UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE LA INGENIERIA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo

PRESENTADA PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

AUTORES

BACH. KENNY ESLEYTHER RUIZ VIEIRA

BACH. WILSON DELGADO RAMOS

CHICLAYO, mayo del 2018

FIRMA DEL ASESOR Y JURADOS DE TESIS

_____

Ing. Carlos Rojas Ortiz
ASESOR

_____ _____

Ing. Gilberto Martin Ampuero Pasco
PRESIDENTE

Ing. Segundo José Castillo Zumarán
SECRETARIO

_____

Ing. Francisco Richard Herrera Piscoya
VOCAL

DEDICATORIA

Dedico esta tesis a Dios y a mis padres porque sin ellos no hubiera llegado a donde estoy ahora.

A mi hermano por su apoyo moral y buenos consejos que siempre estuvo ayudándome y dándome aliento.

A mis amigos que siempre me ayudaron en todo lo que pudieron y logramos mucho juntos y a mis animalitos que fueron fuente de inspiración para mí.

A mis Maestros que gracias a sus enseñanzas, apoyo y buenos ejemplos pude llegar a donde estoy.

Kenny Ruiz

DEDICATORIA

Dedico esta tesis a Dios y a mis padres porque sin ellos no hubiera llegado a donde estoy ahora.

A mis hermanos por su apoyo moral y buenos consejos que impulsan a seguir adelante.

A mis tíos y primos que siempre fueron el pilar fundamental durante la carrera profesional.

A mis Maestros que gracias a sus enseñanzas, apoyo y buenos ejemplos.

Wilson Delgado

AGRADECIMIENTO

Nuestro agradecimiento a todas las personas que nos ayudaron con sus conocimientos, valores y principios morales a lo largo de nuestra carrera profesional, y además con su apoyo, consejos y aclarando inquietudes en la elaboración y desarrollo de la presente tesis.

Al Ingeniero Vladimir Sabino Gonzales Mechan, por la orientación y ayuda que nos brindó para la realización de esta tesis, por su apoyo, amistad y exigencia que nos permitieron aprender mucho más que lo estudiado y poder completar una base más solidad en el desarrollo profesional.

A nuestro asesor de tesis el Ingeniero Carlos Rojas Ortiz por la orientación y ayuda que nos brindó para realizar esta tesis, su paciencia, amistad y consejos que nos ayudaron a entender y mejorar el tema expuesto en esta tesis.

CONTENIDO

ÍNDICE DE ILUSTRACIÓN

ÍNDICE DE TABLAS

RESUMEN

En esta tesis se presenta una solución de seguridad perimétrica open source, para que cubra los requerimientos de una red perimetral DMZ y todos los servicios internos que contengan. Además, se muestra la instalación del software pfSense en un ambiente de pruebas controlado para luego ser puesto en producción. En el primer capítulo se presenta la realidad problemática y riesgos de la información, y la importancia de esta. En el segundo capítulo se muestra el marco teórico en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una institución educativa superior y las contramedidas que pueden ser adoptadas.

En el tercer capítulo se muestra los materiales y métodos para explicar el escenario de desarrollo de la tesis, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware. En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo, para generar resultados. Se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en el cuarto capítulo, se plasma en los componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas. Para ello se aplicarán las configuraciones apropiadas que permitan realizar las tareas de monitoreo, bloqueo y restricciones del tráfico web con la finalidad de proteger los datos de la institución. Finalmente, en el quinto capítulo se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado.

ABSTRACT

This thesis presents an open source perimeter security solution, to cover the requirements of a DMZ perimeter network and all the internal services that it contains. In addition, the installation of the pfSense software is shown in a controlled testing environment and then put into production. In the first chapter we present the problematic reality and risks of the information, and the importance of it. The second chapter shows the theoretical framework in detail and in a technical manner, the risks, threats against the integrity of a computer network of a higher educational institution and the countermeasures that can be adopted.

The third chapter shows the materials and methods to explain the thesis development scenario, its requirements and its needs without specifying any product, software or hardware. In the fourth chapter we present the criteria that were taken into consideration for the selection of the most suitable solution for the scenario proposed in the third chapter, to generate results. The security policy that must be applied in the solution selected in the fourth chapter is developed, it is embodied in the components that comprise it and its performance is evaluated in a testing environment. For this purpose, the appropriate configurations will be applied to carry out the tasks of monitoring, blocking and restricting web traffic in order to protect the data of the institution. The fourth chapter presents the criteria that were taken into consideration for the selection of the most suitable solution for the scenario proposed in finally, the fifth chapter presents the conclusions that emerge from the analysis of the proposed scenario, as well as the recommendations for maintain an adequate level of security.

CAPITULO I: INTRODUCCION

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Las universidades actualmente cuentan con tecnologías de la información (TI) para todos sus procesos administrativos, dando lugar a un incremento de ataques externos a sus instalaciones tecnológicas, pero en algunos casos no están en las condiciones de contratar o comprar un sistema de seguridad perimetral, por ende es de vital importancia mejorar la gestión de la seguridad perimetral de su red telemática, con bajo costo y mayor eficiencia para detectar incidencias o ataques, dando lugar a fácil mantenimiento y mejora de seguridad a sus procesos operativos con TI de software libre.

El que una institución privada o pública no cuente con una buena gestión del Firewall de seguridad, los procesos se pueden ver afectados en una magnitud parcial por personas maliciosas que solo buscan causar perjuicios a las organizaciones, e incluso en una paralización total de los procesos, el firewall cuenta con las siguientes funciones para la red:

Control de tráfico de red desde y a hacia Internet.

Protección contra ataques externos.

Control de usuarios.

Generación y administración de VPNs

Gestión de ancho de banda de internet

IDS (Sistema de detención de intrusos)

Antivirus corporativo

Medidas de seguridad contra virus.

Mecanismos Activo y Pasivos.

Al optar por un criterio bien estructurado ante la madurez de la seguridad informática para resguardar la información crítica y procesos internos en las universidades, no solo se espera mitigar los incidentes de seguridad en las aplicaciones y bases de datos a través de una adecuada gestión de la seguridad informática de la red informática, sino que también se desea obtener mayor confiabilidad de los docentes, empleados, estudiantes, rectorado, y público en general respecto de la seguridad perimetral de la red.

El siguiente proyecto se basa en la seguridad perimetral en la red telemática de la Universidad Nacional Pedro Ruiz Gallo que frente a las amenazas externas que se encuentran para la red, tanto que estas amenazas ponen en riesgo la información que tienen las universidades, información relevante y de mucha importancia para su desarrollo como institución ya que su

seguridad tiene que estar actualizada y preparada para todo tipo de amenazas de los hackers de hoy en día.

Muchas veces los firewalls protegen la red privada de posibles amenazas, pero este firewall no es lo suficientemente efectivo ya que no suelen ser adecuadamente dimensionadas, ocasionando la explotación de vulnerabilidades y por lo tanto no es lo suficientemente seguro.

Específicamente el contar con un buen sistema de seguridad perimetral, permite a las universidades que la red se encuentre bien protegida ante una amenaza externa o controlando el tráfico de internet aparte de habilitar funcionalidades como las que pueden ser las de filtrar páginas web que solo necesitan los usuarios de la red. Esto facilita que un usuario con conocimientos básicos pueda dar permisos a ciertas IPs la salida a internet sin restricciones.

El problema de la seguridad perimetral en los servicios es porque otras personas entran en la red de manera informal ya sea porque conocen algunos procesos de la red o personas en este caso personal que ya no laboran en la institución y que tienen información de la red y hacen mal uso de ella como es proporcionando contraseñas de redes privadas que solo debe hacer uso los usuarios de la entidad

Para reducir los riesgos de ataques que puedan afectar los activos informáticos de la universidad, en especial los datos e información, el presente trabajo propone una solución de seguridad perimetral a través de implementar un firewall UTM de software libre robusto, eficiente y seguro que permita proteger la red de posibles amenazas, en el caso de las amenazas externas este Firewall protegerá la información que entra y sale de la red evaluándola y designando si es útil que esta información sea utilizada, es de vital importancia tener seguridad perimetral en un lugar como este ya que se trabajan con información sensible y muy importante.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿En qué medida la implementación de una solución de seguridad perimetral open source en la red telemática de la Universidad Nacional Pedro Ruiz Gallo, permitirá proteger los servicios académicos?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Incrementar la seguridad de los servicios académicos en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

1.3.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico del estado de la seguridad perimetral en la red telemática de la Universidad Nacional Pedro Ruiz Gallo con uso de open source.
- Diseñar una solución basada en open source.
- Análisis de resultados del impacto de la implementación de un firewall open source en la gestión de la seguridad perimetral en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

1.4. JUSTIFICACIÓN

1.4.1. PERTINENCIA DE LA INVESTIGACIÓN

La presente investigación es justificada y es importante por las siguientes razones:

Es oportuna por que el tema de la Gestión de la Seguridad Perimetral es inherente cuando se analiza, diseña o implementa soluciones basados en tecnologías de la información como soporte a los procesos de la gestión la seguridad perimetral de la red telemática de la Universidad Nacional "Pedro Ruiz Gallo", que se desarrolle sin el soporte tecnológico informático de seguridad adecuado. Por tanto, al implementar un firewall en la gestión de la seguridad perimetral de la Red Telemática. Es necesario considerar como parte de su gestión, los riesgos que están asociados a los mismos. Es conveniente, porque la Red Telemática de la Universidad Nacional "Pedro Ruiz Gallo", tomada como caso de estudio, pertenece a un sector en el cual se les exige obligatoriamente implementar sistemas que gestionen la seguridad de la información, para mitigar los riesgos operativos asociados a las tecnologías y la continuidad de la gestión de la seguridad perimetral de la red telemática de la Universidad Nacional "Pedro Ruiz Gallo".

Este proyecto de tesis pretende aportar con este marco metodológico. Y práctico que tiene como objetivo solucionar el problema de gestión de seguridad perimetral en una universidad.

Por tanto, esta investigación pretende aplicar buenas prácticas de las normas internacionales ISO/IEC 27001 y ISO/EC 27002 2011, pero debidamente dimensionadas a sus capacidades y a las exigencias de las normativas de la Red Telemática y la OCCI en estas actividades.

1.4.2. RELEVANCIA DE LA INVESTIGACIÓN

En términos de relevancia, esta tesis pretende aportar con el método de gestión de riesgos de Tecnología de la información, una propuesta empírica que le permite a los responsables de la gestión de la seguridad de la información y de la continuidad de la gestión de la seguridad perimetral de la red telemática de la Universidad Nacional "Pedro Ruiz Gallo".

La Red Telemática de la Universidad Nacional "Pedro Ruiz Gallo "es beneficiaria directo, porque es la entidad tomada como caso de estudio. Les permitirá a los responsables de la Red Telemática e incluso a las áreas de control interno y Auditoria, contar con una herramienta "usable" y "adecuada" para logar cumplir con sus metas de evaluación de los escenarios de exposición al riesgo y disminuir así de manera preventiva, los potenciales incidentes de

seguridad perimetral. Proporcionando una protección más óptima de su información y podrá gestionar el acceso de los usuarios.

1.5. LIMITACIONES

El estudio de esta tesis solo se verá orientado solo a los ataques de accesos no autorizados.

CAPITULO II: MARCO TEORICO

2.1. ANTECEDENTES BIBLIGRÁFICOS DEL PROBLEMA

2.1.1. A NIVEL INTERNACIONAL

TITULO	IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL
UNIVERSIDAD	UNIVERSIDAD POLITÉCNICA DE MADRID
FECHA	Septiembre 2013
AUTOR(ES)	CARLOS MANUEL FABUEL DÍAZ
RESUMEN	El problema que pretendieron solucionar fue la seguridad perimetral de una Red de datos de una organización. Lo que hicieron para evaluar y solucionar el problema básicamente fue diseñar y posteriormente implantar un sistema de seguridad perimetral, para ello primero se han establecido las bases teóricas de los principales elementos de seguridad que conforman dichas implementaciones y finalmente se ha desarrollado un entorno adecuado para unos requisitos establecidos. Finalmente llegaron al resultado de lograr diseñar una metodología de gestión de incidencias, planificar las tareas a seguir cuando se produce cada una de las posibles incidencias para asegurar su óptimo funcionamiento y definir una gestión de la propia plataforma. (Dias, 2013)
ANÁLISIS DE RELACIÓN CON LA TESIS	La relación con la investigación está dada por la aplicación de pruebas para ver el funcionamiento de la red perimetral y se ha visto conveniente indicar, que los aspectos que se va tomar en cuenta de este antecedente, para desarrollar nuestra propuesta de tesis: Su forma que han probado su propuesta de solución. Como lo han evaluado. El modelo de implementación de la estrategia

TITULO	ESQUEMA DE SEGURIDAD PERIMETRAL APLICABLE A UNA PYME MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE
UNIVERSIDAD	ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
FECHA	2016
AUTOR(ES)	RAÚL JAVIER HONORES QUINDE
RESUMEN	El problema que pretendieron solucionar fue la falta de control y monitoreo en las transferencias de los datos que entran o salen de una MYPE por medio del internet. Por tanto, lo que hicieron para solucionar el problema fue implementar la plataforma pfSense (está basada en el sistema operativo FreeBSD) y aplicar las configuraciones apropiadas. Los resultados obtenidos fue proteger los datos de la institución mejorando el control y monitoreo de tráfico de la información que viaja a través de la red por medio de correos electrónicos, almacenamiento en la nube, mensajerías instantáneas o navegadores web y mejorar las tareas de monitoreo, bloqueo y restricciones del tráfico web. (Honores Quinde, 2016)
ANÁLISIS DE RELACIÓN CON LA TESIS	La relación con la investigación está dada por la aplicación de pfSense la cual permitirá hacer controles de tráfico de correos por la nube. Los aspectos de este antecedente de tesis que vamos a tomar en cuenta para desarrollar nuestra propuesta son: - El fundamento teórico la cual nos indica que la aplicación de pfSense permitirá hacer controles de tráfico de correos por la nube.

2.1.2. A NIVEL NACIONAL

TITULO	EFECTO DE LA IMPLEMENTACIÓN DEL SISTEMA PFSENSE EN LA SEGURIDAD PERIMETRAL LÓGICA EN LOS SERVICIOS DE LA RED TRONCAL DE LA UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA, IQUITOS – 2016
UNIVERSIDAD	UNIVERSIDAD PRIVADA DE LA SELVA PERUANA
FECHA	2016
AUTOR(ES)	DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, SILVA LEDESMA JONY RENE
RESUMEN	El problema que pretendieron solucionar fue como encontrar nuevas soluciones informáticas para resguardar la información contenida en los servidores y clientes, porque se han originado dudas sobre la fiabilidad y protección que brinda el sistema de seguridad. Para solucionar o mitigar el problema, se implementó el firewall lógico "PfSense V. 2.3 con núcleo FreeBSD - UNIX" en la UNAP. Para determinar el efecto se realizó el tipo de investigación aplicada con diseño experimental de con pre test y post test para los doce servicios que cuenta la red interna de la UNAP (Portal Web, Repositorio, Sistema Académico, Firewall, Biblioteca, Aula Virtual, Siaf, Openfire, Coa, Antivirus, Siseg, Sisper). Utilizando muestreo por conveniencia. Se consideró la población del número de intentos de vulnerabilidad extremadamente grande. De tal manera de calcular la muestra para cada servidor de 1,069 intentos de vulnerabilidad, determinando el número de vulnerabilidades exitosas con la red original y comparándolo con el número de vulnerabilidades exitosas en la red implementada. Llegando a los resultados de mejorar la seguridad perimetral lógica de la red interna. Al comparar el número de vulnerabilidades antes y después del cambio en la configuración de la red perimetral lógica, se pudo medir una disminución en el número de vulnerabilidades en promedio en términos porcentuales del 91.83 %, con lo que se determina que el efecto sobre la seguridad perimetral lógica en los servicios de red fue de mejora. (DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, 2016)
ANÁLISIS DE RELACIÓN CON LA TESIS	La relación con la presente investigación está dada por la búsqueda de originar un efecto o cambio en la seguridad de la red, que se reflejara en el número de vulneraciones a la red perimetral lógica. Al comparar el número de vulnerabilidades antes y después del cambio en la configuración de la red perimetral lógica. En relación con la propuesta de tesis, podemos indicar qué los aspectos de este

	antecedente de tesis a tomar en cuenta para desarrollar la propuesta es: El fundamento teórico. Sus resultados. Su forma de evaluar.
TITULO	DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA EMPRESA PEQUEÑA
UNIVERSIDAD	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FECHA	2012
AUTOR(ES)	JORGE LUIS VALENZUELA GONZALES
RESUMEN	En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado. En el primer capítulo se presenta el estado actual y riesgos de la información, y la importancia de la misma. Se presenta además la seguridad perimetral de la red de datos como parte de una problemática mayor. La seguridad de la información. En el segundo capítulo se muestra en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una empresa pequeña y las contramedidas que pueden ser adoptadas. En el tercer capítulo se explica el escenario de trabajo, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware. En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo. En el quinto capítulo, se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en el cuarto capítulo, se plasma en los componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas. Finalmente se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado. (GONZALES, 2012)
ANÁLISIS DE RELACIÓN CON LA TESIS	Se determina el efecto de seguridad perimetral lógica en los servicios de red fue de mejora. Por lo tanto, nos alienta a continuar desarrollando nuestra tesis para cumplir con los objetivos generales. Tiene una relación con nuestra tesis por que comparar el número de vulnerabilidades antes y después del cambio en la configuración de la red perimetral lógica.

