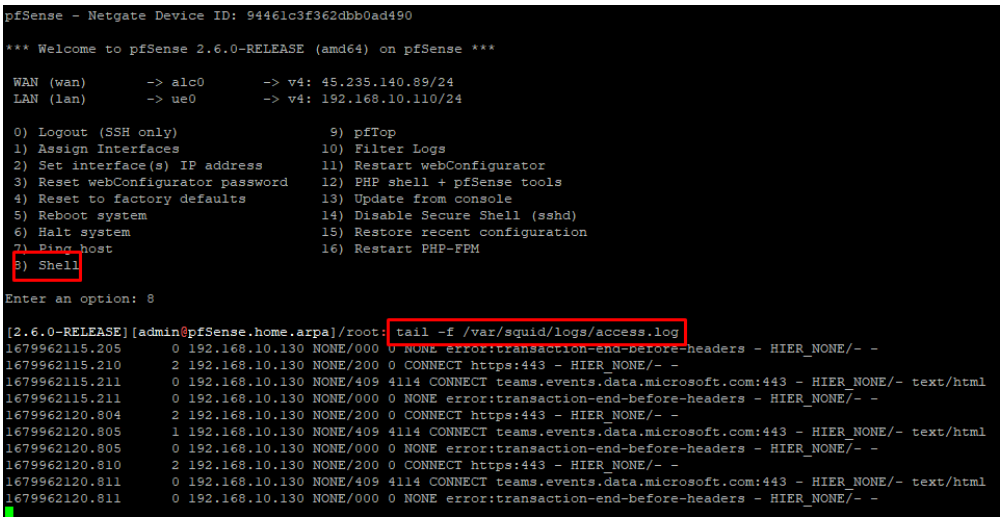


Figura 311. Análisis de logs.

Como se puede apreciar se obtiene la lectura de los logs del Squid y se puede revisar como trabaja el bloqueo del Squid proxy server.

SQUIDGUARD

Dentro del menú servicios se selecciona la opción **SquidGuard Proxy Filter.**

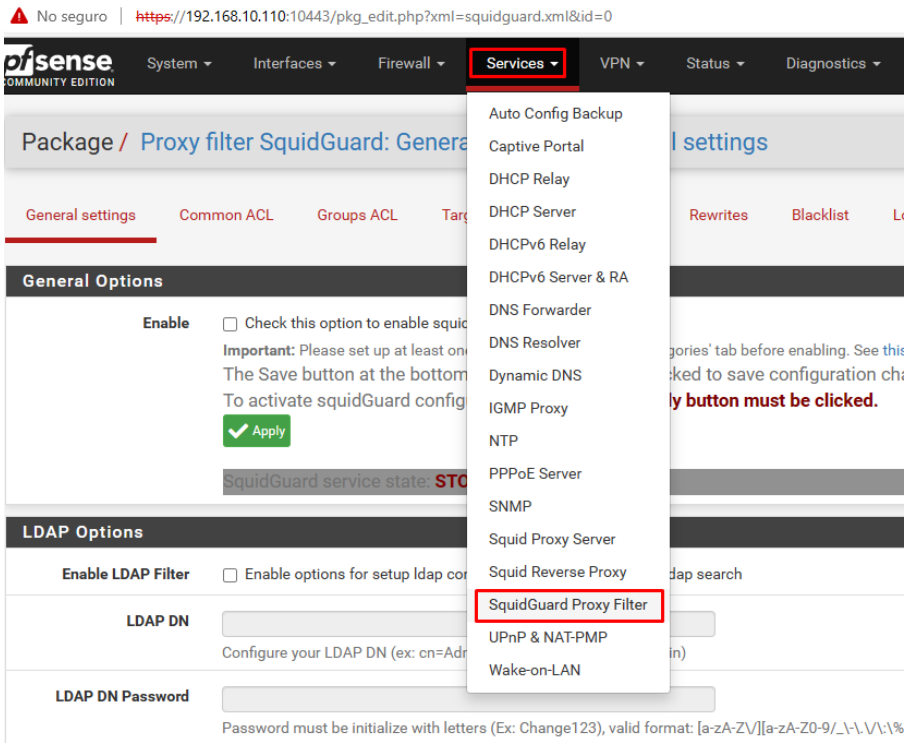
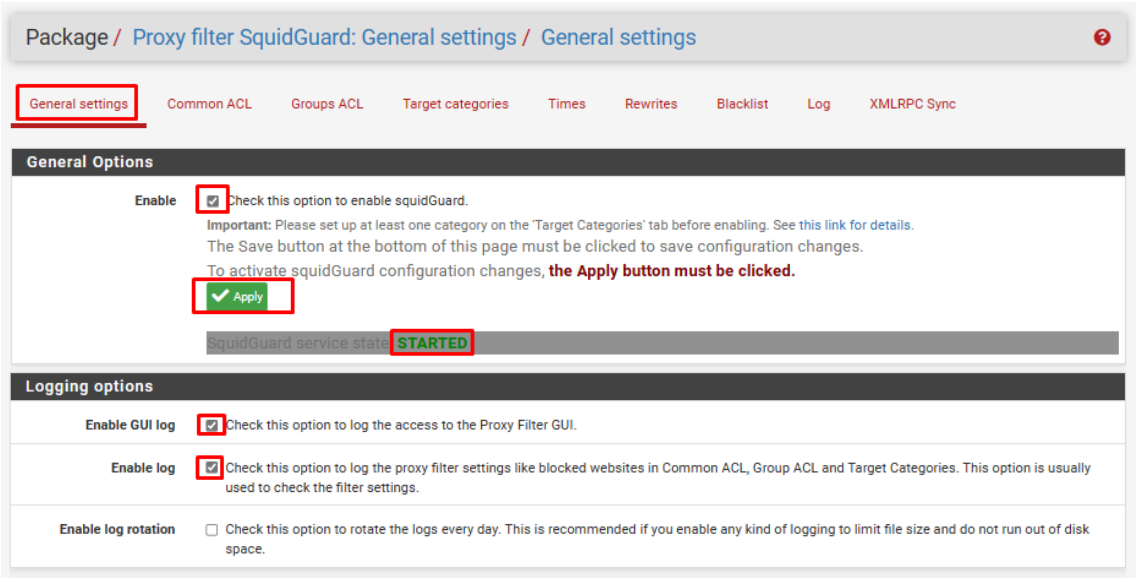


Figura 32. SquidGuard Proxy Filter.

