

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

“ESQUEMA DE SEGURIDAD PERIMETRAL APLICABLE A UNA
PYME MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE
LIBRE”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

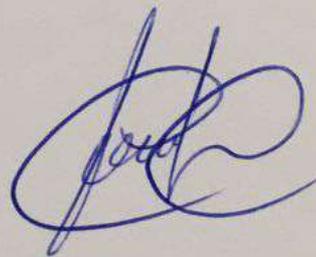
RAÚL JAVIER HONORES QUINDE

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

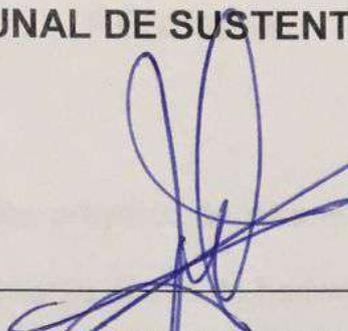
A mi esposa que siempre estuvo respaldándome con su paciencia y comprensión y a mi familia por el apoyo incondicional y los buenos consejos que me supieron dar.

A handwritten signature in blue ink, consisting of several loops and flourishes, positioned at the bottom center of the page.

DEDICATORIA

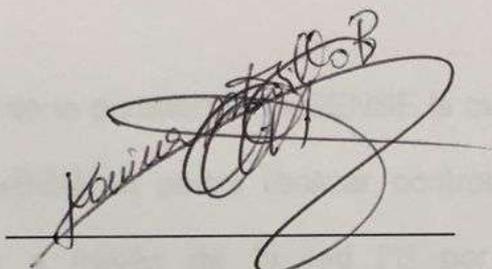
A mi madre por todo lo bueno que ha
hecho por mí.

TRIBUNAL DE SUSTENTACIÓN



ING. LENIN FREIRE

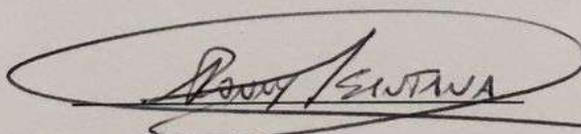
DIRECTOR MSIA



MGS. KARINA ASTUDILLO

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC



MGS. RONNY SANTANA E.

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

RESUMEN

El principal objetivo de este proyecto de esquema de seguridad perimetral aplicable a una PYME mediante el uso de herramientas de software libre es brindar un control y monitoreo en las transferencias de los datos que entran o salen de una empresa por medio del internet.

Con la implementación de la plataforma PFSENSE la cual está basada en el sistema operativo FreeBSD se podrá realizar controles del tráfico de la información que viaja a través de la red [1] por medio de correos electrónicos, almacenamiento en la nube, mensajerías instantáneas o navegadores web, para ello se aplicaran las configuraciones apropiadas que permitan realizar las tareas de monitoreo, bloqueo y restricciones del trafico web con la finalidad de proteger los datos de la institución.

ÍNDICE GENERAL

AGRADECIMIENTO	II
DEDICATORIA	III
TRIBUNAL DE SUSTENTACIÓN	IV
RESUMEN	V
ÍNDICE GENERAL.....	VI
ÍNDICE DE FIGURAS.....	VIII
CAPÍTULO 1.....	1
GENERALIDADES	1
1.1 DESCRIPCIÓN DEL PROBLEMA	1
1.2 SOLUCIÓN PROPUESTA.....	2
CAPÍTULO 2.....	4
DESARROLLO DE LA SOLUCIÓN	4
2.1 ANÁLISIS DE SITUACIÓN ACTUAL	4
2.2 VULNERABILIDADES EN LA TRANSFERENCIA DE DATOS.....	6
2.3 PLATAFORMA DE SEGURIDAD.	7
2.3.1 INSTALACIÓN DE PLATAFORMA.....	9
2.3.2 PUESTA EN MARCHA EN LOS USUARIOS.	11
2.4. TOPOLOGÍA DE RED.	12

2.5 CONFIGURACIÓN DE REGLAS PARA ASEGURAR LA INFORMACIÓN	14
2.5.1 SEGURIDAD DE ACCESO PARA LA PLATAFORMA.....	15
CAPÍTULO 3.....	26
ANÁLISIS DE RESULTADOS.....	26
3.1 PRUEBA DE FILTRADO WEB.	26
3.2 PRUEBAS DE CONEXIÓN.....	26
3.3 MONITOREO DE DATOS.	29
3.4 RESULTADOS OBTENIDOS.....	30
CONCLUSIONES Y RECOMENDACIONES	31
BIBLIOGRAFÍA.....	33

ÍNDICE DE FIGURAS

Figura 2.1. Configuración de las tarjetas WAN y LAN.....	10
Figura 2.2. Pantalla de ingreso de las credenciales.....	11
Figura 2.3. Interfaz de la red LAN en la plataforma PFSense.....	12
Figura 2.4. Topología para asegurar la red.....	13
Figura 2.5. Asignación de puerto seguro para la plataforma.....	16
Figura 2.6. Grupo de equipos a gestionar.....	17
Figura 2.7. Grupo de puertos seguros para internet y PFSense.....	18
Figura 2.8. Grupo de puertos configurados para la NAT.....	19
Figura 2.9. Configuración de reglas para el firewall.....	20
Figura 2.10. Lista de reglas para el firewall.....	21
Figura 2.11. Lista de control de acceso.....	23
Figura 2.12. Configuración del DHCP.....	24
Figura 3.1. Conexión reservada para la maquina Windows Xp.....	27
Figura 3.2. Pruebas de conexión desde Windows Xp.....	27
Figura 3.3. Conexión de puertos permitidos hacia internet.....	28
Figura 3.4. Acceso al PFSense desde afuera.....	29
Figura3.5. Informe de las conexiones y tráfico de red.....	30

INTRODUCCIÓN

Las pequeñas y medianas empresas (PYMES) durante sus actividades cotidianas generan un considerable volumen de información, en su mayoría contienen documentos muy delicados y que requieren de un adecuado tratamiento para que se mantengan intactos y a la vista únicamente del personal autorizado ya que de lo contrario podría repercutir en la fuga de datos y comprometer el normal funcionamiento y crecimiento institucional.

En la actualidad con el avance de la tecnología y la incorporación de equipos tecnológicos como herramienta de trabajo para gestionar la información de las empresas, es necesario que estos sean monitoreados de forma adecuada y permanente para que la información almacenada se pueda conservar intacta para su posterior utilización.

Es necesario que las empresas cuenten con un adecuado esquema de seguridad perimetral básico que les permita estar protegida ante posibles amenazas a la seguridad de la información, tomando en cuenta que el tráfico a través de la red internet cada día se incrementa convierte a este recurso en indispensable para el envío y recepción de la información.

