IMPLEMENTACIÓN DE SEGURIDAD EN LA MIGRACIÓN DE SERVIDORES CON SOFTWARE DE LICENCIA A SOFTWARE LIBRE

IMPLEMENTATION OF SECURITY IN THE MIGRATION OF SERVERS WITH LICENSED SOFTWARE TO FREE SOFTWARE

Diego Javier Bastidas Logroño [1*]

[1] Escuela Superior Politécnica de Chimborazo, Espoch Sede Orellana. Ecuador. ORCID: https://orcid.org/0000-0003-3924-7468. Correo: diego.bastidas@espoch.edu.ec.

Myriam Valeria Ruiz Salgado [2]

[2] Escuela Superior Politécnica de Chimborazo, Espoch Sede Orellana. Ecuador. ORCID: https://orcid.org/0000-0002-5180-9542. Correo: myriam.ruiz@espoch.edu.ec

Diego Omar Guilcapi Lunavictoria[3]

[3] Ministerio de Educación, Loreto - Orellana. Ecuador. ORCID: https://orcid.org/0009-0001-4550-1736. Correo: omardiego2106@hotmail.com

William Bladimir Cevallos Cevallos [4]

[4] Escuela Superior Politécnica de Chimborazo, Espoch Sede Orellana. Ecuador. ORCID: https://orcid.org/0000-0003-3924-7468. Correo: wcevallos@espoch.edu.ec

*** Autor para correspondencia:** diego.bastidas@espoch.edu.ec

Resumen

Se escribe este estudio enfocándonos en los principales problemas de seguridad de los protocolos TCP/IP junto con la implementación de tres servicios principales: Firewall, Servidor de Archivos y Correo Electrónico. Debido a que se han encontrado muchas vulnerabilidades en varios entornos de red con software con licencia y de ésta manera dar solución a los problemas de seguridad, conectividad y comunicación de la red de datos tomando como caso práctico la red de la Dirección Provincial de Salud de Chimborazo migrando el software del servidor a open source, enfocándonos los principales problemas de funcionamiento y seguridad de los protocolos pertenecientes a la capa de red, internet, transporte y aplicación del modelo en la intranet, los que una vez evidenciados, sirvieron para hacer la reingeniería de la topología de red.

Palabras clave: Servidores con Open Source; Software Pfsence; Intranet.

Abstract

This study is written focusing on the main security problems of TCP / IP protocols along with the implementation of three main services: Firewall, File Server and Email. Due to the fact that many vulnerabilities have been found in various network environments with licensed software and in this way provide solutions to the security, connectivity and communication problems of the data network taking as a practical case the network of the Provincial Health Directorate of Chimborazo, focusing on the main problems of operation and security of the protocols belonging to the network layer, internet, transport and application of the model on the intranet, which, once evidenced, served to reengineer the network topology.

Keywords: *Servers with Open Source; Software Pfsence; Intranet*

Fecha de recibido: 08/03/2022
Fecha de aceptado: 01/05/2023
Fecha de publicado: 03/05/2023

Introducción

Este trabajo pretende analizar los aspectos pertinentes a la seguridad de la familia de protocolos TCP/IP, así como de los servicios que se establecen típicamente sobre esta pila de protocolos, tomando como caso práctico la red de datos de la Dirección Provincial de Salud de Chimborazo – Ecuador (DPSCH) realizando una migración del servidor con software con licencia a software libre con CEntOs.

Hoy en día, el uso de TCP/IP se ha extendido prácticamente a la totalidad de las redes de comunicaciones de datos, potenciado fundamentalmente por la expansión de Internet, así como de las redes corporativas y de cooperación asociadas a esta tecnología: Intranets y Extranet. Habitualmente el diseño de las redes se basaba en características como la funcionalidad o la eficiencia, pero no en la seguridad; condiciones que son rentables desde un punto de vista de negocio a corto plazo, pero que pueden resultar caras a largo (Rodríguez, Castro, Gonzalez, Baque, & Tarragó, 2021; Rodríguez, Lucas, Mero, Pisco, & Castro, 2022; Rodríguez, Tarragó, Gálvez, & Pisco, 2020). Para la realización del análisis y diseño de una red segura es necesario conocer los detalles y características de los protocolos de comunicaciones subyacentes, que serán los encargados de transportar la información y datos que desean distribuirse (Cochran, 2012).

A su vez, deberán analizarse los servicios que se proporcionan en dicha red y sus detalles de funcionamiento. La información existente hoy en día, tanto en la bibliografía tradicional (libros, revistas, artículos técnicos.) como en la propia Internet (páginas Web, listas de correo, grupos de noticias, etc.) respecto al tema genérico abordado en este documento, "La Seguridad Informática", así como de las vulnerabilidades y protecciones asociadas, es realmente extensa (Álava, Rodríguez, & Ávila, 2022a, 2022b)..

Materiales y métodos

Se empleó el método de investigación exploratorio para reunir toda la información sobre migración de servidores Windows a CEntOs; y el método experimental para probar el proyecto de migración de servidores

Windows a Linux en base a casos prácticos de estudio (experimentos), se analizará los resultados y los mismos serán difundidos al mundo.
Se emplearán técnicas de la investigación:

- Observación: Se observará las diferentes plantillas web en la red de redes libres para descargar.
- Experimentación: Se probará las diferentes metodologías agiles de desarrollo web.

Generalización: Se sugiere aplicar esta investigación a nivel internacional tomando como muestra inicial la intranet de la Dirección Provincial de Salud de Chimborazo.