Una vez dentro del servicio se posiciona en General Settings y activamos las opciones tal cual muestra la siguiente figura:



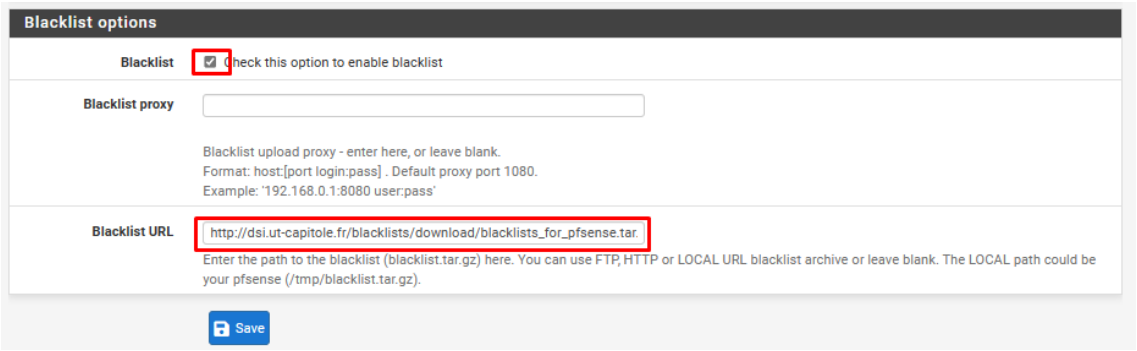


Figura 323. Configuración Parámetros SquidGuard.

Enable: opción para activar el servicio.

Apply: opción para aplicar cambios realizados en el squidguard.

Enable GUI Log: Activar esta opción para poder revisar los logs desde entorno gráfico.

Enable log: Con esta opción se activan los logs, muy útiles para revisar errores futuros.

Blacklist: Opción para activar las listas negras de sitios web.

Blacklist URL: es la dirección de donde se descargan todas las listas negras

Una vez configuradas las opciones necesarias para el buen funcionamiento del SquidGuard. Hay que concentrarse en un punto muy importante de este apartado que es la Base de Datos de Listas Negras la cual se debería descargar desde la web (Blacklist URL) existen varios sitios de donde descargar esta base de datos, pero muchos links están fuera de servicio o las bases están desactualizadas la más fiable y completa se ha encontrado y descargado desde el siguiente link.

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Una vez configurado todos los parámetros necesarios, se aplican los cambios.

Luego, en la opción de Blacklist se realiza la descarga de la Base de Datos de listas negras.

Al momento que termine la descarga de la Base de Datos, se proceden con las pruebas respectivas. (Pedro Moreno, 2023)

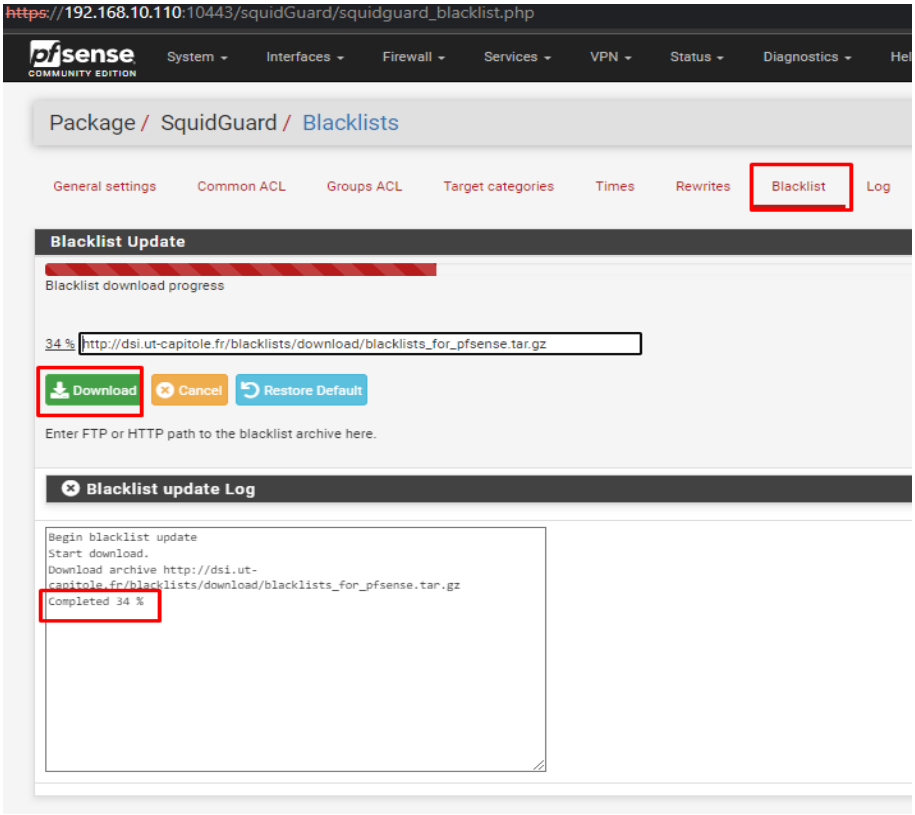


Figura 334. Actualización de Blacklist.