El presente proyecto consiste en un esquema de seguridad basado en una plataforma que efectúa el control y monitoreo del tráfico de la información, mediante la aplicación de una adecuada configuración e implementación de reglas que permitan realizar el control y monitoreo de los datos que viajan por la red con lo cual se incrementara satisfactorios la seguridad perimetral de una red institucional que se encuentre constantemente expuesta a los atacantes, los cuales utilizan herramientas que son cada día más sofisticados y fáciles de utilizar.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

Actualmente con el auge del Internet por la alta demanda y necesidad que tienen las PYMES de estar conectadas a este importante recurso puesto que es indispensable para sus actividades cotidianas, existe también la necesidad de restringir y controlar los datos que entran o salen de una red corporativa.

Con el tráfico de la información que viaja por la red mediante correos electrónicos, mensajerías instantáneas o almacenamiento en la nube, los datos de las empresas quedan expuestos ante posibles ataques los cuales pueden llegar a comprometer seriamente la confidencialidad,

integridad, disponibilidad y la autenticidad de estos al no existir un continuo control y monitoreo.

Entre las comunicaciones cotidianas que se realizan están los envíos de reportes, intercambio de archivos, transferencias bancarias, despacho y recepción de correspondencia, etc. La información que es de vital importancia para la credibilidad y el normal funcionamiento de las actividades cotidianas de una empresa al no estar protegida puede comprometer estos 4 pilares de la seguridad antes de que esta pueda llegar a su legítimo destinatario.

La información que es considerada actualmente como un capital intangible para las empresas e instituciones, no recibe un tratamiento adecuado ya que es tratada y manipulada de forma inapropiada por los usuarios y administradores de red ya que no existen mecanismos de defensa para proteger los equipos que se utilizan para su envío y recepción.

1.2 SOLUCIÓN PROPUESTA

Para mantener la confidencialidad de los datos que viajan por la red se presenta las siguientes soluciones:

Se realizara un esquema de seguridad perimetral mediante el uso de herramientas de software que permita brindar una alta protección de los

datos que entran o salen de la empresa evitando que personas mal intencionadas puedan ocasionar algún tipo de fraude logrando de esta manera proteger los productos y servicios para que estos sean seguros y confiables.

La herramienta de software libre que se propone es PFSENSE, basada en el sistema operativo FreeBSD uno de los sistemas operativos más seguros del mundo, [2] esta herramienta está destinada a cumplir la tarea de un firewall la misma que se adapta considerablemente a las necesidades de una PYME, este producto realiza el filtrado web de manera eficiente permitiendo la restricción del uso de aplicaciones no deseadas lo que facilitara al personal encargado de administrar la red hacer un mejor control y monitoreo del trafico existente [1] con lo cual se podrá brindar una mejor seguridad a la información.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS DE SITUACIÓN ACTUAL

Actualmente las pequeñas y medianas empresas (PYMES) se encuentran involucradas en diversas actividades comerciales entre las cuales podemos citar las empresas agrícolas, ganaderas, camaroneras, bananeras, mineras, comerciales, etc. en su mayoría cuentan con sucursales las cuales pueden estar alejadas entre sí, lo que conlleva a la necesidad de utilizar el internet como una rápida vía para sus comunicaciones permitiendo agilidad en las transferencia o intercambio de información. Con este recurso los usuarios pueden realizar el envío y recepción de reportes, peticiones, intercambio de archivos, transferencias bancarias, despacho y recepción de correspondencia

entre otras tareas relacionadas con el uso de este medio de transporte de datos ya que se ha convertido actualmente en una poderosa herramienta de trabajo.

Las operaciones diarias que consiste en la transferencia permanente de los datos, la realizan los usuarios mediante el uso de sus equipos de trabajo los cuales se encuentran enlazado en red, la información que es destinada a ser enviada pasa libremente a través de un router ya que por lo regular el área de sistemas no cuentan con mecanismos de filtrado de paquetes para realizar un control previo a su envío, es decir no existen las restricciones necesarias para la protección de la información.

La arquitectura en una red de datos de una PYME consiste en topologías de estrella en la cual el acceso a internet se lo realizan a través de un router el mismo que se encuentra enlazado a un switch al cual se interconectan cada uno de los usuarios de la intranet, este tipo de diseño deja muchos huecos de seguridad los cuales en cualquier momento pueden ser aprovechados por personas mal intencionadas que pueden provocar algún evento adverso que pudiera comprometer la confidencialidad de los datos.

Lo único que se realiza en este tipo de diseño con la ayuda de un servidor proxy es la restricción del acceso a ciertas páginas que consumen un considerable ancho de banda, pero esto no es insuficiente

ya que se descuida otra parte importante y fundamental como es el control de los datos institucionales que son enviados por la red hacia las distintas oficinas y sucursales.

En los departamentos de Administración, Financiero, Talento Humano, Marketing se alojan gran cantidad de datos sensibles es por ello que se requiere dar un seguimiento frecuente de la información que utilizan pues de quedar evidenciada por personas no autorizadas podría generar un escenario adverso comprometiendo el avance de la organización.

2.2 VULNERABILIDADES EN LA TRANSFERENCIA DE DATOS

La información que se manipulan en una PYME la cual es necesaria para llevar adelante cada uno de sus procesos se deben manejar con absoluta confidencialidad debido a la importancia de esta ya que los reportes, archivos, correspondencia entre otro documentos que se generan a diario contienen datos críticos y que requieren de un monitoreo adecuado para prevenir que estos lleguen hasta sitios no autorizados, esto nos hace pensar que es necesario un apropiado manejo de la documentación pues de ello depende un crecimiento sostenido de la institucional lo que da como resultado el beneficio y satisfacción de todos los empleados de la corporación.

Una PYME cuenta con departamentos de Marketing, Administración, Contabilidad, Talento Humano, Gerencia, cada una de estas áreas

cuentan con equipos de computación que son provistos del servicio de internet desde el servidor que se encuentra en el área de sistemas, las computadoras de cada usuario reciben el acceso a internet con restricción a ciertas páginas web para mitigar el consumo inapropiado de ancho de banda y evitar la saturación de la red, pero estas medidas quedan limitadas a no estar realizando un monitoreo de la información que entra o sale a la red informática de las empresas a través de algunos medios de envío y recepción como correos electrónicos institucionales, alojamiento de datos en la nube o mensajerías instantáneas que son necesarios y no se puede prescindir de estas herramientas en sus comunicaciones ya que en la actualidad son muy rápidas y permiten un intercambio eficaz de la información.