Población: Todo el personal con acceso a una computadora tomando como referencia a Santo Domingo.

Muestra: La muestra queda delimitada realizando el cálculo correspondiente para la observación por medio de Encuestas. Para la implementación del firewall en la migración de servidores con software de licencia a software libre, se aplicará la encuesta a 63 usuarios.

Procedimientos seguidos para implementar y recuperar toda la infraestructura
Los siguientes componentes, describen, a modo de manual, los procedimientos seguidos para implementar y recuperar toda la infraestructura. Están referenciados, ya que se hace mención a ellos desde la documentación de proyecto.

1. Configuración de VLANs en Switchs

El siguiente procedimiento describe la configuración final de los dos Switchs Cisco Catalyst 2900 que discpone la institución. Para ello se utilizó los siguientes comandos para la creación y asignación de VLANs a un puerto específico del swtich:

```
Switch#vlan database (crear la base de datos para la vlan)
Switch(vlan)#vlan vlan_number (crea una vlan)
Switch(vlan)#exit
Switch(config)#interface fastethernet 0/X (entramos a una inter)
Switch(config)#encapsulation dot1q
Switch(config-if)#switchport access vlan vlan_number (asigna Vla
Switch(config-if#end
```

Para los respectivos enlaces trocales, se utilizó los siguientes comandos:

```
sw(Config.)#interafce fastethernet 0/X
sw(Config-if)#switchport mode trunk
```

Aplicado todos estos comandos a la configuración requerida para cada uno de los swtich, nos quedarían configuradas las vlans de la siguiente forma.

Switch 1

```
Switch#show vlan
VLAN Name                              Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active
101  SERVIDORES                       active    Fa0/2
102  I_hosts_A                        active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                                Fa0/11, Fa0/17
103  I_hosts_B                        active    Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                                                Fa0/16, Fa0/18, Fa0/19, Fa0/20,
                                                Fa0/21, Fa0/22, Fa0/23
104  I_hosts_C                        active
106  I_hosts_W                        active
Switch#show run
…
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
…
```

Switch 2

```
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
101  servidor                         active
102  I_hosts_A                        active    Fa0/6, Fa0/16
103  I_hosts_B                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9,
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13,
                                                Fa0/15, Fa0/18, Fa0/21
104  I_hosts_C                        active    Fa0/14, Fa0/19, Fa0/20
106  I_hosts_W                        active    Fa0/22,Fa0/23
Switch#show run
…
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!…
```

Una vez terminadas las configuraciones para ambos switch, ya se encuentra lista nuestra red, dividida de forma lógica y ahora se podrá configurar el firewall.

2. Instalación y configuración básica de pfSense

El siguiente procedimiento describe los pasos para instalar pfSense en un equipo de manera permanente y los pasos iniciales para que el sistema sea funcional. Los requisitos son un equipo estándar con arquitectura PC y diversas tarjetas de red, del cual se borrarán todos los datos del disco duro. Antes de preparar la instalación se debe descargar de la página web (www.pfsense.org) oficial el fichero ISO (imagen de un CD) de la última versión estable de pfSense, en este caso la versión 1.2.3. Una vez descargado se graba el fichero ISO en un CD-ROM convencional, con el que se hará la instalación del sistema.

El proceso de instalación es similar a las versiones más actuales de Linux. Carga directamente el sistema plenamente funcional en la memoria RAM del ordenador. Una vez que el sistema está cargado se puede volcar al disco duro o configurarse como un sistema normal (de manera volátil: al reiniciarse el sistema se perdería toda la configuración). Una vez preparado el disco de instalación, se procede a iniciar el sistema arrancando desde el disco (estas opciones dependen del propio equipo). Aparece el menú de arranque:

Figura 1 FreeBSD.

En el menú anterior, se selecciona la primera opción: arranque normal. Esto empezará a detectar el hardware del equipo y a configurar todos los controladores. el siguiente paso es la configuración de los dispositivos de red .Pese a que se pueda realizar toda la configuración de la topología de red a través del siguiente menú, se recomienda configurar solo las interfaces de red LAN y WAN, para posteriormente hacer la configuración más detallada. Lo primero que pregunta es acerca de configurar VLANs (Redes Virtuales), que es caso de seleccionar que no, asignará interfaces de red directamente.

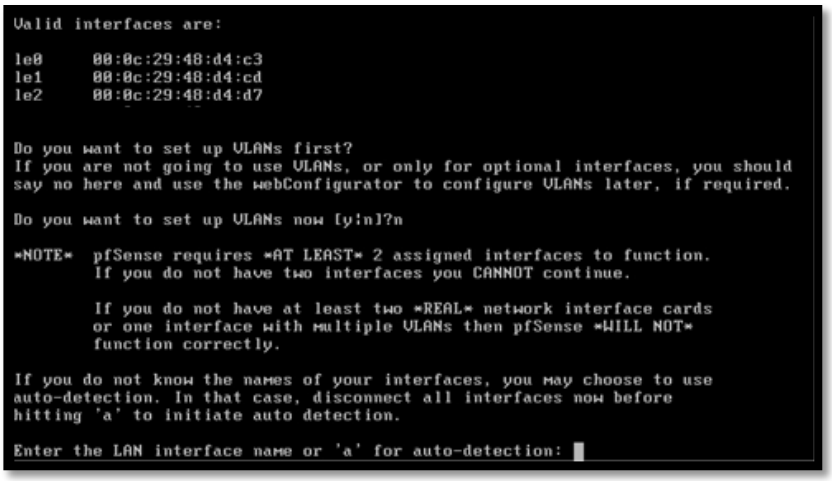

Figura 2. Configuración Consola.