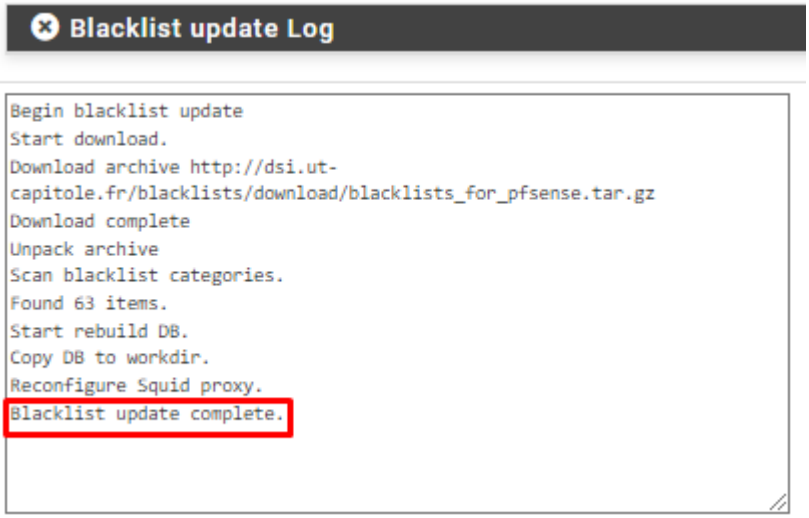


Figura 345. Blacklist actualizada.

Una vez terminada la descarga se procede a crear Groups ACL, para aplicar los cambios ya sea a una dirección IP o subred a la que protegerá el SquidGuard

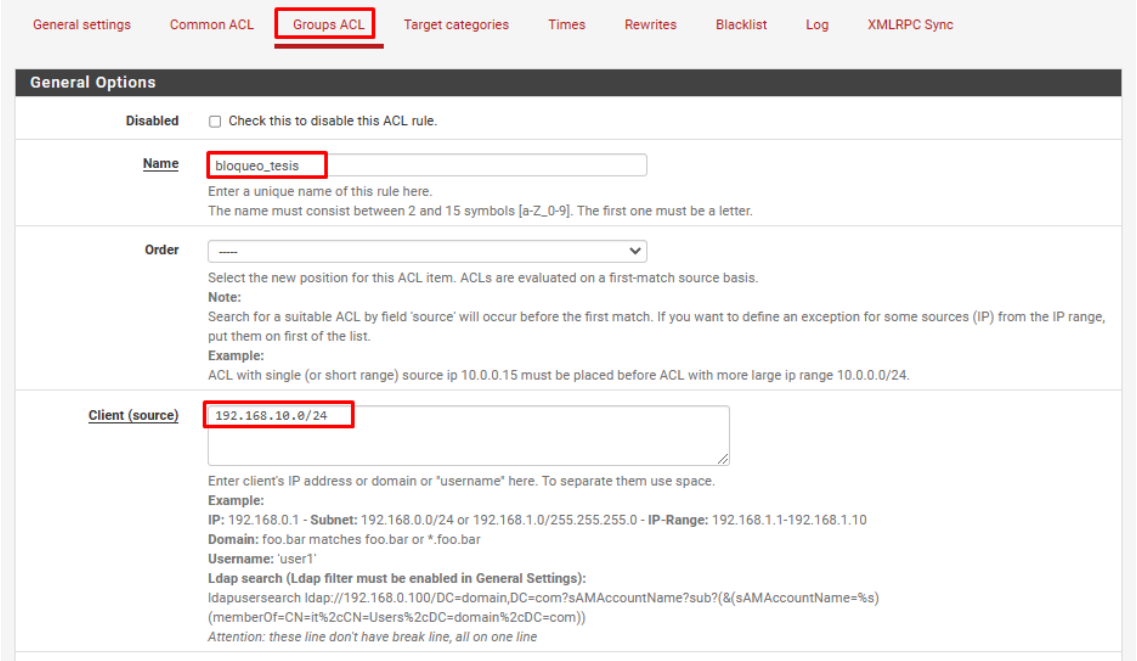


Figura 36. Creación de Grupos ACL.

Para estas pruebas se aplicarán filtros de sitios para adultos, de la base de datos de listas negras blk_blacklists_adult, que se descargó anteriormente.

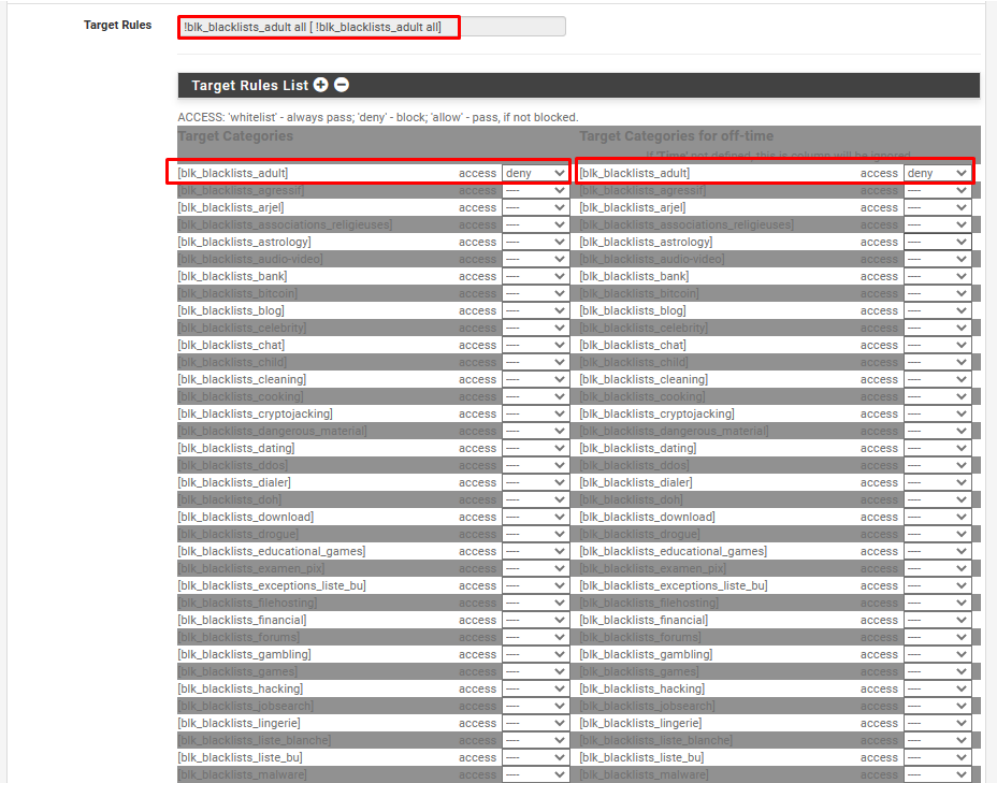


Figura 357. Blacklist existentes.