Es notorio que una PYME se encuentra diariamente en situación de riesgo cuando la información que se envía a diario desde el interior de estas no recibe un monitoreo adecuado por parte del personal de TIC previo a su transferencia, lo mismo sucede con los equipos de los usuarios de red pues no cuentan con mecanismos adecuados de defensa de los datos.

2.3 PLATAFORMA DE SEGURIDAD.

Para el control y monitoreo de los datos que son enviados hacia las distintas sucursales y oficinas principales se ha realizado la implantación

de la plataforma PFSENSE basada en el sistema operativo FreeBSD y que para su instalación requiere pocos recursos de hardware, esta herramienta tiene algunas funciones como las de realizar tareas de un firewall la misma que se adapta considerablemente a las necesidades de una PYME, este producto permite el filtrado web de manera eficiente permitiendo la restricción del uso de aplicaciones no deseadas.

La plataforma es una distribución de software libre y entre sus principales funciones tenemos las siguientes:

- Se puede configurar como Firewall permitiendo y denegando determinado tráfico de la información que entra o sale, así mismo realiza filtrado avanzado de paquetes por protocolos y puertos. [3]
- Realiza redundancia puesto que permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy protocol) en caso de que uno de los cortafuegos se caiga el otro se declara primario. [5]
- Reportes y monitoreo a través de los gráficos RDD se muestra el estado de la Utilización del rendimiento del CPU, Firewall, paquetes enviados y recibidos, manejo de tráfico y ancho de banda. [5]

2.3.1 INSTALACIÓN DE PLATAFORMA

PFSense es una solución muy completa, que esta licenciada bajo BSD lo que significa que es de libre distribución, FreeBSD considerado el sistema operativo más seguro del mundo [4] tiene presente packet filter (PF) (filtro de paquetes sistema de OpenBsd para filtrar el trafico tcp/ip, proporciona además control de ancho de banda y priorización de paquetes.) como estándar desde noviembre de 2004. Cuenta también con la distribución de su propio hardware, estos dispositivos han sido probados en grandes y pequeños entornos de red como el VK-T40E, FW-755, C2758, con esto se simplifica el proceso de seleccionar del hardware adecuado para sus necesidades con la ventaja de contar con un año de soporte para el software PFSense.[3]

El proyecto PFSense es un código abierto adaptado específicamente para uso como cortafuegos y se gestiona en su totalidad mediante interfaz web, además incluye una amplia lista de características relacionadas y un sistema de paquetes que permite más capacidades de expansión.

El software se puede descargar desde su página principal www.pfsense.org, esta plataforma tiene la flexibilidad para ser instalado en una amplia gama de hardware, apoyado en la actualidad por la

arquitectura x86 y x86-64, para soluciones de negocios pequeños o medianos. [1]

La instalación se la realizo de manera virtual con la imagen de PFSense versión 2.2.4 y con una imagen de Windows Xp profesional, para realizar esta práctica es necesario contar con dos tarjetas de red las cuales se utilizaran para ser adaptadas a las conexiones de la WAN con acceso a internet y para la LAN que es la red interna, durante la instalación se cuenta con un asistente el cual nos permite realizar algunas configuraciones previas como son las de asignar las direcciones IP a las dos tarjetas de red, partición y formateo del disco duro, entre otras opciones, es recomendable realizar la instalación de manera predeterminada por cuanto esta se ajusta a la mayoría de las necesidades de una PYME

```

Reloading routing configuration...
DHCPD...

The IP of LAN address has been set to 172.16.20.1/16
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://172.16.20.1/

Press <ENTER> to continue.
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (1386) on pfSense ***

WAN (wan)      -> ae0      -> net: 192.168.2.6/24
LAN (lan)      -> lo0      -> net: 172.16.20.1/16
0) Logout (SSH only)          9) pftop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █

```

Figura 2.1 Configuración de las tarjetas WAN y LAN.

2.3.2 PUESTA EN MARCHA EN LOS USUARIOS.

Cabe señalar que durante la instalación del PFSense se realizaron las configuraciones básicas de las 2 tarjetas de red, para la WAN se asignó la dirección 192.168.2.6/24 con una IP para el Gateway de 192.168.2.1 y para la red interna LAN se asignó la dirección 172.16.20.1/16 con lo cual los administradores podrán acceder al PFSense vía web para luego proceder a realizar las reglas de control y monitoreo de los usuarios de la red corporativa.

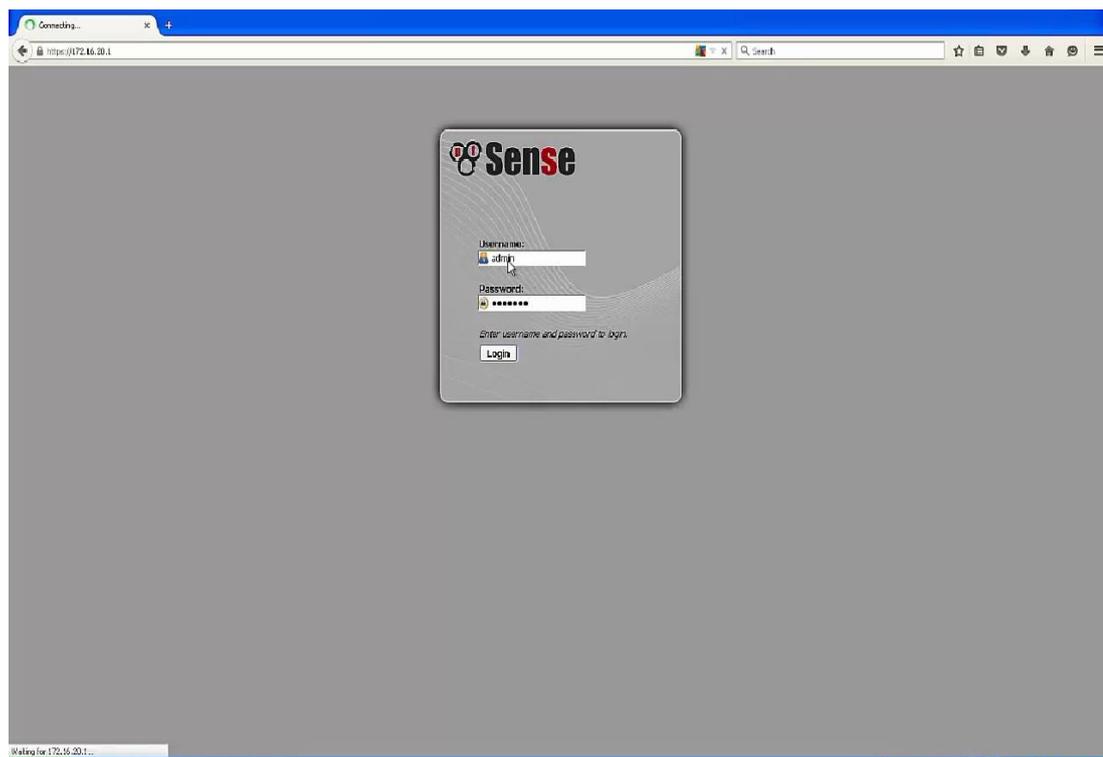


Figura 2.2 Pantalla de Ingreso de las credenciales.

