
**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ**

**CARRERA DE INFORMÁTICA**

**TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA**

**TEMA:**

# SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL

**AUTORES:**

**PABLO RICARDO DELGADO ZAMBRANO**
**LUIS ANTONIO LOOR LOOR**

**TUTOR:**

**LIC. PABELCO YUNEL ZAMBRANO MOREIRA, MGTR.**

**CALCETA, JUNIO 2017**

# DERECHOS DE AUTORÍA

Pablo Ricardo Delgado Zambrano y Luis Antonio Loor Loor, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Lpey de Propiedad Intelectual y su reglamento.

…… …… ……

PABLO R. DELGADO ZAMBRANO LUIS A. LOOR LOOR

# CERTIFICACIÓN DE TUTOR

Pabelco Yunel Zambrano Moreira certifica haber tutelado la tesis SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL, que ha sido desarrollada por Pablo Ricardo Delgado Zambrano y Luis Antonio Loor Loor, previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.……...…….

LIC. PABELCO Y. ZAMBRANO MOREIRA, MGTR

# APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han APROBADO la tesis SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL, que ha sido propuesta, desarrollada y sustentada por Pablo Ricardo Delgado Zambran o y Luis Antonio Loor Loor, previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

…….……..……. ……....……..

ING. HIRAIDA M. SANTANA CEDEÑO, MG. LIC.JOSÉ G. INTRIAGO CEDEÑO, MG

**MIEMBRO** **MIEMBRO**

…….……..……

ING. LUIS C. CEDEÑO VALAREZO, MG.SC

**PRESIDENTE**

# AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López por brindarnos una educación de prestigio y por permitir desarrollar nuestro trabajo de tesis de grado dentro de la institución;

Al Ing. Cesar Moreira por darnos la iniciativa de realizar este proyecto y por ser un pilar fundamental en todo el proceso de desarrollo de nuestro trabajo de tesis, y

Al Ing. Ricardo Chica por el aporte de técnicas e ideas para la ejecución de este trabajo y por estar presente durante todo el proceso de desarrollo e implementación de la tesis.

Los autores

# DEDICATORIA

A Dios por darme la fuerza espiritual y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor, y

A mi familia por el apoyo incondicional, por sus consejos, sus valores, por su amor y por la constante motivación que me ha permitido ser una persona de bien.

.....

PABLO R. DELGADO ZAMBRANO

# DEDICATORIA

A Dios en primer lugar por la salud y vida que me ha prestado durante todo este tiempo y lograr los objetivos propuestos, gracias a su bondad y misericordia, y

A mis Padres que con su gran paciencia y mansedumbre han sabido apoyarme y aconsejarme en todo momento, a mis abuelos, por su cuidado y gran labor durante mi desarrollo y preparación de estudio.

..……..……

LUIS A. LOOR LOOR

# CONTENIDO GENERAL

# CONTENIDO DE CUADROS Y FIGURAS

## RESUMEN

Con el objetivo de mejorar la seguridad de la información en el Data Center de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, se implementó un software de seguridad perimetral firewall basado en código libre y montado en un servidor virtual. Para esto, se realizó la recopilación de información haciendo uso de herramientas tales como encuestas, fichas de observación y entrevistas. Además, se escogieron tres sistemas de seguridad firewall y mediante un estudio comparativo aplicado con la herramienta checklist se determinó el software que se utilizó, en este caso Pfsense. A continuación se procedió a la instalación del sistema sobre la plataforma VMWARE para la virtualización del firewall, y por lo consiguiente a la configuración de las reglas y niveles de seguridad del firewall. Con la puesta en marcha del servidor firewall se obtuvieron resultados en cuanto a la mejora de la protección de los datos y la seguridad en la red, facilitando el control, bloqueo y monitoreo de ataques informáticos a la red interna de la universidad, lo que aportó a la reducción de costos y la gestión de nuevos planes en niveles de seguridad del Data Center en menor tiempo.

## PALABRAS CLAVE

Seguridad firewall, firewall perimetral, protección firewall.

## ABSTRACT

With the objective of improving information security in the Data Center of the Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, a perimeter firewall software was implemented based on free code and mounted on a virtual server. For this, the collection of information was made using tools such as surveys, observation sheets and interviews. In addition, three firewall security systems were chosen and a comparative study applied with the checklist tool determined the software that was used, in this case Pfsense. Then the system was installed on the VMWARE platform for the virtualization of the firewall, and consequently to the configuration of the rules and levels of security of the firewall. With the implementation of the firewall server, results were obtained in terms of improving data protection and security in the network, facilitating the control, blocking and monitoring of computer attacks to the internal network of the university, which contributed Cost reduction and management of new plans at Data Center security levels in less time.



## KEY WORDS

Firewall security, Perimeter firewall, Firewall protection.

# CAPÍTULO I. ANTECEDENTES

## 1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

A nivel mundial toda organización enlazada a Internet está expuesta a infiltraciones o ataques informáticos, y los riesgos se incrementan día a día con el expansivo crecimiento de la red. En Ecuador debido al gran aumento de empresas públicas y privadas conectadas a Internet, es necesario establecer planes de seguridad para proteger la información, por tal motivo, un sistema perimetral firewall es una medida de seguridad imprescindible y responsable, que tiene por objeto prevenir, detener y bloquear ataques externos y el control del uso de internet desde el interior de la organización.

Partiendo del contexto anterior, el Data Center de la Escuela Superior Agropecuaria de Manabí Manuel Félix López no contaba con este tipo de seguridad, lo que implicaba que toda la información que se maneja en el centro de datos estaba expuesta y tenga un nivel más elevado de vulnerabilidad, debido a la rápida evolución de técnicas y mecanismos de ataques informáticos. Además la inexistencia de un servidor firewall en el Data Center de la ESPAM MFL, complicaba el control, bloqueo y monitoreo de todas las infiltraciones informáticas a la red interna, y por ende la pérdida de información privada de la institución.

Debido a esta problemática los autores del presente trabajo se plantearon la siguiente interrogante:

¿De qué manera fortalecer o proteger la seguridad de la información en el Data Center de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López?

## 1.2. JUSTIFICACIÓN

En la actualidad las instituciones públicas y privadas utilizan el internet como una ventaja en la automatización de procesos internos y como una herramienta para el intercambio de información, pero a la par implica ser vulnerable a ataques informáticos y al robo de información, por lo que es imprescindible establecer sistemas de seguridad que permitan fortalecer la confidencialidad de datos. Por otra parte, la seguridad e integridad informática de una empresa es fundamental, por lo tanto los ataques por red y pérdidas de información ocasionan trastornos y no solo la imagen si no también el funcionamiento y progreso de una empresa es perjudicado. Es así, que una plataforma para el control de accesos y protección de los servicios informáticos garantiza un adecuado aprovechamiento de la infraestructura y garantiza la integridad y confidencialidad de la información.

Por esta razón, en la ESPAM MFL era necesario implementar un sistema de seguridad, que permitiera controlar las infiltraciones informáticas de manera eficiente y mitigar riesgos, debido a que es un establecimiento educativo que realiza procesos institucionales a través del internet, y por lo tanto es sensible a la pérdida de información.

Es por esto, que en el Data Center de la Politécnica de Manabí se implementó un sistema de seguridad perimetral firewall, para fortalecer la seguridad de la información compartida en la universidad, lo que permitió monitorear en tiempo real las comunicaciones de la red interna y mejorar la privacidad de la información, además proteger a la red de cualquier intento de acceso no autorizado desde el exterior y de ataques desde el interior; ayudando a la institución a estar más acorde con la tecnología y prepararse ante posibles riesgos de ataques informáticos.

Por otra parte, la importancia de esta tesis de grado, es que la universidad brinde un mejor servicio a la sociedad en lo que respecta a la infraestructura tecnológica adecuada, para protección de la información que se manejan

dentro de la institución, estableciendo planes de seguridad y haciendo uso de nuevas tecnologías tales como un sistema perimetral firewall virtual. Por lo tanto el uso de esta herramienta tecnológica aporta para que la información de los estudiantes, docentes y personal de trabajo de la ESPAM MFL tenga mayor seguridad frente a infiltraciones o ataques informáticos que puedan afectar la integridad de los datos. Además este tipo de sistema realiza el control y generación de reportes de manera online sin aumentar el consumo excesivo de la energía eléctrica.

De acuerdo al marco legal el uso de la tecnología de un servidor firewall virtual se basa por lo estipulado en el Art. 8 literal h de la Ley de Educación Superior y su Reglamento, teniendo como fines contribuir en el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o extensión universitaria.

Es relevante la implementación del firewall en el Data Center de la ESPAM MFL de acuerdo a lo determinado por el actual Gobierno Ecuatoriano, que desde la promulgación de la Constitución en septiembre del 2008, diseñó los "Objetivos del Plan Nacional para el Buen Vivir". Dichos objetivos poseen una relación directa entre el sector de las telecomunicaciones y la sociedad de la información. De acuerdo a esto el Gobierno establece como medio para lograr el cumplimiento del Plan Nacional del Buen Vivir la política de promover el acceso a la información de las nuevas tecnologías, democratizar su acceso y establecer medios para que la mayor cantidad de ciudadanos puedan usarlas. (Reinoso, 2012).

Así mismo, Reinoso (2012) indica que es política pública impulsar de manera eficiente la gestión entre las empresas y las entidades públicas, para lo cual es necesario contar con una infraestructura y la seguridad adecuada para la provisión de servicios públicos, incluidas las telecomunicaciones.

## 1.3. OBJETIVOS

### 1.3.1. OBJETIVO GENERAL

Implementar un sistema de seguridad perimetral firewall en el Data Center de la ESPAM MFL, para fortalecer la seguridad de la información compartida en la universidad.

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar las políticas y mecanismos de seguridad que se manejan en el Data Center de la ESPAM MFL.
- Determinar el software de seguridad perimetral firewall en base a los requerimientos de seguridad apropiados en la universidad.
- Instalar el sistema de seguridad perimetral firewall en el Data Center.
- Efectuar pruebas que verifiquen el adecuado funcionamiento del sistema perimetral firewall.

## 1.4. IDEA A DEFENDER

La implementación del sistema perimetral firewall en el Data Center de la Politécnica de Manabí, permitirá fortalecer la seguridad de la información, definir niveles de confianza y restringir el acceso de determinados usuarios internos o externos a los servicios que brinda la ESPAM MFL a través del centro de datos.

# CAPÍTULO II. MARCO TEÓRICO

## 2.1. HISTORIA DE LA ESPAM MFL

Con 17 años, la Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López" es la principal universidad de la zona norte de la Provincia.

Manabí es una provincia rica en variados recursos. Los contrastes se marcan con fuerza en sus 22 cantones: el mar y sus montañas; la cultura ancestral de su población chola y montubia, que sorprende con una y mil leyendas; su comida típica, muy apreciada por nativos y extraños. (ESPAM, 2016).

Los habitantes del cantón Bolívar han dirigido su mirada a la tierra, pródiga desde siempre y, en ese contexto, se han identificado con la agricultura y la ganadería. Vale recordar que, hubo épocas en que este cantón fue productor y exportador de caucho, madera de balsa, tagua, cacao y algodón; producción disminuida en las últimas décadas, por causas conocidas por todos; pero hoy, con la Presa La Esperanza y el Proyecto Carrizal-Chone, hombres y mujeres con renovados bríos, fincan, otra vez, su ilusión en la tierra. (ESPAM, 2016).

Ello exigía, en Calceta, la presencia de un centro de estudios superiores en las áreas agrícola y pecuaria, de manera que la población estudiantil, con dificultad para trasladarse a universidades fuera de la zona, pudiera alcanzar un título académico, a fin de servir más tarde, no solo al cantón, sino a toda la región. (ESPAM, 2016).

Las gestiones, un largo recorrido, empezaron en el Congreso Nacional y luego en otras instancias desde 1995. Se crea así el INSTITUTO TECNOLÓGICO SUPERIOR AGROPECUARIO DE MANABÍ, ITSAM, mediante Ley Nº. 116, publicada en el R.O. Nº. 935, el 29 de abril de 1996. (ESPAM, 2016).

Tres años después, el Congreso Nacional expidió la Ley Reformatoria que transformaba el Instituto Tecnológico Superior Agropecuario de Manabí, ITSAM, en ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ, ESPAM, cuya Ley 99-25 fue publicada en el R.O. el 30 de abril de 1999. (ESPAM, 2016).

La Escuela Superior Politécnica Agropecuaria de Manabí nace como persona jurídica de derecho público, autónoma, que se rige por la Constitución Política del Estado, Ley de Educación Superior, su Estatuto Orgánico y Reglamentos, para preparar a la juventud ecuatoriana y convertirla en profesionales, conforme lo exigen los recursos naturales de su entorno. La ESPAM inicia sus labores con las carreras de Agroindustria, Medio Ambiente, Agrícola y Pecuaria. Posteriormente, se crea la carrera de Informática, emprendiendo así, un riguroso programa de fortalecimiento académico, con el fin de formar profesionales idóneos que ejecuten proyectos sustentables, generadores de fuentes de trabajo. (ESPAM, 2016).

Ante la demanda de nuevas carreras, los directivos de la ESPAM, no han escatimado esfuerzos para incrementar otras, de tipo empresarial. Es así como desde el año 2003 funcionan dos nuevos programas: Administración Pública y Administración de Empresas, los que se cumplen en horarios nocturnos, al igual que la Carrera de Informática. A partir del año 2007 y, producto de un estudio, los estudiantes tienen una nueva opción: Ingeniería en Turismo. Con ello se busca potenciar a la población manabita, ávida de lograr una profesión acorde con sus aspiraciones. (ESPAM, 2016).

## 2.2. METODOLOGÍA DE DESARROLLO EN CASCADA

El modelo de la cascada, a veces llamado ciclo de vida clásico, sugiere un enfoque sistemático y se caracteriza por proponer actividades secuenciales, claramente agrupadas dentro de fases o ciclos del desarrollo del proyecto, propone hacer un análisis intensivo de requerimientos. El levantamiento de requerimientos es muy riguroso y los Analistas definen a prioridad todos los

requerimientos funcionales y no funcionales relacionados con el proyecto. Normalmente, una fase no puede iniciar sin que la fase anterior haya sido revisada y aceptada por el cliente o usuario final, sin que esto signifique el sistema cumplirá con sus necesidades. (Velásquez, 2013)

Así mismo, Cervantes y Gómez (2012) establecen que las fases del modelo de desarrollo en cascada son las siguientes:

- Análisis y definición de requerimientos. Se trabaja con los clientes y los usuarios finales del sistema para determinar el dominio de aplicación y los servicios que debe proporcionar el sistema así como sus restricciones y requerimientos.

- Diseño del sistema y del software. Se establece una arquitectura del sistema. Durante el diseño del software se identifican los subsistemas que componen el sistema y se describe cómo funciona cada uno y las relaciones entre éstos.

- Implementación y validación de unidades. Consiste en codificar y probar los diferentes subsistemas por separado. La prueba de unidades implica verificar que cada una cumpla su especificación (proveniente del diseño).

- Integración y validación del sistema. Una vez que se probó que funciona individualmente cada una de las unidades, éstas se integran para formar un sistema completo que debe cumplir con todos los requerimientos del software. Cuando las pruebas del sistema completo son exitosas, éste se entrega al cliente.

- Mantenimiento del sistema. Implica corregir errores no descubiertos en las etapas anteriores del ciclo de vida y mejorar la implantación de las unidades del sistema para darle mayor robustez.

## 2.3. SEGURIDAD INFORMÁTICA

Villegas, *et al*., (2011) plantean que la seguridad informática de las tecnologías y de los sistemas de información, es un conjunto de métricas desarrolladas por profesionales que posean competencias y conocimientos que permitan realizar políticas de seguridad, que garanticen la aplicación de salvaguarda contra las pérdidas económicas graves; el deterioro de la imagen pública de la organización; el incumplimiento legal o la fuga de información. Por otra parte la UTTT (2012) establece que la seguridad informática se enfoca a la protección de la infraestructura computacional, la información y todo lo relacionado con la misma. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas o leyes para minimizar los posibles daños.

### 2.3.1. NORMA ISO/IEC27000

La Serie ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la seguridad informática utilizable para cualquier tipo de organización o institución. La serie ISO/IEC 27000 contiene las mejores prácticas recomendadas en seguridad informática para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) (Baldeón y Coronel, 2012).

### 2.3.2. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

Voustass (2010) plantea que el objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, y garantizar la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable.

Así mismo, establece que el objetivo secundario de la seguridad informática consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total, y se puede establecer esa confiabilidad como la unión de seis características esenciales:

- Permanencia
- Accesibilidad
- Disponibilidad
- Confidencialidad
- Integridad
- Aceptabilidad.

### 2.3.3. CLASIFICACIÓN DE LA SEGURIDAD INFORMÁTICA

Los autores de esta investigación resumen que cuando se habla de la clasificación de la seguridad en un sistema informático, se puede encontrar varios tipos, dependiendo de la naturaleza material de los elementos que se utilicen.

#### 2.3.3.1. SEGURIDAD ACTIVA Y PASIVA

- Activa: Son todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos idóneos para evitar el problema. Por ejemplo antivirus, cortafuegos o firewall. (Cervigón y Ramos, 2011).

- Pasiva: Es todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad de un sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo. Por ejemplo copias de seguridad de los datos, discos RAID. (Cervigón y Ramos, 2011).

#### 2.3.3.2. SEGURIDAD FÍSICA Y LÓGICA

- Díaz, *et al*., (2014) definen que la seguridad física se refiere al acceso físico, estructura del edificio, centro de datos, cámaras de seguridad, alarmas, sistema antiincendios, extintores y climatizadores.

- Lógica: se encarga de asegurar el software de un sistema informático. Tales como configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, desarrollo de aplicaciones, VPN, protocolos http, https, transmisión de ficheros ftp (Díaz, *et al*., 2014).

### 2.3.4. POLÍTICAS DE LA SEGURIDAD INFORMÁTICA

De acuerdo con Correa (s.f) las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s.

En este sentido Benítez (2013) considera que la elaboración de las políticas de seguridad informática están fundamentadas bajo la norma ISO/IEC 17799, las cuales son las siguientes:

- Control de acceso (aplicaciones, base de datos, área del Centro de Cómputo, sedes de Las Empresas filiales).
- Resguardo de la Información.
- Clasificación y control de activos.
- Gestión de las redes.
- Gestión de la continuidad del negocio.
- Seguridad de la Información en los puestos de trabajo.
- Controles de Cambios.
- Protección contra intrusión en software en los sistemas de información.
- Monitoreo de la seguridad.
- Identificación y autenticación.
- Utilización de recursos de seguridad.

- Comunicaciones.
- Privacidad.

### 2.3.5. SEGURIDAD PERIMETRAL

Fabuel (2013) argumenta que la seguridad informática es una barrera o frontera lo más inexpugnable posible entre una red interna e Internet, cuyo objetivo es restringir y controlar qué datos entran a nuestra organización o salen de ella. La principal ventaja de este tipo de seguridad es que permite al administrador concentrarse en los puntos de entrada, sin olvidar la seguridad del resto de servidores internos de una red, para protegerlos frente a una posible intrusión.

En este aspecto Tirado (2012) considera que es un agregado de Hardware, Software y políticas para proteger una red en la que se tiene confianza (intranet) de otras redes en las que no se tiene confianza (extranet, internet). Además este autor propone algunos términos que intervienen en la seguridad perimetral:

- Rechazar conexiones a servicios comprometidos
- Permitir solo ciertos tipos de tráfico o entre ciertos nodo
- Proporcionar un único punto de interconexión con el exterior
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet
- Auditar el tráfico entre el exterior y el interior
- Ocultar información nombre de sistemas, topologías de la red, tipos de dispositivos de red, cuentas de usuarios internos, etc.

### 2.3.6. FIREWALL

López (2010) señala que el firewall es un sistema diseñado para detener accesos no autorizados en la red, puede implementarse en hardware, en software o una combinación de los dos anteriores. Estos sistemas son usados

para proteger redes privadas de violaciones de seguridad efectuadas por usuarios, aplicaciones o tráfico no deseado proveniente de redes externas. A través del firewall pasa todo el tráfico que entra o sale de la red y mediante criterios o políticas definidas por el administrador examina cada uno de los paquetes y bloquea aquellos que no son conformes con dichas políticas. (López, 2010).

Así mismo Vásquez *et al*., (2012) determinan que un firewall de seguridad, ubicado entre la LAN e Internet permite o deniega las transmisiones de información que se efectúen entre los equipos considerados y la gran red. Evita que intrusos accedan a la información confidencial, contenida en este Servicio de carácter privado, limitada a usuarios con login y password. Por lo consiguiente Grajales (2011) argumenta que el servidor firewall realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino (es decir, de qué computador provienen y a que computador van dirigidos los paquetes de datos) y el servicio de la red al que se corresponden.