Aplicar cambios y verificar que el servicio este iniciado.

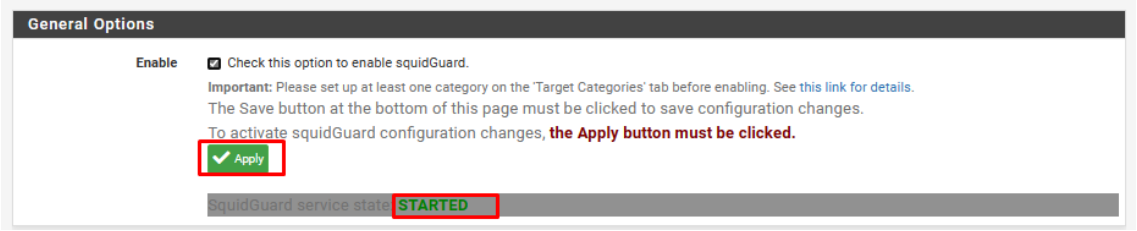


Figura 38. Servicio de SquidGuard activado.

Como se puede apreciar en la siguiente figura Squidguard está bloqueando todos los sitios para adultos (pornografía).

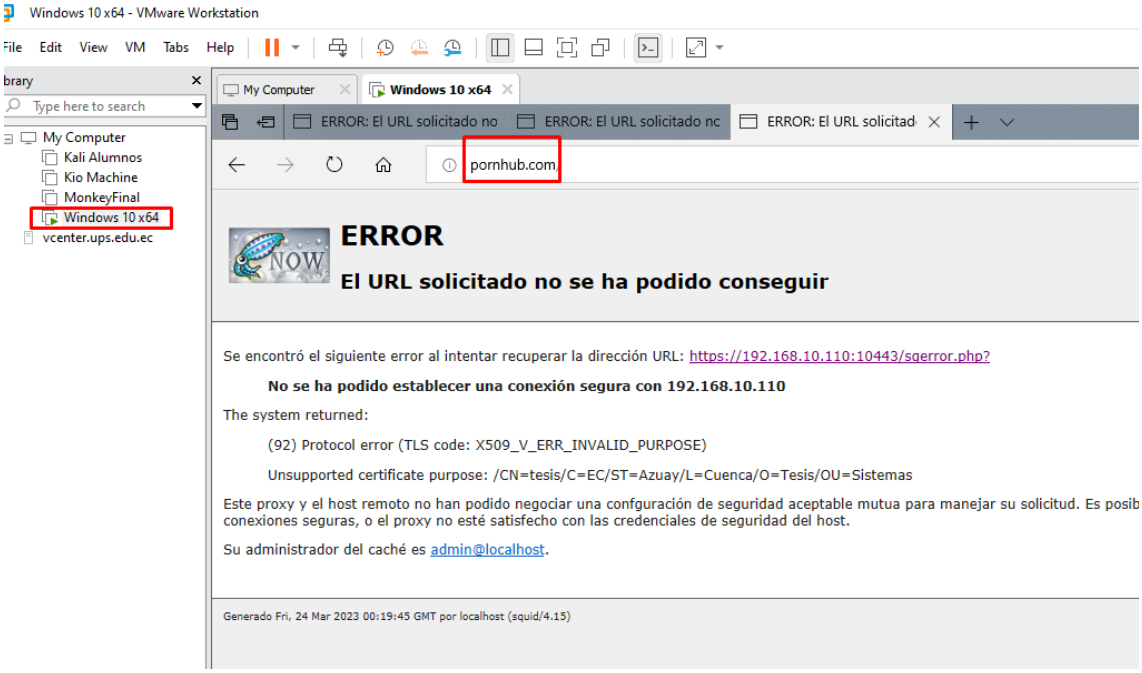
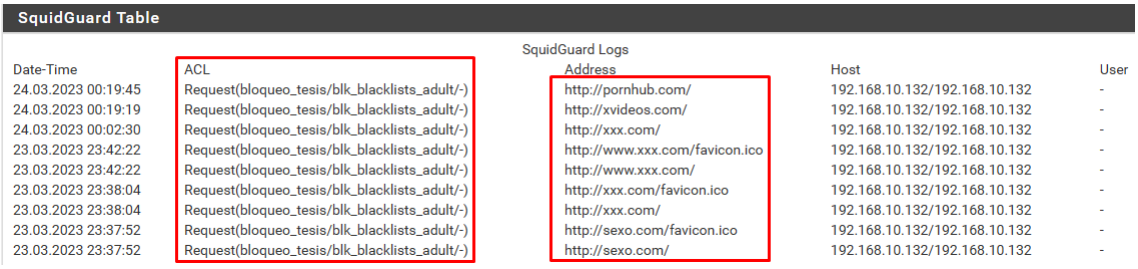


Figura 369. Sitio Web Bloqueado.