2.1.3. A NIVEL REGIONAL

TITULO	IMPLEMENTACIÓN DE UN SISTEMA CRIPTOGRÁFICO A TRAVÉS DE ALGORITMOS AVANZADOS DE ENCRIPTACIÓN PARA MEJORAR LA SEGURIDAD PERIMETRAL DE UNA RED INFORMÁTICA
UNIVERSIDAD	UNIVERSIDAD SEÑOR DE SIPAN
FECHA	2016
AUTOR(ES)	GUEVARA TINOCO ROBERTO CARLOS, LÓPEZ WILLY LLEISON
RESUMEN	Históricamente, la autentificación de paquetes se ha manejado a través de firmas digitales basadas en certificados, usualmente emitidos por una entidad neutral a la comunicación y de confianza de todas las partes. Sin embargo, esta solución no siempre es posible de implementar, debido a factores como los costos, el tiempo limitado de vigencia de los certificados, la necesidad de depositar la confianza en un tercero, y por último el poder, usualmente limitado, de procesamiento de las máquinas. El tema de esta tesis es desarrollar una alternativa de sistema de seguridad para la red informática. El sistema utiliza algoritmos avanzados para la encriptación y desencriptación de los paquetes de información enviados en la entidad de estudio para la protección de datos privados del usuario. El sistema debe poder extenderse para poder incorporar encriptación basada en más algoritmos de este tipo. El desarrollo de este trabajo consiste en un estudio de las componentes a usar, tanto de hardware como de software, incluyendo los conceptos básicos necesarios para su diseño y operación, así como los estándares y metodologías que siguen. (Guevara Tinoco & López López, 2016)
ANÁLISIS DE RELACIÓN CON LA TESIS	La relación con nuestra tesis es que sus objetivos están direccionados a la protección de los datos privados del usuario. Están enfocados esta referencia de tesis con nuestra tesis, en la continua búsqueda de una solución para Lograr mejorar la seguridad perimetral de una red telemática.

2.2. BASES TEÓRICAS

2.2.1. REDES DE COMPUTADORAS

Conjunto de computadoras autónomas interconectadas. Se dice que dos computadoras están interconectadas si pueden intercambiar información. No es necesario que la conexión se realice mediante un cable de cobre; también se pueden utilizar las fibras ópticas, las microondas, los rayos infrarrojos y los satélites de comunicaciones (ANDREW S. , 2009).

Ilustración 1: Red de computadoras.
Fuente: (Salcedo, 2017)**.**

(Salcedo, 2017) dice que la estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

Protocolos de Redes:

(Cisco - CCNA, s.f.)El Protocolo de red o también protocolo de Comunicación es el conjunto de reglas que especifican el intercambio de Datos u órdenes durante la Comunicación entre las entidades que forman parte de una red.

Estándares de redes:

IEEE 802.3, estándar para Ethernet
IEEE 802.5, estándar para Token Ring
IEEE 802.11, estándar para Wi-Fi
IEEE 802.15, estándar para Bluetooth

Para la disciplina científica y la ingeniería que estudia las redes de ordenadores, una red de ordenadores es el conjunto de ordenadores conectados junto con un sistema de telecomunicaciones con el fin de comunicarse y compartir recursos e información.

Se utilizan para el intercambio de información (datos, impresiones, juegos entre otros) de manera más fácil y precisa, toda la información se trasmite a través de ondas por medio del cable de cobre, fibra óptica o por medio del WI – FI.

2.2.2. ARQUITECTURA DE UNA RED EMPRESARIAL

Red de borde

Es el que se conecta a la nube por medio de un router el cual está configurado con una capa de protección, controlando el tráfico y trasmitiendo información a través de la red perimetral, por medio de un cortafuego configurado (Méndez, 2017).

Red perimetral

Permite la conexión de usuarios de redes externas a los servidores y estos servidores se comunican con la red interna para así dar una buena seguridad, ya que si un usuario mal intencionado quiere entrar ilegalmente a la red interna se topará con la DMZ que se interpondrá en su camino (Baca, 2016).

Redes internas

Las redes internas son un conjunto de servidores privados cuyo objetivo es dar según sea su función, servicios a los usuarios internos de la red, como por el ejemplo el servidor SQL, WEB o FTP (Mendez, 2017).

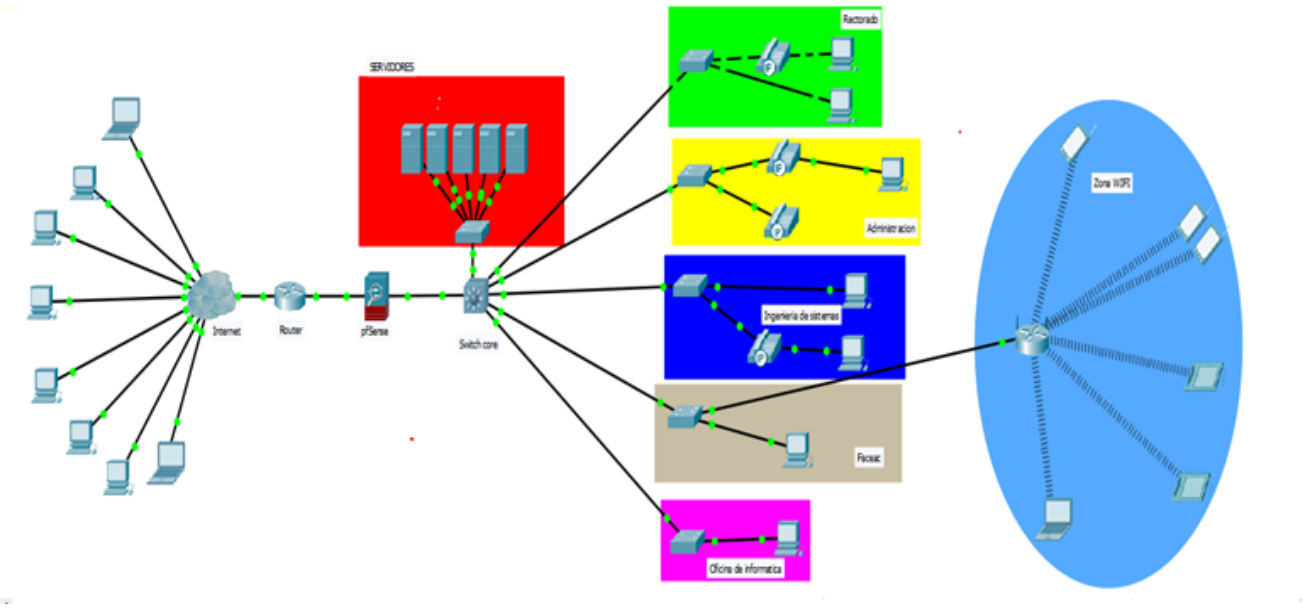


Ilustración 2: Arquitectura de la red interna.
Fuente: Elaboración propia

Identificando componentes principales (Méndez, 2017):

¿Qué Componentes son críticos?

Servidores de aplicaciones (Matricula, Admisión, etc.)
Servidores de base de datos (Matricula, Admisión, Repositorios institucionales).

¿Cuáles son los componentes que debería dar seguridad a los componentes críticos?

Servidores de seguridad perimetral (Firewalls – UTM, IPD/IDS).
Servidores de seguridad interno.
Enrutador de borde.

2.2.3. SEGURIDAD PERIMETRAL

(Sánchez, 2013) Define que la seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Entre estos sistemas cabe destacar los radares tácticos, video sensores, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, concertinas, etc. Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra

óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de soporte (auto soportados, soportados, enterrados, detección visual, etc.).

Al describir que aspectos abarca la seguridad perimetral, se requiere que sea escalable, tolerante a fallos, eficiente, segura y que garantice la gestión de la seguridad.

Entre las zonas de diferente nivel de seguridad de una red corporativa se tiene:

Red interna
Red Externa
DMZ (Zona desmilitarizada)

En este punto la red corporativa de cualquier universidad se conecta con la red púbica, por tal razón es importante reforzar las medidas de seguridad.

¿Qué protege?

Protege la red Interna y la red DMZ (Zona desmilitarizada), contra amenazas provenientes de la red externa (amenazas tales como intentos de intrusión, Malware, Ataque contra la privacidad e integridad, explotación de vulnerabilidades).

¿Cómo debería protegerse?

Reforzando las medidas de seguridad aplicando mecanismos de defensa como Firewalls, Concentradores de VPNs, IDS (Sistema de Detección de Intrusos) que detecta ataques para alarmar al administrador e IPS (Sistema de Prevención de Intrusos) que ejerce control de acceso la cual analiza los datos del ataque y actúa en consecuencia.

¿Qué estrategias existen?

Implementación de reglas de filtrado basado en agregar ataques a servidores y el mecanismo de filtrado basado en el tráfico de protocolo de transferencia de hipertexto, pero no es fácil definir para algunos entornos.

2.2.4. FIREWALL

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea un tráfico específico en función de un conjunto definido de reglas de seguridad. Los cortafuegos han sido una primera línea de defensa en seguridad de red durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas que

pueden ser de confianza y las que no son de confianza fuera de las redes, como Internet. Un firewall puede ser hardware, software o ambos (Cisco, s.f.).

Es un dispositivo hardware o software de seguridad que monitorea el tráfico entrante o saliente de una red y que según sus reglas de seguridad bloquean, permiten o desvían los intentos de ingresar a la red interna de una organización. Los firewalls son la primera defensa de seguridad en una red por más de 25 años.

Si el firewall detecta que el tráfico cumple con las reglas que se le configuraron este tráfico podrá entrar y salir de la red, pero si no cumple con las reglas este tráfico no podrá entrar a la red quedando bloqueado.

Básicamente funcionan como una barrera entre la red interna que tiene información sensible y de confianza ante las amenazas de una red externa como lo es internet, es decir protegen los equipos individuales, servidores o equipos conectados a red ante accesos no permitidos, los cuales pueden robar información privada y confidencial o incluso sabotear el trabajo en la red.

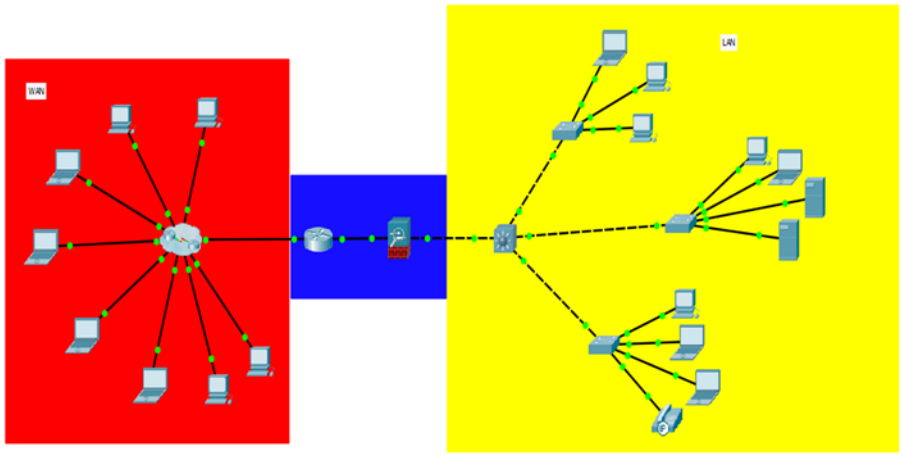


Ilustración 3: Esquema de Firewall.
Fuente: Elaboración propia.

2.2.5. PFSENSE

El software pfSense es una distribución personalizada gratuita y de código abierto de FreeBSD específicamente diseñada para usarse como firewall y enrutador que se administra completamente a través de la interfaz web. Además de ser una plataforma potente y flexible de enrutamiento, incluye una larga lista de características relacionadas y un sistema de paquete que permite una mayor capacidad de expansión sin agregar posibles vulnerabilidades de seguridad a la distribución base (pfSense, s.f.).

Firewall

Configurado de modo firewall, permitiendo y denegando el tráfico de redes por medio de una dirección IP de origen y destino con sus reglas establecidas las IPs quedaran registradas para que la información pueda entrar y salir sin problemas (pfsense, s.f.).

Servidor VPN

Configurado de modo VPN que es una conexión de red que te permite hacer una conexión segura a través de internet para redes privadas en una ubicación remota, todo el tráfico de red pasa por un túnel virtual entre el dispositivo y el servidor VPN (pfsense, s.f.).

Balanceo de Carga

Configurado de modo balanceo de cargas, para que los servicios críticos como servidores web, de correo, de DNS, se encuentre siempre redundado y disponible. Replicando el servicio para distribuir la carga de datos de manera homogénea dando respuestas rápidas a los usuarios sin pagar más (pfsense, s.f.).

Portal Cautivo

Configurado como portal cautivo para identificar el intento de salida hacia internet y redirige a una página de autentificación en donde el usuario pone nombre y contraseña, usado mayormente en zonas wifi de restaurantes, hoteles entre otros (pfsense, s.f.).

Tabla de estado

Tiene la funcionalidad de guardar seguimientos de estados de las conexiones de la red en una tabla detallada. PfSense tiene un número de características que permiten un monitoreo muy fino para el manejo de la tabla de estado (pfsense, s.f.).

Servidor DNS y reenviador de cache DNS

Configurado como servidor DNS el cual traduce las direcciones IP de los servidores para que los equipos clientes tengan acceso a los servicios internos o externos, según sea el caso (pfsense, s.f.).

Servidor DHCP

Configurado como servidor DHCP en el cual se pueden crear VLAN y dar direcciones IP a las distintas VLANs (pfsense, s.f.).

Servidor PPPoE

Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local (DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, 2016).

Enrutamiento estático

PfSense funciona como un enrutador ya que entrega direccionamiento IP (DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, 2016).

2.2.6. VULNERABILIDADES DE RED

(Cisco - CCNA, s.f.) Explica que la vulnerabilidad es el grado de debilidad inherente a cada red y dispositivo. Esto incluye routers, switches, computadoras de escritorio, servidores e, incluso, dispositivos de seguridad. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales:

Tecnológicas:

Debilidades de la seguridad de red
Debilidad del protocolo TCP/IP
El protocolo de transferencia de hipertexto (HTIP), el protocolo de transferencia de archivos (FTP) y el protocolo de mensajes de control de Internet (ICMP) son inseguros por naturaleza.
El protocolo simple de administración de redes (SNMP) y el protocolo simple de transferencia de correo (SMTP) se relacionan con la estructura intrínsecamente insegura sobre la que se diseñó TCP.
Debilidad de los sistemas operativos
Cada sistema operativo tiene problemas de seguridad que se deben resolver.
UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 están registrados en los archivos del Computer Emergency Response Team (CERT) en http://www.cert.org.
Debilidad de los equipos de red
Los diversos tipos de equipos de red, como routers, firewalls y switches, tienen debilidades de seguridad que deben identificarse y evitarse. Sus debilidades incluyen la protección de contraseñas, la falta de autenticación, los protocolos de routing y los agujeros de firewall.

Fuente: (Cisco - CCNA, s.f.)**.**

Configuración:

Debilidad en la configuración	Como se aprovecha la debilidad
Cuentas de usuario no seguras	La información de la cuenta de usuario se puede transmitir de manera insegura a través de la red. Esto expone nombres de usuario y contraseñas a los curiosos.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común se debe a la elección de contraseñas de usuarios deficientes y fáciles de adivinar.
Servicios de Internet mal configurados	Un problema común es activar JavaScript en los navegadores web, lo que permite ataques mediante scripts hostiles cuando se accede a sitios no confiables. Otras posibles fuentes de debilidades incluyen los servicios de terminal mal configurados, FTP o los servidores web (p.ej., Microsoft Internet lnformation Services (llS), servidor HTIP Apache).
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que habilitan los agujeros de seguridad.
Equipos de red mal configurados	Las malas configuraciones del propio equipo pueden causar problemas de seguridad importantes. Por ejemplo, las listas de acceso mal configuradas, los protocolos de routing o las cadenas comunitarias SNMP pueden abrir enormes agujeros de seguridad.

Fuente: (Cisco - CCNA, s.f.)**.**

Política:

Debilidad en las políticas	Como se aprovecha la debilidad
Falta de políticas de seguridad por escrito	Una política no escrita no se puede aplicar sistemáticamente ni se puede hacer cumplir.
Política	Las batallas políticas y las luchas territoriales pueden dificultar la implementación de una política de seguridad sistemática.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, las contraseñas fáciles de decodificar o las contraseñas predeterminadas pueden permitir el acceso no autorizado a la red.
Controles de acceso lógico no aplicados	El monitoreo y las auditorías inadecuadas permiten que los ataques y el uso no autorizado continúen. Esto hace que la empresa desperdicie recursos. Esto puede ocasionar acciones legales o despidos de los técnicos de TI, de la administración de TI o hasta de los directores dela empresa que permiten que estas condiciones no seguras persistan.
La instalación de software y hardware y los cambios no respetan la política	Los cambios no autorizados que se realizan en la topología de la red o la instalación de aplicaciones no aprobadas crean agujeros de seguridad.
No existe plan de recuperación tras un desastre	La falta de un plan de recuperación tras un desastre produce caos, pánico y confusión cuando alguien ataca la empresa.

Fuente: (Cisco - CCNA, s.f.)**.**

Todas estas vulnerabilidades o debilidades pueden dar origen a diversos ataques, incluidos los ataques de código malintencionado y los ataques de red.

2.2.7. SELECCIÓN DEL FIREWALL

Para elegir el firewall se tuvo que analizar entre los firewalls más populares open source en los cuales se analizó sus funciones de protección para una red LAN, a continuación, se presenta un cuadro donde se comparan los firewalls:

Tabla 1: Firewalls de software libre.
Fuente: (LinuxLinks, s.f.).

FIUNCIONES	pfSense	ClearOS	Untangle	IPFire	Smoothwall Express	Shorewall
FIREWALL	✔	✔	✔	✔	✔	✔
SERVIDOR DNS	✔	✔	✔	✘	✔	✔
SERVIDOR DHCP	✔	✔	✔	✘	✔	✔
VPN	✔	✔	✔	✔	✔	✔
BALANCEO DE CARGA NAT	✔	✔	✔	✘	✘	✔
PORTAL CAUTIVO	✔	✘	✔	✘	✔	✘
TABLA DE ESTADO	✔	✔	✔	✔	✔	✔
INTERFAZ AMIGABLE	✔	✔	✔	✔	✔	✔
PROXY	✔	✔	✔	✔	✔	✔
ENRUTAMIENTO	✔	✔	✔	✔	✔	✔
IP VIRTUALES	✔	✔	✔	✘	✘	✘
LIMITE DE ANCHO DE BANDA POR RED	✔	✔	✔	✔	✔	✔
LIMITE DE ANCHO DE BANDA POR IP	✔	✔	✔	✔	✔	✘
LIMITE DE ANCHO DE BANDA POR PUERTOS	✔	✔	✔	✔	✘	✘
SSL	✔	✔	✘	✔	✘	✘
FILTRO DE CONTENIDO	✔	✔	✔	✔	✔	✔

PfSense cumple con las funciones que toda red perimetral debe tener al ser un firewall robusto y no por ser de software libre quiere decir que no tenga un soporte puesto que en su versión pfSense Gold ofrece soporte en caso del que el sistema caiga y no se tenga que depender solamente de las personas que administran la red, haciendo que el trabajo de un administrador de red sea menos drástico con respecto a la seguridad perimetral.