Para la instalación de pfSense se accederá a la consola de administración del servidor, en modo texto. Allí se selecciona la opción ’99) Install pfSense to a hard drive/memory drive, etc’:

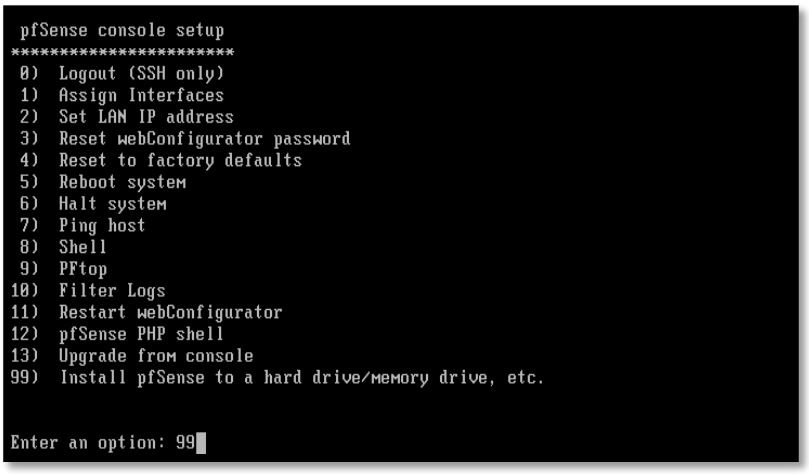

Figura 3. Instalación Pfsence.

Hay que destacar que pfSense está diseñado para trabajar en sistemas con discos duros pequeños, Generalmente con tecnología flash (usando tarjetas de memoria convencionales como discos duros). El asistente de configuración de disco, si se seleccionan todas las opciones por defecto, usará por completo el disco duro del sistema (o el disco duro que se seleccione en el asistente, en el caso de disponer de más de uno). No tiene mucho sentido que no sea así, al ser pfSense una distribución destinada únicamente a trabajar como firewall y router. Dado que el asistente es muy sencillo y permite pocas opciones de configuración, no se muestra ninguna imagen del mismo. Terminada la instalación, se reinicia el sistema y nos mostrará la ventana de configuración y administración en modo consola donde podemos seguir trabajando. Una vez seleccionadas las interfaces, el sistema arranca y presenta la consola de configuración y administración de

pfSense, desde donde se asignarán las direcciones IP de las redes configuradas para poder acceder por web al sistema. Para ello, en el menú de la imagen siguiente, se selecciona la opción '2) Set LAN IP address'.

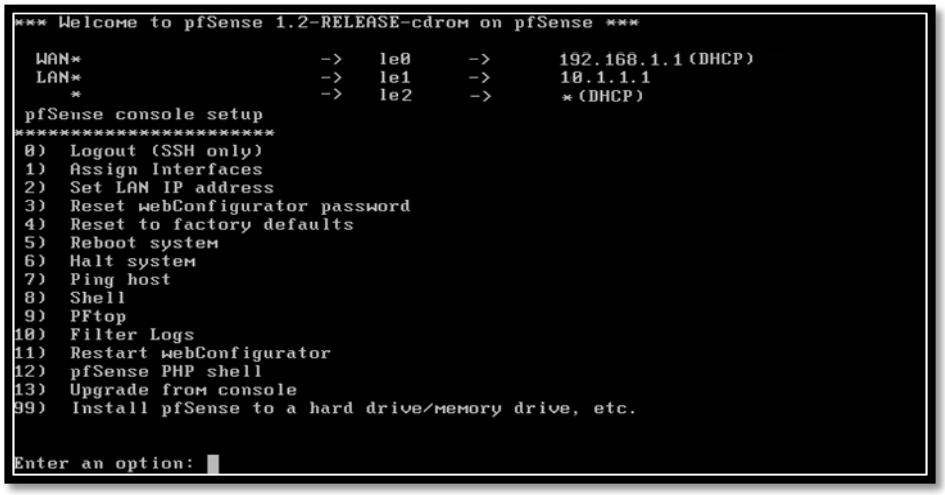

Figura 4. Menú Pfsence

Desde otra máquina conectada al mismo segmento de red que la LAN se accede a través de un navegador web a la dirección de la LAN del firewall. El sistema pide autenticación de usuario y contraseña que por defecto son usuario 'admin' y contraseña 'pfsense'. Al no haber una configuración inicial aparece un asistente, en el primero se configuran los datos de nombre de host, dominio y direcciones DNS.

Figura 5. Claves Pfsence.

El siguiente cuadro, trata la configuración de la interfaz WAN del sistema, que el caso concreto será una dirección IP, pero se puede configurar para acceder a través de ciertos módems de conexión por acceso remoto. El cuadro de configuración es el siguiente:

Figura 6. Conexión remota.

El siguiente paso es la configuración de la interfaz LAN (aquí únicamente se tratará la dirección IP y la máscara de red).

Figura 7. Máscara de red.