#### 2.3.6.1. REGLAS DE UN FIREWALL

Yustas, (s.f) determina que un servidor firewall se divide en varias reglas que permiten definir las características de seguridad del mismo. A continuación se muestra cada una de ellas:

- Simplicidad: En zonas no conflictivas de la red utilice como cortafuegos un enrutador, también denominado encaminador; es una decisión inteligente, pues la operación será igual de válida, pero más eficiente. Por hacer, un símil, es como si en un cruce pone un guardia urbano que sólo decide qué coches pueden pasar y cuáles no, dependiendo de su origen y destino

- Segmentación de direcciones IP: Establecer una división lógica de las direcciones IP de la red extensa (WAN) de la empresa, usar

subdireccionamiento IP para reducir las tablas de los enrutadores (router), y ocultar más fácilmente las direcciones de nuestras subredes IP.

- Canales seguros: La ventaja es que utiliza un túnel cifrado, que permite que los datos sean cifrados al salir de un extremo y descifrados al llegar al otro, evitando posibles escuchas no deseadas. Los túneles cifrados realizan una fase previa de autentificación mutua, de forma que un cortafuego esté seguro de que está hablando con quien quiere. Una vez autentificadas ambas partes, se decide una clave de sesión (quedando establecido el túnel cifrado) que, por seguridad, no tiene que reutilizarse en otra sesión, e incluso suele modificarse periódicamente (cada tantos minutos) para mayor seguridad.

- Prudencia: La utilización de cortafuegos y túneles privados no debe hacernos olvidar algunos puntos importantes de seguridad global:
  a) Solo protegen de extremo a extremo del enlace y no hacen nada frente a personas con malas intenciones que estén dentro de la empresa.
  b) La seguridad de dos redes conectadas a una VPN es siempre la de la red más insegura de ambas, es un canal seguro, pero que puede ser utilizado de modo inseguro.
  c) Los enemigos pueden aún extraer conclusiones a partir del análisis estadístico del volumen y frecuencia del tráfico intercambiado, sin conocer su contenido.

#### 2.3.6.2. IDS

Según Balseca *et al.,* (2013) fundamente que Intrusión Detection System es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Algunas de las características son:

- Deben estar continuamente en ejecución con un mínimo de supervisión.
- Se deben recuperar de las posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.
- Debe utilizar los mínimos recursos posibles.

#### 2.3.6.3. IPS

De acuerdo con Portantier (2013) indica que los sistemas que solo pueden detectar ataques, se conocen como sistemas de Detección de Intrusos (IDS), y los que pueden tomar acciones para bloquear estos ataques se llaman Sistemas de prevención de Intrusos (IPS). Obviamente, los IPS son bastante más complejos que los IDS, y requieren de mayor atención al configurarse, porque pueden bloquear tráfico legítimo e impactar negativamente en la operatoria de la organización.

#### 2.3.6.4. VPN

Una red privada virtual proporciona mediante procesos de encapsulación y cifrado, una red privada de datos, sobre infraestructura de telecomunicaciones públicas, como internet. Las VPN logran esto al permitir que se realice un túnel seguro a través de una red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que están disponibles en las redes privadas. (Vega y Núñez, 2012).

### 2.3.7. PF SENSE

Es una distribución libre de firewall de red, basado en el sistema operativo FreeBSD con un kernel personalizado e incluyendo paquetes de software libre de terceros para la funcionalidad adicional. PfSense software es capaz de proporcionar la misma funcionalidad o más de los servidores de seguridad comercial común, sin ninguna de las limitaciones artificiales. (PfSense, 2015)

De acuerdo con Celis y Andrade (2013) Pfsense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN, con detalle estos servicios son los siguientes:

- Firewall: Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.
- Servidor VPN: Pfsense puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras.
- Servidor de Balanceo de Carga: Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS. También para proveer estabilidad y redundancia en él envió de tráfico a través del enlace WAN evitando los cuellos de botella.
- Portal Cautivo: Este servicio consiste en forzar la autenticación de usuarios en una página web especial de autenticación, para aceptar los términos de uso o para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.
- Tabla de estado: PFSense es un stateful firewall, el cual como característica principal guarda el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la Tabla de estado. Pfsense tiene un enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.
- Servidor DNS y reenviador de cache DNS: Pfsense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.

- Servidor DHCP: También funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.
- Servidor PPPoE: Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local o vía radius.
- Enrutamiento estático: Pfsense funciona como un enrutador ya que entrega direccionamiento IP y hace el nateo hacia afuera.
- Redundancia: Pfsense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primario.
- Reportes Y Monitoreo: A través de los gráficos RDD Pfsense muestra el estado de los siguientes componentes: Utilización de CPU y rendimiento total, estado del Firewall, rendimiento individual por cada interface, paquetes enviados y recibidos por cada interface, manejo de tráfico y ancho de banda.

Por otra parte establecen que para la instalación de Pfsense los requerimientos de hardware son los siguientes.

- Procesador Intel Pentium III, hasta un Intel Xeon, nada de AMD.
- Memoria RAM desde 256 Mb hasta 3 Gb.
- Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA Y SAS-SATA.
- Tarjetas de red cableadas Intel y Realtek (la red inalámbrica solamente funcionan las tarjetas de red marca Atheros).
- Debido a que este software será instalado sobre un servidor o PC dedicado única y exclusivamente, este PC o servidor no necesitara un mouse, solo un teclado y monitor ya que este servidor será administrado remotamente.

### 2.3.8. IPFIRE

IPFire (2016) define qué es una distribución Linux diseñada específicamente para hacer las funciones de cortafuegos (firewall) y routing en una red local y

fue diseñado tanto con modularidad y un alto nivel de flexibilidad en mente. Puede implementar fácilmente muchas variaciones de la misma, como un firewall, un servidor proxy o una puerta de enlace VPN. El diseño modular asegura que se ejecuta exactamente lo que ha configurado para y nada más. Todo es fácil de administrar y actualizar a través del gestor de paquetes.

Por otra parte Suarez (2014) establece que es un sistema operativo muy ligero, por lo que permite su ejecución en equipos actuales y más anticuados, sus requisitos mínimos son un procesador de primera generación de Intel a 333Mhz y 128MB de memoria RAM y 2 interfaces de red, pero según el uso que se le dé necesitará unos requisitos mayores a los indicados.

En este aspecto Soto (2014) determina que por defecto IPFire viene con las siguientes características:

- Servidor Proxy
- Sistema de detección de intrusos
- VPN a través de IPsec y OpenVPN
- Servidor DHCP
- Caché de nombres de dominio.
- Servidor horario.
- Wake-on-Lan.
- Dynamic DNS
- Quality of Service (QoS)
- Firewall saliente.
- Completo Log de todos los sucesos que ocurren en el sistema.
- Servidor de archivos en red
- Servidor de impresora en red.
- Asterisk para centrales VoIP.
- TeamSpeak.
- Servidor grabador de vídeo.
- Servidor de correo y anti spam.
- Servidor antivirus.
- Servidor de streaming. (Soto, 2014).

### 2.3.9. UNTANGLE NG FIREWALL

Untangle (2015) define que es un portal de acceso a la red basado en Debian con módulos montables para aplicaciones de red como bloqueo de correo no deseado, filtrado web, antivirus, anti-programas espías, prevención contra intrusos, VPN, SSL VPN, muros de fuego y más. NG Firewall es una plataforma de nueva generación para el despliegue de aplicaciones basadas en red. La plataforma reúne a estas aplicaciones en torno a una interfaz gráfica de usuario común, base de datos y presentación de informes. Aplicaciones de NG Firewall permiten inspeccionar el tráfico de red de forma simultánea, lo que reduce en gran medida las necesidades de recursos de cada aplicación individual.

Vegas (2010) considera que los requerimientos de Untangle firewall son: Un procesador de 800 Mhz y 512 MB de RAM con un disco de 20 GB como mínimo. Además la lista de funciones y servicios de las que dispone Untangle de forma gratuita son:

- Web Filter
- Spam Blocker
- Virus Blocker
- Spyware Blocker
- Protocol Control
- Firewall
- Reports
- Adblocker
- Open VPN.

## 2.4. DATA CENTERS

Es el centro de misión crítica de toda empresa, construido como un ambiente apropiado y seguro, en el cual se albergan los servidores, equipos de telecomunicaciones y los sistemas de almacenamiento de las instituciones. Los centros de datos son ambientes que demandan la más alta disponibilidad y funcionamiento. (Zambrano, 2014).

Según Emicuri (2012) especifica que el Data Center es un edificio o parte de un edifico que tiene por función principal albergar una sala de informática y sus áreas de soporte, con una infraestructura con el espacio físico suficiente para los equipos informáticos, adecuado sistema de energía, climatización, seguridad, conectividad Internet privada y servicios de operación y suspensión de todos los componentes.

### 2.4.1. TENDENCIAS DE UN DATA CENTER

- Convergencia de múltiples aplicaciones y sistemas
- Velocidades de Transmisión más altas.
- Consolidación y Virtualización Servidores
- Capacidad de Almacenaje Incrementada
- Mayor número de dispositivos, cables y conexiones
- Construcción de Data Centers “Verdes” y sostenibles que reducen el impacto ambiental. (López, 2012).

### 2.4.2. APORTACIÓN DE UN DATA CENTER

De acuerdo a lo establecido por Zambrano (2014) hoy en día, los data center deben resolver diversas problemáticas, tanto en el ámbito de la infraestructura física, como en su aporte al desarrollo del negocio de las organizaciones. Dentro del ámbito de la infraestructura física, los centros de datos deben asegurar su continuidad operacional. Dentro del ámbito del negocio mejorar localidad de servicio para los clientes, optimizar tiempo y manejar grandes volúmenes de información. Por otra parte para Spera (2012) indica que la aportación de los centros de datos en las organizaciones actualmente se orienta a conceptos tales como implementación de grandes servidores, grandes volúmenes de información, virtualización y green IT.

### 2.4.3. SERVIDOR

En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. Por tanto un servidor en informática será un ordenador u otro tipo de dispositivo que suministra una información requerida por unos

clientes (que pueden ser personas, o también pueden ser otros dispositivos como ordenadores, móviles, impresoras, etc.). (Sierra, 2013).

Partiendo del contexto anterior, la empresa ANER (2015) define un servidor como un equipo informático que forma parte de una red y provee servicios a otros equipos cliente, y que pueden haber dos tipos: Servidor dedicado, aquel que dedica todos sus recursos a atender solicitudes de los equipos cliente y servidor compartido que no dedica todos sus recursos a servir las peticiones de los clientes, sino que también es utilizado por un usuario para trabajar de forma local.

#### 2.4.3.1. SERVIDOR LINUX

Gómez (2010) fundamenta que este tipo de servidores son sistemas operativos de la familia Unix, gratuitos, creado mediante la política de “código abierto. Estas características implican un gran ahorro en los costes de instalación de los equipos, pero también una mayor especialización por parte del personal informático. De igual forma Barrios (2013) indica que GNU/Linux es uno de los términos empleados para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL y otra serie de licencias libres.

#### 2.4.3.2. WINDOWS SERVER

La empresa de soluciones de tecnología y comunicaciones AEVITAS (2013) establece que Windows server es una marca que abarca una línea de productos servidor de Microsoft Corporation, consiste en un sistema operativo diseñado para servidores de Microsoft y una gama de productos dirigidos al mercado más amplio de negocios. Windows Server ofrece más control sobre la infraestructura de servidores y red, mejor hosting, protección del sistema

operativo y el entorno de red, herramientas administrativas intuitivas, facilidad de consolidación, virtualización de servidores y aplicaciones.

Así mismo Amortegui (2014) dice que es un sistema operativo de la marca Windows, para servidores que salió al mercado en el año 2003 basado en tecnología NT. En términos generales se podría considerar a Windows server como una versión modificada de Windows xp, no con menos funciones sino que estas están deshabilitadas por defecto para tener un mejor rendimiento y para centrar el uso del procesador en las funciones de servidor.

## 2.5. VIRTUALIZACIÓN

Fuertes *et al.,* (2011) definen a la virtualización como la forma de particionamiento lógico de un equipo físico en diversas máquinas virtuales, para compartir recursos de hardware, como CPU, memoria, disco duro y dispositivos de entrada y salida; por lo tanto de acuerdo con Velázquez (2009) citado por Lugo (2014) manifiesta que la virtualización implica hacer que un recurso físico, como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fuera varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico".

### 2.5.1. VIRTUALIZACIÓN DE SERVIDORES

Velázquez (2009 citado por Lugo (2014) indica que la virtualización de servidores consiste en un computador principal al que los clientes u otros computadores se conectan para obtener archivos o manejar todos los recursos de la red. En la virtualización de servidores es donde se particiona un servidor físico en pequeños servidores virtuales. Por parte según Pachas (s.f) el cómputo del ordenador físico se reparte entre los diferentes sistemas operativos en función de las reglas de proporcionalidad que se establecen.

### 2.5.2. MÁQUINA VIRTUAL

Un sistema informático virtual se denomina “máquina virtual” (VM, Virtual Machine): un contenedor de software muy aislado en el que se incluyen un sistema operativo y aplicaciones. Cada una de las VM autónomas es completamente independiente. Si se colocan múltiples VM en una única computadora, es posible la ejecución de varios sistemas operativos y varias aplicaciones en un solo servidor físico o “anfitrión”. (VMWARE, 2015).

Además para Rouse (2014) la máquina virtual normalmente emula un ambiente de computación físico pero las demandas de CPU, memoria, disco duro, red y otros recursos de hardware son gestionadas por una capa de virtualización que traduce estas solicitudes a la infraestructura de hardware físico subyacente.

# CAPÍTULO III. DESARROLLO METODOLÓGICO

La implementación de un servidor perimetral firewall, fue ejecutada en el Data Center de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, situada en el sitio el Limón de la Ciudad de Calceta, Cantón Bolívar. La misma que tuvo un tiempo de duración de 12 meses calendario, la cual fue desarrollada en base a la metodología de desarrollo de software cascada, la misma que está compuesta por 5 fases que son: Análisis y formulación de requerimientos, diseño, implementación y validación de unidades, integración y validación del sistema y funcionamiento y mantenimiento.

## 3.1. ANÁLISIS Y FORMULACIÓN DE REQUERIMIENTOS

### 3.1.1. DIÁLOGO CON EL ENCARGADO DEL DATA CENTER

En lo que corresponde a esta actividad, para realizar el levantamiento de información se envió un oficio al jefe del departamento de tecnología de la ESPAM-MFL, luego se realizó una visita al Data Center de la universidad y se realizó una entrevista informal con el administrador, donde se dio a conocer el objetivo de estudio de este trabajo.

### 3.1.2. CONOCER LOS TIPOS DE EQUIPOS Y SISTEMAS QUE MANEJA EL DATA CENTER

De acuerdo a esta actividad se realizó un cuestionario al administrador, 40 encuestas a los usuarios del data center (estudiantes, docentes y personal administrativo), y una ficha de observación realizada por los autores de este trabajo, lo que permitió adquirir información acerca de los equipos y sistemas que se manipulan en este centro de datos.

El cuestionario aplicado al administrador permitió conocer que el data center de la ESPAM-MFL no manejaba un sistema perimetral firewall, por otra parte este

departamento cuenta con un servidor Blade c3000 con 2 storage y un servidor HP 2000. (**Anexo 7**).

Con la encuesta que se le realizó, se pudo recopilar información de la perspectiva tenían los docentes, alumnos y personal administrativo de la universidad, acerca de la seguridad que se maneja en el data center y sobre la implementación de un sistema de seguridad perimetral firewall en dicho centro de datos.

Con respecto a la ficha de observación, se comprobó que el data center utiliza servidores virtuales (VMWARE ) y sistemas operativos Linux, como Red Hat 9, Centos 6.5, Fedora 17 y sistemas Microsoft como Windows 7, además en otro contexto los servidores del data center poseen procesadores XEON y memoria RAM de 80 GB. Así mismo se pudo conocer que la universidad cuenta con un canal dedicado de internet, cuyo proveedor es CNT con 100 MB de ancho de banda, 1 MB de subida de archivos y 1 MB de descarga de archivos.

### 3.1.3. IDENTIFICAR EL NIVEL DE SEGURIDAD DEL DATA CENTER

Para identificar los niveles de seguridad del Data Center se utilizó un cuestionario, el cual se le aplicó al administrador, dando a conocer los tipos y niveles de seguridad que se manejaba en los servidores.

Con el cuestionario se determinó que la seguridad del data center está dividida en tres partes. De acceso físico, de acceso lógico y de autentificación. De igual forma se utilizan sistemas VMWARE, Data Protection y equipos de redes de capa tres (Routers). Así mismo, como política de seguridad del data center es que el único encargado del manejo de la seguridad sea el administrador del mismo, es decir, no existen terceras personas que realicen este tipo de tareas.

### 3.1.4. DEFINICIÓN DE REQUERIMIENTOS

En esta actividad se solicitó una entrevista informal al administrador del Data Center, en la cual se obtuvo la información necesaria acerca de los requerimientos generales que debía cumplir el sistema perimetral firewall para la universidad, los cuales fueron los siguientes:

- Firewall a nivel de software
- Sistema independiente
- Basado en código libre
- Virtualizado en VMWARE

#### 3.1.4.1. ESTABLECER LOS NIVELES DE SEGURIDAD DEL SISTEMA PERIMETRAL FIREWALL

Para establecer los niveles de seguridad, se definieron 3 puntos esenciales: seguridad física, seguridad lógica y de autentificación.

En relación a la seguridad física del servidor firewall se tomaron en cuenta los siguientes puntos.

- ✓ Acceso de personal autorizado al centro de datos.
- ✓ Climatización adecuada.
- ✓ Cámara de vigilancia.
- ✓ Conexión eléctrica adecuada.
- ✓ Libre de humedad y agentes nocivos.

En lo que corresponde a la seguridad lógica se definieron los siguientes puntos. Restringir el acceso a los programas y archivos mediante usuario y clave.

- Contar con una zona límite (DMZ) de acceso a los servicios del data center.
- Filtración de paquetes.
- Bloqueo de páginas web.
- Monitoreo de red.
- Conexiones privadas (VPN).
- Sistema de recuperación (backups).

- Generación de reportes de cualquier tipo de acceso a la red interna de la universidad.

Y en cuanto a la seguridad de autentificación del firewall, se basa al usuario y contraseña (único) asignado al firewall que permita ingresar al sistema, ya sea de manera remota o con una conexión directamente en la red interna de la universidad.

### 3.1.5. ANÁLISIS DE SISTEMAS FIREWALL DE CÓDIGO LIBRE

En lo que corresponde a esta actividad, se realizó un análisis de diferentes tipos de servidores firewall, tomando en cuenta que debían ser de código libre, que sean modulares y que se instale como un sistema individual. De acuerdo con estos aspectos se escogieron tres sistemas firewall los cuales fueron IpFire versión 2.17, PfSense versión 2.2.6 y Untangle NG Firewall versión 11.21.

En lo que respecta al software IpFire, es un firewall de código libre que se instala como un sistema operativo individual, y está diseñado con modularidad y un alto nivel de flexibilidad. Se pueden implementar fácilmente muchas variaciones de la misma, como cortafuegos, servidor proxy o una puerta de enlace VPN. El diseño modular asegura que se ejecuta puntualmente lo que se ha configurado. Además cuenta una interfaz web que permite la configuración y administración. (Foto 3.1.)


**Foto 3. 1.** Interfaz web del firewall IPfire.

De acuerdo con el software PfSense, es una distribución basada en código libre, y además cuenta con una interfaz web para su configuración basada en PHP. (Foto 3.2.)

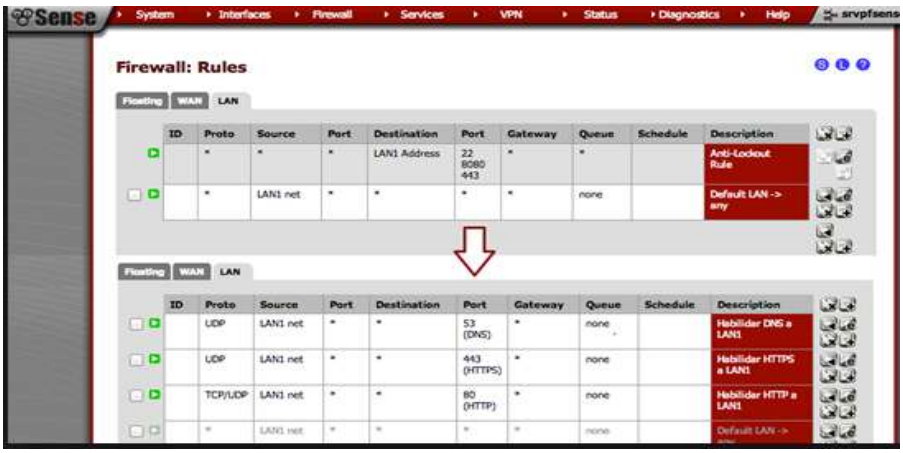



**Foto 3. 2.** Interfaz web del firewall PfSense.

Por otra parte, este firewall cuenta con un gran reconocimiento a nivel mundial, de acuerdo a un estudio realizado por Pudwell (2015) de la empresa IT Central Station, donde establece que este software es unos de los más reconocidos y utilizados a nivel mundial, tal y como lo muestra la figura 3.1.