Una vez que se ha terminado con la instalación de la plataforma se tiene que abrir un navegador de internet desde el equipo Xp digitando la

dirección IP 172.16.20.2.1 la cual ha sido reservada para poder ingresar al PFSense, luego de pulsar aceptar aparecerá la pantalla para poder ingresar las credenciales del administrador tal como se muestra en la figura 2.2, la clave viene por defecto y es pfsense en minúsculas la misma que puede ser modificadas por los administradores de la red.



Figura 2.3 Interfaz de la red LAN en la plataforma PFSense.

2.4. TOPOLOGÍA DE RED.

Mediante el análisis que se ha realizado se ha determinado la necesidad de que una PYME reestructure su diseño o topología de red, tomando en cuenta que básicamente toda organización cuenta con datos sensibles alojados en su servidor así también hay que considerar aquellos servicios y recursos de red necesarios para sus actividades normales los cuales deben de tener una puerta que sea la que determine cuál es el trafico permitido desde internet.

Según el escenario planteado la red de una PYME no se encuentra debidamente segmentada, de tal forma que si un atacante logra vulnerar el servidor que se encuentra expuesto al exterior podría este tener los permisos de acceso a la red al igual que un usuario interno, con la posibilidad de ampliar su ataque a los datos críticos alojados en el servidor.

En la topología propuesta se ha dividido la red administrativa en las siguientes áreas: Administración, Asesoría, Planificación, Marketing, Financiero, Dirección de Operaciones, Talento Humano, Gerencia, todas estas áreas cuentan con acceso a Internet y forman parte de la LAN.

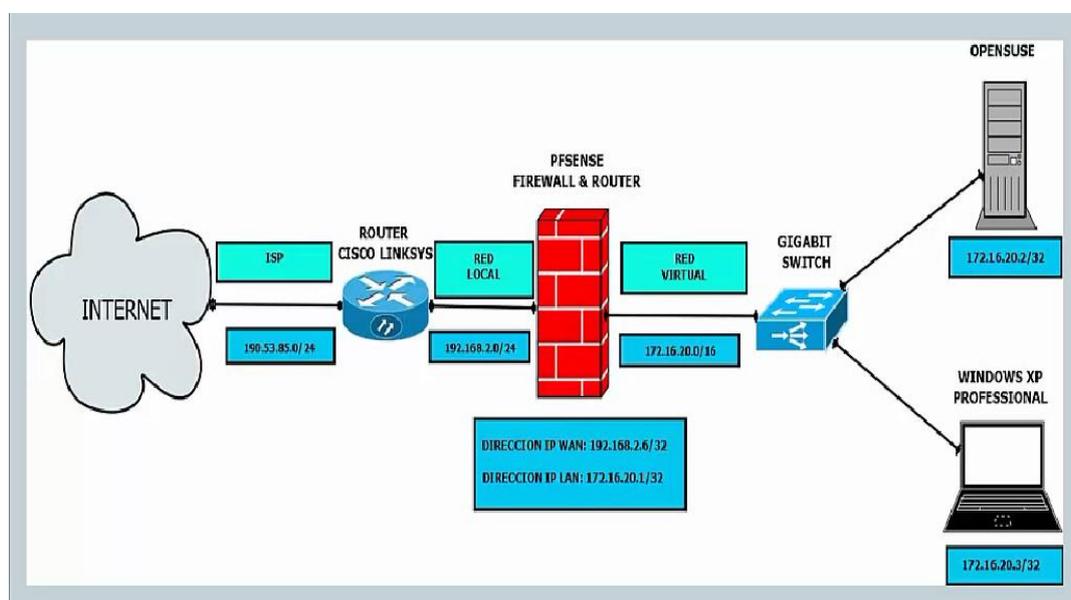


Figura 2.4 Topología para asegurar la Red.

Esta topología cuenta con nuestro Firewall que es el PFSense ubicándolo estratégicamente entre la LAN y la WAN tal como se muestra en la figura 2.4, nos va a servir de perímetro entre ambas conexiones para poder realizar los controles de tráfico requeridos para prevenir posibles ataques a los usuarios y por ende al servidor donde se encuentran alojados los datos sensibles de la institución.

2.5 CONFIGURACIÓN DE REGLAS PARA ASEGURAR LA INFORMACIÓN

Una PYME podría contar con algunos medios, dispositivos o software para su seguridad como son antivirus, servidores proxy, entre otros, los cuales solo sirven para mitigar ciertos males pero no son suficientes para asegurar de mejor manera la red ante posibles ataques a la seguridad de la información.

La finalidad de este proyecto es que a través de la aplicación de reglas apropiadas mediante el uso de la plataforma PFSense poder restringir según sea conveniente, el tráfico de los datos que entran a nuestra red entre las reglas a aplicar podemos citar las siguientes:

- Lo primero que se debe realizar es la creación de los alias, que sirven para crear grupo puertos, grupo de direcciones IP o redes estos alias se utilizan para que las reglas del Firewall sean más flexibles, se debe tener

en cuenta que hay prevalencia de reglas para las que se sitúan por encima de la otra.

- Se debe asignar para los grupos LAN y WAN los puertos que estarán permitidos, usuarios de la LAN estarán permitidos los puertos 53 del DNS, el 80 del HTTP y 443 del HTTPS, el segundo grupo de puertos para la tarjeta WAN van a ser los puertos 443 Y 8080 para darle acceso al computador que utilizar el administrador de la red al sistema del servidor (PFSense).
- Entre las reglas que se van a configurar para el presente trabajo están las de la NAT (Network Address Translation). La cual asigna cuales son los equipos que van a tener salida a internet.
- Para esta práctica se configura las reglas para el DHCP Y DNS

2.5.1 SEGURIDAD DE ACCESO PARA LA PLATAFORMA

Para ello seleccionar la pestaña System luego tendremos una lista de opciones de las cuales elegimos Advanced y se nos mostrara una nueva cinta de opciones de entre ellas damos clic en Admin Access con lo cual podremos ingresar en la caja TCP port el puerto 8080 para brindar mayor protección a nuestro sistema ya que el PFSense trae por defecto habilitado el puerto 443 luego de esto es recomendable que cada cambio que se realiza en la interfaz web sea guardado.