Una vez finalizada la configuración y después de introducir las nuevas credenciales de autenticación (usuario y contraseña especificada en el asistente de configuración) aparecerá la consola web de administración de pfSense:

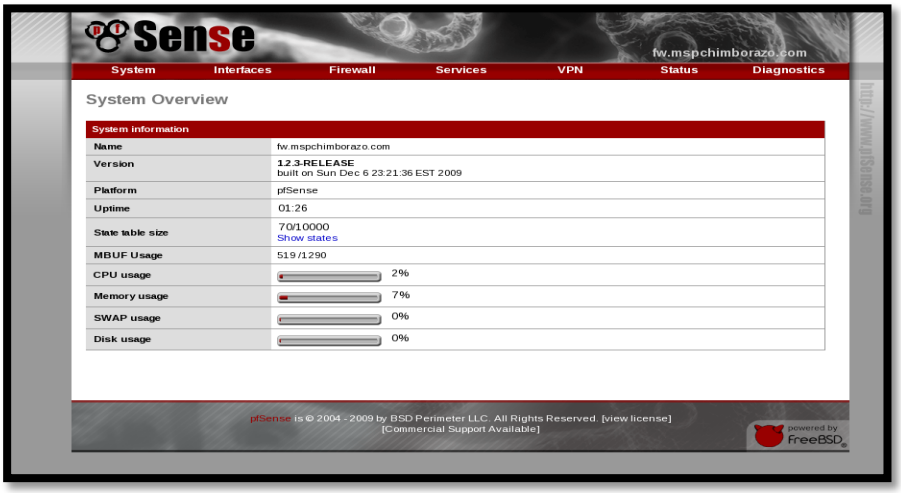

Figura 8. Consola de administración.

Estos son todos los pasos para la instalación y configuración de pfSense en el sistema, ahora falta realizar el resto de configuraciones.

3. Configuración de Interfaces y subredes en pfSense.

Se describe la configuración de las interfaces de red para las distintas subredes configuradas en el sistema. Los requisitos para seguir los pasos de este documento es disponer de un sistema pfSense instalado, como describe el documento DT3.01 y la configuración de los equipos de los equipos de red que permita implementar la topología diseñada. Generalmente se tratará de un entorno dividido en VLAN. La configuración de las VLAN varía en función del equipo, así que es mejor remitirse a la documentación del mismo.En este caso particular se implementará un sistema con 3 interfaces de red físicas, las 2 que se instalarán por defecto (WAN y LAN), y la (OPT), para la salida WAN del otro proveedor de internet. A la vez, de la interface LAN se utilizará para la creación de las VLANs respectivas. A continuación, se detalla la configuración hecha:

Tabla 1. Configuración de las interfaces.

Interface	Network Port	Dirección Red	IP Firewall
WAN	re0	200.107.48.0/24	200.107.48.240
WAN1	re1	192.168.1.0/31	192.168.1.1
LAN	bge0		
SERVIDORES	VLAN 101 en bge0	10.1.1.0/29	10.1.1.1
I_Hosts_A	VLAN 102 en bge0	10.1.2.0/28	10.1.2.1
I_Hosts_B	VLAN 103 en bge0	10.1.3.0/28	10.1.3.1
I_Hosts_C	VLAN 104 en bge0	10.1.4.0/28	10.1.4.1
I_Hosts_W	VLAN 106 en bge0	10.1.6.0/24	10.1.6.1

Para realizar estas configuraciones lo primero es acceder a la interface de administración web de pfSense. Desde allí, se accede al menú 'Interfaces'-> '(assign)' para configurar la asignación de interfaces a redes. Además, se puede configurar el acceso a distintas subredes con una sola interfaz si se conecta a un puerto configurado en el switch como multi-VLAN (trunk). En la figura, se puede ver la configuración de las subredes.

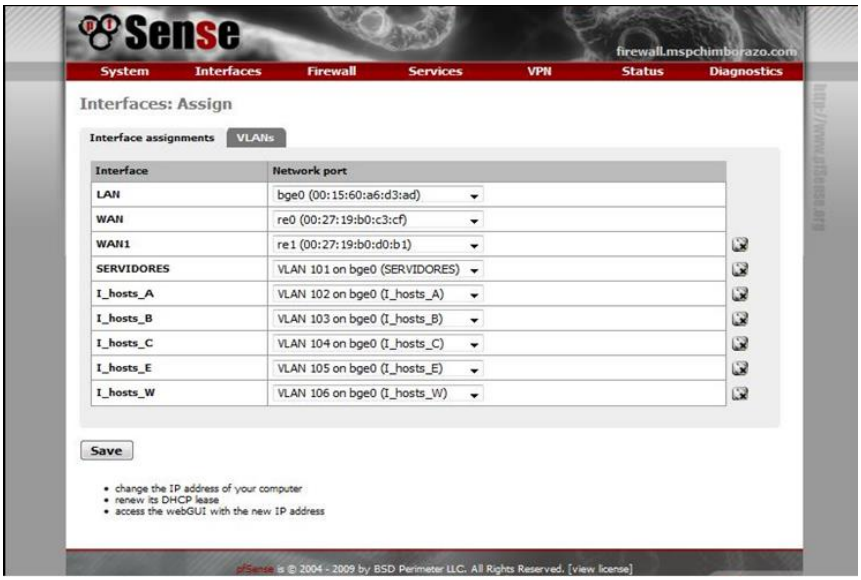

Figura 9. Subredes.

Si se pulsa el botón '+', se podrán añadir subredes asociándolas a una interfaz concreta. Esa interfaz es una interfaz física del sistema o una subinterfaz creada en la pestaña VLAN (Allí se asocia una subinterfaz a una interfaz física y un número de VLAN). En la figura siguiente se puede ver como se han configurado las 5 VLANs que se deben implementar.