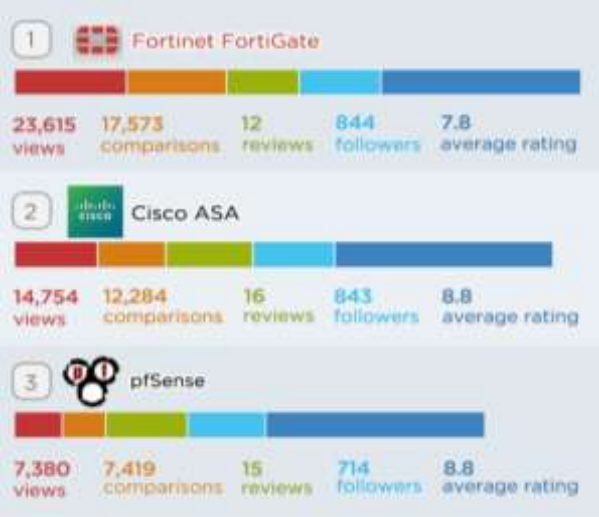



**Figura 3. 1.** Ranking de servidores firewall en 2015.

El software Untangle NG Firewall, es un servidor creado por la empresa privada Untangle y que ofrece una distribución gratuita basada en código libre y que brinda un gran conjunto de aplicaciones de administración de la seguridad de la información para pequeñas, medianas empresas y específicamente para instituciones de educativas. Así mismo es administrable a través de una GUI según lo muestra la foto 3.3.


**Foto 3. 3.** Interfaz gráfica de usuario del firewall Untangle.

### 3.1.6. ESTUDIO COMPARATIVO DE SISTEMAS FIREWALL

Para realizar la comparación de los sistemas firewalls que fueron escogidos y determinar el más óptimo para los requisitos de seguridad de la universidad, se

instaló cada software de forma virtual haciendo uso de la herramienta vmware workstation 11.1, y luego se aplicó un checklist para evaluar cada firewall. (Cuadro 3.1)

**Cuadro 3. 1.** Checklist para realizar comparación de los firewalls.

| **CHECKLIST** | | |
|---|---|---|
| **1. IDENTIFICACIÓN DE LA EVALUACIÓN** | | |
| **PROPÓSITO: ESTUDIO COMPARATIVO DE LOS SISTEMAS FIREWALLS IPFIRE, PFSENSE Y UNTANGLE** | | |
| **PROYECTO:** **SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.** | **SOFTWARE A EVALUAR** ❒ IpFire ❒ PfSense ❒ Untangle | |
| **2. AUTORES** | | |
| **NOMBRES:** DELGADO ZAMBRANO PABLO RICARDO y LOOR LOOR LUIS ANTONIO | | |
| **E-MAIL:** ricky020694@hotmail.com; | **FONO:** | |
| **3. CHECKLIST** | **SÍ** | **NO** |
| ¿EL FIREWALL SE INSTALA COMO UN SISTEMA INDPENDIENTE? | | |
| ¿EL FIREWALL REQUIERE GRAN CANTIDAD DE RECURSOS EN HARDWARE? | | |
| ¿EL FIREWALL PERMITE REALIZAR UNA CONFIGURACIÓN PERSONALIZADA? | | |
| ¿EL FIREWALL CUENTA UN ENTORNO WEB DE ADMINISTRACIÓN? | | |
| ¿EL FIREWALL PUEDE SER INSTALADO COMO SERVIDOR VIRTUAL? | | |
| ¿EL FIREWALL ES COMPATIBLE CON EL SISTEMA VMWARE? | | |
| FILTRADO WEB | | |
| INTERFAZ GRÁFICA AMIGABLE | | |
| CONTROL DE INTRUSOS | | |
| ANTISPAM | | |
| ANTIVIRUS | | |
| ANTIPHISHING | | |
| CONTROL DE USUARIOS | | |
| PERMITE REALIZAR BALANCEO DE CARGA | | |
| PERMITE CONFIGURAR 2 CORTAFUEGOS DENTRO DEL MISMO (REDUNDANCIA) | | |
| TABLA DE ESTADOS DE CONEXIONES ABIERTAS | | |
| SERVIDOR STREAMING | | |
| SERVIDOR DHCP | | |
| SERVIDOR PPPoE | | |
| SERVIDOR VPN | | |
| SERVIDOR DNS | | |
| SERVIDOR GRABADOR DE VIDEO | | |
| SERVIDOR PARA CENTRAL VOIP | | |
| SERVIDOR PROXY | | |
| PORTAL CAUTIVO | | |
| ENRUTAMIENTO ESTÁTICO | | |
| CACHÉ DE NOMBRES DE NOMINIOS | | |

## 3.2. DISEÑO DEL SISTEMA

Para el cumplimiento de esta fase se realizó un esquema del funcionamiento de servidor firewall en la red interna de la ESPAM MFL, para esto se tomó como punto de referencia que el sistema debía estar instalado entre la interface WAN y la interface LAN de la universidad, además se estableció una zona desmilitarizada la cual corresponde a un espacio designado para las aplicaciones web de la institución.

Como muestra la figura 3.2 el servidor firewall cuenta con tres interfaces de red (WAN, LAN y DMZ), es decir, que el sistema actúa como barrera entre la interface WAN y LAN, por lo tanto las conexiones desde fuera de la universidad hacia la red interna de la misma serán restringidas. Así mismo, se protege las conexiones que realicen a través de la interface DMZ, es decir, que un usuario no podrá establecer vínculos hacia la red interna por medio de esta interface.

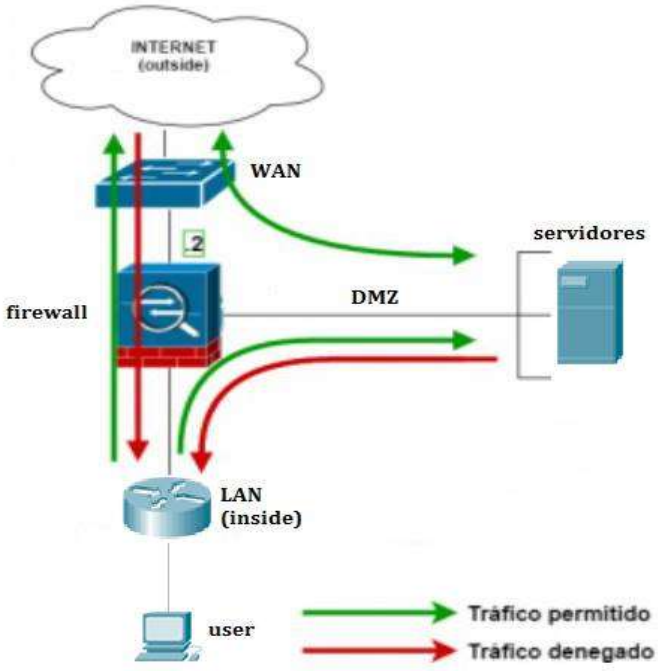



**Figura 3.2.** Funcionamiento del servidor firewall.

## 3.3. IMPLEMENTACIÓN DEL SISTEMA

### 3.3.1. ASIGNACIÓN DE ESPACIO DE ALMACENAMIENTO EN LOS SERVIDORES DEL DATA CENTER DE LA ESPAM MFL

Una vez que se realizó el estudio comparativo aplicando el checklist a cada software, se determinó que Pfsense era el sistema más adecuado para los requisitos de la universidad. Para esto se realizó una entrevista informal con el administrador del Data Center para asignar el respectivo espacio de almacenamiento que requería el firewall en el data center. Para lo cual, nos facilitó un CPU de última generación, con procesador Core i7 y una memoria RAM de 8GB; además se le añadieron 2 tarjetas de red TP-LINK Gigabit PCI Express, disco duro de 500GB y el sistema Operativo Windows 7 de 64 bits.

### 3.3.2. DESCARGAR EL SISTEMA FIREWALL Y PROGRAMAS A UTILIZAR

Para descargar el sistema firewall y demás programas a utilizar, se les realizó desde sus respectivas páginas oficiales, en este caso PfSense, que de acuerdo al estudio comparativo aplicado a Ipfire y Untangle, cuenta con las mejores características de seguridad. Además se realizó la descarga de la máquina virtual VMware Workstation 11.1 para efectuar la virtualización del firewall.

### 3.3.3. INSTALAR EL SISTEMA FIREWALL DE FORMA VIRTUAL EN EL DATA CENTER DE LA ESPAM

Para el cumplimiento de esta actividad, se instaló la máquina virtual VMWARE Workstation 11.1, en el ordenador que está asignado en el Data Center de la ESPAM MFL.

A continuación se procedió a la creación de una máquina virtual en VMWARE para el servidor firewall Pfsense, con nombre (Sistema Firewall) y se asignaron tres tarjetas de red las cuales corresponden a la interface LAN, WAN y DMZ.

Una vez creada la máquina virtual, el paso siguiente fue realizar la instalación del software Pfsense, dentro del sistema de virtualización VMWARE.

### 3.3.4. CONFIGURACIÓN DEL SISTEMA FIREWALL DE ACUERDO CON LOS REQUERIMIENTOS DE SEGURIDAD DE LA UNIVERSIDAD

Finalizada la instalación del pfsense se procedió con la respectiva configuración, lo cual se lo realizó desde la interfaz web, a la que se ingresa con la dirección IP que viene por defecto en el firewall (192.168.1.1) y con el usuario (admin) y contraseña (pfsense).

#### 3.3.4.1. CONFIGURACIÓN DE INTERFACES DE RED

Se ingresó a la configuración de la interface WAN, la cual se le asignó la dirección IP pública con la que cuenta la universidad. Además se establecieron los respectivos DNS de navegación, y a continuación en la máquina virtual se activó el protocolo ssh, que se utiliza para la administración por consola del servidor firewall. Luego se instaló una aplicación llamada putty, en una máquina (cliente). Para esto se le asignó una dirección IP en el rango de la interface WAN del firewall, para poder acceder a la máquina virtual del pfsense de manera remota.

En la configuración de la interface LAN se asignó una dirección IPv4 de clase B de manera estática para la red local de la universidad, así mismo, se asignó una dirección IP a la máquina virtual, la cual debe estar en el mismo rango de la interface LAN del firewall.

Luego se configuró la interface de red DMZ, la cual es la zona desmilitarizada, es decir, se creó una subred independiente para los servidores de aplicaciones de acceso público, los cuales se colocaron en un segmento separado, para controlar y restringir ataques a la red interna. Para esto se le asignó un nombre a la zona DMZ y se estableció una dirección IP estática.

### 3.3.4.2. CONFIGURACIÓN DE REGLAS DE FIREWALL

Se configuró la regla para la interface DMZ, la cual consiste en asignar una zona independiente, para las peticiones realizadas fuera de la red interna hacia los servidores de la universidad.

A continuación se agregó una dirección IP virtual, la cual es la que recibe los paquetes entrantes del sistema y que consolida los recursos a través de una interface de red por cada aplicación alojada. (Foto 3.4)

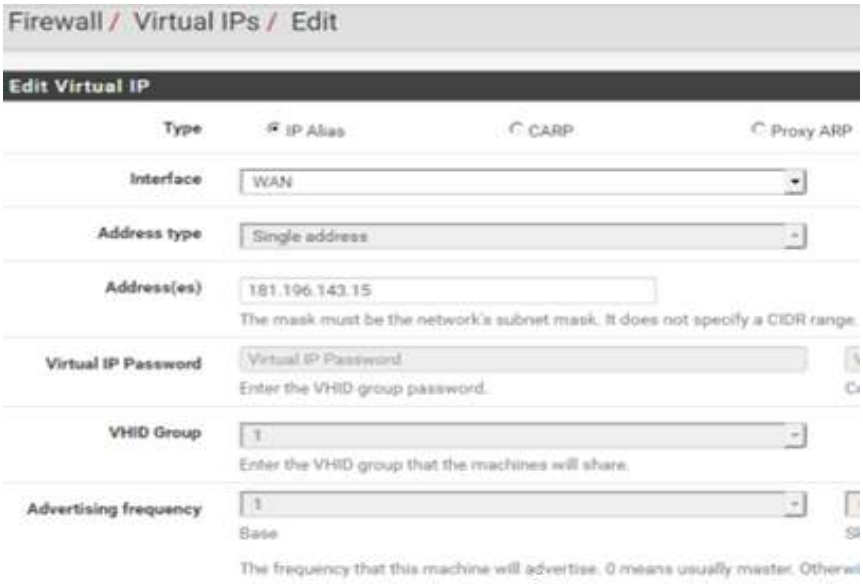



**Foto 3. 4.** Configuración de la dirección IP virtual del servidor pfsense.

Posteriormente, se realizó la configuración de la regla NAT, la que permite que una dirección IP privada se traduzca siempre en una misma dirección IP pública, este modo de funcionamiento permitiría que un host dentro de la red interna de la universidad, pueda ser visible desde cualquier lugar con una conexión a internet. (Foto 3.5)

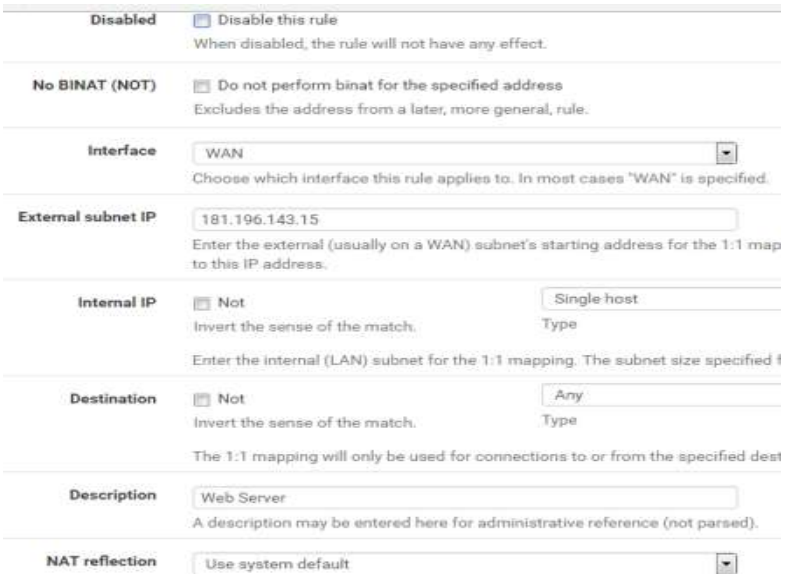



**Foto 3. 5.** Configuración de la regla NAT 1:1.

Luego se configuró el servicio de DHCP para la interface LAN, para permitir asignar direcciones IP de manera dinámica en un rango establecido a la red de la universidad, tanto para la conexión de WLAN. (Foto 3.6)

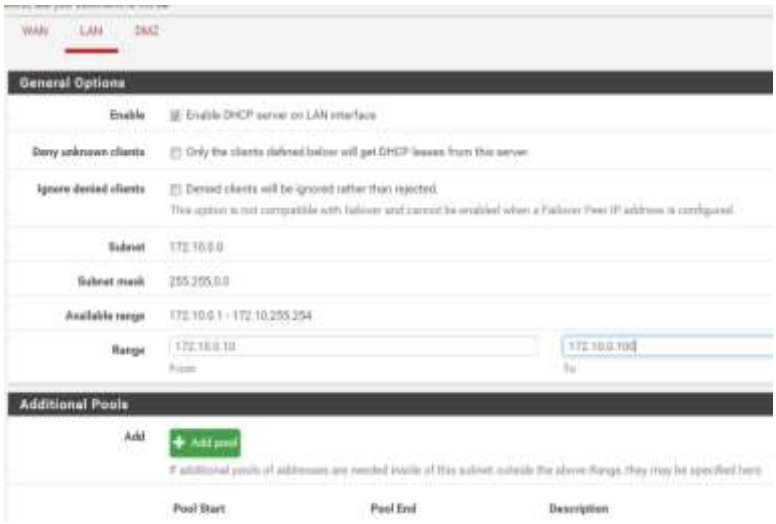



**Foto 3. 6.** Configuración del DHCP en la interface LAN.

A continuación procedimos a establecer la regla para el bloqueo de páginas web, por medio del servidor firewall. Las páginas bloqueadas son Facebook y Twitter, para esto se obtuvieron las direcciones IP de los sitios web, para lo cual se utilizó una página web que facilita todas las IP de las páginas buscadas. (Foto 3.7)

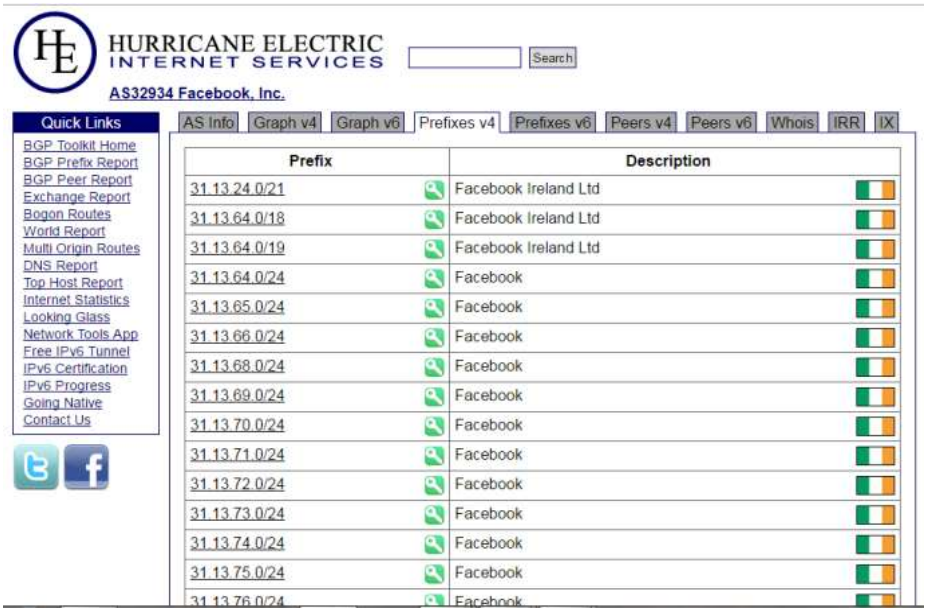



**Foto 3. 7.** Búsqueda de direcciones IP de páginas a bloquear.

Luego en Pfsense para el bloqueo de páginas web se configuró los alias, que son un puerto o un grupo de puertos, una dirección IP o grupo de direcciones IP, una red o un grupo de redes, que permiten ahorrar escritura al configurar las reglas y realizar cambios de forma mucho más fácil al actuar como parámetros. Para esto se ingresaron todas las direcciones IP de las páginas web que fueron bloqueadas en toda la interface LAN. (Foto 3.8)

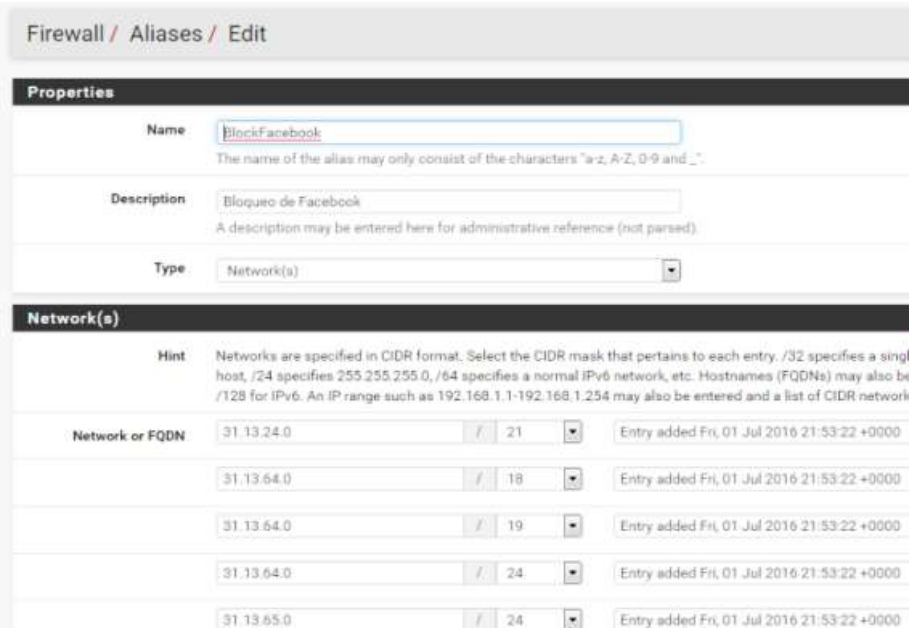



**Foto 3. 8.** Alias para el bloqueo de la página de Facebook.

Una vez creados los alias, se procedió a la creación de la regla, este paso se lo realizó para que cada vez que un usuario se conecte a la interface LAN, sea cableado o inalámbrico, automáticamente bloquee todas las páginas creadas en la regla. (Foto 3.9)