Date-Time	ACL	Address	Host	User
24.03.2023 00:19:45	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://pornhub.com/	192.168.10.132/192.168.10.132	-
24.03.2023 00:19:19	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://xvideos.com/	192.168.10.132/192.168.10.132	-
24.03.2023 00:02:30	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://xxx.com/	192.168.10.132/192.168.10.132	-
23.03.2023 23:42:22	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://www.xxx.com/favicon.ico	192.168.10.132/192.168.10.132	-
23.03.2023 23:42:22	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://www.xxx.com/	192.168.10.132/192.168.10.132	-
23.03.2023 23:38:04	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://xxx.com/favicon.ico	192.168.10.132/192.168.10.132	-
23.03.2023 23:38:04	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://xxx.com/	192.168.10.132/192.168.10.132	-
23.03.2023 23:37:52	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://sexo.com/favicon.ico	192.168.10.132/192.168.10.132	-
23.03.2023 23:37:52	Request(bloqueo_tesis/blk_blacklists_adult/-)	http://sexo.com/	192.168.10.132/192.168.10.132	-

Figura 40. Logs de Bloqueos SquidGuard.

CONFIGURACIÓN ANTIVIRUS

Para la configuración del ClamAV antivirus que viene disponible dentro del Squid Proxy Server, se realizará los siguientes pasos, vaya a la página del SQUID Proxy Server, Antivirus como muestra la siguiente figura:

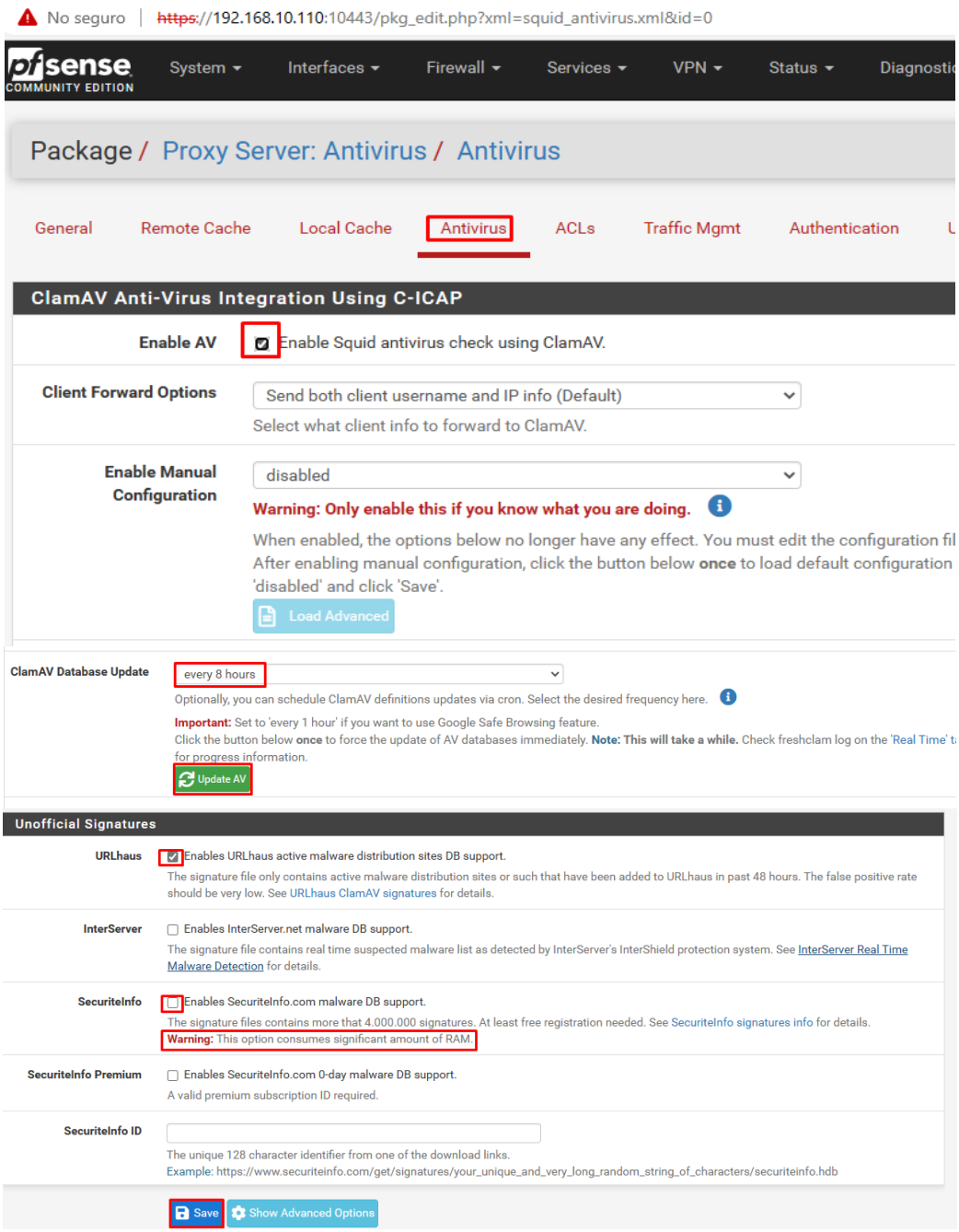


Figura 371. Configuración Antivirus Squid ClamAV.

Dentro de esta página se configuran los siguientes parámetros:

Enable AV: Se selecciona esta opción para activar el antivirus.

ClamAV Database Update: En esta opción se selecciona la frecuencia con la que se desea actualizar la base de datos de firmas de antivirus.

UpdateAV: Con esta opción se actualiza por primera vez la base de datos de firmas de antivirus.

UrlHaus: Es ente apartado tiene varios sitios de definiciones de virus que podrían ayudar a una mejor gestión del análisis de virus, pero tiene sus restricciones o sus avisos en cuanto al consumo de recursos, por lo que se selecciona la primera opción.

Save: Guardar configuraciones, en poco tiempo y se levantará el servicio del Antivirus.