System: Advanced: Admin Access

The changes have been applied successfully. One moment...redirecting to https://172.16.20.1:8080/system_advanced_admin.php in 20 seconds.

Admin Access | Firewall / NAT | Networking | Miscellaneous | System Tunables | Notifications

NOTE: The options on this page are intended for use by advanced users only.

webConfigurator

Protocol: HTTP HTTPS

SSL Certificate: webConfigurator default (55d7006b37c7f8)

TCP port: 8080
Enter a custom port number for the webConfigurator above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes: 2
Enter the number of webConfigurator processes you want to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect: Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

WebGUI Login Autocomplete: Enable webConfigurator or login autocomplete
When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

Figura 2.5 Asignación de puerto seguro para la plataforma.

Otra de las configuraciones iniciales que se realizan es para la NAT, para lo cual se elige la pestaña firewall/NAT, nos desplegamos hasta encontrar la cabecera Network Address Translation y seleccionamos Enable Pure NAT específicamente para nuestro caso pues no voy a usar proxy, en caso de que se desee habilitar el NAT de 1 a 1 también lo pueden realizar desde esta lista de opciones.

2.5.1.1 CONFIGURACIONES DE LOS ALIASES

Los alias nos permite gestionar grupos de puertos así como también grupos de direcciones IP en redes lo que permite que la configuración del cortafuegos sea más limpio y flexible, para comenzar vamos a empezar agregando direcciones IP de equipos conectados a la red, en la figura 2.6 se las puede apreciar la manera en que se realizan estos registros.

The screenshot displays the Mikrotik WinBox interface for configuring Firewall Aliases. At the top, a navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The 'Firewall: Aliases' section is active, showing a red notification bar that reads: "The alias list has been changed. You must apply the changes in order for them to take effect." with an "Apply changes" button. Below this, there are tabs for "IP", "Ports", "URLs", and "All", with "IP" selected. A table lists the following aliases:

Name	Values	Description
Ordenadores	192.168.2.2, 192.168.2.5	Direcciones Ip de Ordenadores
Servidores	192.168.2.3, 192.168.2.4	Direcciones Ip de Servidores Virtuales

Note:
Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

Figura 2.6 Grupo de equipos a gestionar.

Como se manifestó anteriormente dentro de la configuración de los alias se puede configurar un grupo de puertos entre los cuales podremos crear grupos para la navegación a internet otro para poder

dar acceso a mi computadora al sistema PFSense, en la figura 2.7 se puede apreciar la asignación dada al grupo de puertos.

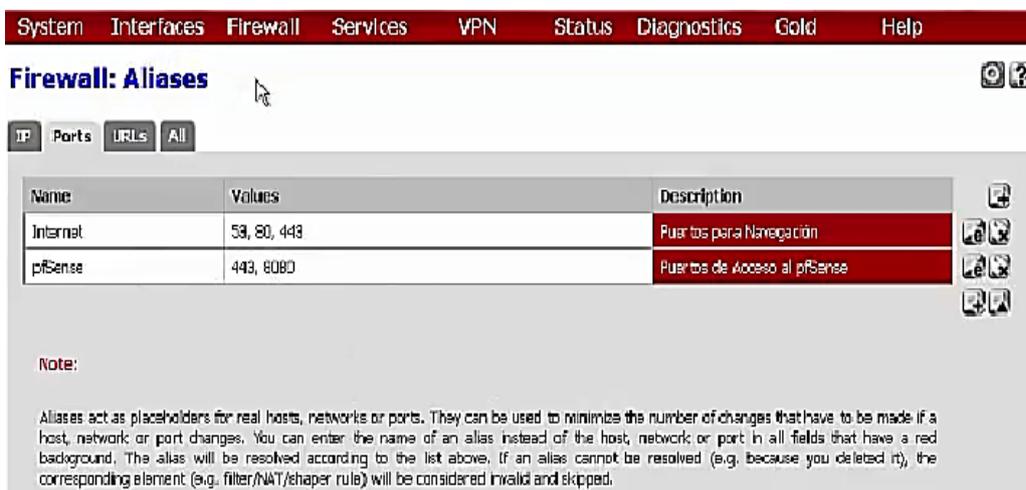


Figura 2.7 Grupo de puertos seguros para internet y PFSense.

2.5.1.2 CONFIGURACIÓN DE LA NAT.

Con la configuración de las reglas de NAT se podrá asignar permisos tales como realizar peticiones o para poder hacer ping por medio de ICMP hacia cualquier destino, estas reglas ya han sido registradas previamente en el aliases y lo que se pretende es que se traduzca cualquier dirección IP dentro de la subred de la LAN hacia la dirección IP de la WAN desde cualquier origen del puerto utilizando los protocolos asignados hacia el destino de dicho puerto y así con el resto de puertos que se han configurado, la figura 2.8 nos muestra lo que se está manifestando.

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Firewall: NAT: Outbound

Port Forward 1:1 Outbound NPt

Mode:

- Automatic outbound NAT rule generation (IPsec passthrough included)
- Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Save

Mappings:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - localhost to WAN
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*	NO	Auto created rule - localhost to WAN
<input type="checkbox"/>	WAN	172.16.0.0/16	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP - LAN to WAN
<input type="checkbox"/>	WAN	172.16.0.0/16	icmp/*	*	icmp/*	WAN address	*	NO	NAT via ICMP
<input type="checkbox"/>	WAN	172.16.0.0/16	tcp/udp/*	*	tcp/udp/53	WAN address	*	NO	NAT via DNS
<input type="checkbox"/>	WAN	172.16.0.0/16	tcp/*	*	tcp/80	WAN address	*	NO	NAT via HTTP
<input type="checkbox"/>	WAN	172.16.0.0/16	tcp/*	*	tcp/443	WAN address	*	NO	NAT via HTTPS

Figura 2.8 Grupo de puertos configurados para la NAT.

2.5.1.3 CONFIGURACIÓN DE REGLAS DEL CORTAFUEGO.

Para configurar las reglas del cortafuegos seleccionamos la pestaña Firewall luego Rules y se nos desplegara una pantalla donde nos encontramos con reglas que vienen predeterminadas, se procede a eliminarlas para de esta manera crear las nuevas reglas y selecciono guardar para que los cambios sean almacenados.

Dentro de la configuración de las reglas del cortafuego es donde voy a utilizar los alias y para continuar con el proceso debemos seleccionar la pestaña LAN del PFSense una vez dentro ya podemos registrar las nuevas reglas entre las cuales tenemos la que permite el acceso de los usuarios a internet a través de los puertos seguros 53, 80 y 443 previamente configurados en el alias, en la figura 2.9 se ilustra esta afirmación.