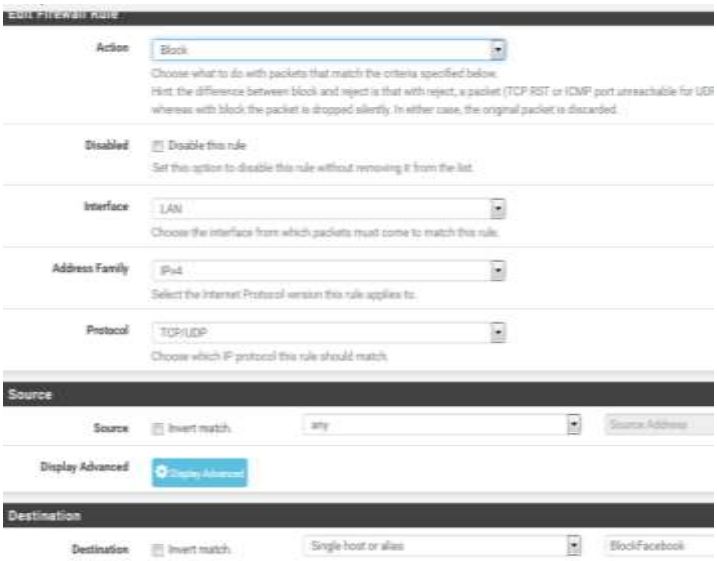



**Foto 3. 9.** Configuración de la regla para el bloqueo de páginas web.

A continuación se configuró el límite del ancho de banda para las áreas del campus universitario; lo que permite controlar el tráfico de peticiones de datos que tienen los usuarios al conectarse al internet. Este paso se puede hacerlo de dos maneras, por medio de interfaces y por subredes de las interfaces, en este caso se lo realizó por subredes. Después se realizó la configuración de la regla para establecer el ancho de banda designado para cada dirección IP de la interface LAN. (Foto 3.10)

**Foto 3. 10.** Reglar para asignar el ancho de banda a la interface LAN.

También se bloquearon algunos puertos para ciertos tipos protocolos, debido a la fuga de información, consumo excesivo de ancho de banda o ataques informáticos por medio de puertos abiertos. (Foto 3.11)

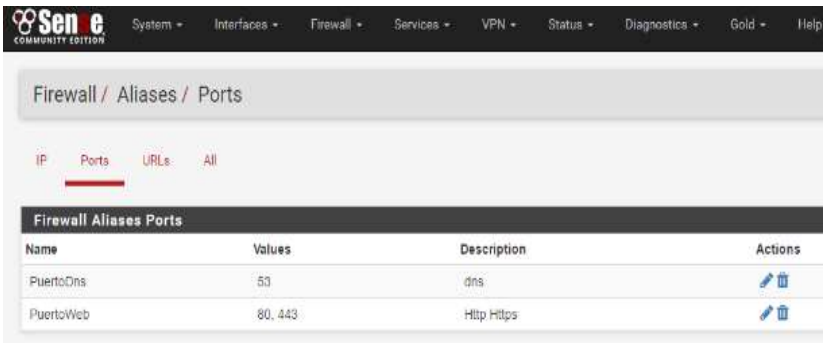



**Foto 3. 11.** Creación de alias para puertos.

En esta parte se realizó la configuración de la regla para el protocolo ICMP en la interface WAN, para que no permita que una persona pueda establecer comunicación a través del comando ping fuera de la red de la universidad hacia la direcciones IP de la universidad. (Foto 3.12)

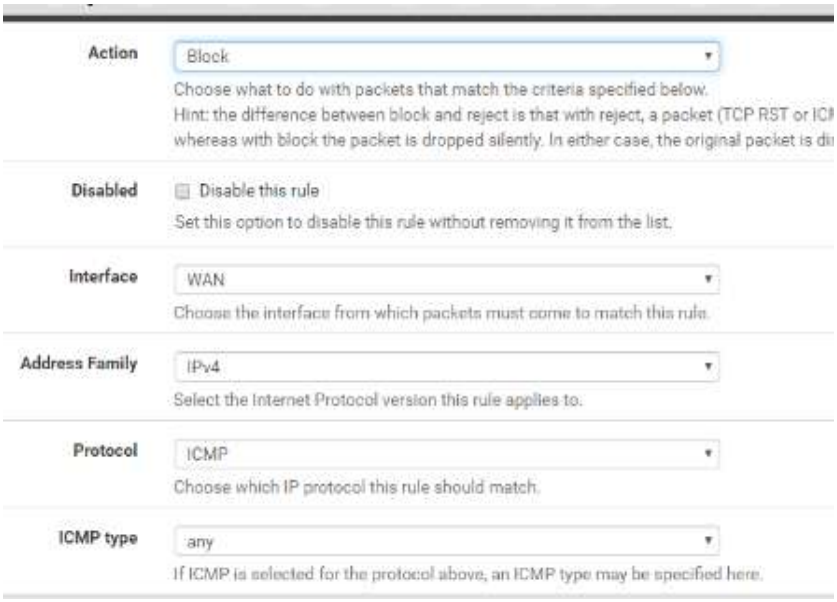



**Foto 3. 12.** Regla del protocolo ICMP.

De la misma forma se agregó una regla para la interface LAN y WAN con el mismo protocolo, evitando hacer ping a las direcciones IP principales de la red interna de la universidad a través de las subredes.

### 3.3.4.3. CONFIGURACIÓN DE UNA RED PRIVADA VIRTUAL

Se agregó el servicio llamado OpenVPN, que permite crear redes privadas virtuales y con el cual el administrador del servidor firewall podrá acceder a la red de la universidad desde cualquier lugar del mundo con una conexión a internet de forma más segura.

Para la configuración de este servicio se creó una entidad emisora de certificados (CA) en el servidor, para establecer conexión a través del servicio OpenVPN.

Luego para dar asegurar la interfaz web del pfsense y evitar el espionaje en caso de tener que realizar alguna configuración de manera remota, se creó el CAs(Certificate Autority Manger. (Foto 3.13)


**Foto 3. 13.** Asignación de certificado interno del pfsense.

Después de realizar la configuración del CAs, se creó otro certificado para que el usuario (administrador del firewall), pueda acceder desde un navegador web al firewall.

A continuación se realizó la configuración del túnel privado, el cual permitirá realizar una conexión exclusiva entre el administrador y el sistema firewall. Y

además se creó el certificado del servidor que se utiliza al momento de acceder al servidor firewall. (Foto3.14)


**Foto 3. 14.** Certificado de acceso remoto al servidor firewall.

También se establecieron las interfaces, el protocolo y el número de puerto donde habrá comunicación con el servidor firewall. En este caso la interface WAN que se comunicará al OpenVPN para acceder a la red interna de la ESPAM desde el exterior. Por otra parte el protocolo que se utilizó fue UDP y el puerto por defecto de OpenVPN es 1194.

Luego se configuró el cifrado de datos al momento de acceder al servidor. Aquí se especificó el uso de la autenticación TLS de criptografía y se generó una clave de autenticación.

A continuación se configuró el túnel de conexión interna, donde se especificó a que dirección privada el cliente tendrá acceso, es decir, todo el tráfico será redirigido a través del túnel privado a la red local de la ESPAM. Además se configuró el número máximo de sesiones simultáneas y la compresión de los datos que pasen por el túnel. También se activó la comunicación remota entre el cliente y servidor. (Foto 3.15)


**Foto 3. 15.** Configuración de túnel de red en VPN.

Luego se habilitaron dos reglas que se utilizan para que se pueda establecer una conexión entre el cliente y el servidor. (Foto 3.16)

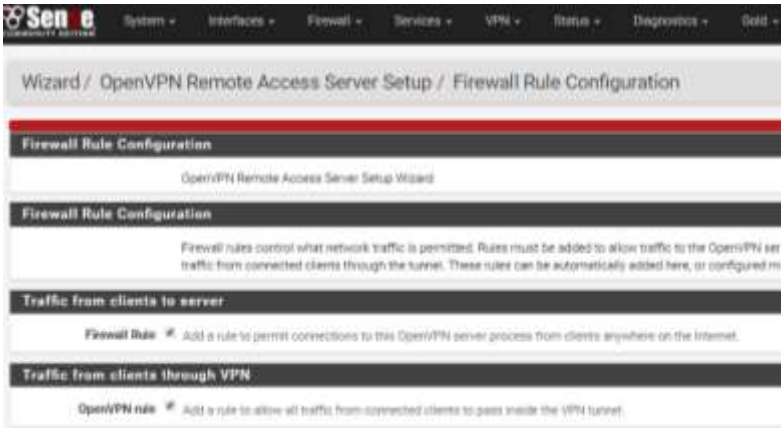



**Foto 3. 16.** Configuración de las reglas del VPN.

El siguiente paso fue crear la cuenta de administrador que se va a utilizar durante el proceso de autentificación. A continuación se creó un certificado de usuario para dicha cuenta, lo que permitirá al usuario tener acceso a al servidor firewall desde cualquier lugar con una conexión a internet. (Foto 3.17)

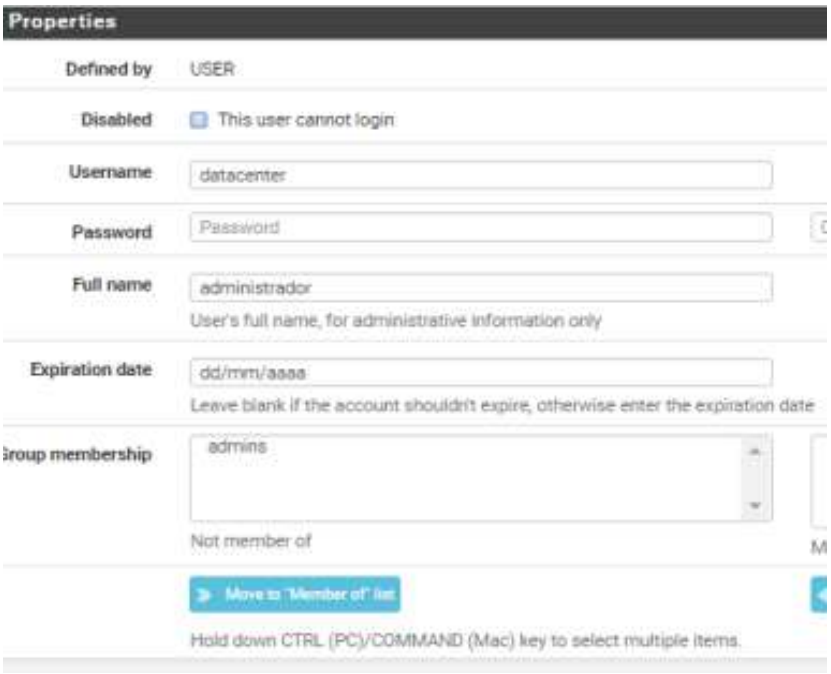



**Foto 3. 17.** Asignación de certificado a la cuenta de usuario administrador.

El siguiente paso fue instalar un paquete llamado openvpn-client-export en el servidor, que permitirá exportar las claves y certificados de pfsense, para realizar la conexión al servidor firewall de manera remota.

Luego de haber instalado el paquete del cliente vpn, se descargó el archivo que se instaló en una máquina cliente, para poder establecer la comunicación con el servidor a través del túnel privado.

Después de terminar la instalación se ingresó al OpenVPN GUI que apareceré en el escritorio de la máquina cliente, e ingresamos con usuario y contraseña del servidor firewall para establecer la conexión con el sistema. (Foto 3.18)

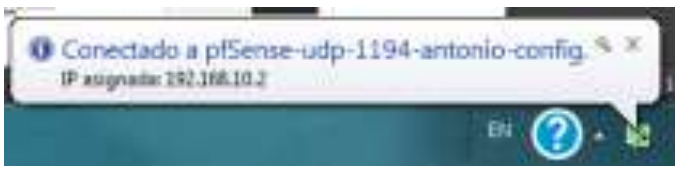



**Foto 3. 18.** Conexión al firewall a través de VPN.

## 3.4. INTEGRACIÓN Y VALIDACIÓN DEL SISTEMA

### 3.4.1. EVALUAR Y CORREGIR CADA NIVEL DE SEGURIDAD DEL SISTEMA FIREWALL

En esta actividad se verificó el correcto funcionamiento del sistema perimetral firewall en los niveles de seguridad de las interfaces de red con sus respectivas reglas.

Primero se corrigió la seguridad física del servidor, verificando que en la maquina donde está alojado el firewall, no estuviera expuesto a cualquier riesgo de humedad, agentes nocivo y que tuviera la climatización correcta. Para esto se realizó una visita al data center. **(Anexo 9)**

Posteriormente se evaluó la parte de seguridad lógica del firewall, teniendo como parte principal las interfaces de redes que estén conectadas, para dar la funcionalidad inicial del servidor.

- Se verificó que las reglas de firewall configuradas sobre la interfaces de red WAN, LAN y DMZ estuvieran activas para restringir, bloquear y validar al momento de recibir peticiones de los usuarios, cada una con la respectiva dirección IP. (Foto 3.19)

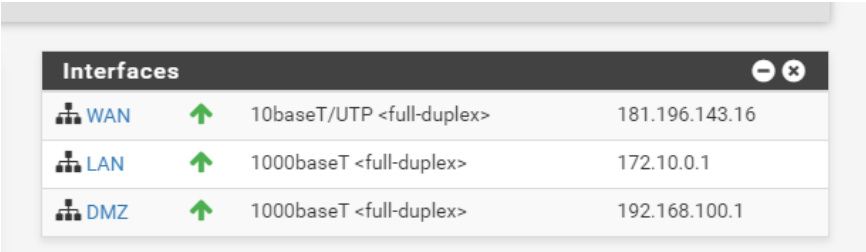



**Foto 3. 19.** Interfaces de red activas (WAN, LAN, DMZ).

- El siguiente paso fue revisar que estén activadas las reglas del servicio OpenVPN. Lo que permitirá establecer la comunicación a través del túnel privado entre el administrador del Data Center y servidor firewall. En la foto 3.20 se muestra que las reglas están corriendo adecuadamente.


**Foto 3. 20.** Reglas del servicio OpenVPN.

- Así mismo, se procedió a evaluar que el firewall asigne correctamente las direcciones virtuales IP para la zona DMZ. Entonces cada vez que se realice una petición para acceder a cualquier servicio web de la universidad, el sistema firewall asignará una IP virtual, por lo tanto el usuario no podrá conocer la IP real de la aplicación web. (Foto 3.21)

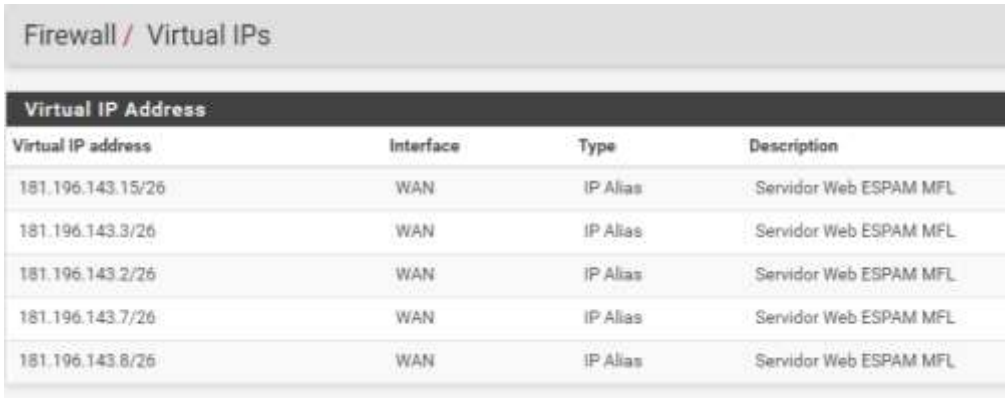



**Foto 3. 21.** Direcciones IP virtuales asignadas por el firewall.

- Además se realizó la verificación de la regla NAT 1:1, para comprobar que las IP virtuales estén asignadas correctamente al segmento de direcciones IP de la zona DMZ, es decir, al momento que un usuario acceda a una aplicación web de la universidad, el firewall asigne una dirección IP interna y una dirección IP virtual. (Foto 3.22)


**Foto 3. 22.** Regla NAT 1:1.

- Luego se comprobó que los servicios activados en el firewall, tales como como DHCP, VPN, SSH estén corriendo debidamente. (Foto 3.23).


**Foto 3. 23.** Servicios del Firewall.

- A continuación se realizó un diagnóstico generado por el pfsense, para comprobar las direcciones IP, que son bloqueadas por servidor firewall. En este caso se realizaron pruebas tomando en cuenta la página de Twitter. (Foto 3.24)

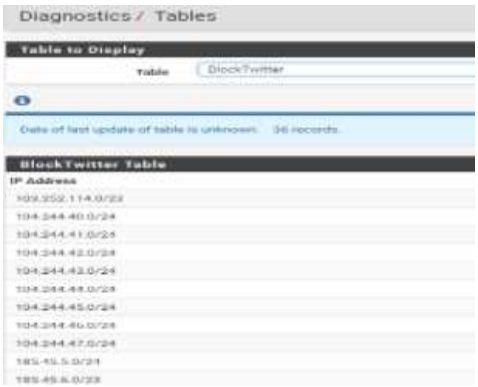



**Foto 3. 24.** Bloqueo de Pagina.

- También se comprobó que el servidor firewall no permita el acceso a las páginas web bloqueadas dentro de la configuración del mismo, en este caso se lo realizó pruebas con la página web de Facebook. (Foto 3.25).

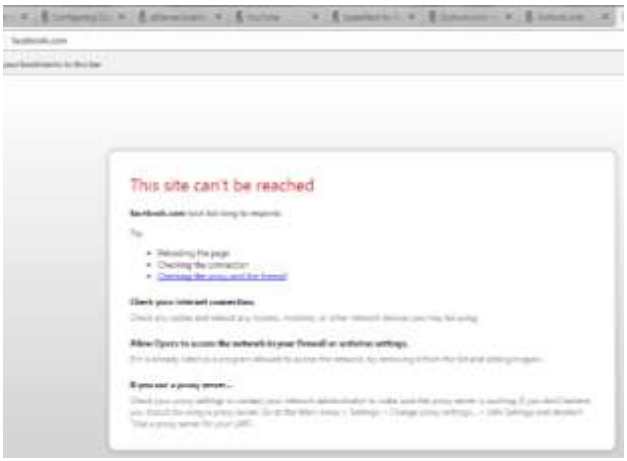



**Foto 3. 25.** Reporte de bloqueo de páginas.

- Después se comprobó que los límites de anchos de banda agregados para las interfaces de red tengan la velocidad adecuada, en este caso se lo realizó utilizando el medidor de velocidad de CNT para la carrera de computación. Mostrando una velocidad de 16,02 Mb de descarga y 15,36 Mb de subida. (Foto 3.26)


**Foto 3. 26.** Test de Velocidad.

- El paso siguiente fue verificar el bloqueo del protocolo ICMP se realice correctamente, el cual permite bloquear conexiones por medio del comando ping a las direcciones IP o host del servidor firewall. Para esto, desde una máquina cliente realizamos ping a la dirección IP de la

interface DMZ, y como muestra la foto 3.27 el protocolo ICMP bloquea la conexión.

**Foto 3. 27.** Prueba de protocolo ICMP.

- Luego se realizó un ingresó al servidor firewall desde una máquina cliente con una conexión a internet fuera de la red de la ESPAM, para comprobar que el firewall establezca la conexión correctamente por medio del servicio OpenVPN. (Foto. 3.28)

Remote Access Espam UDP:1194 Client Connections

| Common Name | Real Address | Virtual Address | Connected Since | Bytes Sent | Bytes Received |
|---|---|---|---|---|---|
| antonio | 181.113.183.187:52091 | 192.168.10.2 | Mon Jul 11 20:19:54 2015 | 259.41 MiB | 20.20 MiB |

Running

**Foto 3. 28.** Servicio OpenVPN.

- Así mismo se evaluó el estado de la dirección IP de la puerta de enlace que trabaja el Pfsense, para comprobar si estaba haciendo el monitoreo correspondiente a la interface WAN, de la que proviene el internet a toda la universidad. (Foto 3.29)

Gateways

| Name | Gateway | Monitor | RTT | RTTsd | Loss | Status | Description |
|---|---|---|---|---|---|---|---|
| WANGW | 181.196.143.1 | 181.196.143.1 | 69.272ms | 28.486ms | 0.0% | Online | |

**Foto 3. 29.** Puerta de enlace del servidor activa.

- Finalmente se verificó que el Pfsense cuenta con un sistema de respaldo (backup) con todas las configuraciones realizadas y que permita restaurar todo el sistema en caso de pérdida de firewall por daños físicos. (Foto 3.30)

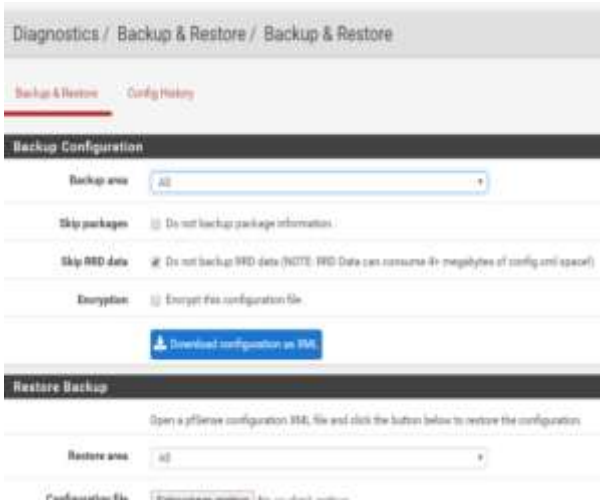



**Foto 3. 30.** Respaldo o Backup.

Como punto final se revisó la autentificación al servidor firewall que sea seguro y que cumpla con los datos ingresados durante la configuración, es decir, que solo ingrese con el usuario y contraseña especificados. Para lo cual se lo realizó realizando una conexión dentro y fuera de la red de la universidad. (Foto 3.31)


**Foto 3. 31.** Autentificación del Pfsense.

### 3.4.2. MONITOREO DE LA RED Y GENERACIÓN DE REPORTES

Para comprobar el tráfico generado a través de la interface WAN se realizó un escaneo, el cual se puede realizar cada vez que sea necesario. En la foto 3.32 se muestra el tráfico de datos en subida (bandwidth in) y de bajada (bandwidth

out) que tiene la interface de red de la WAN. Lo que corresponde a un tráfico estable y sin muchas variaciones, vale recalcar que estos valores pueden variar cada vez que se realice el monitoreo.