2.2.8. POLÍTICAS DEL FIREWALL

(Microsoft, 2016) Describe que, en el firewall, deberán crearse reglas de reenvío. Dado que el firewall bloquea o reenvía todo el tráfico entrante, saliente y entre redes virtuales, se necesitan muchas reglas de firewall. Además, todo el tráfico entrante llegará a la dirección IP pública del servicio de seguridad (en puertos diferentes) para ser procesado por el firewall. El procedimiento recomendado es crear un diagrama de los flujos lógicos antes de configurar las subredes y las reglas de firewall para evitar tener que modificar más adelante.

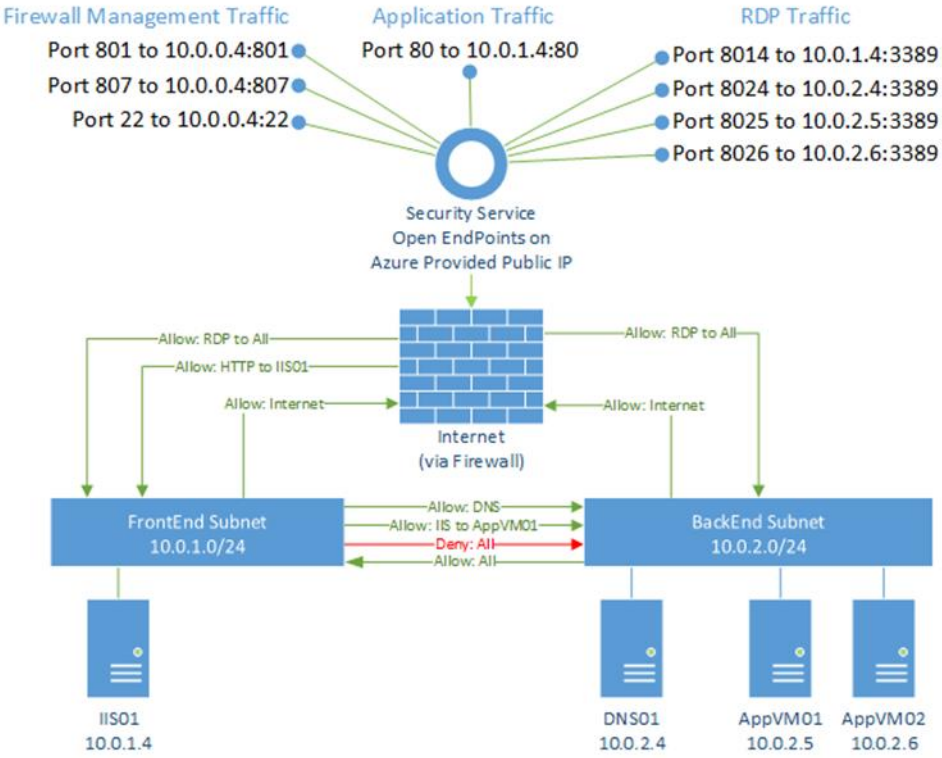


Ilustración 4: Ilustración lógica de las reglas del Firewall.
Fuente: (Microsoft, 2016).

2.2.9. ARQUITECTURA DE UNA RED PERIMETRAL

(Hernández , 2016) Describe que las arquitecturas de Seguridad Perimetral engloban los diferentes esquemas en los que es posible configurar soluciones de perímetro, tales como Firewalls/UTM /NGFW para cumplir con los niveles de Seguridad requeridos en las organizaciones.

Dichas arquitecturas deben de ser diseñadas de acuerdo a requerimientos que colaboren a que se lleve a cabo de manera correcta, la operación de día a día con el propósito de minimizar riesgos considerando la integridad, disponibilidad y confidencialidad de la información que es propiedad de la empresa.

Para la implementación de alguna arquitectura, se requiere evaluar las necesidades de una empresa analizando su operación ininterrumpida, sus recursos y los servicios que se brindan, además de su distribución geográfica. Algunos sistemas que hay que tomar en cuenta son: Intranets, Sitios de comercio electrónico, conmutadores, video vigilancia IP, ERP, CRM, bases de datos, entre otros. Una vez identificados todos estos puntos se debe de considerar también a qué usuarios se les brindaran los servicios, es decir, si son internos, si son usuarios en el Internet, o si se usarán por empleados fuera de la oficina central, en sucursales, etc. Con estos datos es posible plantear una arquitectura adecuada para cada situación, las arquitecturas propuestas se pueden combinar para brindar más ventajas de manera conjunta.

Ventajas:

- Administración simple.
- Arquitectura más económica.
- Estructura recomendada para puntos remotos donde se alojan sólo algunos servicios críticos, sin acceso directo a una LAN de usuarios, ej. Una granja de servidores Web.

Desventajas:

- Si se compromete el firewall, toda la red se verá afectada.
- Si se compromete un servidor o cualquier otro equipo, el atacante tendrá la posibilidad de continuar con los demás equipos sin más barreras de protección.

2.2.10. TIPOS DE SERVIDORES

(Claranet, 2012) Explica que, en el campo de la informática y las telecomunicaciones, por servidor se entiende "un equipo informático que forma parte de una red y provee servicios a otros equipos". Existen muchísimos tipos de servidor según su función y su contenido, cada día más, como ocurre con todos los elementos que siguen teniendo un papel determinante en el panorama tecnológico y de Internet. Estos son algunos de los tipos más comunes de servidores que podemos encontrar en el mercado:

- **Servidor de impresiones:** controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión.
- **Servidor de correo:** almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.
- **Servidor de fax:** almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas del fax.

- **Servidor de la telefonía:** realiza funciones relacionadas con la telefonía, como es la de contestador automático, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet.
- **Servidor proxy:** realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., depositar documentos u otros datos que se soliciten muy frecuentemente), también proporciona servicios de seguridad, o sea, incluye un cortafuego.
- **Servidor del acceso remoto (RAS):** controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes y reconoce la petición de la red.
- **Servidor web:** almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.
- **Servidor de base de datos:** provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.
- **Servidor de Seguridad:** Tiene software especializado para detener intrusiones maliciosas, normalmente tienen antivirus, antispyware, antimalware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques, los servidores de seguridad varían dependiendo de su utilización e importancia.

2.2.11. MODELO STRIDE

(Mejía, 2008) Menciona que el modelo STRIDE establece un marco que ayuda a identificar amenazas como: Suplantación de identidad, manipulación de datos, repudio, divulgación de información, denegación de servicio y elevación de privilegios.

- La suplantación de identidad es la capacidad que tiene una persona o dispositivo para acceder a recursos que han sido autorizados para otra persona o dispositivo, utilizando técnicas de engaño técnicas o sociables.
- La alteración de datos es la modificación de información, como por ejemplo un ataque de sesión hacking (secuestro), o alterar datos en una transmisión, etc.
- El repudio es la capacidad de negar que algo ha ocurrido. Un ejemplo de repudio sería que un usuario cargue datos dañinos en el sistema cuando en este no se puede realizar un seguimiento de la operación.
- La divulgación de información implica la exposición de información ante usuarios que se supone que no deben disponer de ella. Un ejemplo de divulgación de información es la capacidad de un intruso para leer archivos médicos confidenciales a los que no se le ha otorgado acceso.

- Los ataques de denegación de servicio privan a los usuarios del servicio normal. Un ejemplo de denegación de servicio consistiría en dejar un sitio Web inaccesible al inundarlo con una cantidad masiva de solicitudes HTTP.
- La elevación de privilegios es el proceso que siguen los intrusos para realizar una función que no tienen derecho a efectuar. Para ello, puede explotarse una debilidad del software o usar las credenciales de forma ilegítima.

Tabla 2: Ejemplos de las funciones del modelo STRIDE.
Fuente: (Mejía, 2008)**.**

Tipos de amenazas	Ejemplos
Suplantación	- Falsificación de mensajes de correo electrónico. - Reproducir paquetes de autentificación
Alteración	- Alterar datos durante la transmisión - Cambiar datos en archivos
Repudio o rechazo	- Eliminar el archivo esencial y denegar este hecho. - Adquirir un producto y negar posteriormente que se adquirido
Divulgación de información	- Exponer la información en mensajes de error - Exponer el código de los sitios web
Denegación de servicio	- Inundar una red con paquetes de sincronización - Inundar una red con paquetes ICMP(Internet Control Message Protocol) falsificados
Elevación de privilegios	- Explotar la saturación de un búfer para obtener privilegios en el sistema - Obtener privilegios de administrador de forma legítima.

Para ello puede utilizar dos enfoques básicos:

- Utilizar el modelo STRIDE para identificar las amenazas
- Utilizar listas de categorías de amenazas

Tabla 3: Diferentes hilos o tipos de amenazas que afectan a cada tipo de elemento.
Fuente: (Mejía, 2008)**.**

ELEMENTO	S	T	R	I	D	E
Entidad externa	✓		✓			
Proceso	✓	✓	✓	✓	✓	✓
Almacén de datos		✓	✓	✓	✓	
Flujo de datos		✓		✓	✓	

Para tomar un acercamiento metódico, se debe trabajar por encima de la pila: Desde las amenazas a la red, a través de las amenazas al host, y finalmente las amenazas a la aplicación. Por lo que, durante este paso, deberá realizar las siguientes tareas:

a. Identificar las amenazas de red
b. Identificar las amenazas de host
c. Identificar las amenazas de aplicación

La realidad en el mundo de la seguridad es que se reconoce la presencia de amenazas y se gestiona sus riesgos (Guitierrez, 2011).

Hay dos tipos de análisis de riesgo en seguridad de la información:

Análisis Cualitativo de Riesgos

Existen varias formas de conducir un análisis cualitativo de riesgos.

Un método usa un modelo basado en escenarios. Este enfoque es mejor para las grandes ciudades, estados y países porque no es práctico intentar enumerar todos los activos, que es el punto de partida para cualquier análisis cuantitativo de riesgos.

Por ejemplo, cuando un gobierno nacional típico enumera todos sus activos, la lista tendría cientos o miles de cambios y ya no sería precisa. Con el análisis cualitativo de riesgos, la

investigación es exploratoria y no siempre se puede graficar o demostrar matemáticamente. Se centra en la comprensión de por qué existe el riesgo y cómo varias soluciones funcionan para resolver el riesgo (Pars, 2014).

Análisis cuantitativo de riesgos

El análisis cuantitativo de riesgos utiliza un modelo matemático que asigna una cifra monetaria al valor de los activos. El costo de las amenazas se realiza El costo de las implementaciones de seguridad. Se basa en fórmulas específicas para determinar el valor de las variables de decisión de riesgo (Cisco - CCNA, s.f.).

2.2.12. AMENAZAS INFORMATICAS

(Tarazona T, 2007) Define que básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores), fallas en los sistemas de procesamiento de información, desastres naturales y actos maliciosos o malintencionados, algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DDoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

FTP

El acrónimo de FTP es protocolo de transferencia de ficheros (File Transfer Protocol) y es un software cliente/servidor que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP (Ordenadores y portatiles, 2014).

NAT

Traducción de Dirección de Red. Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red (especialmente Internet). Cada computadora tiene una dirección IP distinta (generalmente no válida para Internet) (Alegsa, 2010).

VPN

(Red Privada Virtual) Tecnología de redes que permite la extensión de una red de área local sobre una red pública o no controlada (como internet). Por ejemplo, crear una red entre distintas computadoras utilizando como infraestructura a internet. Evidentemente debe haber mecanismos de protección de los datos que se manejan (Alegsa, 2010).

DNS

(Sistema de nombres de dominio) Sistema de Nombres de Dominio. Conjunto de protocolos y servicios para la identificación/conversión de una dirección de internet expresada en lenguaje natural por una dirección IP (Alegsa, 2010).

ROUTER

Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red (Alegsa, 2010).

IDS

(Sistema de detección de intrusos) Sistema que detecta manipulaciones no deseadas en el sistema, especialmente a través de internet. Las manipulaciones pueden ser ataques de hackers malintencionados (Alegsa, 2010).

FreeBSD

(FreeBSD, 2013) describe que es un avanzado sistema operativo para arquitecturas x86 compatibles (incluyendo Pentium® y Athlon™), amd64 compatibles (incluyendo Opteron, Athlon 64 y EM64T), Alpha /AXP, IA-64, PC-98 y Ultra SPARC. FreeBSD es un derivado de BSD, la versión de UNIX desarrollada en la Universidad de California, Berkeley. FreeBSD es desarrollado y mantenido por un numeroso equipo de personas. El soporte para otras arquitecturas está en diferentes fases de desarrollo (FreeBSD, 2013).

DMZ

(Zona desmilitarizada) que se sitúa entre la red interna y la red externa (normalmente Internet). La función de una DMZ es permitir las conexiones tanto desde la red interna como de la externa, mientras que las conexiones que parten de la DMZ solo puedan salir a la red interna (Muycomputer, s.f.).

DDoS

Un ataque distribuido de denegación de servicio o DDoS es el bombardeo de solicitudes simultáneas de datos a un servidor central. El atacante genera estas solicitudes desde múltiples sistemas comprometidos.

Al hacerlo, el atacante espera agotar el ancho de banda de Internet y la RAM del objetivo. El objetivo final es bloquear el sistema del objetivo e interrumpir su negocio (Cisco, s.f.).

ALTERACIÓN

Implica la modificación maliciosa de datos. Los ejemplos incluyen cambios no autorizados realizados a datos persistentes, como el contenido en una base de datos, y la alteración de datos a medida que fluye entre dos computadoras a través de una red abierta, como Internet (Microsoft , 2017).

2.4. HIPÓTESIS

2.4.1. FORMULACIÓN DE LA HIPÓTESIS

La implementación de un firewall open source permitirá incrementar la seguridad perimetral en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

CAPITULO III: MATERIALES Y METODOS

3.1. VARIABLES Y OPERACIONALIZACIÓN DE VARIABLES

Tabla 4: Variables e indicadores.
Fuente: Elaboración Propia.

Variables	Definición conceptual	Dimensión	Indicadores	Instrumento
INDEPENDIENTE Implementación de una solución de seguridad perimetral open source	Políticas de seguridad que se usan para proteger los servicios la información sensible entre redes LAN y WAN	Implementación	Firewall instalado, configurado y en producción validado por el administrador de la red telemática de la Universidad Nacional Pedro Ruiz Gallo	Entrevista con el administrador de la red dando conformidad de la instalación del firewall
DEPENDIENTE Seguridad de la red telemática de la Universidad Nacional Pedro Ruiz Gallo	Referida a la forma en que las reglas del firewall estén configuradas para controlar el acceso de los usuarios y tráfico que entra y sale de la red	Vulnerabilidad	Cantidad de intentos de acceso no deseados, tratando de vulnerar la seguridad de la red telemática de a la Universidad	Ficha de reporte de incidencias

3.2. TIPO DE ESTUDIO Y DISEÑO DE INVESTIGACIÓN

3.2.1. TIPO DE INVESTIGACIÓN

La siguiente investigación es una investigación no experimental y descriptiva. La finalidad es aplicada porque permitirá la mejora a un problema.

3.3. POBLACIÓN Y MUESTRA EN ESTUDIO

3.3.1. POBLACIÓN

En este estudio hemos considerado 7 servicios los cuales la red telemática proporciona, los cuales se desean proteger de los intentos de ingresos no deseados, debido a que estos servicios funcionan a todo el año, se produce un sin fin de intentos de ingreso mal intencionado por ello definimos que la población es infinita.

3.3.2. MUESTRA

Debido a que los servicios cuentan con un número alto de intentos de ingreso no deseado a lo largo de su tiempo de uso, aplicamos la fórmula de población infinita para determinar el tamaño de la muestra que en este caso será el número de ingresos a tomar en cuenta.

Formula:

$$\mathbf{n= \frac{Z^2 \times p \times q}{e^2}}$$

Donde:

n: Tamaño de la muestra.
Z: Nivel de confianza, cuyos valores más frecuentes son:

Tabla 5: Nivel de confianza.
Fuente: Elaboración Propia.

Z	Nivel de confianza		
	90% (0.9)	95% (0.95)	99% (0.99)
	1.645	1.96	2.58

e: Error máximo permitido en el muestreo.
p: Población de éxito (lo que se espera encontrar).
q: Población de fracaso.

Debido a que no se conoce exactamente la población de éxito y fracaso se toma a p (50%) y q (50%).

Considerando un margen de error de 3% y un nivel de confianza del 95% obtenemos.

$$\mathbf{n= \frac{1.96^2 \times 0.5 \times 0.5}{0.03^2} = 1067}$$

En promedio se determinó como tamaño de muestra que hay 1067 ataques de accesos no deseados exitosos que serán divididos entre los 7 servicios que tiene la red telemática, ya que se utilizaran para atacar a los servicios antes y después del firewall.

3.4. MÉTODOS, TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.4.1. OBSERVACIÓN

Es la captura de la información visual de lo que ocurre en la realidad para identificar los problemas que se están dando según su estudio. Es indispensable tener en cuenta que para estudiar adecuadamente todo el problema es necesaria posible información.

3.4.2. ENTREVISTAS

Las entrevistas se usan para recolectar información en forma verbal, usando preguntas que propone el que va a entrevistar. Quienes responderán estas preguntas serán las personas involucradas.

3.4.3. REGISTRO DE INCIDENCIAS

Para este estudio se utilizó como instrumento las fichas de reporte de incidentes en la red donde se registraron los datos de los eventos de consulta que proporciona el administrador de una red telemática.