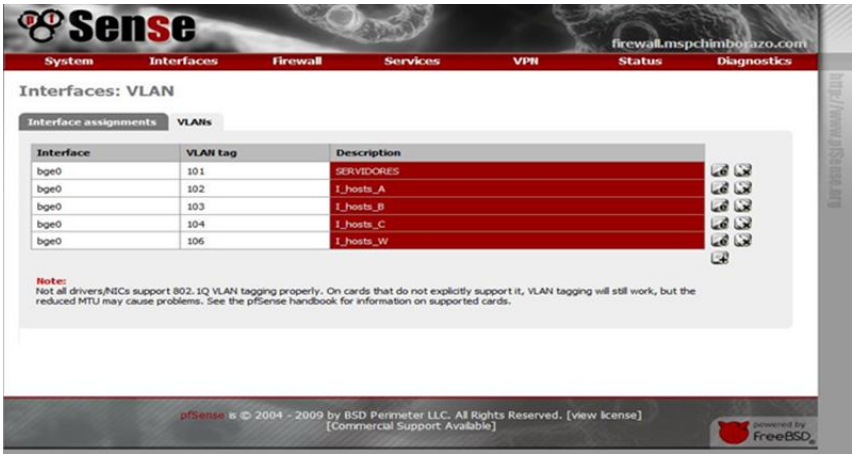

Figura 10. VLANs

Una vez creadas y/o asignadas las interfaces, desde el menú 'Interfaces' se puede seleccionar cada una de ellas y configurar sus parámetros. Además, se les puede cambiar el nombre. En la figura siguiente se ve la configuración de la red SERVIDORES.

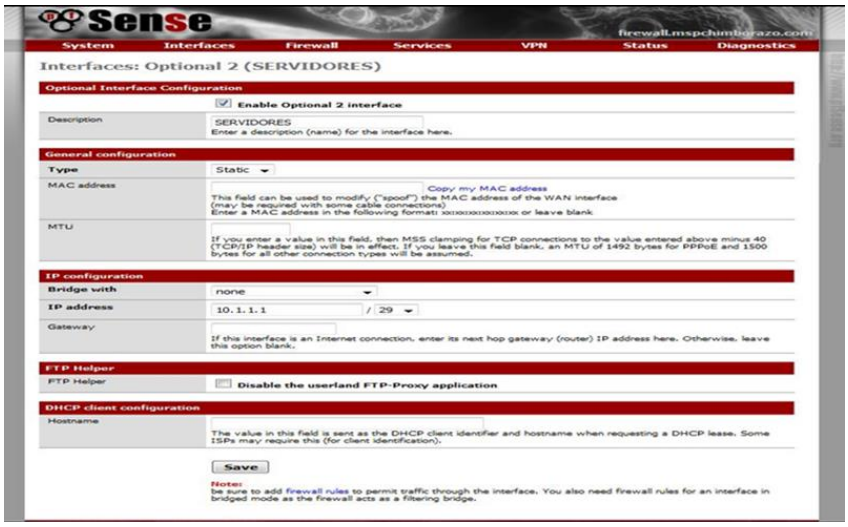

Figura 11. Configuración de servidores.

Así, se configuran todas las interfaces tal y como se han indicado. Además, se podría configurar alguna como 'bridge' entre dos subredes. Pero no es el caso en nuestra red. Además, si alguna interfaz está configurada para recibir la dirección por DHCP (en nuestro caso, la conexión a internet ADSL, para la OPT WAN1), se tendrá que configurar aquí. Desde los menús de interfaz se configuran los parámetros de red. Una vez, configurados, se pueden consultar desde el menú 'Status' -> 'Interfaces'. Allí aparece la configuración y una pequeña estadística del tráfico enviado y recibido. Además, si alguna interfaz está configurada para recibir la dirección por DHCP (en nuestro caso, la conexión a internet ADSL, para la OPT WAN1), se tendrá que pedir la renovación aquí. En la figura siguiente se detalla el estatus de las interfaces configuradas, así como la presencia de un botón llamado '*release'* en la interface WAN1 para la renovación de su dirección IP.