**Foto 3. 32.** Tráfico de la interfaz WAN.

A continuación se realizó el monitoreo de la interface LAN. En la foto 3.33 se observa el tráfico generado. Mostrando mayor alteración en lo que respecta a las peticiones de usuarios, variando desde 0 hasta 2,5 Mb de peticiones realizas.

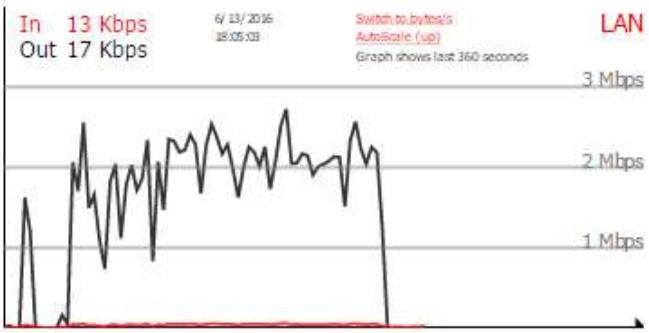



**Foto 3. 33.** Tráfico de la interfaz LAN.

Así mismo se realizó el monitoreo respectivo para el tráfico de red de la interface DMZ, que es donde se alojan los servidores de aplicaciones de la universidad. Para comprobar que el ingreso por parte de los usuarios a las aplicaciones web de la universidad sean controladas por el firewall, por lo tanto, se observa alteración y peticiones de usuarios, es decir, hay acceso activo a las aplicaciones almacenadas en el data center de la universidad. (Foto 3.34)

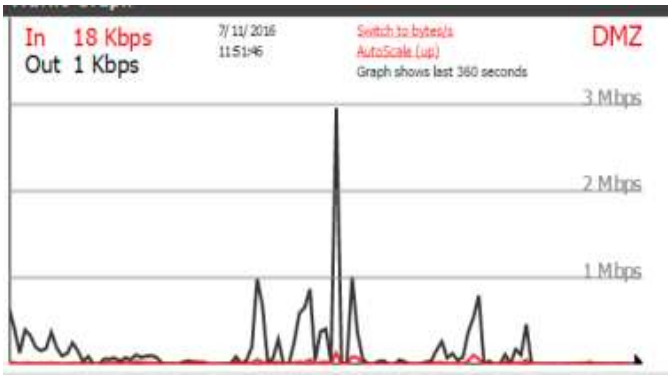



**Foto 3. 34.** Tráfico de la interfaz DMZ.

Por otra parte, se realizó el monitoreo del tráfico generado en la conexión de acceso remoto por medio de OpenVPN al servidor firewall, para verificar que el que el sistema realice el control respectivo de las alteraciones que se genera en la red, para esto, se estableció una conexión privada por un lapso de tiempo fuera de la universidad, y de acuerdo a eso se muestran las alteraciones de tráfico de red. (Foto 3.35)

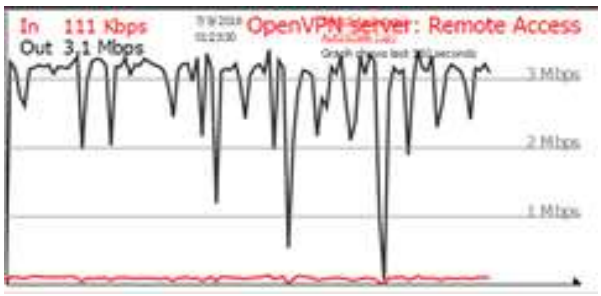



**Foto 3. 35.** Tráfico del OpenVPN.

A continuación se verificó que el firewall Pfsense genere los reportes respectivos. Para lo cual, se realizó una conexión fuera de la red de la universidad al servidor firewall, para comprobar que el sistema genere el reporte pertinente de la comunicación establecida. (Foto 3.36)


**Foto 3. 36.** Reporte de conexión OpenVPN.

Así mismo, se verificó que el firewall realice reportes de los usuarios que han tenido conexión a la red interna LAN, que puede ser por medio de enlaces inalámbricos o cableados. De esta manera el administrador puede conocer la dirección IP, dirección Mac, Host y tiempo de conexión de cada usuario. (Foto 3.37)


**Foto 3. 37.** Reportes de Usuarios conectados.

## 3.5. MANTENIMIENTO DEL SISTEMA

Una vez realizadas las correspondientes pruebas de funcionamiento al sistema firewall Pfsense, se creó un manual de usuario con todos los pasos detallados de instalación, configuración y manejo del sistema perimetral firewall con el objetivo de proporcionar una guía para el administrador del Data Center de la universidad, y con esto tener facilidad al realizar el mantenimiento respectivo al servidor.

# CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

## 4.1. RESULTADOS

Con la implementación del servidor perimetral firewall en el Data Center de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, se obtuvieron los siguiente resultados.

### 4.1.1. FASE 1

De acuerdo con el primer objetivo se realizó una encuesta a un total de 20 estudiantes y 20 encuestas aplicadas a docentes y personal administrativo de la universidad, para obtener información de la necesidad de implementar un sistema perimetral firewall.

Con respecto al gráfico 4.1 refleja que un 42% de los docentes, estudiantes y personal administrativo acceden al menos una vez por semana a los servicios que ofrece el data center de la ESPAM MFL, el 17 % es correspondiente al acceso que se realiza día por medio, diariamente el 29%, el 8% mensualmente y como restante que corresponde al 4% respondieron que nunca acceden a estos servicios.

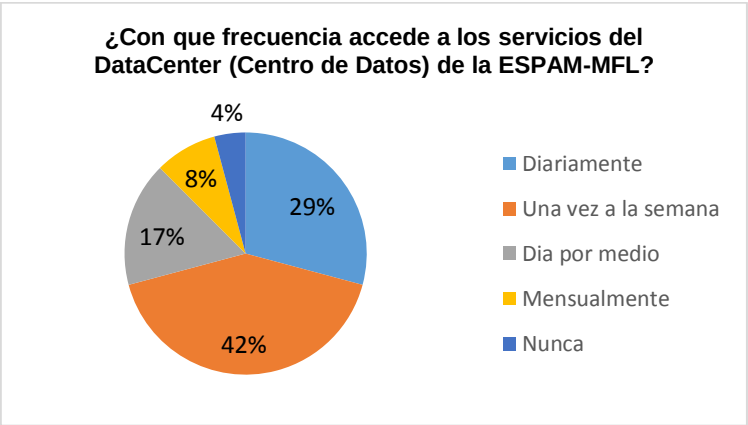



**Gráfico 4. 1.** Resultados de la primera pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

El gráfico 4.2 demuestra que el 54% de los usuarios de los servicios del data center, se ejecutan de manera rápida, y el 46% consideran que dichos servicios no se ejecutan de manera óptima.

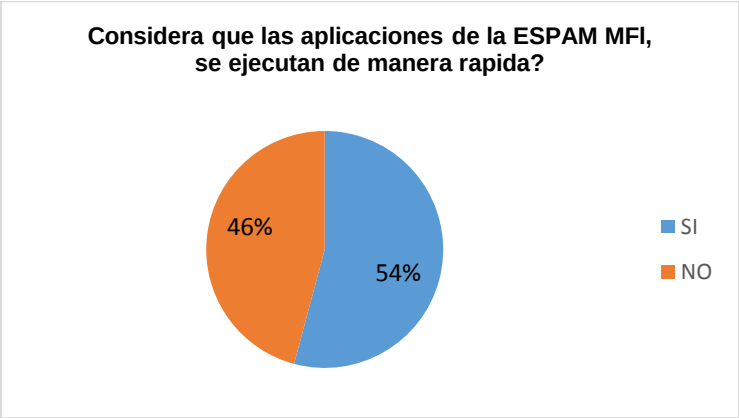



**Gráfico 4. 2.** Resultados de la segunda pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

En relación al gráfico 4.3 define que el 67% de las personas encuestadas, consideran que las aplicaciones de la ESPAM MFL se ejecutan de forma segura, mientras tanto que el 33% establece que no.

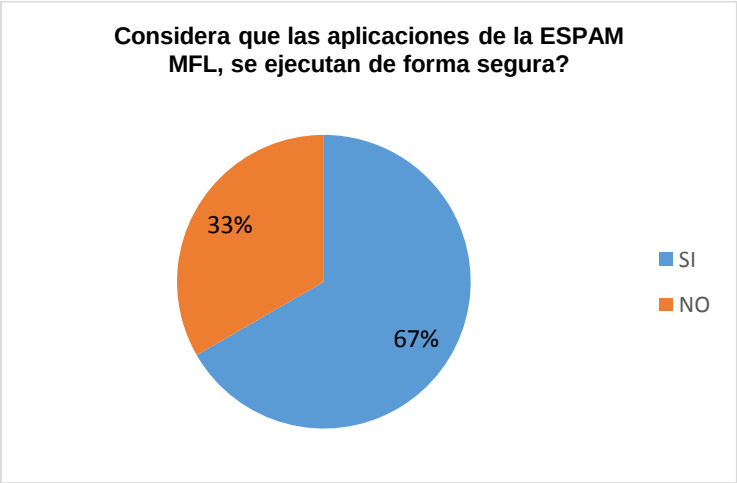



**Gráfico 4. 3.** Resultados de la tercera pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

De acuerdo con el gráfico 4.4 establece que el 92% de los encuesta dicen que si se debe mejorar la seguridad de los servicios que ofrece el data center, por otra parte el 8% de los encuestados consideran que no se debe mejorar.

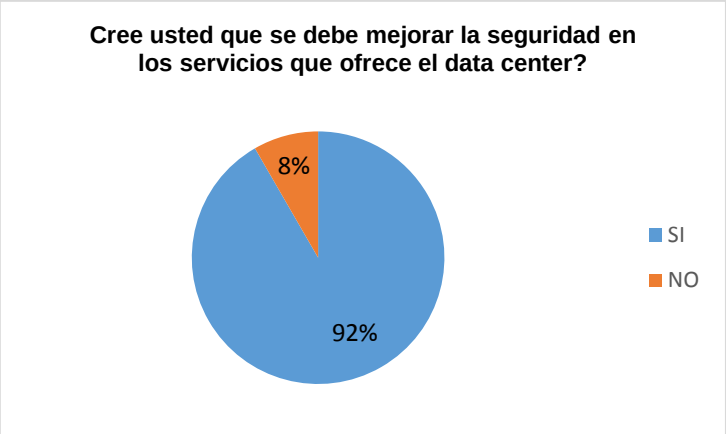



**Gráfico 4. 4.** Resultados de la cuarta pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

Según el gráfico 4.5 demuestra que el 67% de las personas encuestadas han tenido algún problema de seguridad al momento de utilizar los servicios del data center, así mismo el 33% respondió que no ha tenido ningún tipo de inconveniente de seguridad.

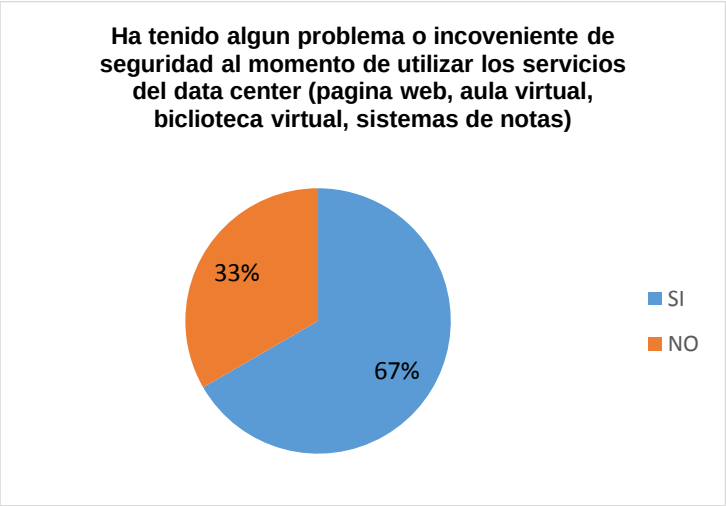



**Gráfico 4. 5.** Resultados de la quinta pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

El gráfico 4.6 demuestra que el 67% de los encuestados conoce acerca de un sistema de seguridad perimetral firewall, por lo tanto el 33% no conoce de este tipo de software.

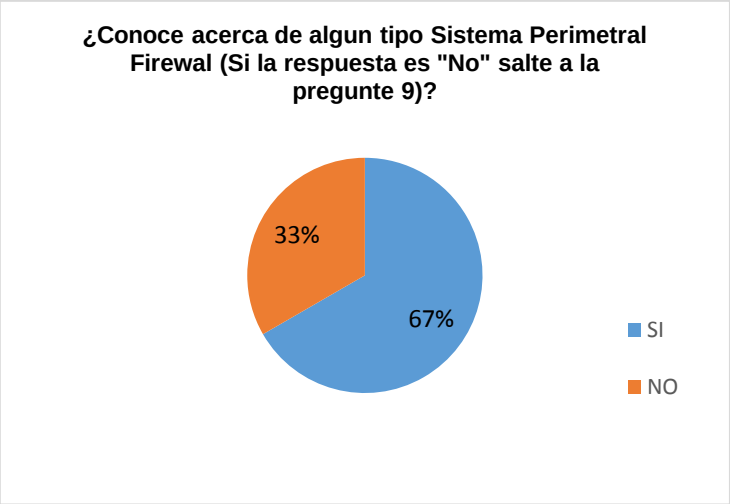



**Gráfico 4. 6.** Resultados de la sexta pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

En el gráfico 4.7 se observa que el 94% de las encuestas aplicadas, respondieron que si es necesario la implementación de un sistema de seguridad perimetral firewall, y sólo un 6% estable que no es necesario.

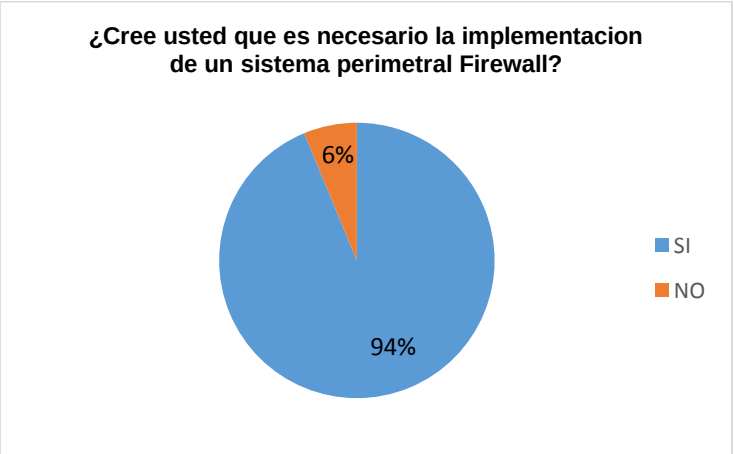



**Gráfico 4. 7.** Resultados de la séptima pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

Así mismo con los resultados del gráfico 4.8 se determinó que el 81% de las personas encuestadas establecen que si se mejorará la seguridad de los datos del data center de la ESPAM MFL, por otra parte un 19% considera que con la implementación de este sistema no mejorará la seguridad de la información.

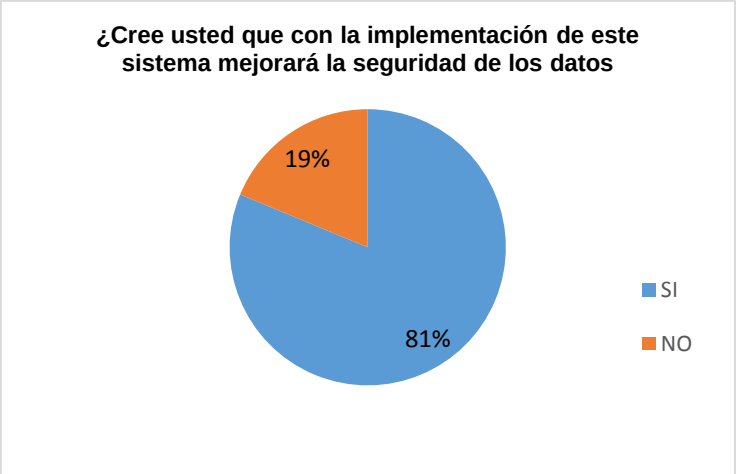



**Gráfico 4. 8.** Resultados de la octava pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

En el gráfico 4.9 se muestra que 75% de los encuestados consideran que las software de código libre son eficientes, mientras que un 25% establece no son eficientes.

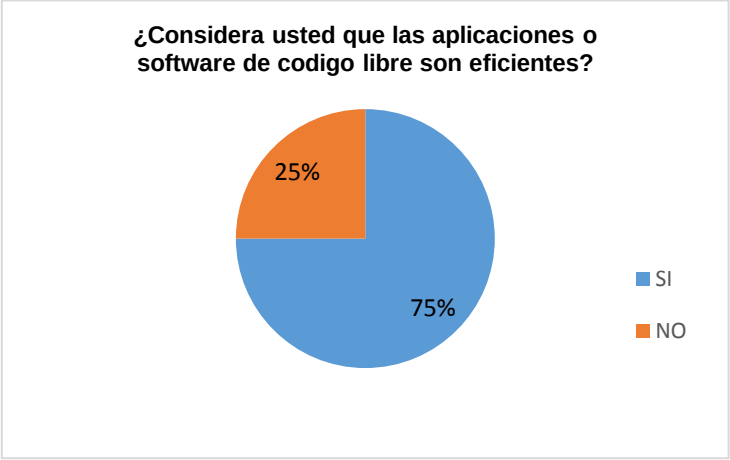



**Gráfico 4. 9.** Resultados de la novena pregunta de encuesta aplicada a docentes, estudiante y personal administrativo.

Luego de realizar la encuesta se escogieron tres servidores firewall los cuales son IpFire, PfSense y Untangle NG Firewall, y se aplicó un estudio comparativo haciendo uso de la herramienta checklist, con la que se pudo obtener resultados de las características negativas y positivas con las que cuenta cada firewall.

En el cuadro 4.1, se muestra los resultados del checklist aplicado para el software IpFire.

**Cuadro 4. 1.** Resultados del checklist aplicado al firewall IpFire.

| **CHECKLIST** | | |
|---|---|---|
| ▪ **IDENTIFICACIÓN DE LA EVALUACIÓN** | | |
| **PROPÓSITO: ESTUDIO DEL SISTEMA IPFIRE** | | |
| **PROYECTO:** **SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.** | **SOFTWARE A EVALUAR** ❒ IpFire | |
| ▪ **AUTORES** | | |
| **NOMBRES:** DELGADO ZAMBRANO PABLO RICARDO y LOOR LOOR LUIS ANTONIO | | |
| **E-MAIL:** ricky020694@hotmail.com; Luis_all25@hotmail.com | **FONO:** | |
| ▪ **CHECKLIST** | **SÍ** | **NO** |
| ¿EL FIREWALL SE INSTALA COMO UN SISTEMA INDPENDIENTE? | X | |
| ¿EL FIREWALL REQUIERE GRAN CANTIDAD DE RECURSOS EN HARDWARE? | | X |
| ¿EL FIREWALL CONFIGURACIÓN PERSONALIZADA? | X | |
| ¿EL FIREWALL CUENTA UN ENTORNO WEB DE ADMINISTRACIÓN? | X | |
| ¿EL FIREWALL PUEDE SER INSTALADO COMO SERVIDOR VIRTUAL? | X | |
| ¿EL FIREWALL ES COMPATIBLE CON EL SISTEMA VMWARE? | X | |
| FILTRADO WEB | X | |
| INTERFAZ GRÁFICA AMIGABLE | X | |
| CONTROL DE INTRUSOS | X | |
| ANTISPAM | X | |
| ANTIVIRUS | X | |
| ANTIPHISHING | | X |
| CONTROL DE USUARIOS | | X |
| PERMITE REALIZAR BALANCEO DE CARGA | | X |
| PERMITE CONFIGURAR 2 CORTAFUEGOS DENTRO DEL MISMO (REDUNDANCIA) | | X |
| TABAL DE ESTADOS DE CONEXIONES ABIERTAS | X | |
| SERVIDOR STREAMING | X | |
| SERVIDOR DHCP | X | |
| SERVIDOR PPPoE | | |
| SERVIDOR VPN | X | |
| SERVIDOR DNS | X | |
| SERVIDOR GRABADOR DE VIDEO | X | |
| SERVIDOR PARA CENTRAL VOIP | X | |
| SERVIDOR PROXY | X | |
| PORTAL CAUTIVO | | X |
| ENRUTAMIENTO ESTÁTICO | | X |
| CACHÉ DE NOMBRES DE NOMINIOS | X | |

De acuerdo al gráfico 4.10, se muestra en porcentaje que el software Ipfire con respecto a las características recopiladas, cuenta con un nivel de eficiencia del 74% de las respuestas corresponde a SI, mientras que el 26% corresponde a respuestas negativas.