CAPITULO IV: RESULTADOS

4.1. EVALUACIÓN DE LA SEGURIDAD PERIMETRAL

En el caso del Portal web se utiliza y evalúa la muestra con el objetivo de burlar la seguridad perimetral antes de instalar el firewall Open Source para comprobar el estado de efectividad del firewall existente, para ello utilizamos 152 ataques de accesos no autorizados a cada servicio tomando en cuenta el tipo de ataque y descubrimos que al portal web, lograron 78 ataques de accesos no autorizados exitosos, quedando al descubierto que 74 intentos no son exitosos, por ende se muestran registrados en el gráfico en calidad de intentos de accesos logrados, dejando en evidencia la baja calidad de protección al servicio de portal web, antes de implementar el firewall.

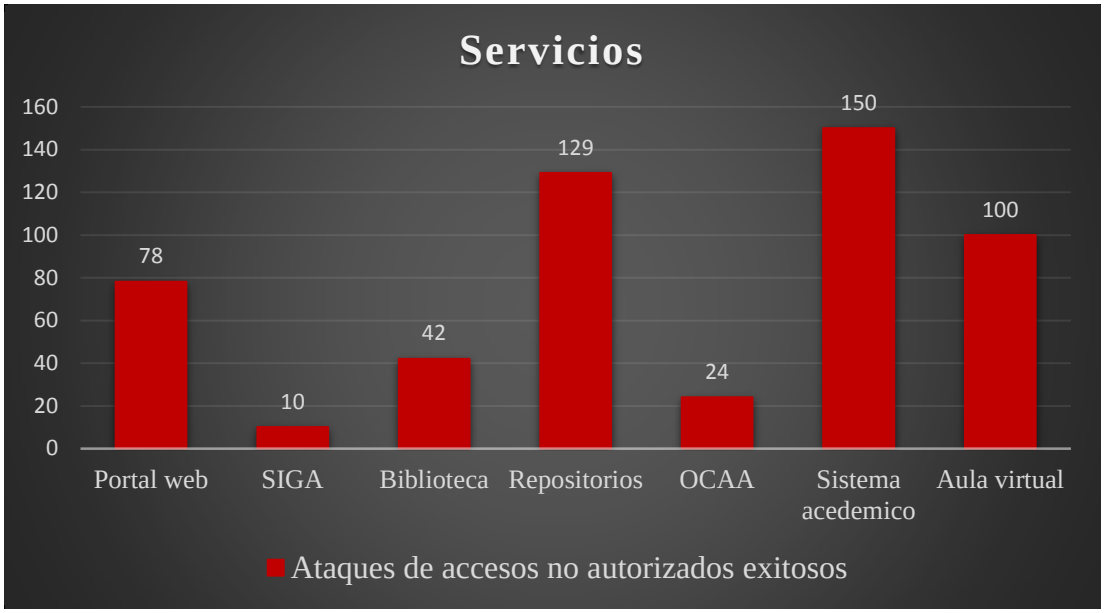


Ilustración 5: Análisis de la vulnerabilidad de los servicios antes de la implementación de una solución de seguridad perimetral open source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

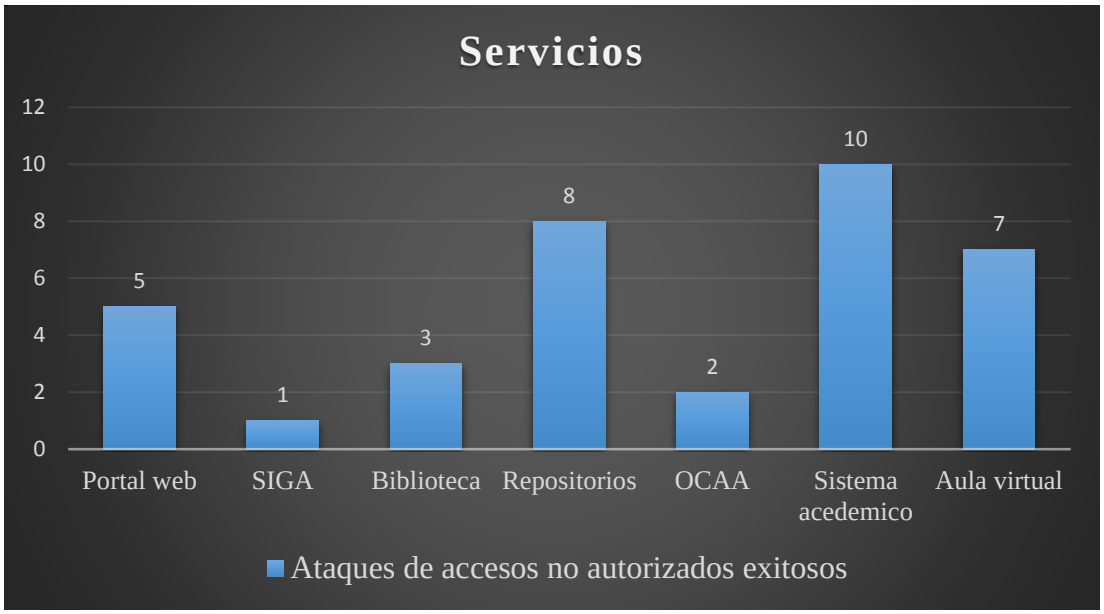


Ilustración 6: Análisis de la vulnerabilidad de los servicios después de la implementación de una solución de seguridad perimetral open source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Al realizar el análisis de los sistemas de seguridad perimetral en los servicios de la red telemática de la Universidad Nacional Pedro Ruiz Gallo antes y después de la implementación de una solución de seguridad perimetral open source, se determinó que el promedio de ataques de accesos no autorizados exitosos antes de la implementación del sistema que fue de 104.5 con desviación estándar de 98.33 ingresos, sin embargo después de la implementación el promedio fue de tan solo del 4.88 con una desviación estándar de 3.18 ingresos, se puede observar existe una diferencia del 99.63 de ataques de accesos no autorizados exitosos en promedio a favor del firewall de seguridad perimetral, también se puede observar que el número máximo y mínimo de ingresos antes de la implementación del firewall fue de 150 y 10 respectivamente, mientras que después de la implementación fue de 10 y 1 respectivamente.

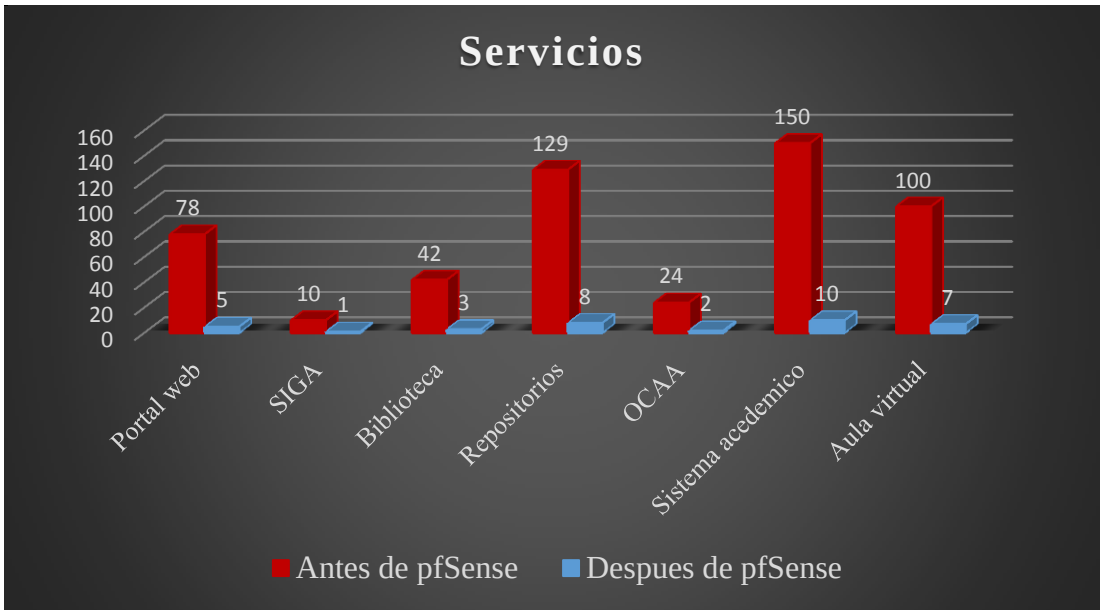


Ilustración 7: Comparativa de la vulnerabilidad en la seguridad perimetral antes y después de la implementación de una solución de seguridad perimetral open source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Por lo tanto, se procede a comparar los intentos de ingreso no deseados antes y después del firewall y así ver que tan efectivo fue la implementación de este.

En cuanto al PORTAL WEB se observa que hubo una reducción del 94%:

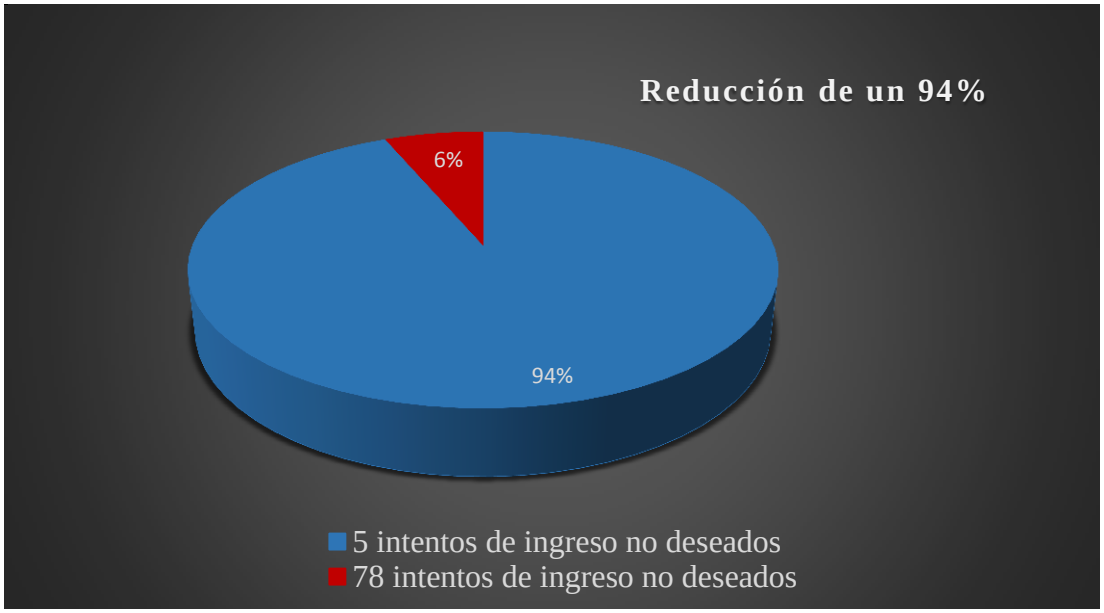


Ilustración 8: Porcentaje de mejora.

En cuanto al SIGA se observa que hubo una reducción del 90%:

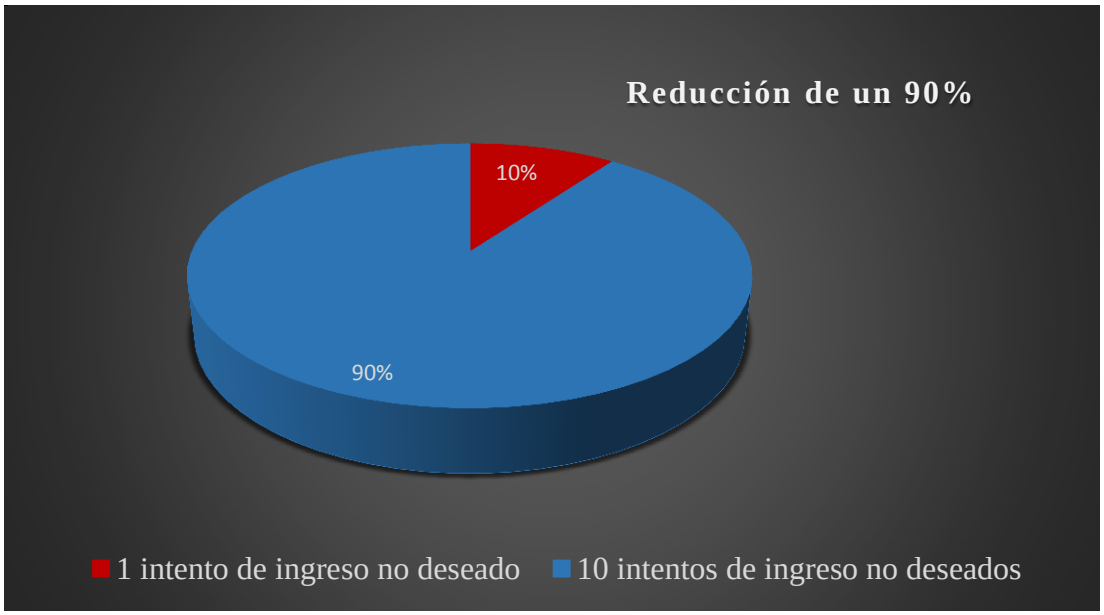


Ilustración 9: Porcentaje de mejora.

En cuanto a la BIBLIOTECA se observa que hubo una reducción del 93%:

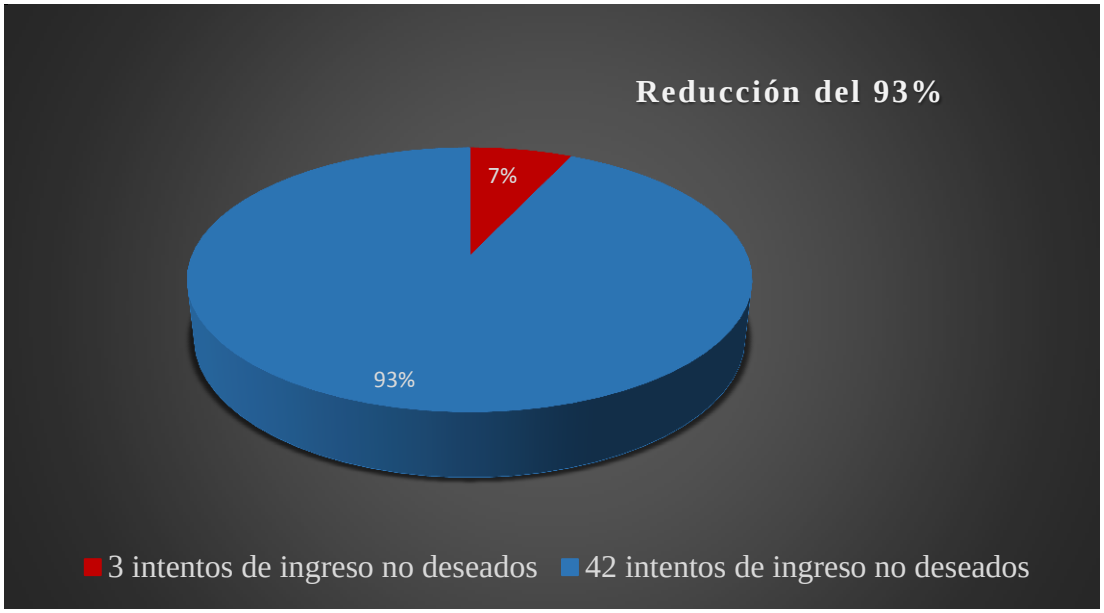


Ilustración 10: Porcentaje de mejora.

En cuanto a los REPOSITORIOS se observa que hubo una reducción del 96%:

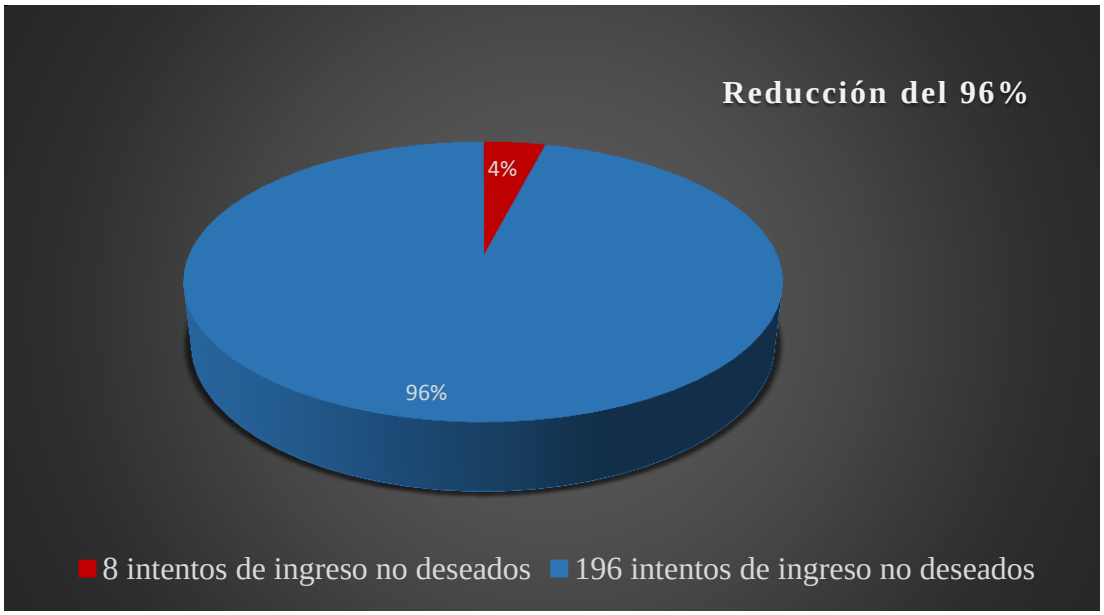


Ilustración 11: Porcentaje de mejora.