Firewall: Rules: Edit	
Edit: Firewall rule	
Action	<input type="text" value="Pass"/> <p>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.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="text" value="LAN"/> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<input type="text" value="IPv4"/> Select the Internet Protocol version this rule applies to
Protocol	<input type="text" value="TCP/UDP"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="LAN net"/> Address: <input type="text" value=""/> / <input type="text" value="127"/> <p><input type="button" value="Advanced"/> - Show source port range</p>
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="127"/>
Destination port range	from: <input type="text" value="(other)"/> <input type="text" value="Internet"/> to: <input type="text" value="(other)"/> <input type="text" value="Internet"/> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the &#34;to&#34; field empty if you only want to filter a single port</p>
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything, if you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	<input type="text" value="Conexión hacia al Internet"/> You may enter a description here for your reference.

Figura 2.9 Configuración de reglas para el Firewall.

Una vez que se acepta y se guardan los cambios estos se pueden visualizar en la pantalla siguiente la misma que se muestra de forma automática, en ella se puede pasar el mouse por sobre cada una de las reglas creadas y se mostrara la información correspondiente contenida como son los puertos a los cuales se tienen acceso en donde la figura 2.10 muestra lo que se está manifestado.

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Firewall: Rules

! The firewall rule configuration has been changed. You must apply the changes in order for them to take effect. Apply changes

Floating WAN LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	8080 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	IPV4 ICMP	LAN net	*	*	*	*	none		Conexion via ICMP
<input checked="" type="checkbox"/>	IPV4 TCP,UDP	LAN net	*	*	Internet	*	none		Conexion hacia al Internet

pass
 pass (disabled)

match
 match (disabled)

block
 block (disabled)

log
 log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Puertos para Navegación - 3

Items: 3/3

53	DNS
80	HTTP
443	HTTPS

Figura 2.10 Lista de reglas para el Firewall.

2.5.1.4 CONFIGURACIÓN DEL DNS.

Entre los cambios que se realizan para configurar el servidor DNS está el de seleccionar el DNS Resolver el cual se puede seleccionar desde la interfaz gráfica del PFSense después se asigna el puerto 53, las interfaces que van a escuchar serán LAN Y Localhost, las interfaces de salida también serán LAN y Localhost además hay que habilitar la condiciones del forwarding de lo contrario no se podrá conectar hacia el internet, una vez que se haya realizado estos cambios se procede a guardarlos.

2.5.1.5 LISTAS DE ACCESO.

Para las listas de acceso se escoge el rango de direcciones IP de la LAN 172.16.20.0 con una máscara de 16 bit, con las listas de control de acceso se puede especificar quienes puede pasar por el servidor DNS para el acceso a internet en la figura 2.11 se puede apreciar la creación de la lista de acceso.

The screenshot shows the Mikrotik WinBox interface for configuring DNS Resolver Access Lists. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main title is 'Services: DNS Resolver: Access Lists'. Below the title are tabs for General Settings, Advanced settings, and Access Lists. The 'New Access List' dialog is open, showing the following configuration:

- Access List name:** Red Local
- Action:** Allow (selected from a dropdown menu). Below the dropdown, there is explanatory text: 'Choose what to do with DNS requests that match the criteria specified below. Deny: This action stops queries from hosts within the netblock defined below. Refuse: This action also stops queries from hosts within the netblock defined below, but sends a DNS code REFUSED error message back to the client. Allow: This action allows queries from hosts within the netblock defined below. Allow Snoop: This action allows recursive and nonrecursive access from hosts within the netblock defined below. Used for cache snooping and ideally should only be configured for your administrative host.'
- Networks:** A table with columns for Network, CIDR, and Description. One entry is visible: Network: 172.16.20.0, CIDR: 16, Description: LAN.
- Description:** Red Local. Below the text box, it says 'You may enter a description here for your reference.'

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Figura 2.11 Lista de control de acceso.

2.5.1.6 SERVIDOR DHCP.

Habilitamos el servidor DHCP para la LAN en donde la subred es la 172.16.0.0 con una máscara de red es de 255.255.0.0 y el rango disponible que va desde la 172.16.20.10 hasta la 172.16.255.245 el cual se ha decidido dejarlo por defecto, los DNS Server serán los servidores de Google, el Gateway es la dirección IP de la LAN y tendrá asignada la IP de 172.16.20.1, la figura 2.12 muestra la configuración de DHCP.

<input type="checkbox"/> Deny unknown clients If this is checked, only the clients defined below will get DHCP leases from this server.							
Subnet	172.16.0.0						
Subnet mask	255.255.0.0						
Available range	172.16.0.1 - 172.16.255.254						
Range	<input type="text" value="172.16.20.10"/> to <input type="text" value="172.16.255.245"/>						
Additional Pools	If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here. <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th>Pool Start</th> <th>Pool End</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Pool Start	Pool End	Description	<input type="text"/>	<input type="text"/>	<input type="text"/>
Pool Start	Pool End	Description					
<input type="text"/>	<input type="text"/>	<input type="text"/>					
WINS servers	<input type="text"/> <input type="text"/>						
DNS servers	<input type="text" value="8.8.8.8"/> <input type="text" value="8.8.4.4"/> <input type="text"/> <input type="text"/> <p><small>NOTE: Leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.</small></p>						
Gateway	<input type="text" value="172.16.20.1"/> <small>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network. Type "none" for no gateway assignment.</small>						
Domain name	<input type="text"/> <small>The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.</small>						
Domain search list	<input type="text"/> <small>The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.</small>						
Default lease time	<input type="text"/> seconds <small>This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.</small>						
Maximum lease time	<input type="text"/> seconds <small>This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.</small>						
Fallover peer IP:	<input type="text"/> <small>Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's</small>						

Figura 2.12 Configuración del DHCP.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 PRUEBA DE FILTRADO WEB.

La plataforma Pfsense ha comprobado el tráfico web aplicando los distintos filtros de navegación, en la figura 3.4 se puede apreciar la lista de conexiones entrantes y salientes, de detectarse alguna actividad no autorizada por las reglas que se ha configurado en nuestra plataforma este tráfico será automáticamente rechazado por nuestro firewall.

Única y exclusivamente se podrá tener acceso a los recursos de red a través de los puertos que fueron habilitados durante las reglas que se realizaron en el Firewall PFSense, tal es el caso de los puertos 53, 80, 443, los cuales fueron asignados para que los usuarios tengan salida a través de estos, en el caso de los equipos donde se va a realizar el

control y monitores por medio de la plataforma de seguridad se ha habilitado los puertos 8080 y 443 para una conexión más segura.