**Gráfico 4. 10.** Resultados del checklist aplicado al firewall IpFire.

A continuación se muestran los resultados obtenidos del checklist aplicado al software Pfsense. (Cuadro 4.2).

**Cuadro 4. 2.** Resultados del CheckList aplicado al firewall Pfsense.

| **CHECKLIST** | | |
|---|---|---|
| • **IDENTIFICACIÓN DE LA EVALUACIÓN** | | |
| **PROPÓSITO: ESTUDIO DEL SISTEMA PFSENSE** | | |
| **PROYECTO:** **SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.** | **SOFTWARE A EVALUAR** ❒ PfSense | |
| • **AUTORES** | | |
| **NOMBRES:** DELGADO ZAMBRANO PABLO RICARDO y LOOR LOOR LUIS ANTONIO | | |
| **E-MAIL:** ricky020694@hotmail.com; Luis_all25@hotmail.com | **FONO:** | |
| • **CHECKLIST** | **SÍ** | **NO** |
| ¿EL FIREWALL SE INSTALA COMO UN SISTEMA INDPENDIENTE? | X | |
| ¿EL FIREWALL REQUIERE GRAN CANTIDAD DE RECURSOS EN HARDWARE? | | X |
| ¿EL FIREWALL CONFIGURACIÓN PERSONALIZADA? | X | |
| ¿EL FIREWALL CUENTA UN ENTORNO WEB DE ADMINISTRACIÓN? | X | |
| ¿EL FIREWALL PUEDE SER INSTALADO COMO SERVIDOR VIRTUAL? | X | |
| ¿EL FIREWALL ES COMPATIBLE CON EL SISTEMA VMWARE? | X | |
| FILTRADO WEB | X | |
| INTERFAZ GRÁFICA AMIGABLE | X | |

| | | |
|---|---|---|
| CONTROL DE INTRUSOS | X | |
| ANTISPAM | X | |
| ANTIVIRUS | X | |
| ANTIPHISHING | X | |
| CONTROL DE USUARIOS | X | |
| PERMITE REALIZAR BALANCEO DE CARGA | X | |
| PERMITE CONFIGURAR 2 CORTAFUEGOS DENTRO DEL MISMO (REDUNDANCIA) | X | |
| TABLA DE ESTADOS DE CONEXIONES ABIERTAS | X | |
| SERVIDOR STREAMING | | X |
| SERVIDOR DHCP | X | |
| SERVIDOR PPPoE | X | |
| SERVIDOR VPN | X | |
| SERVIDOR DNS | X | |
| SERVIDOR GRABADOR DE VIDEO | | X |
| SERVIDOR PARA CENTRAL VOIP | X | |
| SERVIDOR PROXY | X | |
| PORTAL CAUTIVO | X | |
| ENRUTAMIENTO ESTÁTICO | X | |
| CACHÉ DE NOMBRES DE NOMINIOS | X | |

Con respecto a el gráfico 4.11 se determina que el software PfSense es una herramienta compleja, debido a que el porcentaje de satisfacción en base a las características de seguridad que maneja es de un 89% de satisfacción con respecto a un 11%, lo que da como resultado que es un software óptimo para cumplir con el objeto de estudio planteado.


**Gráfico 4. 11.** Resultados del checklist aplicado al firewall PfSense.

Así mismo el firewall Untangle demostró tener características con un nivel bajo de seguridad, tal como lo muestra el cuadro 4.3, obteniendo un 52% de respuestas positivas y un 48% de respuestas que negativas. (Gráfico 4.12)

**Cuadro 4. 3.** Resultados del CheckList aplicado al firewall Untangle.

| **CHECKLIST** | | |
|---|---|---|
| • **IDENTIFICACIÓN DE LA EVALUACIÓN** | | |
| **PROPÓSITO: ESTUDIO DEL SISTEMA UNTANGLE** | | |
| **PROYECTO:** **SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.** | **SOFTWARE A EVALUAR** ❒ Untangle | |
| • **AUTORES** | | |
| **NOMBRES:** DELGADO ZAMBRANO PABLO RICARDO y LOOR LOOR LUIS ANTONIO | | |
| **E-MAIL:** ricky020694@hotmail.com; Luis_all25@hotmail.com | **FONO:** | |
| • **CHECKLIST** | **SÍ** | **NO** |
| ¿EL FIREWALL SE INSTALA COMO UN SISTEMA INDPENDIENTE? | X | |
| ¿EL FIREWALL REQUIERE GRAN CANTIDAD DE RECURSOS EN HARDWARE? | | X |
| ¿EL FIREWALL CONFIGURACIÓN PERSONALIZADA? | X | |
| ¿EL FIREWALL CUENTA UN ENTORNO WEB DE ADMINISTRACIÓN? | X | |
| ¿EL FIREWALL PUEDE SER INSTALADO COMO SERVIDOR VIRTUAL? | X | |
| ¿EL FIREWALL ES COMPATIBLE CON EL SISTEMA VMWARE? | X | |
| FILTRADO WEB | X | |
| INTERFAZ GRÁFICA AMIGABLE | X | |
| CONTROL DE INTRUSOS | X | |
| ANTISPAM | X | |
| ANTIVIRUS | X | |
| ANTIPHISHING | X | |
| CONTROL DE USUARIOS | | X |
| PERMITE REALIZAR BALANCEO DE CARGA | | X |
| PERMITE CONFIGURAR 2 CORTAFUEGOS DENTRO DEL MISMO (REDUNDANCIA) | | X |
| TABAL DE ESTADOS DE CONEXIONES ABIERTAS | | X |
| SERVIDOR STREAMING | | X |
| SERVIDOR DHCP | X | |
| SERVIDOR PPPoE | | X |
| SERVIDOR VPN | X | |
| SERVIDOR DNS | X | |
| SERVIDOR GRABADOR DE VIDEO | | X |
| SERVIDOR PARA CENTRAL VOIP | | X |
| SERVIDOR PROXY | | X |
| PORTAL CAUTIVO | | X |
| ENRUTAMIENTO ESTÁTICO | | X |
| CACHÉ DE NOMBRES DE NOMINIOS | | X |


**Gráfico 4. 12**. Resultados del checklist aplicado al firewall Untangle.

En el gráfico 4.13 se muestra los resultados de las características positivas de los tres firewalls analizados, donde el 89% corresponde a PfSense, el segundo lugar pertenece al Ipfire con un 74% y en tercer lugar Untangle con el 52%.

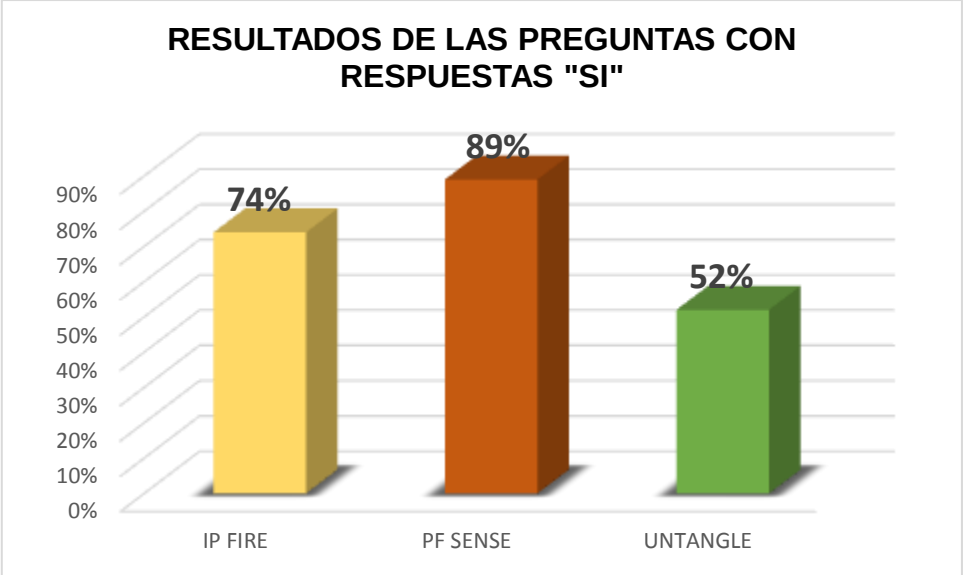



**Gráfico 4. 13.** Resultados de respuestas positivas de los tres servidores firewalls.

Así mismo se obtuvo resultados de las características negativas de cada firewall, que de acuerdo al gráfico 4.14 especifica que el software Untangle obtuvo el 48% de no eficiencia en seguridad, por otra parte Ipfire alcanzó un 26% y por ultimo PfSense demostró que cuenta con un 11% de resultados negativos en relación al nivel de seguridad ofrecido.

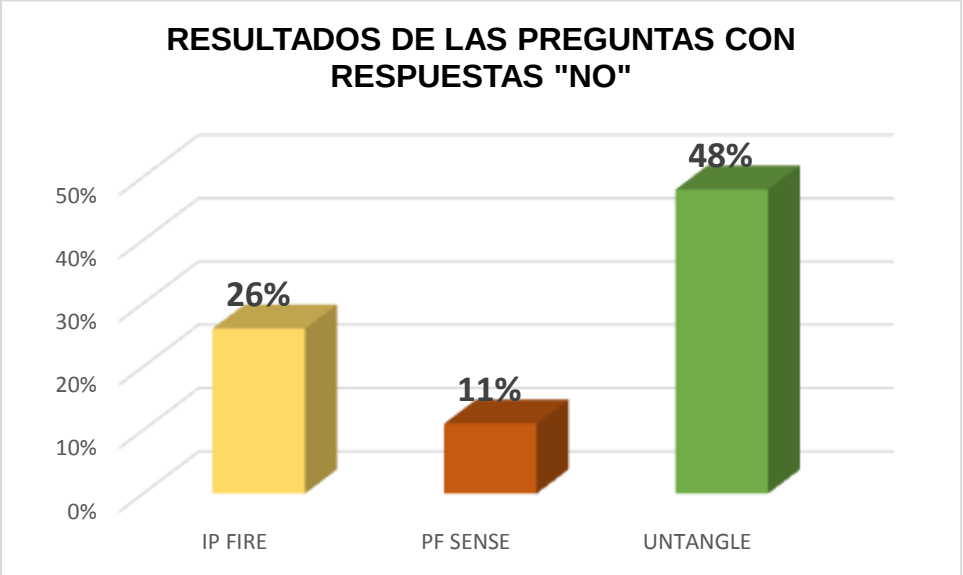



**Gráfico 4. 14.** Resultados de respuestas negativas de los tres servidores firewalls.

Luego del análisis y el estudio comparativo de los firewalls escogidos, se obtuvieron los resultados de las características con las que cuenta cada uno, con lo que se determinó que el software PfSense es un firewall con reconocimiento a nivel mundial, encontrándose en el tercer lugar del ranking de firewalls en el 2015, además posee características más estables de seguridad en relación al software IPfire y Untangle. Por lo tanto es la opción más eficiente para los requisitos del data center de la ESPAM MFL, lo que permitió cumplir con el segundo objetivo planteado en este trabajo.

### 4.1.2. FASE 2

En el anexo 10 se muestra como resultado la máquina física donde se encuentra instalado el firewall Pfsense, de acuerdo con el diseño de funcionamiento del firewall antes establecido, donde indicia que el sistema debe estar instalado entre la interface WAN y LAN, así mismo, contar con un segmento separado el cual corresponde a la interface DMZ para las aplicaciones web de la universidad.

### 4.1.3. FASE 3

Con la puesta en marcha de la fase de implementación de la metodología utilizada, se pudo obtener resultados satisfactorios que permitieron cumplir con el tercer objetivo del presente trabajo, el cual corresponde a la instalación del sistema. En la foto 4.1 se muestra la interface gráfica principal del sistema perimetral firewall, con las características de hardware, interfaces de red y direcciones IP establecidas durante la instalación.

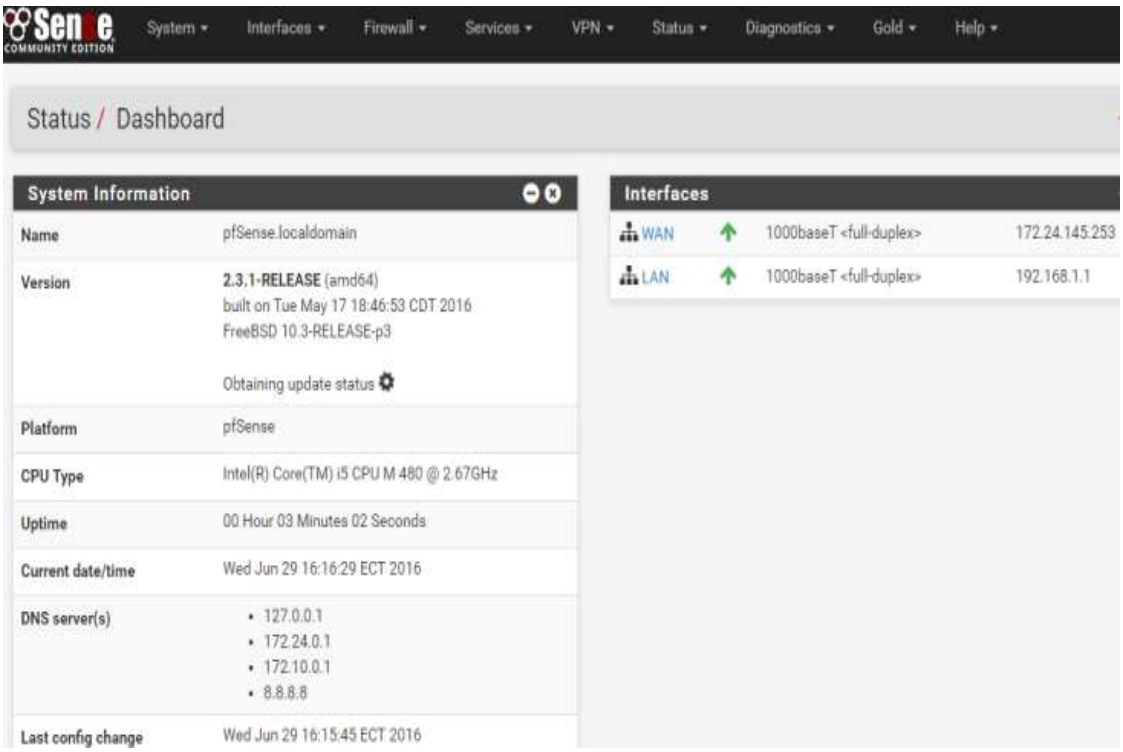



**Foto 4. 1.** Página principal del Pfsence.

### 4.1.4. FASE 4

A continuación, los autores justifican la idea a defender planteada en este proyecto, la misma que está enfocada en que la implementación del sistema perimetral firewall en el data center de la Politécnica de Manabí, permitirá fortalecer la seguridad de la información, debido a que anteriormente no existía este tipo de seguridad y no se podía realizar las actividades que este sistema cumple. Así mismo, al finalizar la fase de integración y validación del sistema se obtuvo los resultados esperados para cumplir con el último objetivo de este trabajo.

De acuerdo con lo antes mencionado, se muestra detalladamente como el firewall permite bloquear accesos inadecuados y llevar un control detallado del tráfico generado en la red de la universidad.

La foto 4.2, muestra como el firewall ha restringido el acceso hacia la red de la universidad a través de ciertos protocolos, por otra parte se demuestra que el sistema da acceso solo a los protocolos y puertos establecidos durante la configuración.

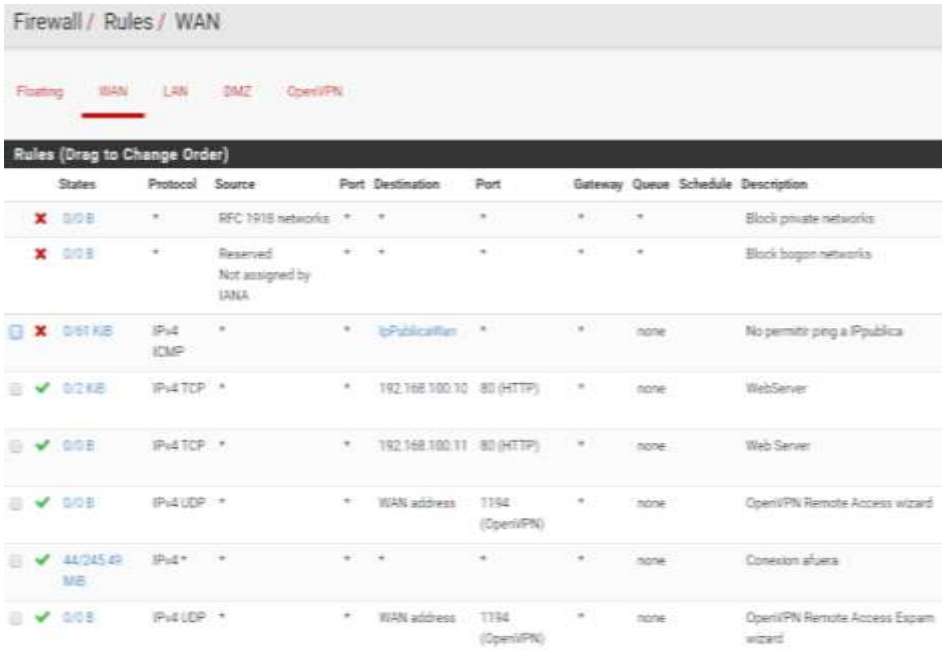



**Foto 4. 2.** Reglas configuradas en la interface WAN.

Además, al estar conectados a la red interna de la universidad e intentar ingresar a unas de las páginas web que fueron bloqueadas durante la configuración, vemos como el sistema firewall deniega el acceso a la misma. (Foto 4.3)

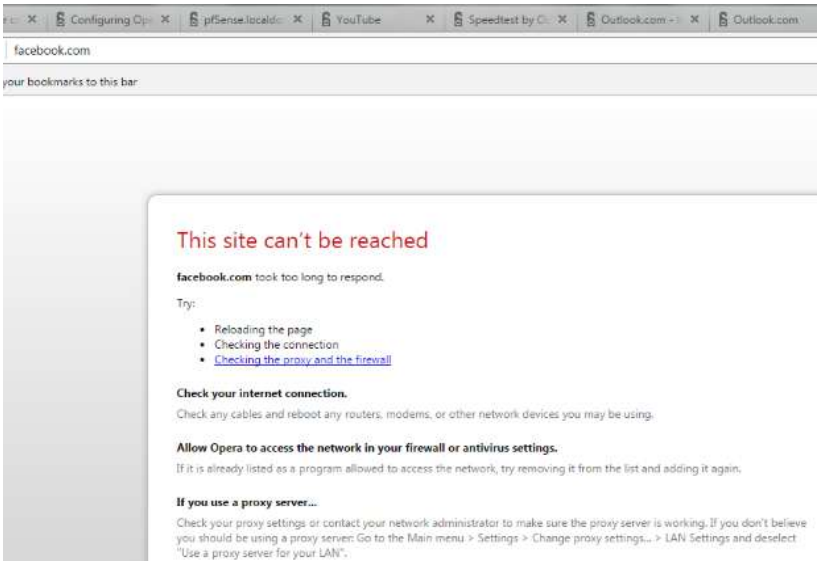



**Foto 4. 3.** Comprobación de bloqueo de páginas web

En la siguiente foto 4.4 se observa como las reglas agregadas en la interface DMZ, no permiten establecer comunicación con la red interna de la universidad, es decir, que si usuario conectado a internet fuera de la red de la ESPAM y quiere acceder a la interface LAN por medio de la zona desmilitarizada, el firewall automáticamente bloquea la conexión, dando mayor seguridad a la red interna en caso de intentos de robo o plagio de información.