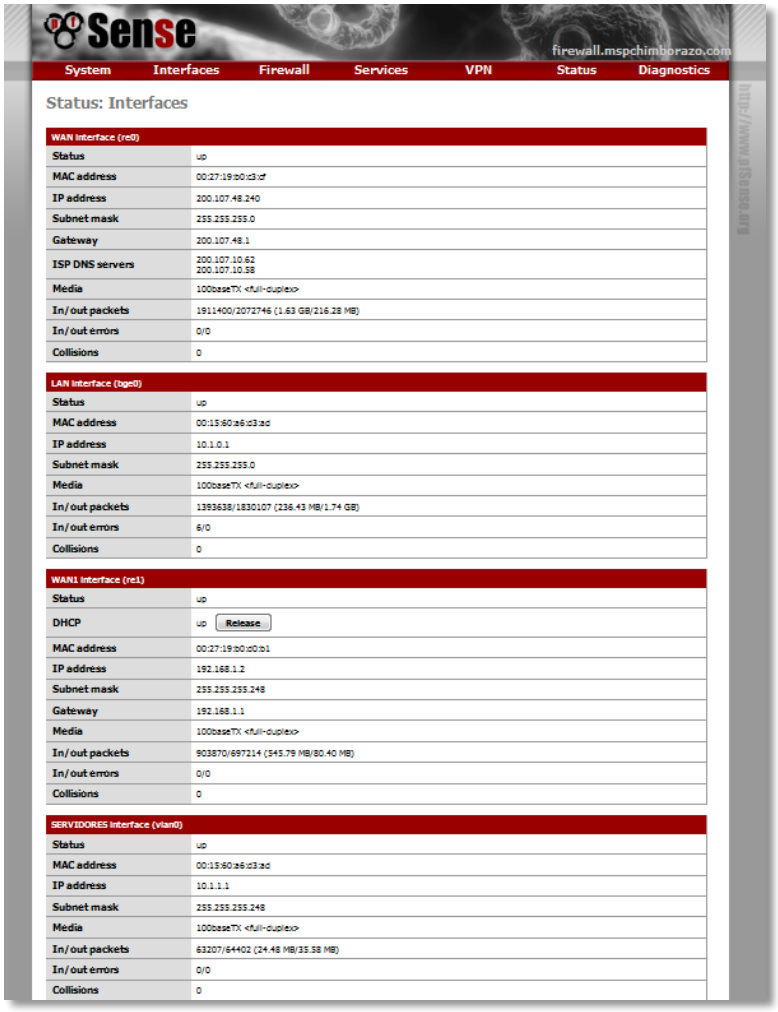

Figura 12. Configuraciónes Bridge.

4. Configuración de Interfaces y subredes en pfSense

En este punto, el sistema está configurado para tener conectividad en las redes definidas pero no se ha implementado ningún sistema de concesión de direcciones automático (DHCP) tal y como está previsto. Para hacerlo utilizaremos a pfSense como servidor DHCP y DNS. Empezaremos primero configurando DHCP, para ello accedemos a la interfaz web de pfSense y al menú 'Services'-> 'DHCP Server'. Básicamente, en un servidor DHCP se le dan los valores que deben asignar a los clientes y el los reparte. Además, permiten la creación de reservas que sirven para asociar una configuración determinada a un único cliente según su dirección física. La implementación del servicio de DHCP de pfSense permite, como opción, que solo la conexión de usuarios (habilitando 'deny unknown clients' y 'enable static ARP entries') tengan una reserva.

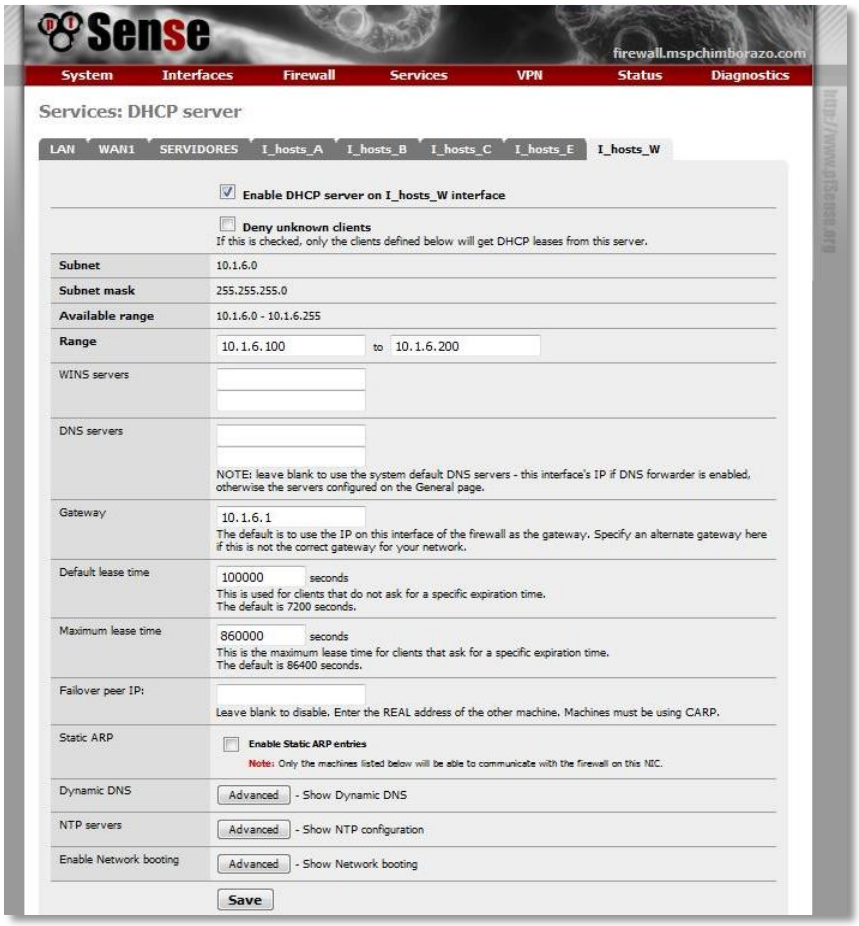

Figura 13. Configuración básica de DHCP para la red wireless de la implementación.

Con las interfaces configuradas y el servidor DHCP habilitado para cada subred, ya se tiene la topología configurada. Yendo a 'Services' -> 'DNS forwarder'activaremos el DNS (servidor de nombres) que incorpora pfsense y, además, le diremos que haga uso de asignaciones que realice el DHCP de pfSense, tal como muestran las dos primeras casillas de verificación de la pantalla que figura. Resulta ideal poner en lista de nombres de máquinas (que pueden verse en la figura de más abajo) todas las maquinas que den servicios a la red (servidores e impresoras). De esta forma la resolución de nombres para los servicios será altamente eficaz.