3.2 PRUEBAS DE CONEXIÓN

Se desea primeramente comprobar la conexión de los ordenadores al PFSense para lo cual hay que habilitar la WAN mediante las reglas de Firewall tal como se lo realizan con la LAN, entre estas configuraciones tenemos que la interfaz es la WAN, la versión del TCP/IP es la IPV4, el protocolo será TCP, el origen es single host or alias para el caso de los ordenadores, el destino va a ser el mismo firewall y los puertos destinos van a ser pfsense los mismos que ya fueron configurados en las reglas de los alias, una vez efectuado estos cambios procedemos a guardarlos.

También debemos habilitar la máquina que se va a conectar con el PFSense, está ya tiene una IP fija según el esquema de la topología propuesta la cual es la 172.16.20.3 para ello hay que seleccionar el DHCP Leases que se encuentra dentro de la opción Status luego capturar la MAC address de la conexión de red, y la ingresamos en el DHCP edit static finalmente se guardan los cambios y ya tendremos reservada la dirección IP para la máquina Windows Xp.

DHCP Static Mappings for this interface.				
Static ARP	MAC address	IP address	Hostname	Description
	00:0c:29:d9:1f:02	172.16.20.3	winxp	

Figura 3.1. Conexión reservada para la maquina Windows XP.

Una vez que hemos terminado la configuración abrimos una consola dentro de nuestro Windows Xp para hacer la prueba hay que reiniciar la conexión con `ipconfig /release`, luego limpiamos el cache DNS con el comando `ipconfig /flushdns` para verificar que se ha logrado establecer las conexiones esto se lo puede visualizar en la figura 3.3, para ello hay que verificar que me pueda conectar desde afuera es decir desde mi computadora al servidor Firewall del PFSense, esto nos muestra que las máquinas están funcionando correctamente.

```

C:\>ipconfig /release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.

C:\>ipconfig /renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  : = local.local
    IP Address . . . . . : 172.16.20.3
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 172.16.20.1

C:\>_

```

Figura 3.2. Pruebas de conexión desde Windows XP.

La siguiente configuración es para que los ordenadores por medio de los puertos 443 y 8080 se puedan conectar al Firewall.

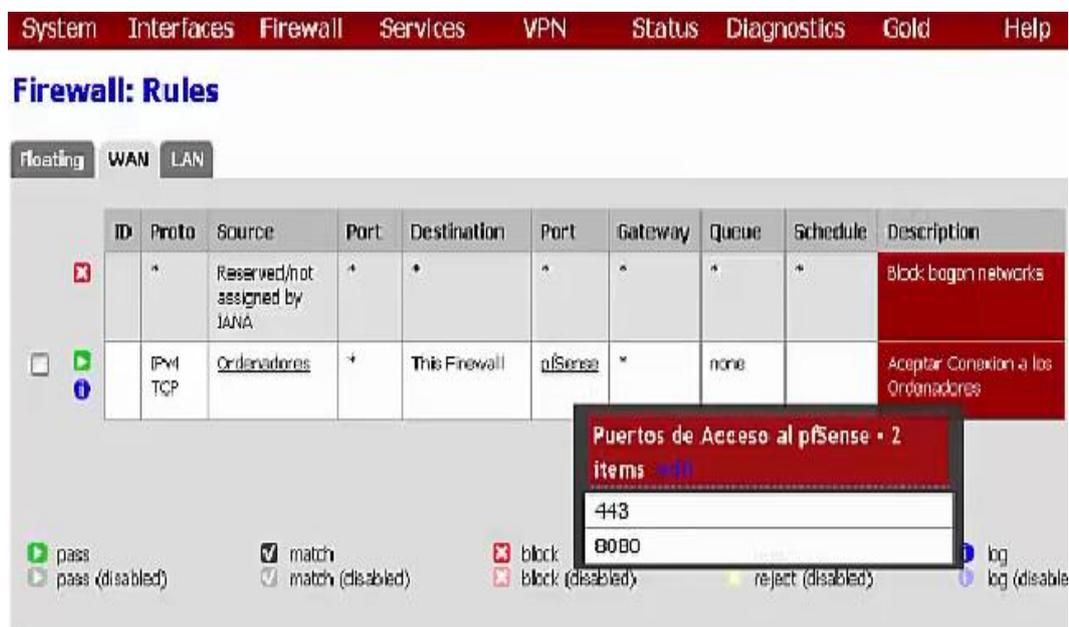


Figura 3.3. Conexión de puertos permitidos hacia internet.

En la siguiente prueba vamos a verificar la conexión al Firewall desde afuera, abriendo un navegador web e ingresando la dirección `https://fw1.remnd.local:8080` que son los parámetros que se configuraron durante el proceso de asignación de reglas con las opciones del PFSense, la figura 3.4 muestra la interfaz para poder ingresar las credenciales el acceso que se obtiene.

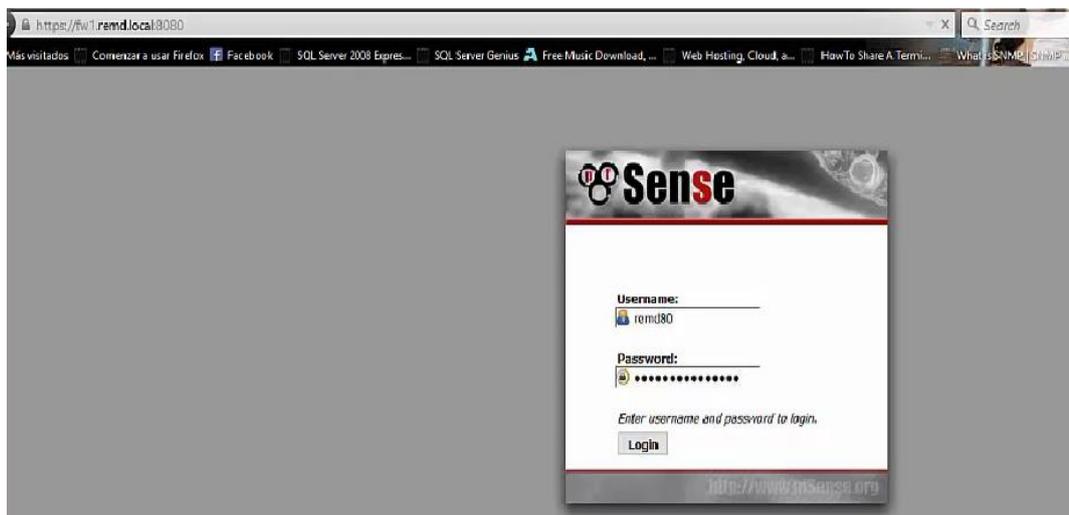


Figura 3.4 Acceso al PFSense desde afuera.