En cuanto a los OCAA se observa que hubo una reducción del 92%:

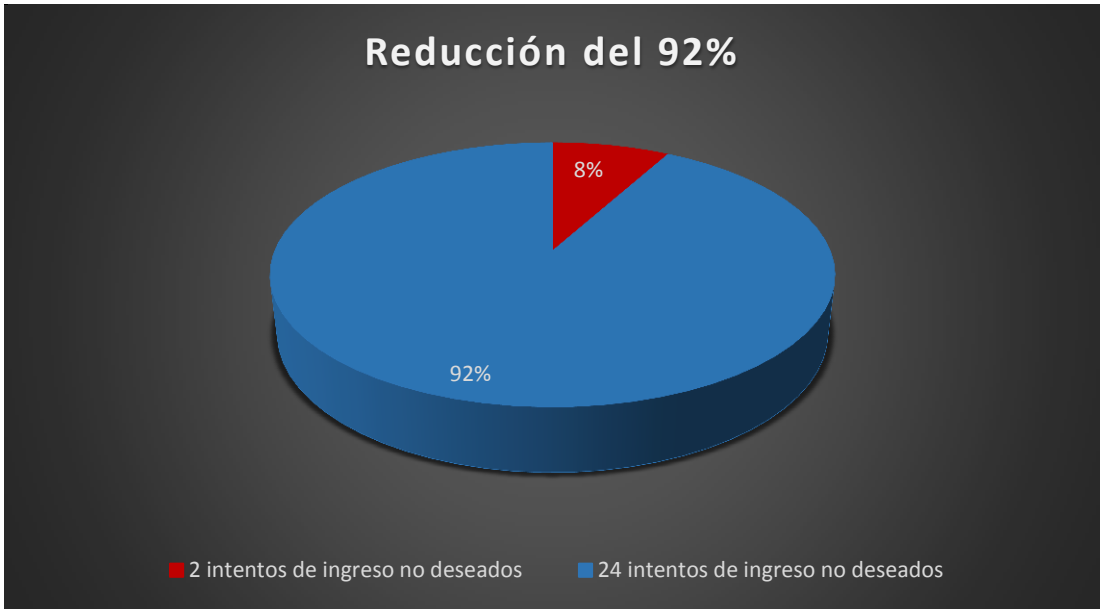


Ilustración 12: Porcentaje de mejora.

En cuanto a los SISTEMA ACADEMICO se observa que hubo una reducción del 96%:

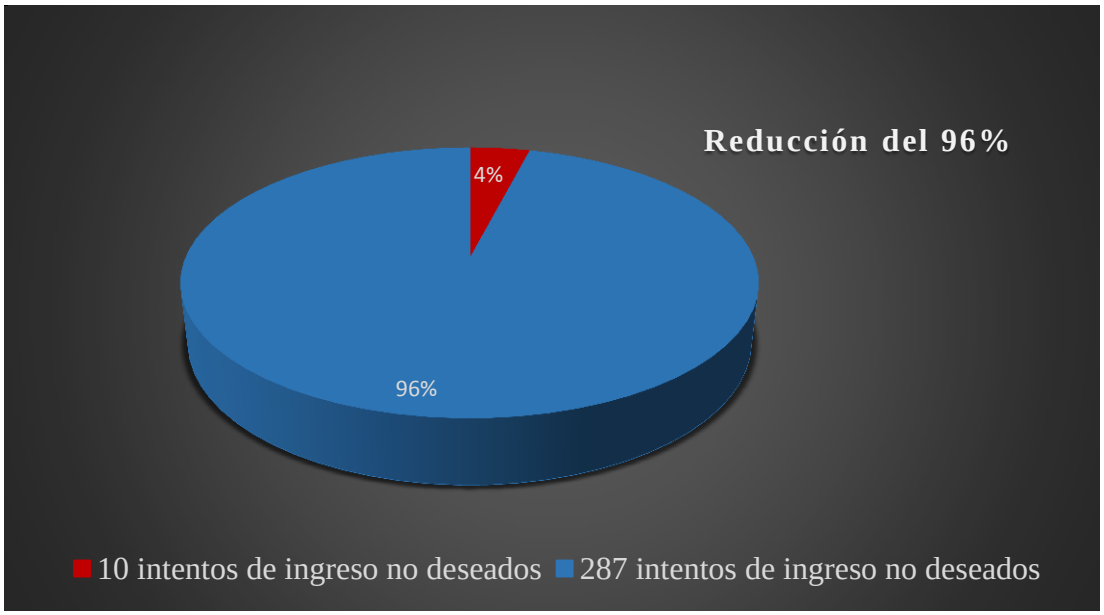


Ilustración 13: Porcentaje de mejora.

En cuanto a los AULA VIRTUAL se observa que hubo una reducción del 95%:

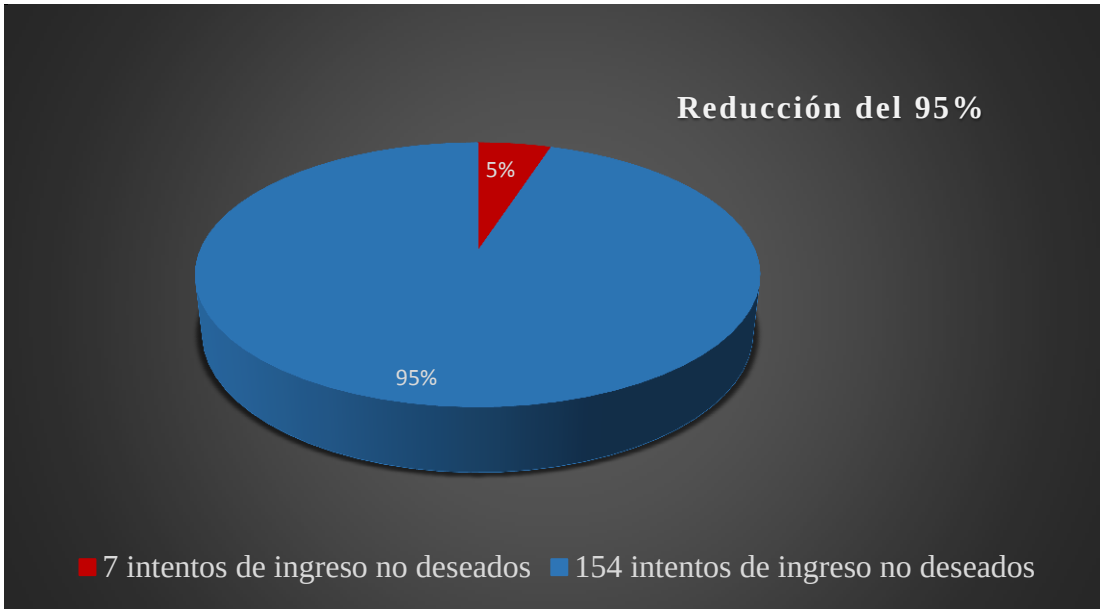


Ilustración 14: Porcentaje de mejora.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

El objetivo de esta tesis fue incrementar significativamente la seguridad de base de datos y aplicaciones en la red telemática de la Universidad Nacional Pedro Ruiz Gallo, implementando un firewall basado en FreeBSD (pfSense), habiéndose cumplido el objetivo general y luego de hacer análisis y comparaciones entre los antecedentes encontrados, los resultados son los siguientes:

- Se pudo encontrar la existencia de ataques a cada uno de los 7 servicios que la red telemática de la UNPRG ofrece. Se detectaron vulnerabilidades con un promedio de 113 por servicio siendo el mayor acceso no deseado al "SISTEMA ACADÉMICO" con 287 y el menor "SIGA" con 10.

- Se implementó y configuró el sistema pfSense para la gestión de la seguridad perimetral tal como consta en el Acta de Instalación.

- Después de la instalación y puesta en producción el firewall pfSense se pudo detectar un significativo descenso de las vulnerabilidades en la red siendo un promedio de 5.14 y el servicio de "SISTEMA ACADEMICO" con 10 y el menor "SIGA" con 1.

Con esto podemos afirmar que la implementación del firewall pfSense aumentó la seguridad perimetral dentro de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

5.2. RECOMENDACIONES

- La seguridad interna de la red telemática depende mucho del diseño y una adecuada implementación de las políticas de seguridad dentro de la institución, las cuales deben ser actualizadas y modificadas de manera continua ante las crecientes amenazas informáticas de personas que buscan dañar y sabotear el trabajo de la Universidad Nacional Pedro Ruiz Gallo.

- Las amenazas y vulnerabilidades a la red telemática siempre están mejorando y desarrollándose de manera mucho más eficiente, por lo que las políticas de seguridad de la red deben realizarse de manera anticipada, evitando así que los servicios queden vulnerables.

- Se recomienda a la red telemática de la Universidad nacional Pedro Ruiz Gallo que tome en cuenta los resultados obtenidos, para la mejora continua de la seguridad perimetral de sus servicios.

- Se recomienda prudencia al ser implementada en otras instalaciones de redes telemáticas o en cualquier institución dedicadas a la búsqueda continua de mejorar la seguridad para sus servicios internos de red. Ya que su arquitectura de red puede ser diferente.

- Se recomienda mejora continua en su utilización como parte de la innovación.

CAPITULO VI: REFERENCIAS BIBLIOGRÁFICAS

Alegsa, L. (05 de 12 de 2010). *Alegsa*. Obtenido de Diccionario de informática y tecnología: http://www.alegsa.com.ar/Diccionario/diccionario.php

ANDREW S. , T. (03 de 01 de 2009). *redes-de-computadoras-tanenbaum-4ta-edicion-espanol.* Obtenido de juliorestrepo.wordpress.: https://juliorestrepo.files.wordpress.com/2010/08/redes-de-computadoras-tanenbaum-4ta-edicion-espanol.pdf

Baca, G. (2016). *Introducción a la seguridad informática.* Mexico D.F: Grupo Editorial Patricia.

Cisco - CCNA. (s.f.). *Introducción a las redes*. Obtenido de Tipos de vulnerabilidades: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11.2.1.3

Cisco. (s.f.). *¿Qué es un ataque DDoS?* Obtenido de https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

Cisco. (s.f.). *¿Qué es un cortafuegos?* Obtenido de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Claranet. (09 de 08 de 2012). *Claranet*. Obtenido de ¿Qué tipos de servidores hay?: https://www.claranet.es/about/news/que-tipos-de-servidores-hay.html

DA SILVA DE OLIVEIRA DIAZ RENZO GIANCARLO, S. L. (2016). *ALICIA - Acceso libre a información Científica para la innovación.* Obtenido de Efecto de la Implementación del Sistema PfSense en la Seguridad Perimetral Lógica en los Servicios de la Red Troncal de la Universidad Nacional de la Amazonía Peruana, Iquitos-2016 .

Dias, C. M. (Septiembre de 2013). *Universidad Politécnica de MAdrid.* Obtenido de Implantación de un sistema de seguridad perimetral: http://oa.upm.es/22228/

FreeBSD. (13 de 11 de 2013). *FreeBSD*. Obtenido de Acerca de FreeBSD: https://www.freebsd.org/es/about.html

GONZALES, J. L. (02 de 08 de 2012). *PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.* Obtenido de DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD PERIMETRAL DE UNA RED DE COMPUTADORAS PARA UNA EMPRESA PEQUEÑA: http://tesis.pucp.edu.pe/repositorio/handle/123456789/1448

Guevara Tinoco, R. C., & López López, W. L. (02 de 2016). *USS - REPOSITORIO INSTITUCIONAL.* Obtenido de Implementación de un sistema criptográfico a través de algoritmos avanzados de encriptación para mejorar la seguridad perimetral de una red informática: http://repositorio.uss.edu.pe/handle/uss/350

Guitierrez, F. (25 de Febrero de 2011). *Modelado de amenazas*. Obtenido de Amenazas: http://seguridadenlanube.blogspot.pe/2011/02/el-modelado-de-amenazas-de-seguridad-es.html

Hernández , D. (01 de 08 de 2016). *Cerouno*. Obtenido de Tipos de Arquitectura en Seguridad Perimetral: http://blog.cerounosoftware.com.mx/tipos-de-arquitectura-en-seguridad-perimetral

Honores Quinde, R. J. (16 de Febrero de 2016). *ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.* Obtenido de ESQUEMA DE SEGURIDAD PERIMETRAL APLICABLE A UNA PYME MEDIANTE EL USO DE HERRAMIENTAS DE SOFTWARE LIBRE: https://www.dspace.espol.edu.ec/handle/123456789/37411

LinuxLinks. (s.f.). *LinuxLinks*. Obtenido de 6 mejores soluciones de firewall de código abierto: https://www.linuxlinks.com/firewall/

Mejía, W. (julio de 2008). *WillyXoft*. Obtenido de Modelado de Amenazas: https://willyxoft.wordpress.com/articulos/modelado-amenazas/

Mendez, L. (17 de 02 de 2017). *Redes Empresariales*. Obtenido de Blog Cisco Latinoamérica: https://gblogs.cisco.com/la/en-leobardo-quieres-incrementar-la-eficiencia-en-tu-negocio-domina-tu-borde-de-red/

Microsoft . (17 de 08 de 2017). *Microsoft Azure*. Obtenido de Amenazas de Microsoft Threat Modeling Tool: https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool-threats

Microsoft. (01 de 02 de 2016). *Microsoft Azure*. Obtenido de Ejemplo 3: Creación de una red perimetral para proteger las redes con un firewall, enrutamiento definido por el usuario y grupo de seguridad de red: https://docs.microsoft.com/es-es/azure/virtual-network/virtual-networks-dmz-nsg-fw-udr-asm

Muycomputer. (s.f.). *Muycomputer*. Obtenido de DMZ: qué es, para qué sirve y como activarla en un router D-Link: https://www.muycomputer.com/2014/01/13/que-es-dmz-dlink/

Ordenadores y portatiles. (2014). *Ordenadores y portatiles*. Obtenido de ¿Qué es y para qué sirve FTP?: http://www.ordenadores-y-portatiles.com/ftp.html

Pars, L. (12 de mayo de 2014). *Guatewares*. Obtenido de Modelo STRIDE de Microsoft: http://www.guatewares.com/2014/05/modelo-stride-de-microsoft.html

pfsense. (s.f.). *Descripción general de pfSense*. Obtenido de pfsense: https://www.pfsense.org/about-pfsense/

Salcedo, L. (29 de 12 de 2017). *Mi diario Python*. Obtenido de Redes de Computadoras - Protocolos y Tipos de Redes de Computadoras: http://www.pythondiario.com/2017/12/redes-de-computadoras-protocolos-y.html

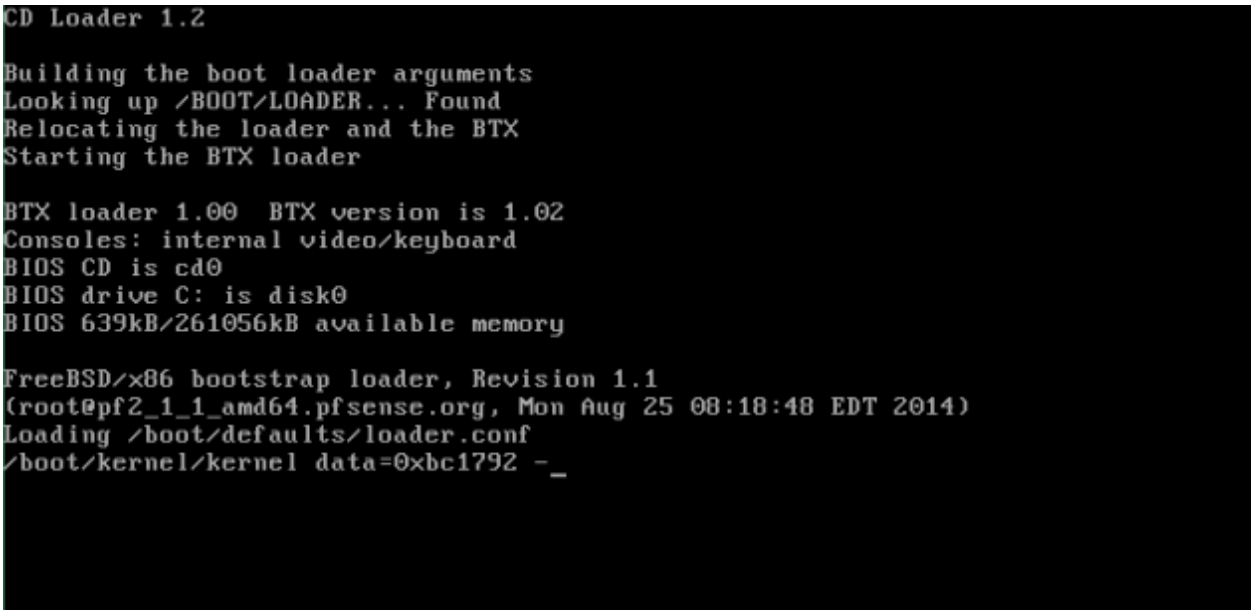
Sánchez, V. (11 de 01 de 2013). *Elementos básicos de la seguridad perimetral.* Obtenido de wordpress: https://vicentesanchez90.files.wordpress.com/2013/01/elementos-basicos-de-la-seguridad-perimetral.pdf

Tarazona T, C. (2007). *Amenazas informáticas y seguridad de la información.* Obtenido de Derecho Penal Y Criminología: https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