Para revisar el estado de los servicios, se puede realizar lo siguiente:

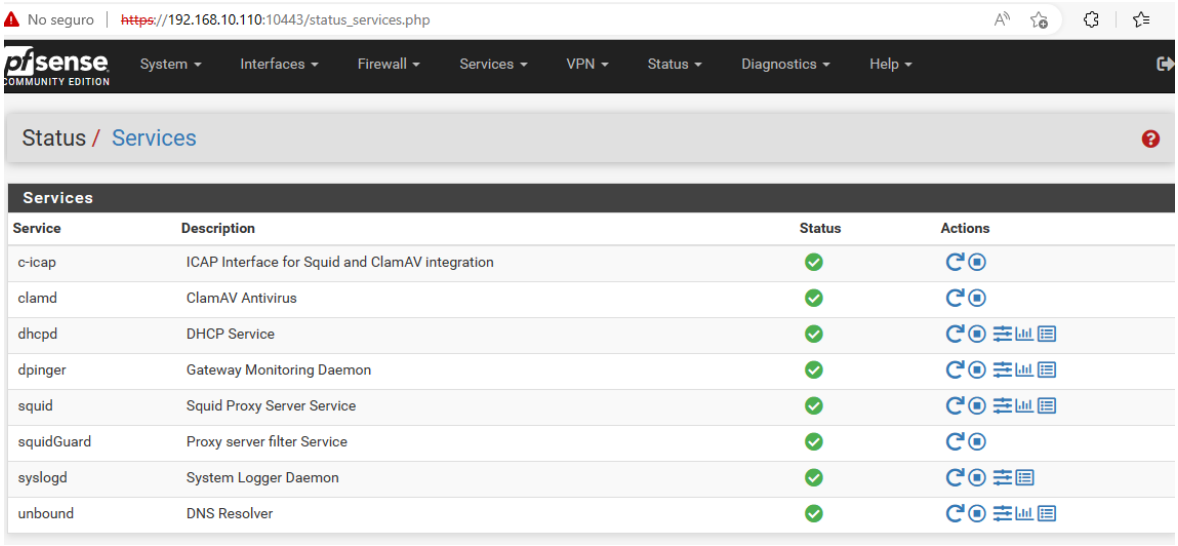


Figura 42. Estado de Servicios.

Una vez verificado que todos los servicios estén funcionando correctamente, realizaremos un test de Detección de Virus en la Web utilizando el archivo de EICAR (European Institute Antivirus Research) test file de la siguiente direccion

(http://www.vsantivirus.com/eicar-test.htm) lo que se hace es intentar descargar el archivo de virus de la primera url disponible (http://www.eicar.org/download/eicar.com). Como se aprecia en la siguiente figura el pfsense con su herramienta antivirus ClamAV realizan el bloqueo (vsantivirus, 2022).

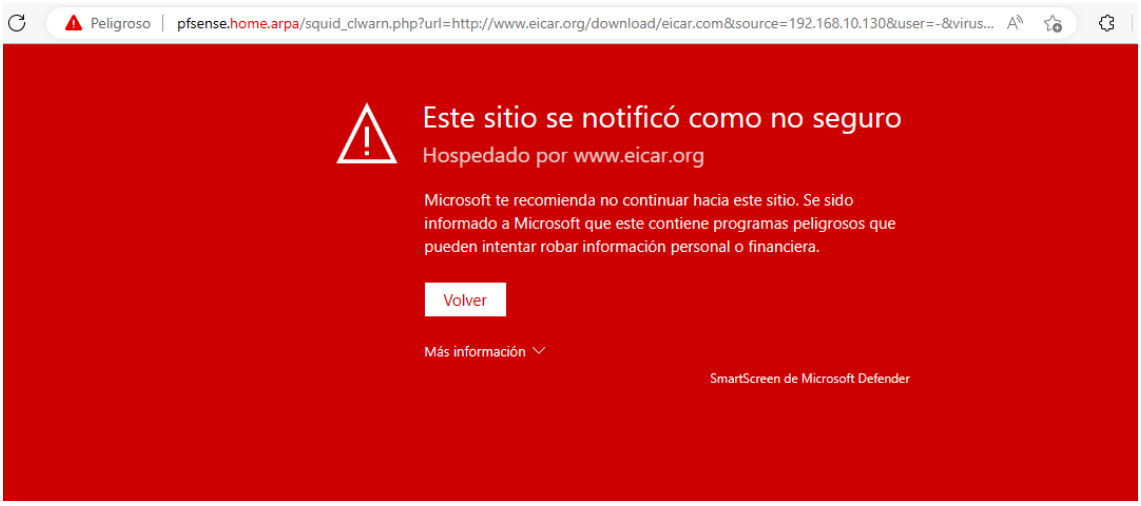


Figura 383. Sitio Web Bloqueado por Antivirus ClamAV.

ANÁLISIS Y PRUEBAS DE RENDIMIENTO

Una vez integrada y aplicada la solución de ciberseguridad durante un periodo de 10 días, en una pequeña empresa como caso real, se encontraron resultados positivos, con un alto nivel de efectividad.

Análisis de resultados de bloqueos mediante Squid Blacklist

Para realizar una restricción de URL se realizó un bloqueo por categorías existentes en SQUID, existen muchas categorías denominadas blacklist de las cuales se seleccionaron seis para las pruebas respectivas (blk_blacklists_malware, blk_blacklists_phishing, blk_blacklists_hacking, blk_blacklists_social_networks, blk_blacklists_adult, blk_blacklists_dangerous_material), a continuación, una lista de todas las categorías existentes:

blk_blacklists_adult	blk_blacklists_dating	blk_blacklists_lingerie
blk_blacklists_sexual_education	blk_blacklists_agressif	blk_blacklists_ddos
blk_blacklists_liste_blanche	blk_blacklists_shopping	blk_blacklists_arjel
blk_blacklists_dialer	blk_blacklists_liste_bu	blk_blacklists_shortener
blk_blacklists_associations_religieuses	blk_blacklists_doh	blk_blacklists_malware
blk_blacklists_social_networks	blk_blacklists_astrology	blk_blacklists_download
blk_blacklists_manga	blk_blacklists_special	blk_blacklists_audio-video
blk_blacklists_drogue	blk_blacklists_marketingware	blk_blacklists_sports
blk_blacklists_bank	blk_blacklists_educational_games	blk_blacklists_mixed_adult
blk_blacklists_stalkerware	blk_blacklists_bitcoin	blk_blacklists_examen_pix
blk_blacklists_mobile-phone	blk_blacklists_strict_redirector	blk_blacklists_blog
blk_blacklists_exceptions_liste_bu	blk_blacklists_phishing	blk_blacklists_strong_redirector
blk_blacklists_celebrity	blk_blacklists_filehosting	blk_blacklists_press
blk_blacklists_translation	blk_blacklists_chat	blk_blacklists_financial
blk_blacklists_publicite	blk_blacklists_tricheur	blk_blacklists_child
blk_blacklists_forums	blk_blacklists_radio	blk_blacklists_update
blk_blacklists_cleaning	blk_blacklists_gambling	blk_blacklists_reaffected
blk_blacklists_vpn	blk_blacklists_cooking	blk_blacklists_games
blk_blacklists_redirector	blk_blacklists_warez	blk_blacklists_cryptojacking
blk_blacklists_hacking	blk_blacklists_remote-control	blk_blacklists_webmail
blk_blacklists_dangerous_material	blk_blacklists_jobsearch	blk_blacklists_sect

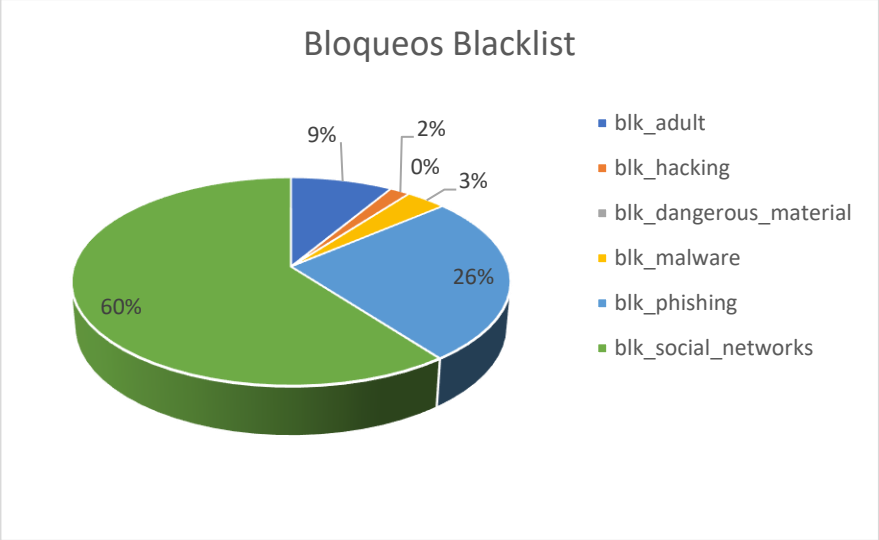


Figura 44. Pruebas de Bloqueo Blacklist.

La efectividad se la puede medir de acuerdo con la acción de bloquear cierto tráfico, sin embargo, dependerá de los datos que contiene las blacklist para definir a un sitio web dentro de cada categoría, existiendo a posibilidad de que algún sitio no se encuentre dentro de una blacklist a pesar de pertenecer a este grupo, en este caso sería necesario agregar el dominio de la URL específicamente.

Análisis de resultados de bloqueos mediante ClamAV Antivirus

Clamav Antivirus es un servicio dentro del Squid Proxy Server él cual está muy bien integrado con pfsense, Este antivirus ayuda con el análisis de páginas que no son seguras y podrían tener alguna complicación con el acceso. Para realizar un análisis de los sitios catalogados como peligrosos se toma en consideración los siguientes criterios: (LBT Cloud, 2020)

- Páginas Peligrosas(pishing).
- El archivo contiene un virus (Download).
- El contenido no es confiable (Virus).
- Páginas visitadas test.

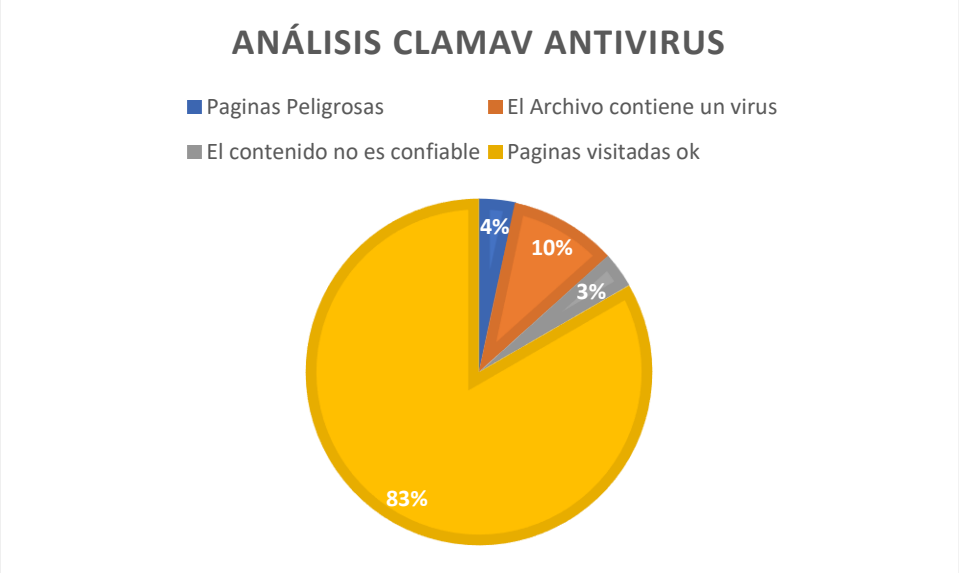


Figura 45. Análisis de Antivirus Clamav.