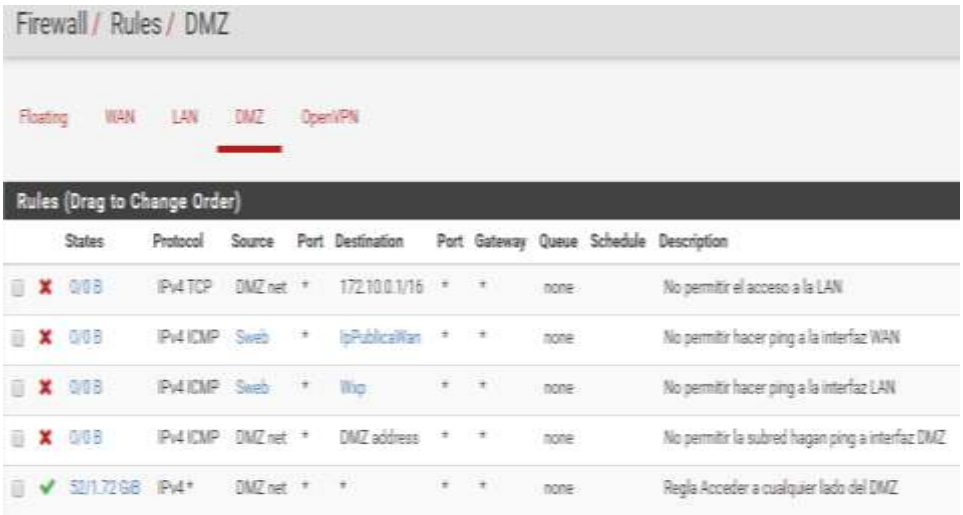



**Foto 4. 4.** Reglas configuradas en la interface DMZ.

A continuación se muestra como el firewall por medio del protocolo ICMP, bloquea las conexiones que se quieran establecer a la red de la univerdad a través del comando ping. (Foto 4.5)

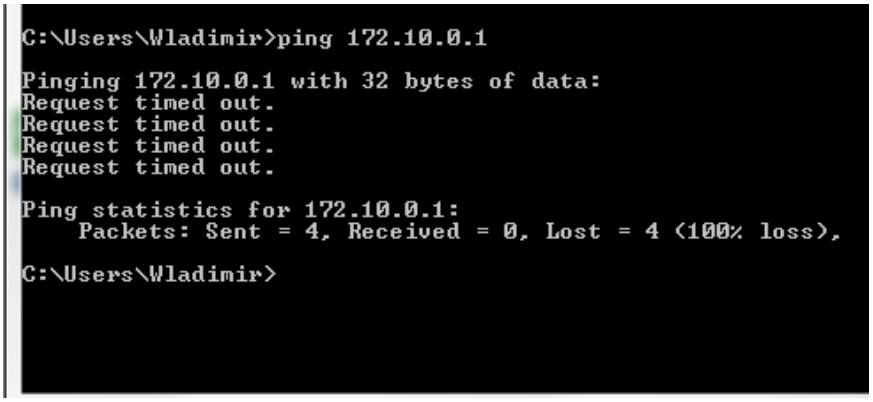
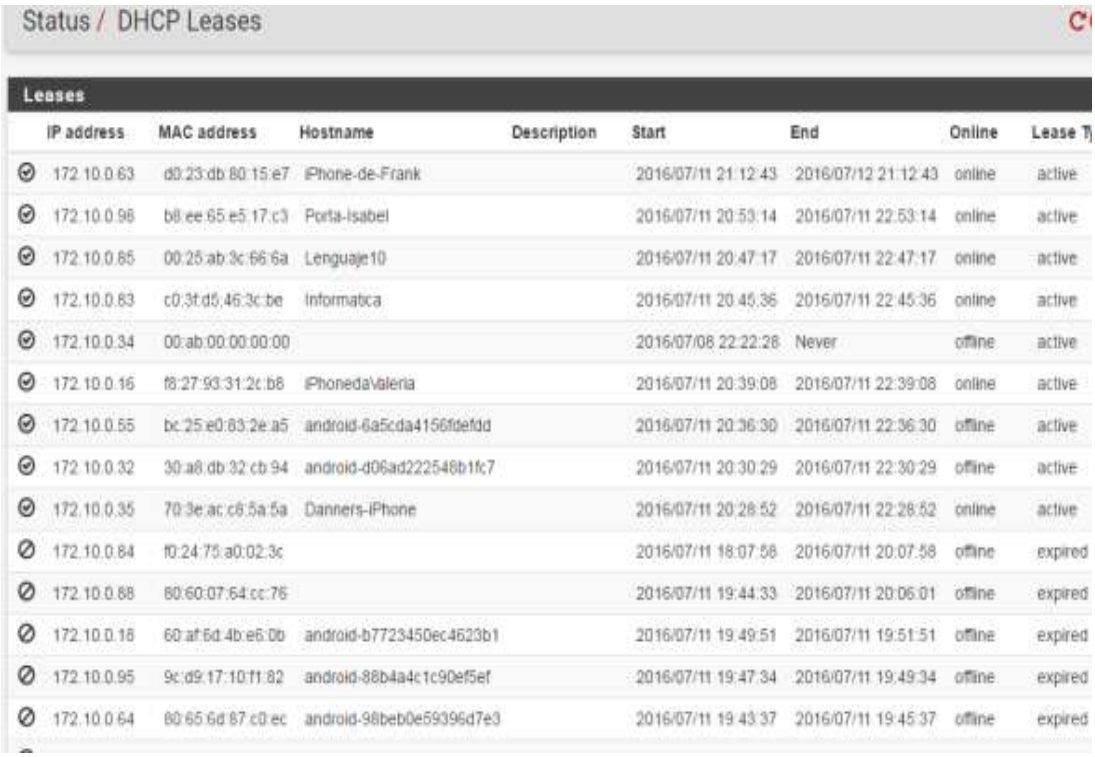



**Foto 4. 5.** Bloqueo del comando ping con el protocolo ICMP.

A continuación se observa como el firewall controla y genera reportes de las conexiones que se realizan a la red de la universidad, lo que permite al administrado del Data Center controlar y contar un registro detallado de los accesos que tiene la red. (Foto 4.6)


Status / DHCP Leases

Leases

| IP address | MAC address | Hostname | Description | Start | End | Online | Lease T |
|---|---|---|---|---|---|---|---|
| 172.10.0.63 | d0:23:db:80:15:e7 | iPhone-de-Frank | | 2016/07/11 21:12:43 | 2016/07/12 21:12:43 | online | active |
| 172.10.0.98 | b8:ee:65:e5:17:c3 | Porta-Isabel | | 2016/07/11 20:53:14 | 2016/07/11 22:53:14 | online | active |
| 172.10.0.85 | 00:25:ab:3c:66:6a | Lenguaje10 | | 2016/07/11 20:47:17 | 2016/07/11 22:47:17 | online | active |
| 172.10.0.83 | c0:3f:d5:46:3c:be | Informatica | | 2016/07/11 20:45:36 | 2016/07/11 22:45:36 | online | active |
| 172.10.0.34 | 00:ab:00:00:00:00 | | | 2016/07/08 22:22:28 | Never | offline | active |
| 172.10.0.16 | f8:27:93:31:2c:b8 | iPhoneda\Valeria | | 2016/07/11 20:39:08 | 2016/07/11 22:39:08 | online | active |
| 172.10.0.55 | bc:25:e0:83:2e:a5 | android-6a5cda4156fdefdd | | 2016/07/11 20:36:30 | 2016/07/11 22:36:30 | offline | active |
| 172.10.0.32 | 30:a8:db:32:cb:94 | android-d06ad222546b1fc7 | | 2016/07/11 20:30:29 | 2016/07/11 22:30:29 | offline | active |
| 172.10.0.35 | 70:3e:ac:c6:5a:5a | Danners-iPhone | | 2016/07/11 20:28:52 | 2016/07/11 22:28:52 | online | active |
| 172.10.0.84 | f0:24:75:a0:02:3c | | | 2016/07/11 18:07:58 | 2016/07/11 20:07:58 | offline | expired |
| 172.10.0.88 | 80:60:07:64:cc:76 | | | 2016/07/11 19:44:33 | 2016/07/11 20:06:01 | offline | expired |
| 172.10.0.16 | 60:af:6d:4b:e6:0b | android-b7723450ec4623b1 | | 2016/07/11 19:49:51 | 2016/07/11 19:51:51 | offline | expired |
| 172.10.0.95 | 9c:d9:17:10:f1:82 | android-88b4a4c1c90ef5ef | | 2016/07/11 19:47:34 | 2016/07/11 19:49:34 | offline | expired |
| 172.10.0.64 | 80:65:6d:87:c0:ec | android-98beb0e59396d7e3 | | 2016/07/11 19:43:37 | 2016/07/11 19:45:37 | offline | expired |

**Foto 4. 6.** Reporte de usuarios que han accedido a la red.

En la siguiente foto 4.7, se observa como el firewall Pfsense crea una lista de reportes con los accesos que se ha tenido a través del servicio OpenVPN al servidor firewall.

**Last 50 OpenVPN Log Entries. (Maximum 50)**

| Time | Process | PID | Message |
|---|---|---|---|
| Jul 14 11:41:21 | openvpn | 8493 | antonio/181.113.178.118:65237 MULTI_sva: pool returned IPv4=192.168.10.2, IPv6=(Not enabled) |
| Jul 14 11:41:23 | openvpn | 8493 | antonio/181.113.178.118:65237 send_push_reply(): safe_cap=940 |
| Jul 14 12:41:28 | openvpn | | user 'antonio' authenticated |
| Jul 14 13:37:32 | openvpn | 8493 | antonio/181.113.178.118:65237 [antonio] Inactivity timeout (--ping-restart), restarting |
| Jul 14 13:38:31 | openvpn | | user 'antonio' authenticated |
| Jul 14 13:38:37 | openvpn | 8493 | 181.112.1.190:49157 [antonio] Peer Connection Initiated with [AF_INET]181.112.1.190:49157 |
| Jul 14 13:38:37 | openvpn | 8493 | antonio/181.112.1.190:49157 MULTI_sva: pool returned IPv4=192.168.10.2, IPv6=(Not enabled) |
| Jul 14 13:38:38 | openvpn | 8493 | antonio/181.112.1.190:49157 send_push_reply(): safe_cap=940 |
| Jul 14 13:42:23 | openvpn | 8493 | antonio/181.112.1.190:49157 [antonio] Inactivity timeout (--ping-restart), restarting |
| Jul 14 14:20:48 | openvpn | | user 'antonio' authenticated |
| Jul 14 14:20:48 | openvpn | 8493 | 181.113.178.118:64180 [antonio] Peer Connection Initiated with [AF_INET]181.113.178.118:64180 |

**Foto 4. 7.** Reporte de accesos remotos al servidor firewall.

Posteriormente se muestran de todos los estados de conexión activos en el servidor firewall pfsense, con su protocolo, información de IP e información de estado, además en la dirección IP muestra la conexión de origen y de destino donde se obtuvo la comunicación, paquetes y cantidad de paquetes. Cada conexión a través del servidor tendrá dos estados, uno que entra en el servidor y uno que sale del cortafuego. (Foto 4.8)

**States**

| Interface | Protocol | Source -> Router -> Destination | State | Packets | Bytes |
|---|---|---|---|---|---|
| LAN | tcp | 77.234.42.23:80 <- 172.10.0.65:49234 | ESTABLISHED:ESTABLISHED | 206 / 463 | 16 KiB / 561 KiB |
| WAN | tcp | 181.196.143.16:44202 (172.10.0.65:49234) -> 77.234.42.23:80 | ESTABLISHED:ESTABLISHED | 206 / 463 | 16 KiB / 561 KiB |
| LAN | tcp | 64.233.177.188:5228 <- 172.10.0.83:46152 | ESTABLISHED:ESTABLISHED | 34 / 29 | 5 KiB / 3 KiB |
| WAN | tcp | 181.196.143.16:20026 (172.10.0.83:46152) -> 64.233.177.188:5228 | ESTABLISHED:ESTABLISHED | 34 / 29 | 5 KiB / 3 KiB |
| LAN | tcp | 64.233.177.188:5228 <- 172.10.0.11:33897 | ESTABLISHED:ESTABLISHED | 8 / 9 | 2 KiB / 1 KiB |

**Foto 4. 8.** Estados de conexión activos en el servidor firewall.

En esta parte se describe la información sobre el filtrado de paquetes que ha realizado el firewall PfSense en la red de la universidad, donde se revelan estadísticas de la interfaces, con número de paquetes que han ingresado y salido de la red, bloqueos, estadísticas de la tabla de estado, configuración de los límites de velocidad, estado de reglas y contadores de bytes. (Foto 4.9)

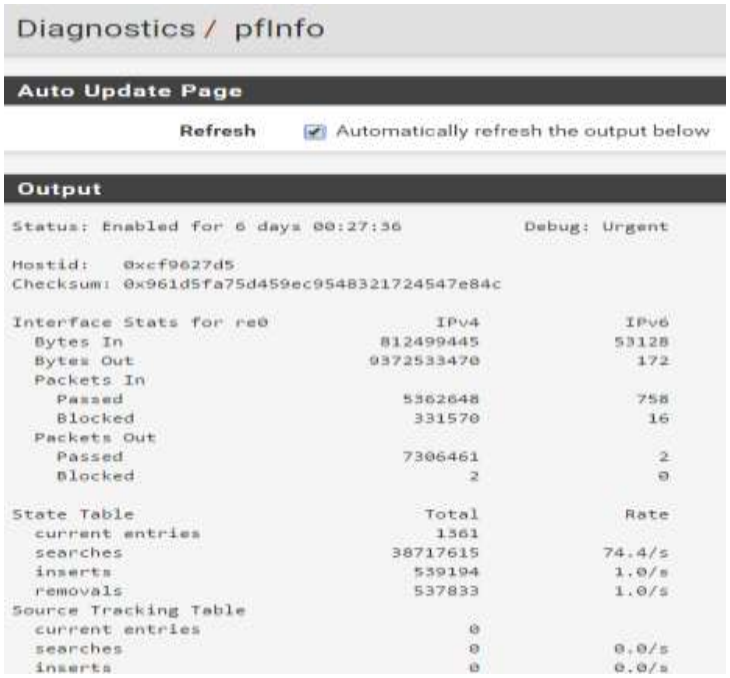



**Foto 4. 9.** Reporte de filtrado de paquetes.

Por otra parte, se muestra una lista de bloqueos de direcciones ip con sus respectivos puertos que han intentado acceder de manera inadecuada a través de las interfaces de red, mostrando el protocolo, fecha, hora, fuente y destino. (Foto 4.10)

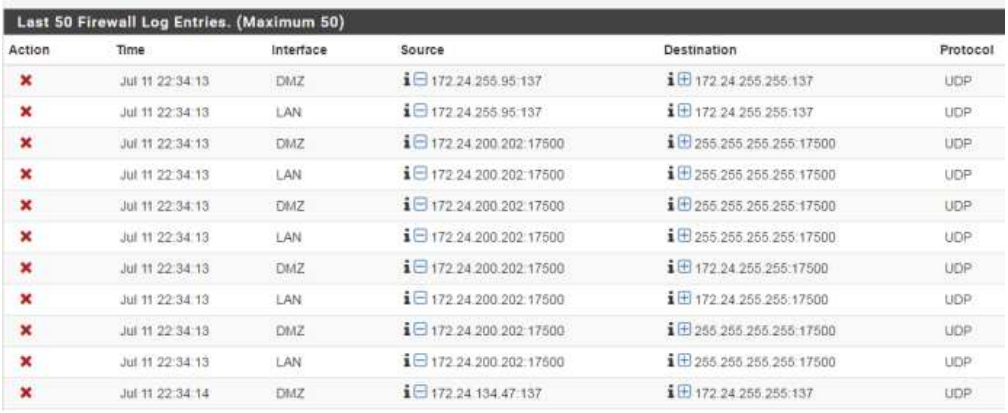
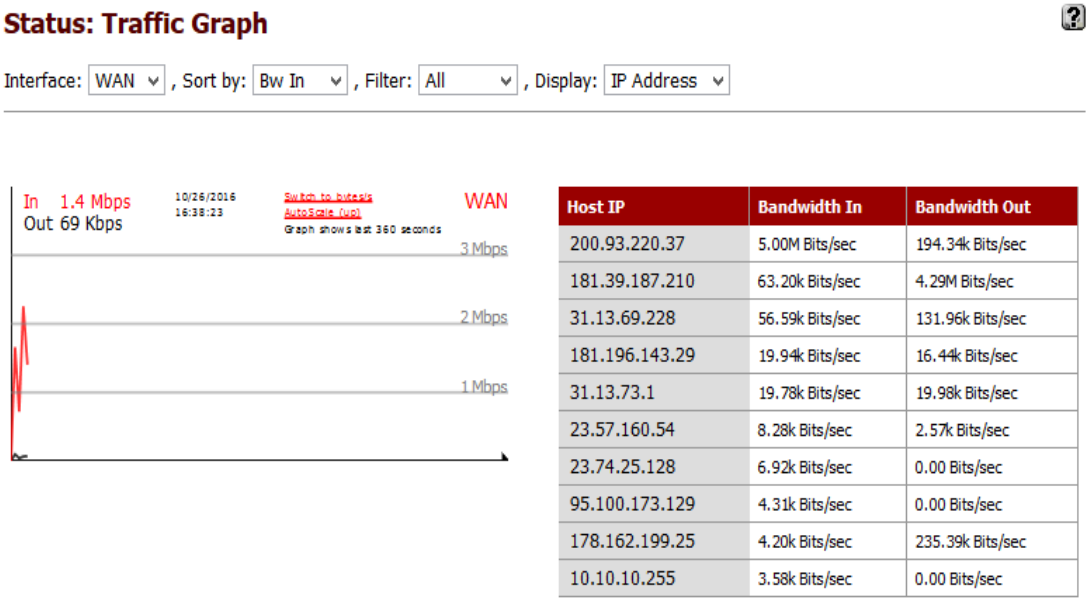



**Foto 4. 10.** Lista de direcciones ip bloqueadas por el servidor firewall.

También Pfsense permite mostrar en tiempo real los estados del tráfico de una interface, el mismo que incluye información tales como la dirección IP, velocidad de descarga y de subida que utiliza la petición realizada. (Foto 11)




| Host IP | Bandwidth In | Bandwidth Out |
|---|---|---|
| 200.93.220.37 | 5.00M Bits/sec | 194.34k Bits/sec |
| 181.39.187.210 | 63.20k Bits/sec | 4.29M Bits/sec |
| 31.13.69.228 | 56.59k Bits/sec | 131.96k Bits/sec |
| 181.196.143.29 | 19.94k Bits/sec | 16.44k Bits/sec |
| 31.13.73.1 | 19.78k Bits/sec | 19.98k Bits/sec |
| 23.57.160.54 | 8.28k Bits/sec | 2.57k Bits/sec |
| 23.74.25.128 | 6.92k Bits/sec | 0.00 Bits/sec |
| 95.100.173.129 | 4.31k Bits/sec | 0.00 Bits/sec |
| 178.162.199.25 | 4.20k Bits/sec | 235.39k Bits/sec |
| 10.10.10.255 | 3.58k Bits/sec | 0.00 Bits/sec |

**Foto 4. 11.** Tráfico generado en la interface WAN.

Además el firewall permite llevar un control del tráfico generado en la red por intervalos de tiempo. En este caso se lo realizó en un intervalo de 8 horas, mostrando el ancho de banda utilizado, de entrada (in-pass) y de salida (out - pass), ancho de banda de las peticiones bloqueadas y el total de ancho de banda utilizado. Lo que facilita al administrador del sistema, tener un diagnóstico de las conexiones que se realizan a la red de la universidad. (Foto 12)

.