3.3 MONITOREO DE DATOS.

A través del menú se pueden agregar Widgets los cuales sirven para ver más información de la funcionalidad del servidor PFSense, como son las interfaces, los registros del firewall, lo que se está bloqueando, lo que se está accediendo, los servicios como el DHCP el NTPD, APINGER, el DNS, además cuenta con una tabla de grafico donde se puede ver el ancho de banda entrante y saliente.

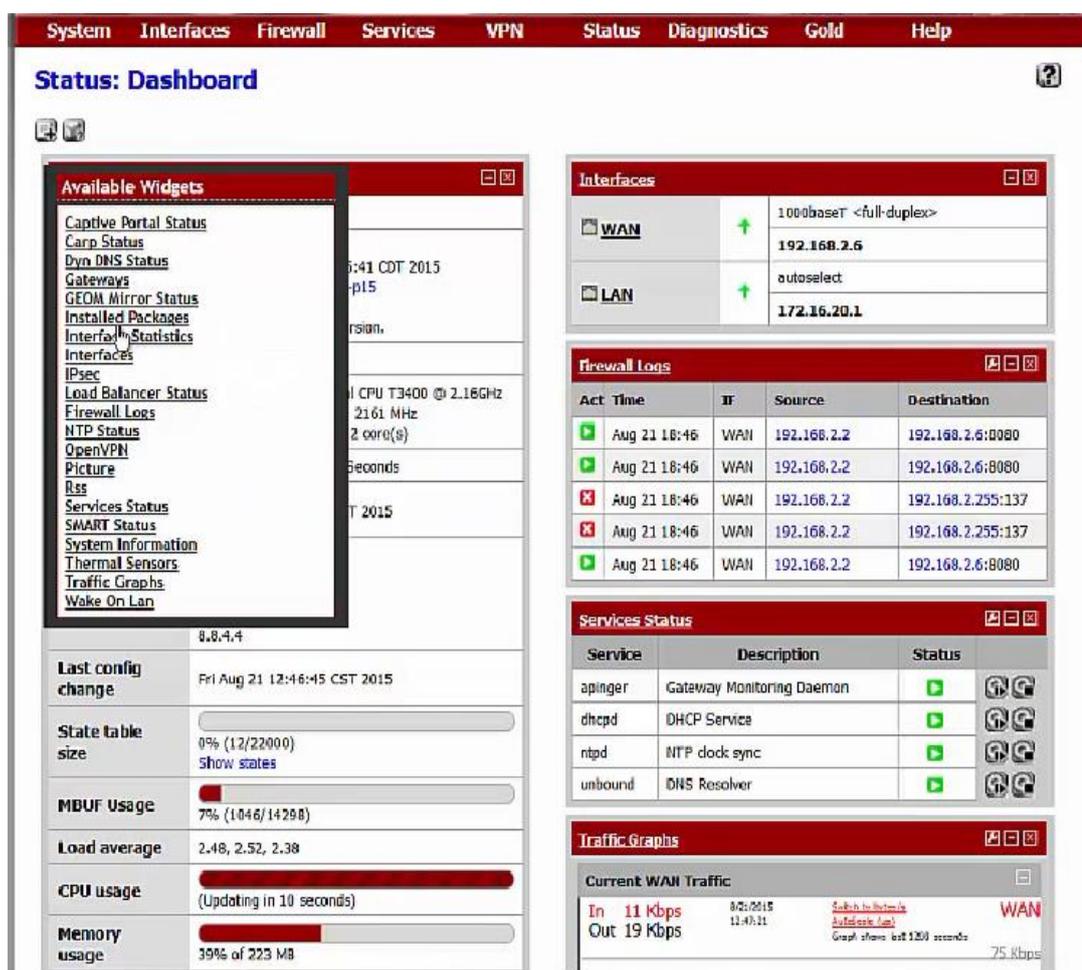


Figura 3.5 Informe de las conexiones y tráfico de red

3.4 RESULTADOS OBTENIDOS

La plataforma nos brinda información mediante la tabla de estado, entre la información y los resultados que nos da el Firewall PFSense esta el reporte del tráfico de la red además las conexiones abiertas y establecidas, aquí también se pueden observar los puertos que fueron asignados a la interfaces de la WAN así como también a la LAN, incluso se puede visualizar los servicios y protocolos que esta habilitados.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La Plataforma PFSense basada en el sistema operativo FreeBSD ha sido de mucha ayuda para el control y monitoreo del tráfico de los datos que entran o salen de una PYME lo que conlleva a que la información crítica este mejor protegida ante posibles ataques que pudieran provocar la alteración o pérdida de la información.
2. El acceso al internet mediante una WAN es indispensable para las operaciones cotidianas de una organización pues se la realiza de manera frecuente para cubrir las necesidades en cuanto a las transferencias de los datos, esto supone el interés en los administradores ya que es de mucha importancia controlar el acceso hacia ellas.
3. El uso de firewall es un mecanismo de defensa perimetral que nos permite establecer reglas para controlar y establecer permisos sobre la

autorización o no de los datos que entran o salen de una red, hoy en día la tecnología avanza y gracias a esto resulta relativamente asequible para las pequeñas y medianas empresas contar con muy buenos sistemas de seguridad sin necesidad de recurrir a la adquisición de costosos equipos.

RECOMENDACIONES

1. Se recomienda a los administradores de red realizar respaldos de la información antes de realizar algún cambio en la configuración de las reglas de seguridad del Firewall.
2. Se recomienda realizar la suscripción para recibir soporte de software puesto que el PFSense es una poderosa herramienta que tiene una amplia gama de servicios los cuales no se los ha comprobado en este trabajo.
3. Se recomienda utilizar políticas DLP para incrementar el abanico de funcionalidades con las que cuenta la plataforma.
4. Es conveniente realizar la optimización en los segmentos de red para evitar direcciones no permitidas con esto se lograría incrementar la seguridad que proporciona el firewall.

BIBLIOGRAFÍA

[1]Sense, OpenSourceSeguridad, <https://www.pfsense.org/getting-started>,

fecha de consulta agosto del 2015

[2]FreeBSD, About FreeBSD's Technological Advances,

<https://www.freebsd.org/features.html>, fecha de consulta Septiembre del 2015

[3]Sense, OpenSourceSeguridad, <https://www.pfsense.org/products>, fecha de

consulta de noviembre del 2015

[4]FreeBSD, The FreeBSD Project, <https://www.freebsd.org/>, fecha de

consulta noviembre del 2015, página 263

[5]Sense, Latest Stable Version (Community Edition),

<https://www.pfsense.org/download/>, fecha de consulta Diciembre del 2015