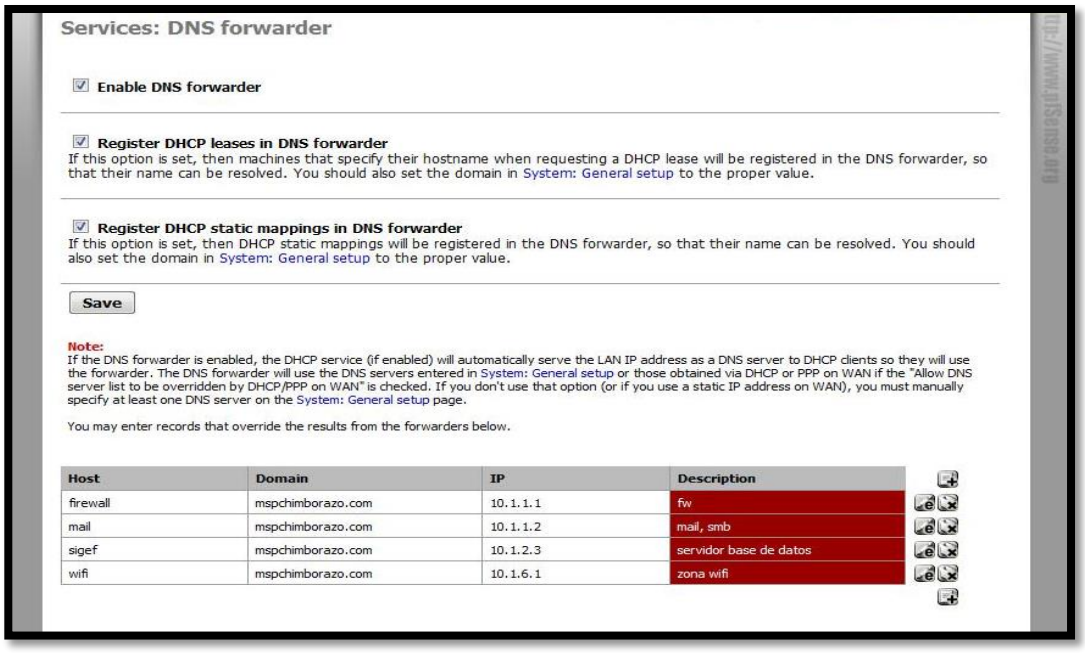

Figura 13. DNS.

Hasta aquí están hechas ya todas las configuraciones declaradas en este apartado. Previamente se debe haber migrado el servidor de software con licencia a software libre con CentOs.

Resultados y discusión

Los datos presentados en este estudio fueron comúnmente aceptados observando una aceptación en la Dirección Provincial de Salud de la ciudad Riobamba. Las preguntas de la encuesta y su respectivo resultado es el siguiente para probar si es un proyecto factible.

1 ¿Por motivos de seguridad le gustaría migrar servidores con software de licencia a software libre?

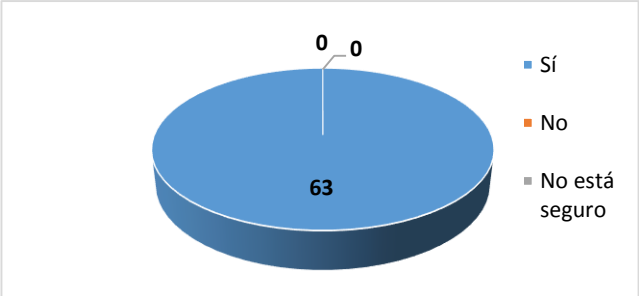

Figura 15. Encuesta, Pregunta N° 1.

2. ¿Por qué le gustaría migrar servidores con software de licencia a software libre?

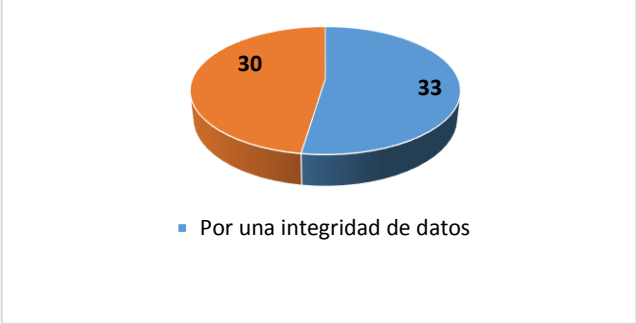

Figura 16. Encuesta, Pregunta N° 2.

El 100% de las personas encuestadas considera que la migración de servidores Windows a servidores Linux brindará mayor seguridad informática a una institución. El 50.2% (33 Usuarios) del personal encuestado

considera que la Implementación del firewall en la migración de servidores con software de licencia a software libre es fiable, el 49.8% (30 Usuarios) considera que la que la Implementación del firewall en la migración de servidores con software de licencia a software libre mejorará la seguridad en la información.

3. ¿Porque es importante tener un firewall seguro en *open source* con pfsence?

El 50.2% (33 Usuarios) del personal encuestado considera que la Implementación del firewall en la migración de servidores con software de licencia a software libre permitirá administrar servidores con tecnología de punta con *open source*, el 49,8% (30 Usuarios) considera que la Implementación del firewall en la migración de servidores con software de licencia a software libre permitirá mantener integridad en la información.

4 ¿Qué beneficios observaría para su vida la implementación del firewall en la migración de servidores con software de licencia a software libre?

El 56.4% (37 Usuarios) del personal encuestado considera que este tipo de migración mantendrá actualizado en los entornos de software libre adaptados al gobierno ecuatoriano. El 43.6% (26 Usuarios) considera que este tipo de migración mantendrá las 4 libertades del software libre (0: Poder usar el programa con cualquier propósito. 1: Poder estudiar cómo funciona el programa y poder modificarlo. 2: Poder distribuir copias del programa. 3: Poder mejorar el programa y poder compartir dichas mejoras para beneficio de todos).

5 ¿Le gustaría Implementar un firewall en la migración de servidores con software de licencia a software libre?