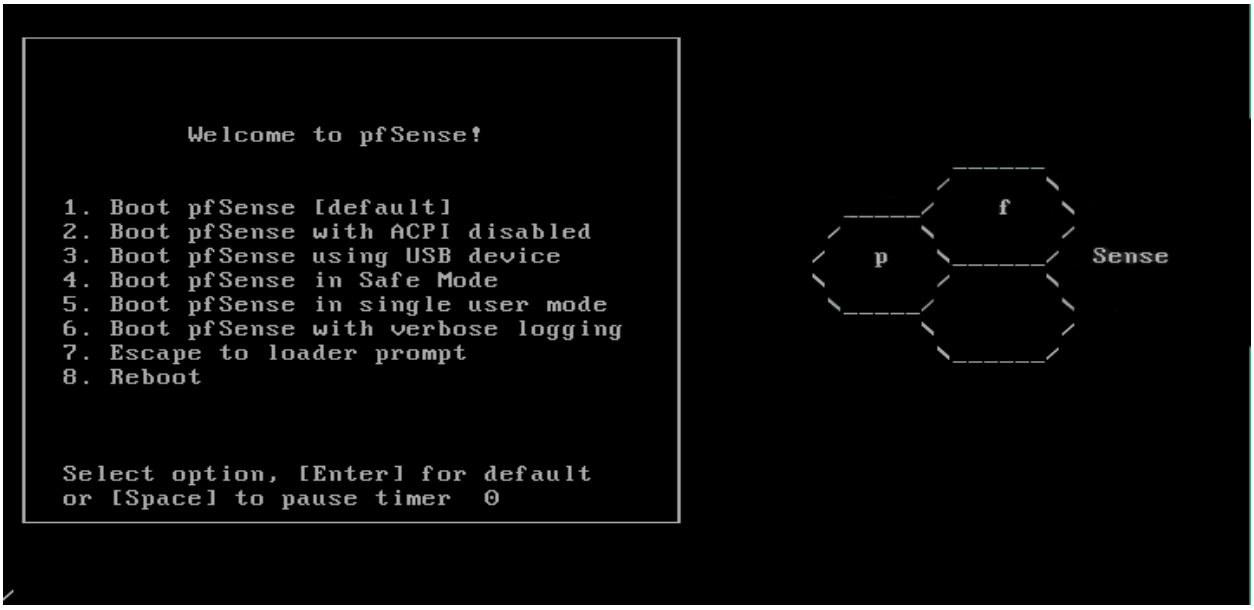
ANEXOS

Anexo 1: Instalación del firewall pfSense

Espere que se identifica la configuración

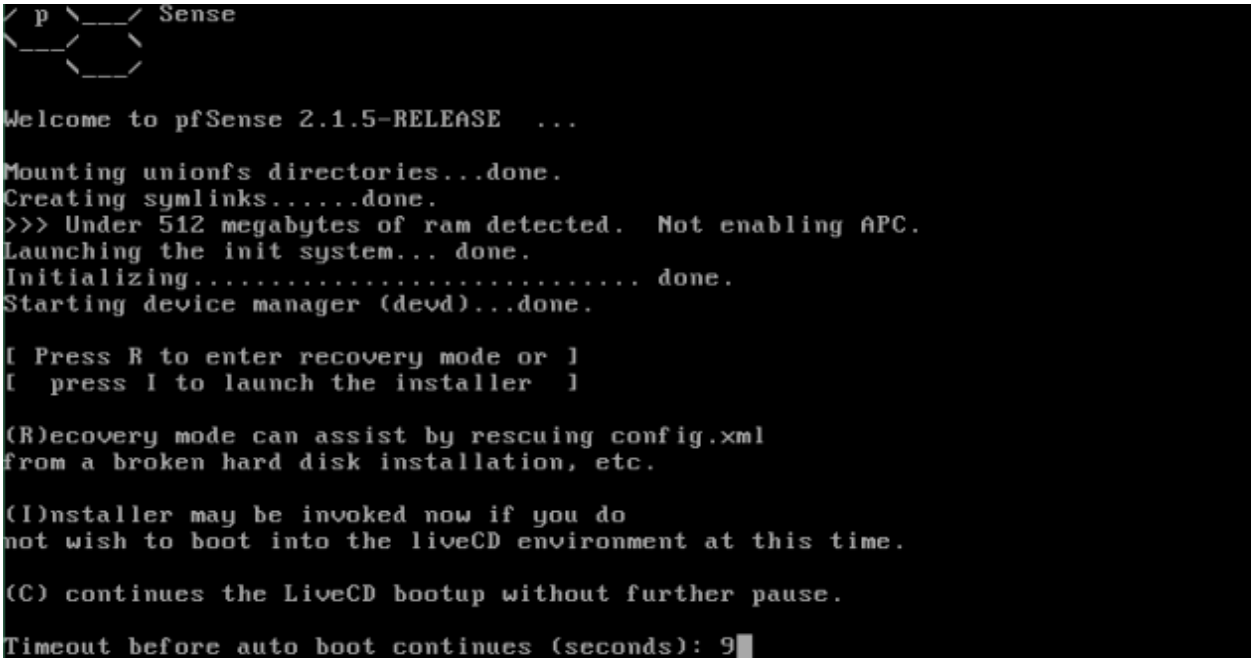


Luego nos quedamos con una pantalla como esta

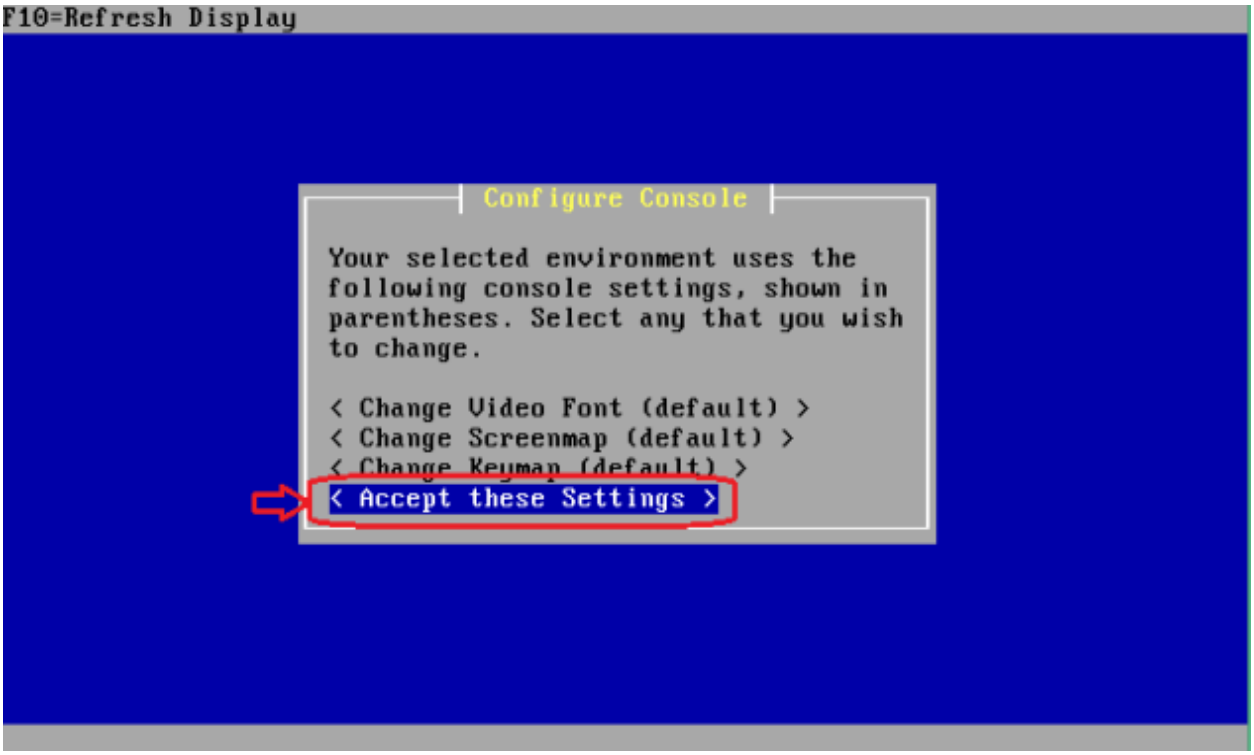


Presiona entrar o espere que se iniciar la instalación por defecto

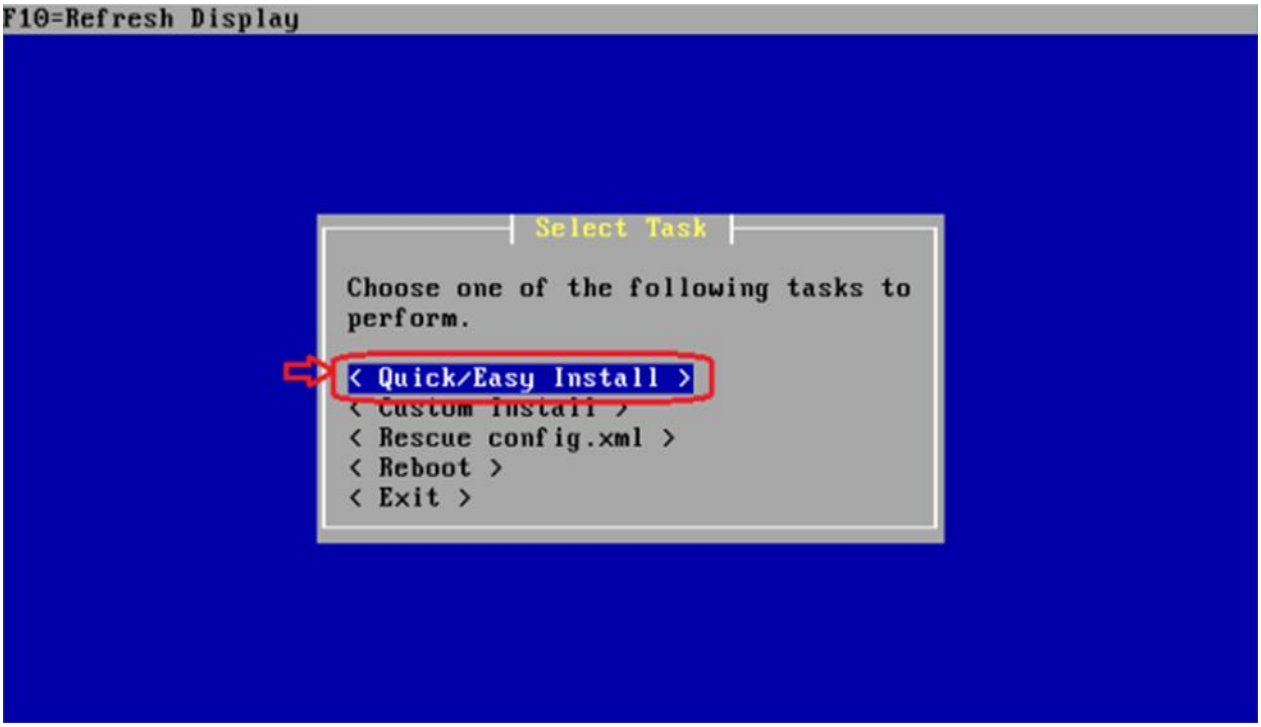
Cuando tenga esta pantalla, presiona la tecla “i” para instalar PfSense



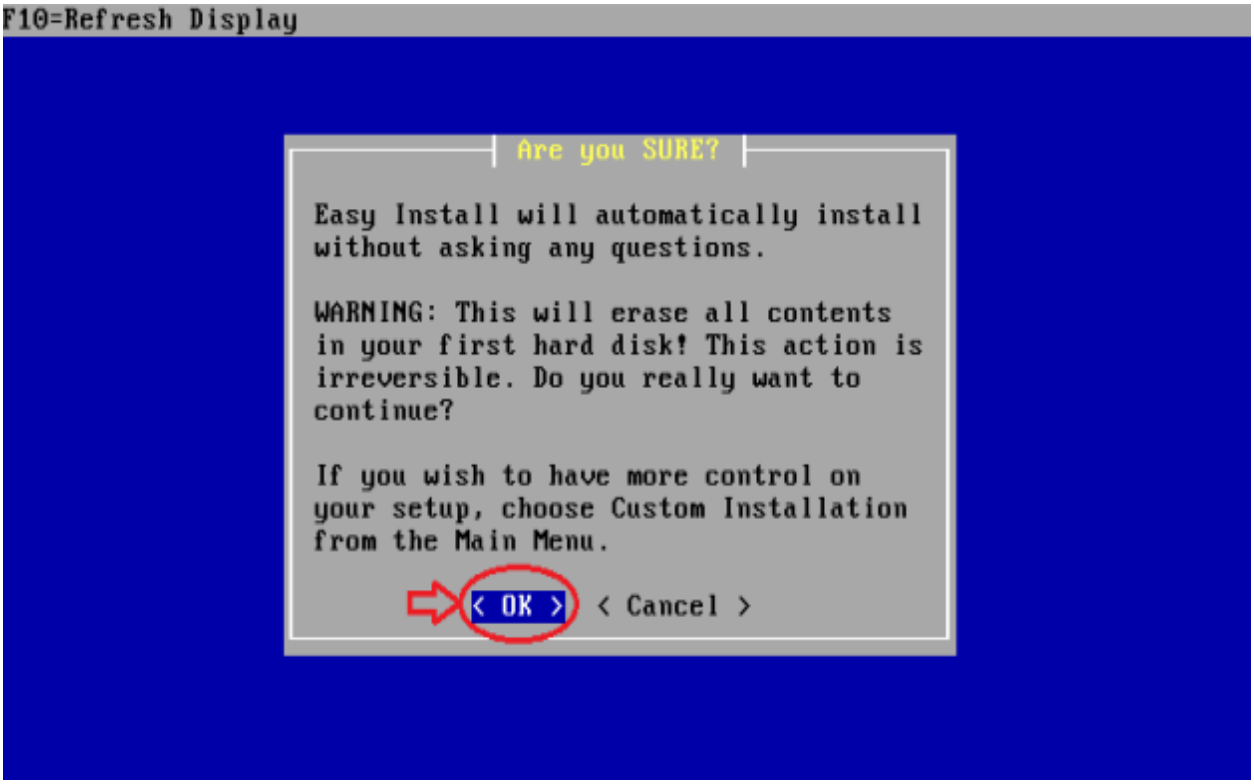
Acepta las configuraciones por defecto ya en compatible para todo caso



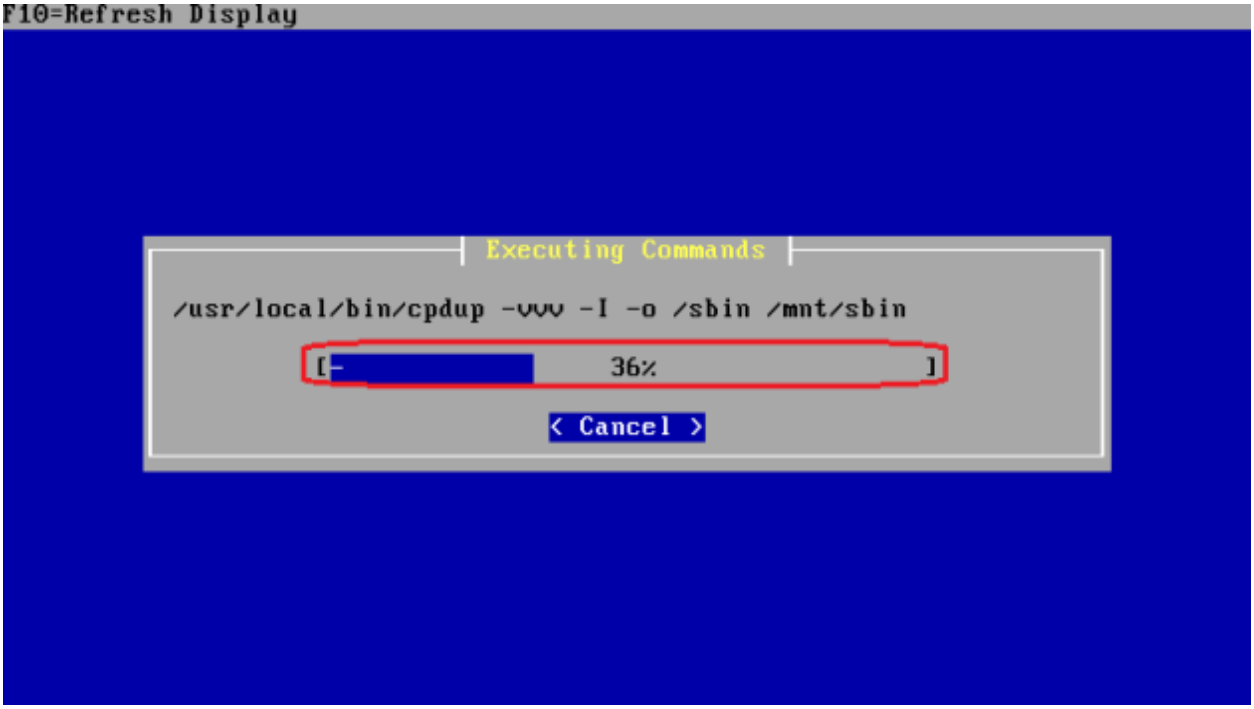
Acepta la instalación sencilla y rápida


F10=Refresh Display
Select Task
Choose one of the following tasks to perform.
< Quick/Easy Install >
< Custom Install >
< Rescue config.xml >
< Reboot >
< Exit >

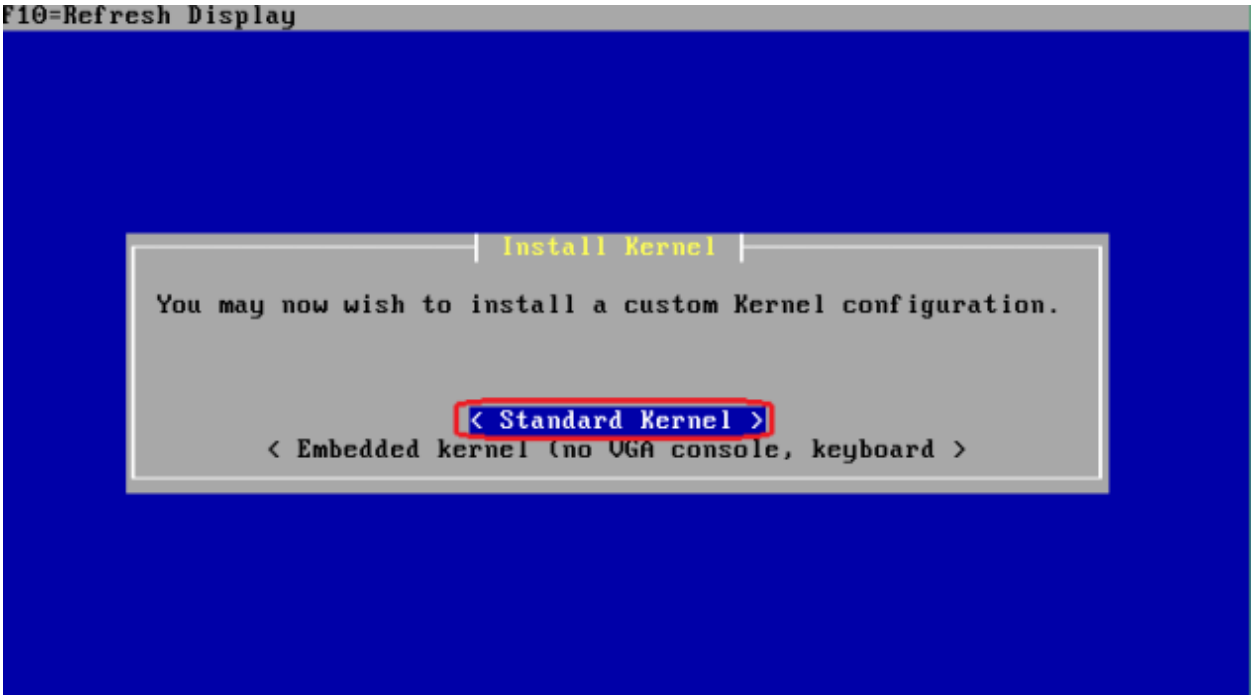
Presiona ok


F10=Refresh Display
Are you SURE?
Easy Install will automatically install without asking any questions.
WARNING: This will erase all contents in your first hard disk! This action is irreversible. Do you really want to continue?
If you wish to have more control on your setup, choose Custom Installation from the Main Menu.
< OK >
< Cancel >