De acuerdo a la gráfica el riesgo con mayor porcentaje son las descargas y es aquí donde se dan la mayoría de las infecciones de virus desde la web, siendo un factor de riesgo muy alto y probable del día a día.

Gestión de ancho de banda

Una correcta regulación del ancho de banda dentro de una red local siempre es importante para evitar saturación de servicios o cortes por alto consumo de ancho de banda en la red, un equipo puede afectar a los demás usuarios, interrumpiendo las tareas de la empresa, afectando la continuidad del negocio, por lo que es importante evitar al máximo este tipo de riesgos. De igual manera las restricciones de ancho de banda entregaron resultados positivos.

Considerando el tipo de actividades realizadas en la empresa, se recomendó colocar un limitante de velocidad tanto de subida como de bajada de 20 MB para toda la red local, ya que al no ser muchos dispositivos no han tenido la necesidad de la creación de subredes o Vlans, otra opción que tiene la empresa es asignar direcciones IP fijas para los equipos y las restricciones se las podrá crear con asignaciones directas hacia direcciones IP y mantener un registro y control más detallado.

Los equipos mantienen las limitaciones de ancho de banda configuradas, sin superar el valor establecido, sin embargo, los empleados supieron indicar que sintieron lentitud en la red para realizar sus tareas, por lo que se podría considerar

incrementar valores o asignar valores para cada equipo, valores que deben ser discutidos y detallados por la dirección de la empresa.

7. Conclusiones

La ciberseguridad en una empresa siempre será importante considerarla como un factor indispensable para la protección de los activos internos, las herramientas para protección y seguridad informática evolucionan día a día junto con la tecnología, sin embargo los atacantes también buscan nuevas formas de vulnerar la seguridad, dependiendo de la infraestructura que disponga la empresa el trabajo de un atacante será de poca o mucha complejidad, el objetivo de buscar una solución para esto, es aplicar una metodología de seguridad como barrera ante los riesgos informáticos, no debe una empresa exponer su seguridad sin disponer de un método de protección ante las muchas amenazas existentes en la red, para disminuir los riesgos.

Las herramientas de ciberseguridad son creadas por empresas de seguridad con la idea de brindar varias opciones a elegir a las personas encargadas de administrar la seguridad informática de una empresa, considerando el tipo de empresa, usuarios, presupuestos, mercado, etc. Las PYMES son un grupo muy grande existente en Ecuador por lo que es urgente brindar apoyo y conocimiento sobre ciberseguridad para evitar que los atacantes se aprovechen del desconocimiento y la situación vulnerable en la que se pueden encontrar.

Existen muchas herramientas gratuitas que apoyan a la ciberseguridad de hogares y empresas, Pfsense es una herramienta gratuita que cubre estas necesidades, presenta muchos módulos que pueden ayudar para la ciberseguridad a nivel de PYMEs, presenta un grado de efectividad bastante bueno, dependiendo de los parámetros de configuración y las reglas creadas, mismas que se configuran de acuerdo a las políticas internas de las empresas y experticia del administrador, sin embargo los beneficios que nos entrega Pfsense son muy buenos, permitiendo tener un grado de seguridad y saber que ya no se encontrará una empresa totalmente expuesta a la voluntad de los atacantes y riesgos de la web.

Pfsense y todas las herramientas gratuitas de ciberseguridad a más de ser muy útiles para las pequeñas y medianas empresas, brindan un sentido de responsabilidad a los administradores, para que no exista un pretexto de altos costos para no asumir la idea de tener un método de protección activo en sus empresas, concientizando a las personas involucradas en tecnologías de la información y/o personas encargadas de tomar decisiones dentro de una empresa.

Referencias

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos.

Rodríguez Rincón, E. Y. (2018). Metodologías de ingeniería social.

Camacho Nieto, N. A. (2016). Una breve mirada a la ingeniería social (Bachelor's thesis, Universidad Piloto de Colombia).

Trigo, S., Castellote, M., Podestá, A., Ruiz de Angeli, G., Lamperti, S., & Constanzo, B. (2017). Ransomware: seguridad, investigación y tareas forenses.

iso.org. (2021). *ISO EC 27001.* Obtenido de https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top

García, A. A. (2019). Ciberseguridad: ¿ Por qué es importante para todos?. Siglo XXI Editores México.

Callegari, O. (2008). Firewall/Cortafuegos. Revistas negocios de seguridad, 180-184.

Arantón-Areosa, L. (2008). Sobre virus y antivirus... Enfermería Dermatológica, 2(4), 38-41.

INCIBE, (2020), Que son y para qué sirve los SIEM IDS IPS, https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Neira Burneo, S. (2016). Inclusión financiera de las pymes en el Ecuador.

Jurado, F., Yarad, V., & Carrión, J. (2020). Análisis de las características del sector microempresarial en latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. REVISTA CIENTÍFICA ECOCIENCIA, 7(1), 1-26. https://doi.org/10.21855/ecociencia.71.303

Diazgranados, H. (31 de agosto de 2021). latam kaspersky. Obtenido de latam kaspersky: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Hernandez, S., Fernandez, C., & Baptista, L. (2010). *Metodología de la Investigación.* 5th ed. Mexico: MCGraw-Hill Interamericana.

LBT Cloud (2020) Squid, SquidGuard, Lightsquid y Clam-AV en pfSense Parte I - Tech LBT (lobobrothers.com).

Vsantivirus (2002), Pruebe si realmente su antivirus lo está protegiendo, http://www.vsantivirus.com/eicar-test.htm

Pedro Moreno,(2023) PfSense, SquidGuard Shallalist y Su Remplazo dsi.ut-capitole.fr. , https://pmorenoit.blog/2023/01/06/pfsense-squidguard-shallalist-y-su-remplazo-dsi-ut-capitole-fr/