El 100% del personal encuestado considera que el Implementar del firewall en la migración de servidores con software de licencia a software libre. Mejorará la seguridad en la intranet y extranet en un entorno de red.
El resultado principal del proyecto es una herramienta poderosa y flexible, dentro del marco de trabajo de una plataforma y un entorno de servidores Linux con *open source* en nuestro caso práctico la migración al sistema operativo CentOs, ya que es un poderoso sistema operativo fiable y con seguridad integral comprobada. Además al comprobar un excelente firewall para evitar ataques hemos tomado el PFsence, como medio de defensa ante posibles atacantes de cualquier intranet – extranet de las que podamos ser víctimas.

Discusión

La información ha sido desde siempre un bien invaluable y protegerla ha sido una tarea continua y de vital importancia. A medida que se crean nuevas técnicas para la transmisión de la información, los curiosos idean otras que les permitan acceder a ella sin ser autorizados (Arana, Villa, & Polanco, 2013).. Las redes de computadores no son la excepción (Alarcón, 2010). Actualmente, se puede hacer una infinidad de transacciones a través de Internet y para muchas de ellas, es imprescindible que se garantice un nivel adecuado de seguridad. Esto es posible si se siguen ciertas reglas que se pueden definir según la necesidad de la entidad que las aplica (Ramos García, 2015).

La seguridad no es solo una aplicación de un nuevo programa capaz de protegernos, es más bien un cambio de conducta y de pensar. Hay que adueñarse del concepto seguridad e incluso volverse algo paranoico para que en cada labor que se desempeñe, se piense en seguridad y en cómo incrementarla (Ruiz Caldas, 2019)..

Actualmente existe una gran gama de distribuciones Linux encargadas de ofrecer soluciones de seguridad para las redes, lo cual se consigue a través de una serie de distribuciones Linux que se encargan de convertir un pequeño y limitado equipo de cómputo, en un medio de Seguridad Informática, que se encargará de brindar la seguridad y conectividad que las instituciones con un entorno de red necesitan (Carrera, Blanco, Pérez, & Villazón).

Conclusiones

La utilización de un sistema operativo como pfSense como firewall para la red es la mejor, no solo porque soluciona el problema de seguridad TCP/IP que presentaba la intranet, sino también porque es una herramienta que facilita la administración y la futura implementación de servicios en base a sus características de diseño y funcionalidad. Se debe implementar un sistema de cortafuegos (firewall), y pasarela a nivel de aplicación (proxy), que permitan incrementar en mayor número la seguridad y control de acceso a la información.

Agradecimientos

A Dios por la libertad que nos dio a sus hijos e hijas.

Referencias

Alarcón, J. C. C. (2010). El vínculo entre seguridad nacional y migración en México. *Revista mexicana de política exterior*(88), 9-43. Retrieved from https://revistadigital.sre.gob.mx/index.php/rmpe/article/download/668/633

Álava, W. L. S., Rodríguez, A. R., & Ávila, X. L. A. (2022a). Impacto del uso de la tecnología en la formación integral de los estudiantes de la carrera tecnologías de la información. *Journal TechInnovation*, *1*(2), 71-77. Retrieved from https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/download/21/36

Álava, W. L. S., Rodríguez, A. R., & Ávila, X. L. A. (2022b). Redes inalámbricas, su incidencia en la privacidad de la información. *Journal TechInnovation*, *1*(2), 104-109. Retrieved from https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/download/25/42

Arana, J. R., Villa, L. A., & Polanco, O. (2013). Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. *Ingeniería y competitividad*, *15*(1), 127-137. Retrieved from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-30332013000100012

Carrera, M. L. G., Blanco, Y. H., Pérez, Y., & Villazón, J. G. G. Herramienta para la Migración y Administración de Servicios Telemáticos (HMAST). Retrieved from http://wsl.softwarelivre.org/2015/0015/herramienta-para-la-migracion-y-administracion-de-servicios-telematicos-HMAST-wsl-2015.pdf

Cochran, D. (2012). *Twitter bootstrap web development how-to*: Packt Pub.

Ramos García, J. M. (2015). La política migratoria mexicana y la seguridad fronteriza con Estados Unidos: cambio y continuidad, 2012-2014. *Región y sociedad*, *27*(64), 351-382. Retrieved from https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-39252015000300011

Rodríguez, A., Castro, V. F. R., Gonzalez, A. D. C. R., Baque, N. A. C., & Tarragó, J. C. P. (2021). Aplicaciones de la Inteligencia Artificial en técnicas de minería de procesos. *Serie Científica de la Universidad de las Ciencias Informáticas, 14*(7), 136-155. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=8590663

Rodríguez, A., Lucas, H. B. D., Mero, C. J. Á., Pisco, R. J. L., & Castro, F. I. G. (2022). Método computacional de recomendación sobre la evaluación del aprendizaje bajo el paradigma constructivista. *Serie Científica de la Universidad de las Ciencias Informáticas, 15*(1), 178-187. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=8590599

Rodríguez, A., Tarragó, J. C. P., Gálvez, D. L. D., & Pisco, R. L. (2020). Modelo de formación constructivista en el proceso Enseñanza-Aprendizaje virtual. *Serie Científica de la Universidad de las Ciencias Informáticas, 13*(11), 175-184. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=8590367

Ruiz Caldas, A. J. (2019). Migración de servidores a la nube de Microsoft Azure para mejorar la continuidad de los servicios TI, de la fiduciaria en el año 2018. Retrieved from https://repositorio.usil.edu.pe/bitstreams/b240ffb1-29f9-45bd-8750-0a83d29c272d/download