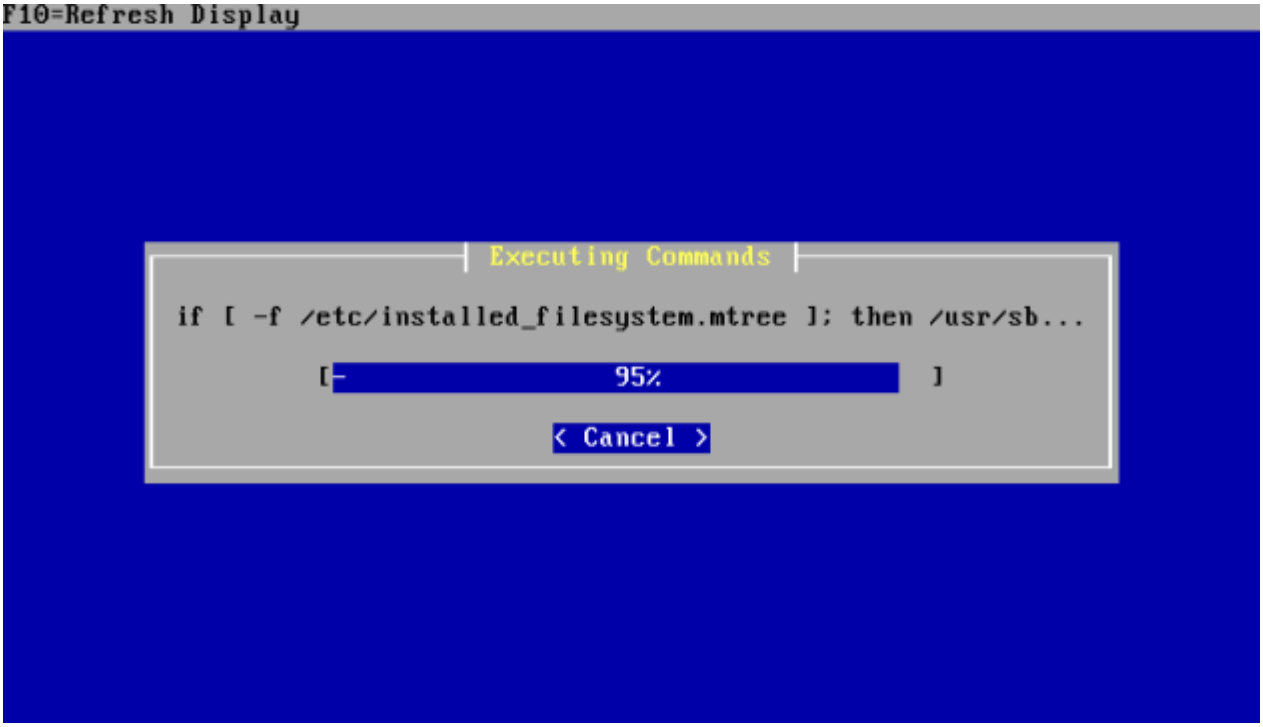
Espera que se instale PfSense



Selecciona el núcleo [kernel] estándar



Espere la instalación completa de sistemas de fichero



Ahora, desengancha la ISO y presiona enter para reiniciar

Así, hemos terminado la instalación de PfSense

Ahora presionamos F1 para arrancar el firewall

Procedemos a asignar interfaces, es decir a identificarlas, hn0 será para la WAN y hn1 será para la LAN y para hacer esto marcamos la opción "1"

Nos pedirá configurar VLANs en este caso le diremos que no

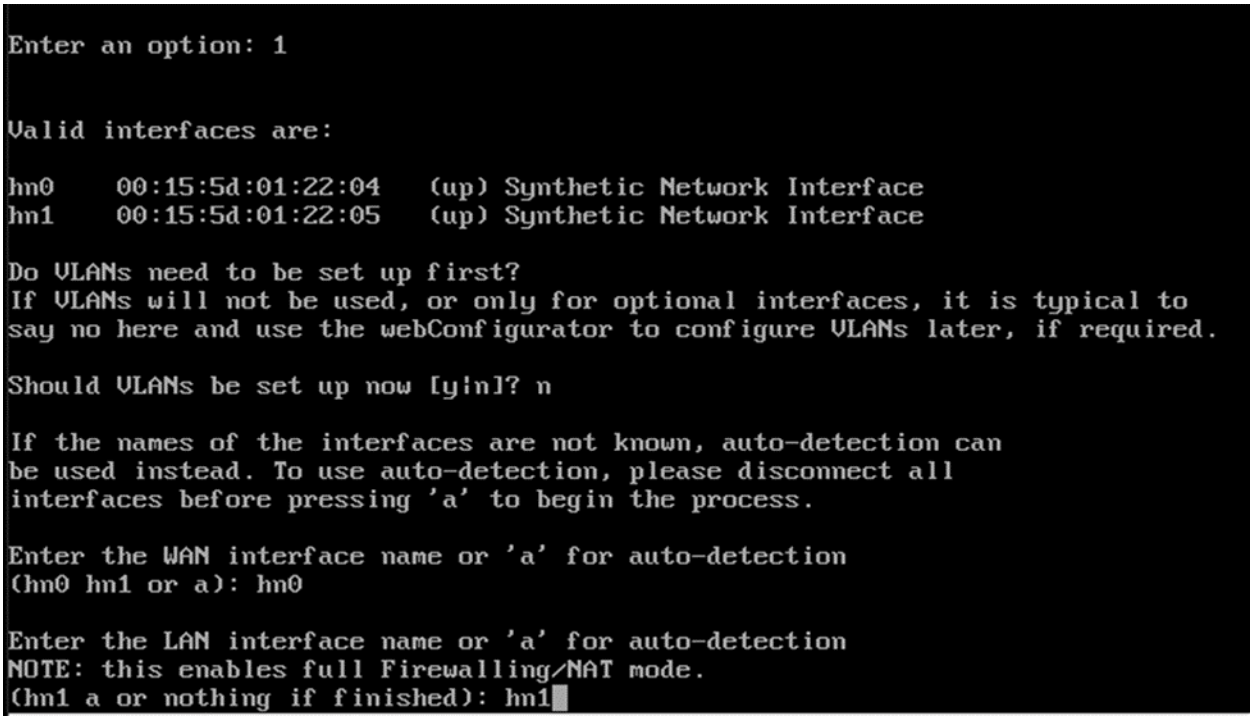
```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 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: 1

Valid interfaces are:

hn0    00:15:5d:01:22:04   (up) Synthetic Network Interface
hn1    00:15:5d:01:22:05   (up) Synthetic Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]?
```

```
 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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: 1

Valid interfaces are:

hn0    00:15:5d:01:22:04   (up) Synthetic Network Interface
hn1    00:15:5d:01:22:05   (up) Synthetic Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n
```

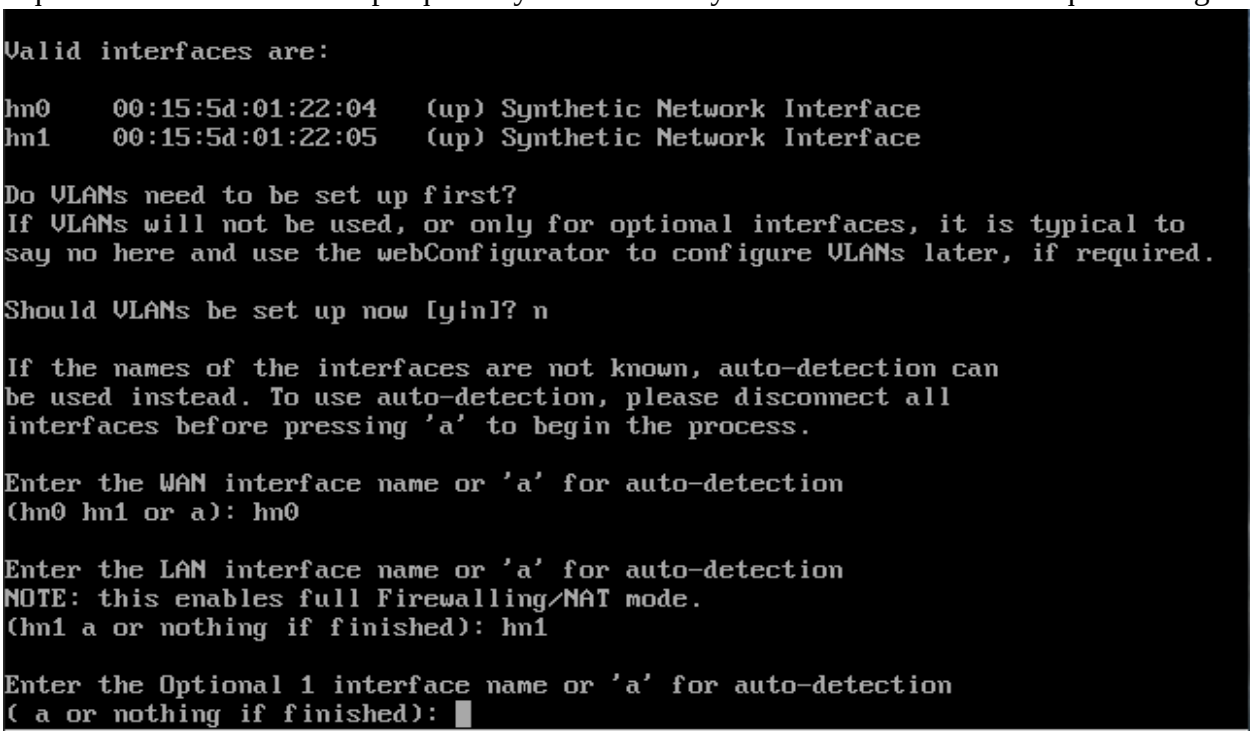
Nos pide que identifiquemos la interface de la WAN, aquí es hn0 y hn1 para la interface de la LAN

```
 6) Halt system                          15) Restore recent configuration
 7) Ping host                            16) Restart PHP-FPM
 8) Shell

Enter an option: 1

Valid interfaces are:

hn0    00:15:5d:01:22:04   (up) Synthetic Network Interface
hn1    00:15:5d:01:22:05   (up) Synthetic Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a):
```

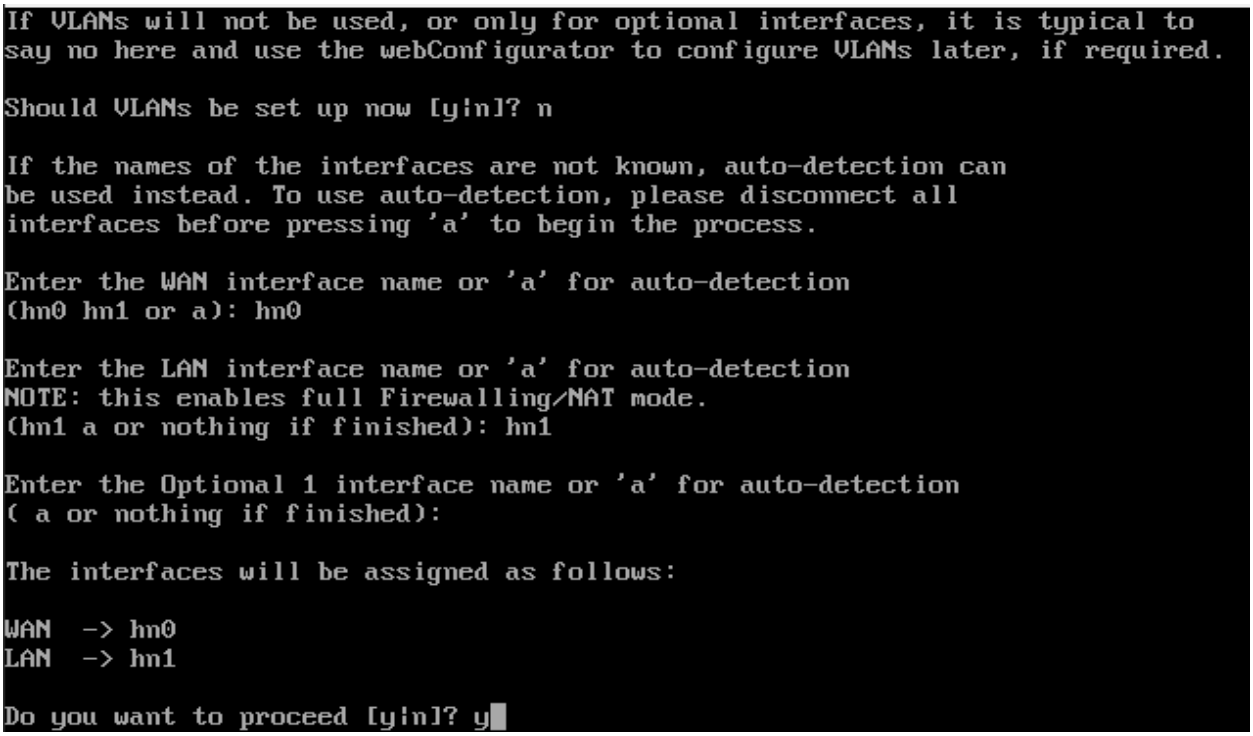
```
 6) Halt system                          15) Restore recent configuration
 7) Ping host                            16) Restart PHP-FPM
 8) Shell

Enter an option: 1

Valid interfaces are:

hn0    00:15:5d:01:22:04   (up) Synthetic Network Interface
hn1    00:15:5d:01:22:05   (up) Synthetic Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0
```

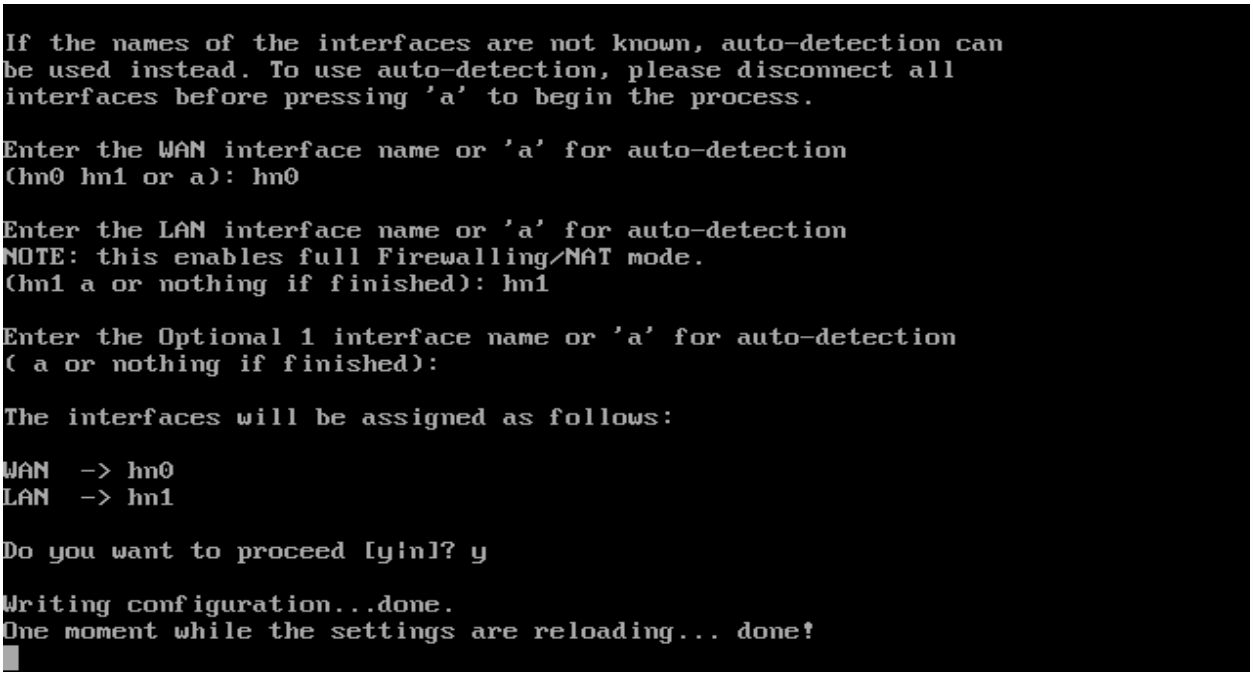


Aquí damos enter porque ya no hay más interfaces que asignar



Aquí te pregunta si deseas procesar lo configurado, aquí le diremos que si





Aquí podemos observar que ya asigno las interfaces especificadas anteriormente

```
WAN  -> hn0
LAN  -> hn1

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
*** Welcome to pfSense 2.3.4-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP
 LAN (lan)       -> hn1        -> v4: 192.168.

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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:
```

Ahora estableceremos interface con la opción “2”

```
*** Welcome to pfSense 2.3.4-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP
 LAN (lan)       -> hn1        -> v4: 192.168

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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: 2

Available interfaces:

1 - WAN (hn0 - dhcp)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure:
```

Seleccionamos “1” para configurar la WAN, cabe resaltar que estas IPs son las que te da por defecto el firewall

```
*** Welcome to pfSense 2.3.4-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP
 LAN (lan)       -> hn1        -> v4: 192.168

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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: 2

Available interfaces:

1 - WAN (hn0 - dhcp)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 1
```

Nos pide que configuremos la IPV4 vía DHCP pero aquí configuraremos una IP estática y diremos que NO

```
 WAN (wan)       -> hn0        -> v4/DHCP
 LAN (lan)       -> hn1        -> v4: 192.168.1

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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: 2

Available interfaces:

1 - WAN (hn0 - dhcp)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n
```

Aquí colocaremos la IP estática con su máscara y la puerta de enlace se agrega por defecto y damos enter para continuar

```
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
```

Aquí pide que configuremos IPV6 vía DHCP simplemente le daremos enter, lo mismo para el protocolo http que pregunta para que se pueda entrar poniendo http://10.1.X.Y y le diremos que NO porque no queremos eso, sino con el protocolo https, así: https://10.1.X.Y y damos enter.

```
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Damos enter para continuar

```
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to 192.168      /24

Press <ENTER> to continue.
```

Aquí se configuro la IP de la WAN

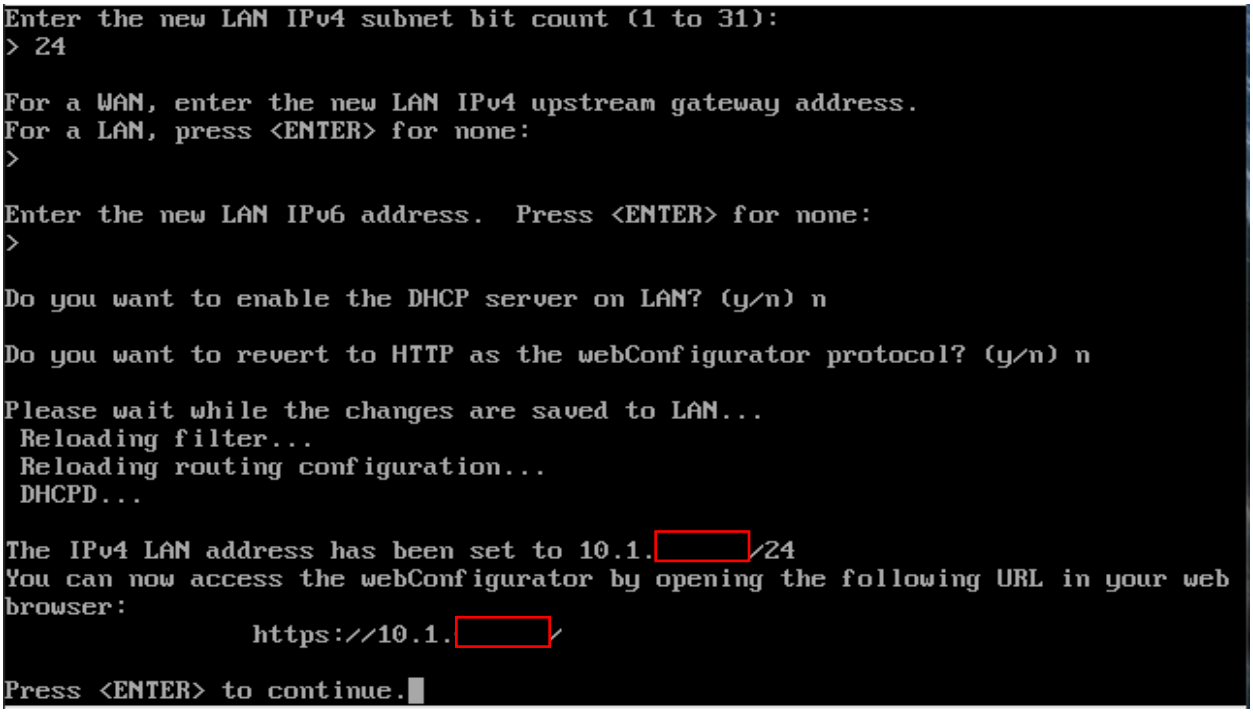
```
Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to 192.168.      24

Press <ENTER> to continue.
*** Welcome to pfSense 2.3.4-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> hn0        -> v4: 192.168.      24
 LAN (lan)       -> hn1        -> v4: 192.168.1.35/24

 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) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update 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:
```

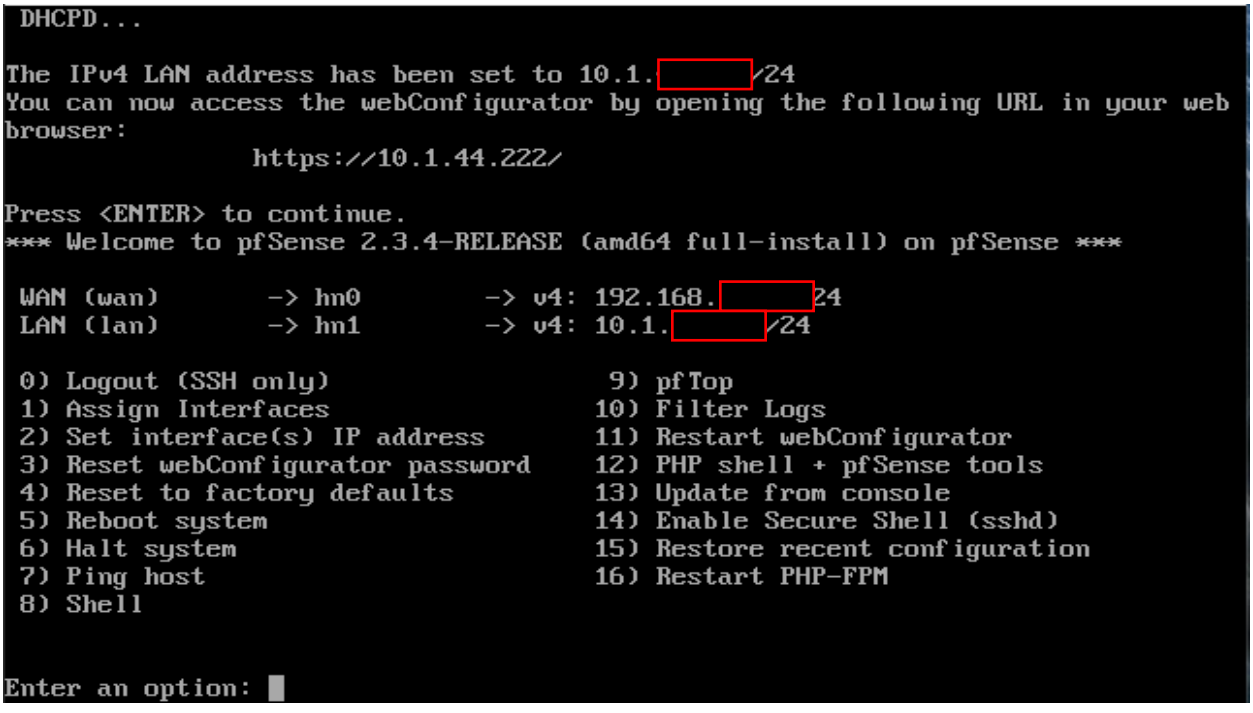
Ahora aremos lo mismo para la LAN

```
Enter an option: 2

Available interfaces:

1 - WAN (hn0 - static)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.1.

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

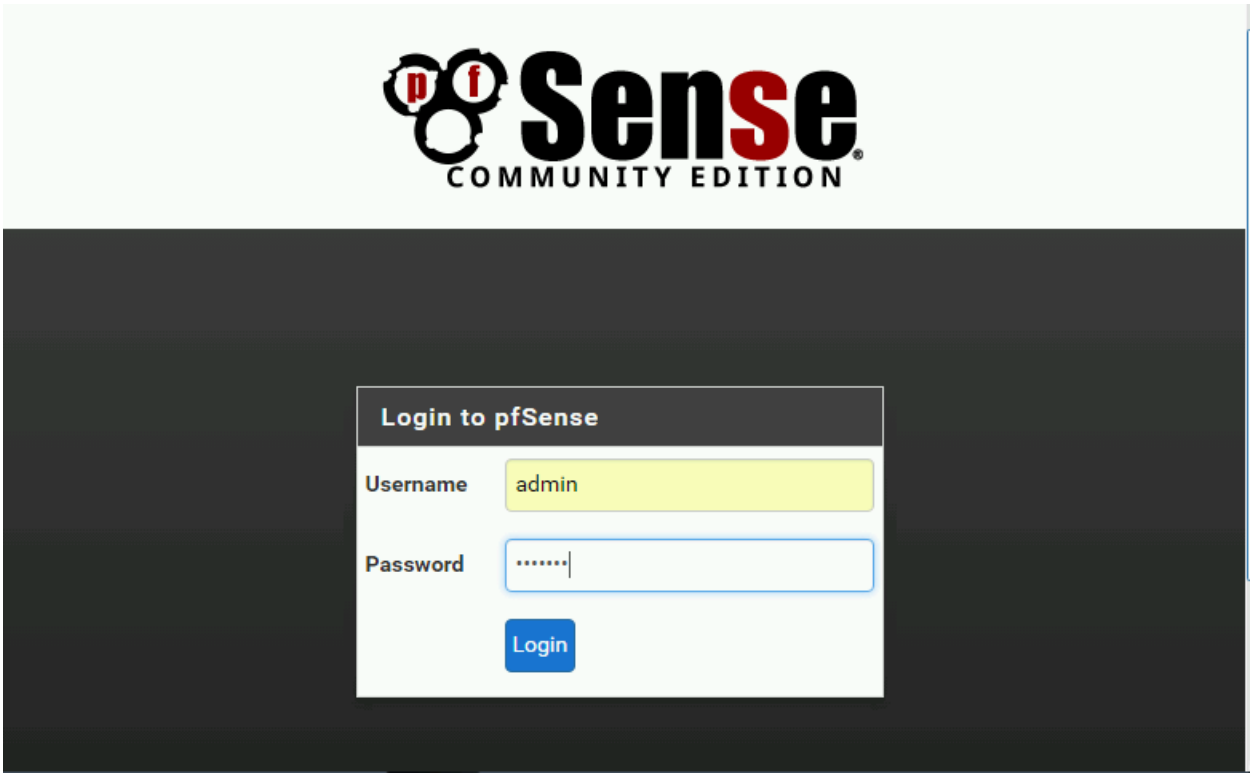
Nos dirá si queremos que la LAN de a sus equipos conectados IP vía DHCP y le diremos que NO

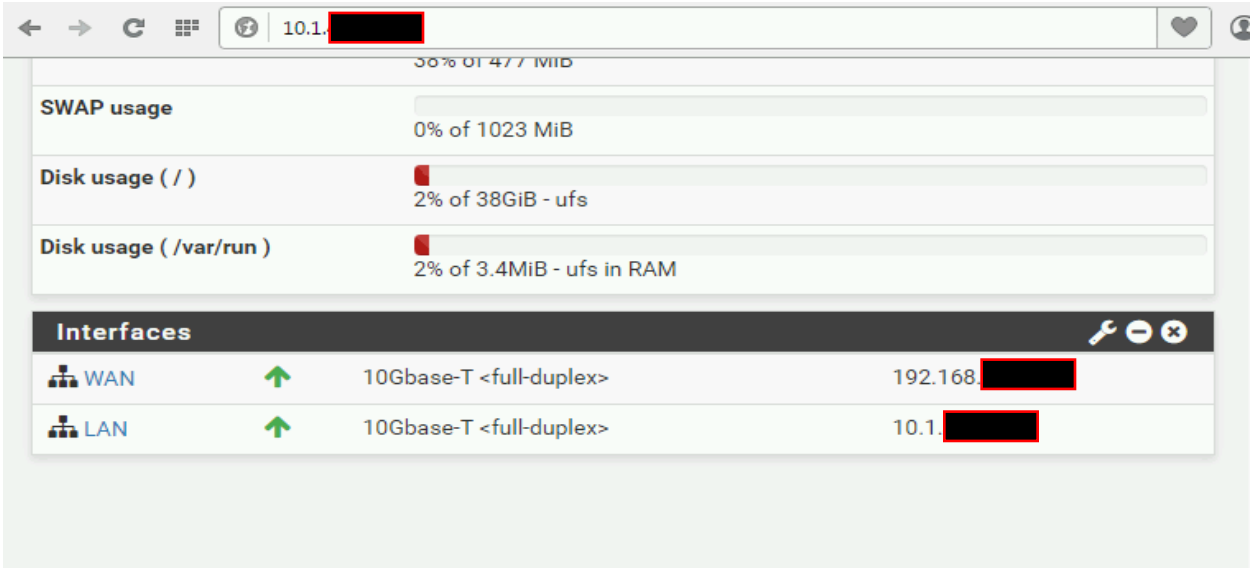
```
2 - LAN (hn1 - static)

Enter t      ber of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.1.44.222

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```





Aquí entraremos a la interface WEB con la dirección https://10.1.X.Y en el navegador de nuestra preferencia e ingresamos el usuario y la contraseña.


pfSense
COMMUNITY EDITION
Login to pfSense
Username
admin
Password
Login


10.1.[redacted]
SWAP usage
0% of 1023 MiB
Disk usage (/)
2% of 38GiB - ufs
Disk usage (/var/run)
2% of 3.4MiB - ufs in RAM
Interfaces
WAN
10Gbase-T <full-duplex>
192.168.[redacted]
LAN
10Gbase-T <full-duplex>
10.1.[redacted]

Anexo 2: Formato de entrevista al administrador.

Entrevista para el Administrador de la red telemática	UNIVERSIDAD DE LAMBAYEQUE

Nombre del entrevistado:_____	Fecha de la entrevista: ____/____/____

Objetivo: Incrementar significativamente la seguridad de base de datos y aplicaciones en la red telemática de la UNPRG, a través de open source.

1. ¿Cómo califica la seguridad perimetral actual?

   _____

2. ¿Qué opina de la rapidez de respuesta ante amenazas del firewall actual?

   _____

3. ¿Basado en su experiencia considera que el firewall actual es eficiente?

   _____

4. ¿El firewall actual le permite controlar la seguridad con rapidez y eficiencia?

   _____

5. ¿Basado en su experiencia considera que las instituciones educativas superiores deben optar por firewall open source en caso de bajos presupuestos?

   _____

6. ¿Considera importante que el firewall de información puntual y precisa de los ataques y control de tráfico de la red?

   _____

Anexo 3: Acta de instalación del software.

ACTA DE INSTALACIÓN DEL SOFTWARE

UNIVERSIDAD DE LAMBAYEQUE

Para demostrar la conformidad de la instalación se le pide llenar estos campos que se muestran a continuación.

Fecha de instalación:	
Responsable de la instalación:	

DATOS DE LA INSTITUCIÓN

Nombre de la institución:	
Dirección:	
Tipo de institución:	

DATOS DEL SOFTWARE

Nombre:	
Versión:	

OBSERVACIONES	

Firma de los tesistas

Firma del administrador de red

Anexo 4: Hoja de reporte de intervención técnica.

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
OFICINA GENERAL DE SISTEMAS INFORMÁTICOS

ÁREA DE ADMINISTRACIÓN DE RED TELEMÁTICA

Juan XXIII 1091 – Ciudad Universitaria Lambayeque- Telf. 74283091 - Anexos Red Telemática566 /566 email: oosi@unprg.edu.pe

REPORTE DE INTERVENCIÓN TÉCNICA RIT N° _____ - 2016 – DUIS-AAR

Fecha: _____ Hora: _____

DEPENDENCIA Y OFICINA(que solicita):

Teléfono / Anexo:_____

PERSONAL DE APOYO (Asistencia en la atención)

ASUNTO

ACCIONES (X :Acción realizada — : Acción no realizada)

01 ☐ Estudio, diseño y/o entrega de requerimiento técnico para implementación de red de comunicaciones para su posterior integración a la Red Telemática.

02 ☐ Configuración, verificación y/o soporte de servicios de Redes (Inicio de sesión en el dominio, Acceso a recursos compartidos en red: Archivos e Impresoras, netmeeting, FTP, Mail, Web)

03 ☐ Implementación de nuevo Sistema de Cableado Estructurado y Red de Comunicaciones e Integración a la Red Telemática UNPRG. Se instalaron ..... Salidas de Telecomunicacion (TO)

04 ☐ Instalacion de salida de telecomunicacion adicional en la infraestructura de Red Telemática (instalación del cableado horizontal y de salidas de telecomunicación)

05 ☐ Instalación y configuracion de equipos de conectividad inalambrica e integracion a la Red Telemática UNPRG

06 ☐ Soporte del Sistema de Cableado estructurado de Comunicaciones y conectividad de dispositivos de Red

07 ☐ Unión de equipo al dominio UNPRG (servidor, computadora o impresora).

08 ☐ Soporte del software informatico (sistema de información / base de datos)

09 ☐ Configuracion / mantenimiento de opciones de usuario del dominio UNPRG.

10 ☐ Asesoria / Supervision / Recepcion de hardware, sistemas de información y/o telecomunicaciones

11 ☐ Instalación de nuevo teléfono VOIP

12 ☐ Soporte del teléfono VOIP

13 ☐ Permisos de llamada de los usuario del teléfono VOIP

14 ☐ Instalacion y/o actualizacion del antivirus. Escaneo y eliminacion de virus, spyware y otros codigos maliciosos.

15 ☐ Actualización del sistema operativo y otros Software

16 ☐ Formateo, instalacion y actualizacion del sistema operativo y del software de oficina.

17 ☐ Instalacion de Software de Ofimatica, utilitarios y otros software.

18 ☐ Instalación y/o configuracion de Impresora, Grabadora DVD u otro hardware de computo

19 ☐ Diagnóstico de estado y operatividad de hardware y software de computo

20 ☐ Mantenimiento preventivo y/o correctivo del Hardware (componentes internos de Computadora Desktop)

DETALLE DE ACCION REALIZADA U OTRAS ACCIONES:

FECHAS Y HORAS DE REALIZACION DE TRABAJO[dd/mm - Hr/Min (a horas o min); dd/mm2 - Hr2/Min2 (a horas o min) ; etc]

IDENTIFICACION DE EQUIPO HARDWARE Y/O COMPONENTES DE RED (Switch, Computadora, Salida de Telecomunicación, Gabinete, etc)

EQUIPO, MARCA Y MODELO / COMPONENTE DE RED	IDENTIFICADOR	INFORMACIÓN TÉCNICA O AREA DE TRABAJO

OBSERVACIONES / SUGERENCIAS(Generar y referenciar N° de Constancia de Recepcion y de Entrega de materiales si es necesario)

CONFORMIDAD DE INTERVENCIÓN TÉCNICA

Administrador de Red Telemática

Nombres, DNI, Sello y Firma:

Jefe / Responsable de Dependencia