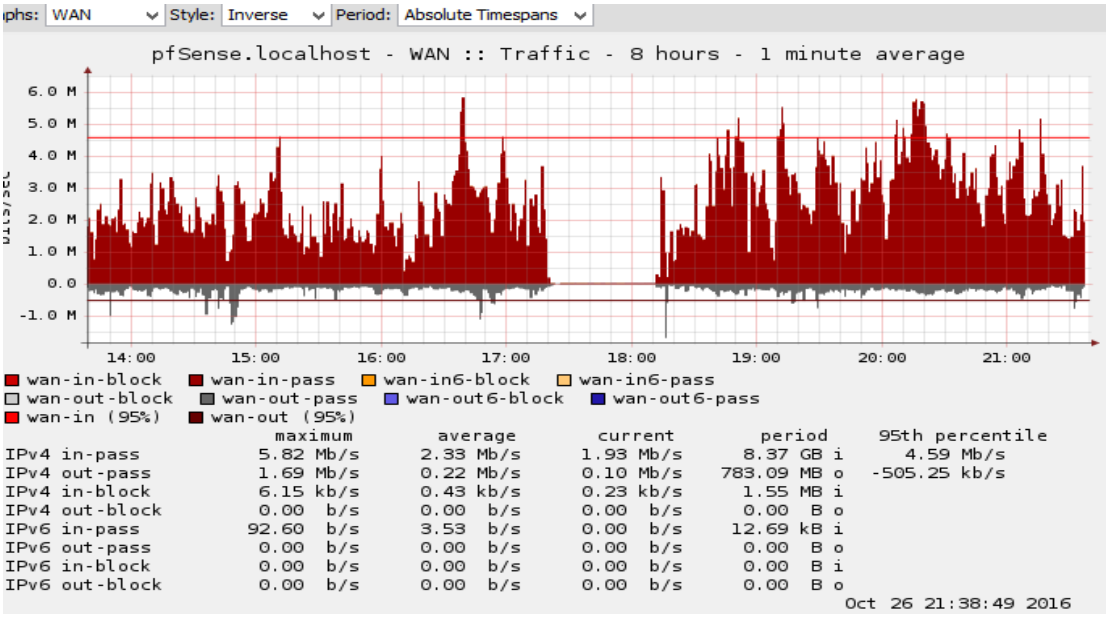



**Foto 4. 12.** Tráfico generado en la interface WAN en un intervalo de 8 horas.

De la misma forma el sistema puede mostrar el tráfico generado durante una semana y mensual, permitiendo tener un registro del porcentaje de conexiones a la red de la universidad y el ancho de banda utilizado. (Foto 4.13)

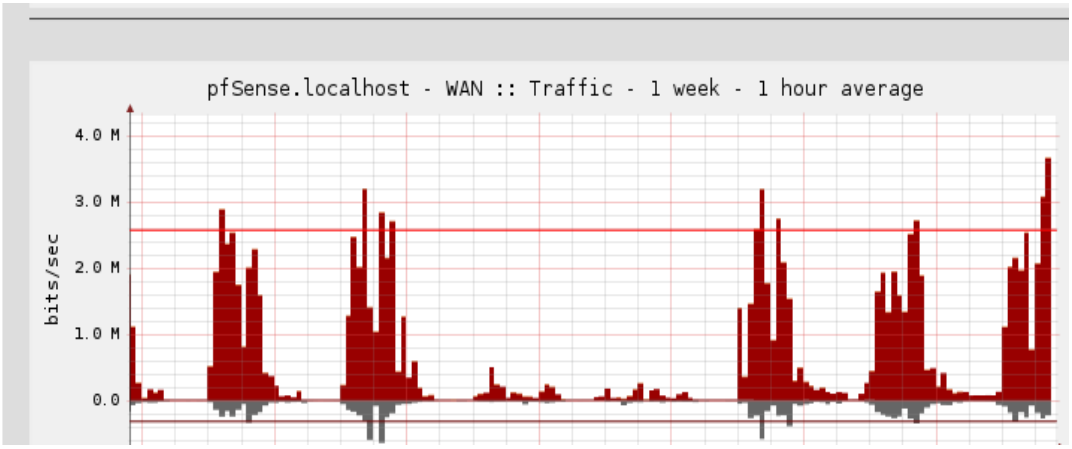



**Foto 4. 13.** Tráfico generado en la red en un período de una semana.

En la siguiente foto 4.14, se muestra un registro de tráfico de red generado en el periodo de un mes, de conexiones de la universidad y el ancho de banda utilizado.

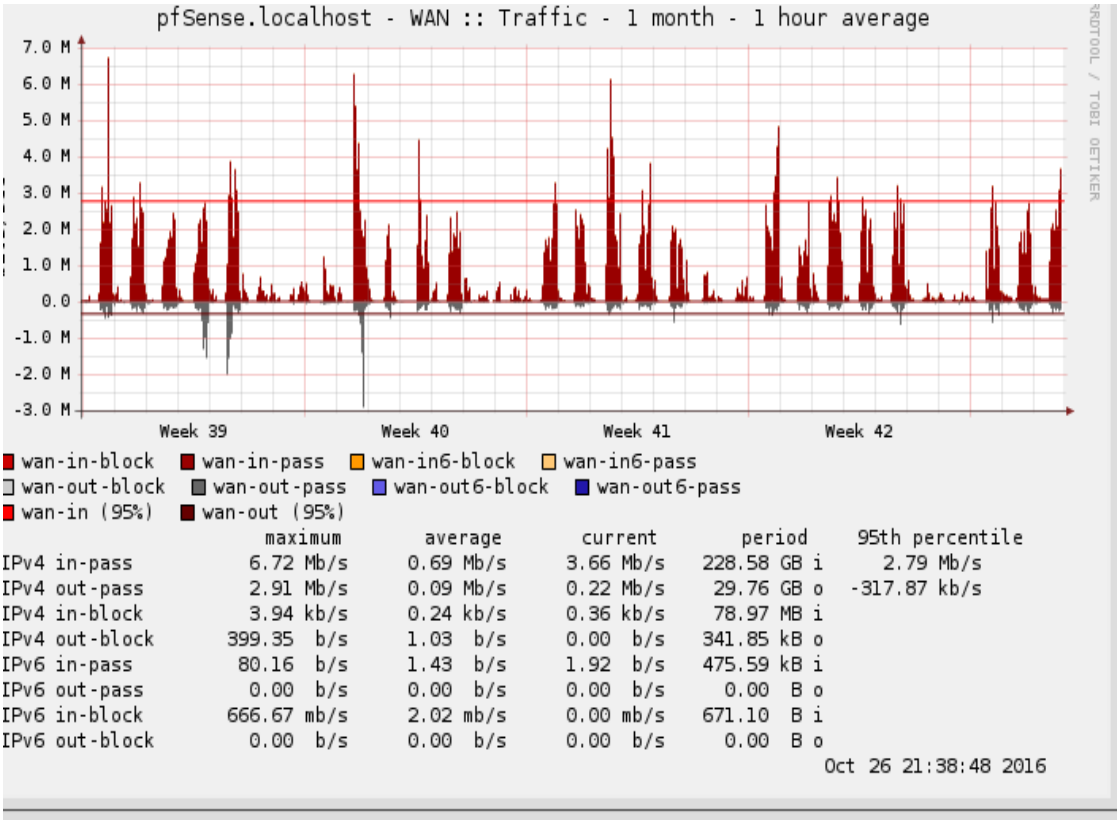



**Foto 4. 14.** Tráfico generado en la red en un período de un mes.

### 4.1.5. FASE 5

De acuerdo con los resultados de la fase de mantenimiento, en el **Anexo 17** se puede observar el manual de usuario del sistema perimetral firewall, el mismo que consta de los pasos detallados de la instalación y configuración que fue aplicada en este trabajo. Con esto se logró contar una guía para la persona encargada en dicho momento del manejo del firewall.

## 4.2. DISCUSIÓN

Con los resultados obtenidos durante el proceso de realización de este trabajo, se evidenció que la red de la ESPAM MFL no contaba con un servidor firewall para la protección de la información y para los sistemas que maneja dicho departamento, lo que implicaba que no se podía tener un control, bloqueo y monitoreo adecuado de infiltraciones informáticas a la red de la universidad.

Partiendo del contexto anterior, Gutiérrez (2014) define que la seguridad de una red informática, es el conjunto de herramientas y normas de seguridad para la protección de los equipos activos dentro de la misma. Por lo tanto la plataforma: “Pfsense” es un sistema de seguridad que restringe, separa y analiza todo el tráfico generado en la red.

Por otra parte se hace énfasis a los servidores firewall a nivel de hardware, que según lo establecido por Fabuel (2013), son dispositivos electrónicos externos que se colocan entre la computadora o red y el modem que da acceso a Internet, y su objetivo es controlar las comunicaciones y conexiones con el exterior, tanto entrantes como salientes. Los firewalls por hardware proporcionan una línea de defensa adicional contra ataques procedentes del exterior, por ser dispositivos separados que controlan sus propios sistemas operativos, así que proporcionan una línea adicional de defensa contra ataques, pero su mayor inconveniente es su precio.

Por lo consiguiente, se realizó un análisis del trabajo de Padilla (2012), el cual define la importancia de un servidor firewall en una red local. Por otra parte establece que el modelo de seguridad del servidor firewall Zentyal se basa en brindar una mayor seguridad mediante la configuración predeterminada, y que cuando este sistema actúa como cortafuegos, normalmente se instala entre la red interna y el router conectado a Internet para ofrecer un monitoreo total de la red.

De acuerdo con el argumento anterior, la implementación de un servidor firewall de código libre permitió fortalecer la seguridad de la información. Además facilita el monitoreo, generación de reportes, gestionar y filtrar la totalidad del tráfico entrante y saliente entre la red interna de la ESPAM MFL y la internet.

Es por esto, que los autores de este trabajo establecen que el firewall de código libre “Pfsense”, ofrece un gran nivel de administración y seguridad, convirtiéndolo en la propuesta optima respecto al monitoreo y control de tráfico de una red en particular.

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONESP

- Con el levantamiento de información se determinó que el Data Center de la ESPAM MFL no contaba con la seguridad adecuada para la cantidad de información que se gestiona en este departamento, conjuntamente con la inexistencia de un sistema de seguridad perimetral firewall, no se llevaba un control y monitoreo apropiado del tráfico generado en la red, lo cual se reflejaba en una mayor vulnerabilidad de la información.

- Luego de realizar un análisis de requerimientos informáticos para mejorar la seguridad de la información y de comparar 3 posibles alternativas de software para uso en el Data Center, se determinó que PfSense es el indicado, teniendo en cuenta que pertenece a la línea de software libre, se encuentra entre los primeros 3 mejores programas de seguridad a nivel mundial y es compatible con el hardware de la institución, manejando niveles óptimos de seguridad.

- Con la instalación del firewall PfSense, implementado sobre la plataforma de virtualización VMWARE, se obtuvo como resultado que dichos sistemas son compatibles y que cumple con la misma funcionalidad que un firewall de nivel físico. Además la ventaja de tener servidores virtualizados optimiza la utilización de recursos de hardware.

- Una vez realizadas todas las pruebas correspondientes del servidor firewall PfSense, se verificó que dicho sistema realiza un escaneo global de la red interna de la universidad, además da la facilidad de llevar un control y generar reportes sobre las peticiones de los usuarios. Por lo tanto permite al administrador del data center de la ESPAM MFL conocer detalladamente todo el tráfico generado en la red.

## 5.2. RECOMENDACIONES

- Los procesos de seguridad que se manejan en el Data Center, deben contar con planes de contingencia que estén en constante actualización para mejorar la fiabilidad de la información, debido al eminente crecimiento de ataques informáticos, creación de nuevas vulnerabilidades y robo de información.

- Realizar actualizaciones periódicas del sistema Pfsense, con la finalidad de mantener niveles altos de protección y desempeño.

- Es imprescindible aplicar técnicas de ataques informáticos de acuerdo con la versión del sistema firewall, con el propósito de obtener nuevos métodos de defensa para la seguridad de la información.

- Capacitar periódicamente a los encargados del Data Center, en temas de seguridad informática, con el objetivo de mantener niveles óptimos de protección

# BIBLIOGRAFÍA


ANER (División Sistemas). 2015. Definición de Servidor. (En línea). Consultado, 16 de Nov. 2015. Formato HTML. Disponible en http://www.anerdata.com/que-es-un-servidor.html

Baldeón, M y Coronel, C. 2012. Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002. Sangolquí-Pichincha, EC. ESPE.

Balseca, L; Romero, C; Sáenz, F. 2013. Estado del arte en la detección de intrusiones en Redes 802.1. Sangolquí-Pichincha, EC. ESPE.

Barrios, J. 2013. Configuración De Servidores Con GNU/Linux. (En línea). Consultado, 16 de nov. 2015. Formato HTML. Disponible en http://www.etnassoft.com/biblioteca/configuracion-de-servidores-con-gnulinux/

Benítez, M. 2013. Políticas de la seguridad informática. (En línea). Consultado, 16 de nov. 2015. Formato PDF. Disponible en http://www.gestionintegral.com.co/wpcontent/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf

Celis, C y Andrade, C. 2013. Diseño e implementación de un sistema de seguridad perimetral para una empresa usando la herramienta pfsense. (En línea). Consultado, 09 de Jul. 2015. Formato PDF. Disponible en https://seguridadinformaticaufps.wikispaces.com/file/view/PFSENSE.pdf

Cervigón, A y Ramos, M. 2011. Seguridad Informática. 1 ed. Madrid. p 200.

Cervantes, O y Gómez, M. 2013. Taxonomía de los modelos y metodologías de desarrollo de software más utilizado. Cuajimalpa, MX. Unión de Universidades de América Latina y el Caribe Distrito Federal, Organismo Internacional. p 37 - 47.

Correa, J. S.f. Manual de políticas y estándares en seguridad informática. (En línea). Consultado, 16 de nov. 2015. Formato PDF. Disponible en http://www.intenalco.edu.co/MP_V01.pdf

Díaz, R; Pérez, Y; Proenza, Y. 2014. Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Santiago-Holguín, Cu. Ciencias Holguín. Vol. 2. p 1-14.

Fabuel, C. 2013. Implantación de un sistema de seguridad perimetral. Tesis. Ing. Técnica de Telecomunicación. UPM. Madrid. ES. p 227.

Fuertes, W; Rodas, F; Toscano, D. 2011. Evaluación de ataques UDP Flood utilizando escenarios virtuales como plataforma experimental. Tunja, CO. Universidad Pedagógica y Tecnológica de Colombia Vol. 20. p 37-53.

Gómez, R. 2010. Administración de servidores Linux. (En línea). Consultado, 21 de mayo de 2015. Formato PDF. Disponible en https://www.informatica.us.es/~ramon/articulos/AdminLinuxUbuntuFedora.pdf

Grajales, B. 2011. Análisis de tráfico para la red de datos de las instituciones educativas del núcleo 5 de la ciudad de Pereira. (En línea). Consultado, 16 de nov. 2015. Formato PDF. Disponible en http://recursosbiblioteca.utp.edu.co/dspace/bitstream/11059/4700/1/6213821G743.pdf

Gutiérrez, G. 2014. Optimización de la seguridad de la red de datos del Ibunam bajo Pfsense. Tesis. Ing. Informática. Universidad Nacional Autónoma de México. MX. p 375.

López, A. 2010. Diseño de un prototipo que permita evaluar la viabilidad de un firewall en redes scada. (En línea). Consultado, 14 de may. 2015. Formato PDF. Disponible en http://www.konradlorenz.edu.co/images/stories/articulos/PROTOTITPO_FIREWALL_REDES_SCADA.pdf

López, L. 2012. Data Center Diseño Sostenible. (En línea). Consultado, 15 de May. 2015. Formato PDF. Disponible en https://www.bicsi.org/uploadedFiles/BICSI_Website/Global_Community/Presentations/Andean/DIA%201%20CONF%202%20HUBBELL.pdf

Lugo, N. 2014. Tecnologías de virtualización en los sistemas informáticos de las organizaciones empresariales del Estado Zulia. Zulia, VEN. Telématique. Vol. 13. P 49-67.

Portantier, F. 2013. Gestión de la Seguridad Informática. 1 ed. Argentina. p 192.

Padilla, H. 2012. Investigación, análisis e implementación de un servidor de virtualización dedicado, para integrar un servidor de correo zimbra virtualizado con un servidor multitarea zentyal físico como controlador de dominio, firewall y proxy utilizando herramientas como tecnologías de software libre. Tesis. Ing. Sistemas. Universidad Politécnica Salesiana. Quito-Pichincha, EC. p 250.

Reinoso, D. 2012. Control y protección de datos virtuales en Ecuador. (En línea). Consultado, 14 de dic. 2015. Formato HTML. Disponible en http://www.falconipuig.com/cyberlex/control-y-proteccion-de-datos-virtuales-en-ecuador/

Rouse, M. 2014. Máquina Virtual. (En línea). Consultado, 16 de nov. 2015. Formato HTML. Disponible en http://searchdatacenter.techtarget.com/es/definicion/Copy-of-virtual-machine-VM

Sierra, M. 2013. Que es un servidor y principales tipos de servidores. (En línea). Consultado, 15 de May. 2015. Formato PDF. Disponible en http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57:herramientas-informaticas&Itemid=179

Soto, J. 2014. IP Fire-Un firewall de código abierto. (En línea). Consultado, 09 de Jul. 2015. Formato HTML. Disponible en http://blog.capacityacademy.com/2013/12/03/ipfire-firewall-open-source/

Tirado, E. 2012. Sistema de seguridad perimetral, instalación y configuración de Endian firewall. (En línea). Consultado, 16 de Nov. 2015. Formato PDF. Disponible en https://seguridadinformaticaufps.wikispaces.com/file/view/seguridad+perimetral+con+Endian+Firewall.pdf

Untangle. 2015. Untangle NG firewall. (En línea). Consultado, 12 de Jul. 2015. Formato HTML. Disponible en https://www.untangle.com/untangle-ng-firewall

UTTT (Universidad Tecnológica de Tula – Tepeji). S.f. Seguridad Informática. (En línea). Consultado, 14 de may. 2015. Formato PDF. Disponible en http://www.uttt.edu.mx/noticiastecnologicas/pdfs/abril_20-04-2012.pdf

Vásquez, F y Gabalán, J. 2012. La administración de la información como potenciadora de la gestión del proceso investigativo en una institución de educación superior. Medellín, CO. Revista Interamericana de Bibliotecología. Vol. 35. P313-326.

Vega, O y Núñez, S. 2012. Influencia del volumen de tráfico sobre túnel VPN IPSEC/UDP en enlaces WAN. Zulia, VEN. Telématique. Vol. 11. p 84-98.

Vegas, G. 2011. Untangle (En línea). Consultado, 14 de Jul de 2015. Formato PDF. Disponible en https://gabrielvegas.wordpress.com/2010/05/24/untangle/

Velázquez, J. 2013. Desarrollo en Cascada (Waterfall) VS Desarrollo Agile-SCRUM. (En línea). Consultado, 10 de feb. 2017. Formato PDF. Disponible en http://www.northware.mx/wp-content/uploads/2013/04/Desarrollo-cascada-vs-Desarrollo-Agile.pdf

Villegas, M; Meza, M; León, P. 2011. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática. Zulia, VEN. Telématique. Vol. 10. p 1-16.

VMWARE. 2015. Definición de Máquina virtual. (En línea). Consultado, 16 de nov. 2015. Formato HTML. Disponible en http://www.vmware.com/latam/virtualization/how-it-works

Voutssas, J. 2010. Preservación documental digital y seguridad informática. México Distrito Federal, MX. Revista Científica Scielo. Vol. 24.

Yustas, J. S.f. Que es un cortajuegos (firewall) para Internet. (En línea). Consultado, 14 de may. 2015. Formato PDF. Disponible en http://www.acta.es/medios/articulos/internet/010095.pdf

Zambrano, R. 2014. Data Center más que alojamiento. Chile. Revista América TIC. 3 ed. p 3 - 5.

# ANEXOS

# ANEXO 1
# CUESTIORARIO APLICADO AL ADMINISTRADOR DEL DATA CENTER, ACERCA DE LA SEGURIDAD QUE MANEJA EL CENTRO DE DATOS

## CUESTIONARIO PARA EL ADMNISTRADOR DEL DATA CENTER

1) EXISTEN DOCUMENTOS DE POLÍTICAS DE SEGURIDAD?
   SI ✓
   NO___

2) QUE NIVELES DE SEGURIDAD SE MANEJAN EN EL DATA CENTER?
   De acceso Físico
   De acceso lógico
   De autenticación

3) QUE TIPOS DE SEGURIDAD SE MANEJAN EN EL DATA CENTER?
   Estan establecida en la política de Data Center.

4) QUE TIPOS DE SISTEMAS SE USAN PARA LA SEGURIDAD?
   Sistemas VMWARE
   Data Protection, Hakiro, Vadmin, etc

5) EXISTEN UN MECANISMO DE SEGURIDAD EN EL DATA CENTER?
   SI

6) QUE TIPOS DE SERVIDORES UTILIZAN PARA AQUELLA SEGURIDAD?
   Se utilizan Sistemas cyuron de Redes de capa 3: Router.

7) EXISTEN TERCERAS PERSONAS QUE MENEJEN LA SEGUIRDAD DEL DATA CENTER?
   No.

# ANEXO 2
# CUESTIONARIO APLICADO AL ADMINISTRADOR DEL DATA CENTER, ACERCA DE LOS EQUIPOS QUE SE UTILIZAN EN EL MISMO.

## CUESTIONARIO PARA EL ADMNISTRADOR DEL DATA CENTER

1. **Existe actualmente un Sistema de FIREWALL en el Data Center de la ESPAM MFL?**

   SI ___
   NO ✓

2. **En caso afirmativo que tipo de firewall se encuentra implementado.**

   ---

3. **Cuáles son las principales aplicaciones o programas que se ejecutan a través del Data Center**

   Servidores de Base de Datos, Aplicaciones, Internet, Repositorios, etc.

4. **Cree que es necesario la implementación de un sistema firewall?**

   Si ✓
   No ___

5. **Cuales seria la función principal para implementar o actualizar el sistema firewall?**

   Mantener una mejor Seguridad perimetral para los Servidores

6. **Cuáles son las características de hardware y software actuales del data center?**

   Servidor Blade C3000, con 2 storage HP P2000

7. **Sería compatible con los sistemas actuales de la ESPAM MFL, la implementación de un Firewall sobre código abierto?**

   Si, el Firewall es independiente de los Servidores Sistemas Operativos etc.

8. **Que requerimientos mínimos serían necesarios que cumpliera el sistema perimetral?**

   Un Servidor con 6 GB RAM 2 Core en Procesador, 600 GB HD

9. **En qué aspectos considera que mejoraría la prestación de servicios ofrecidos por el data center con la implementación de un sistema perimetral firewall?**

   Seguridad y Confiabilidad

10. **Con los equipos (Hw, SW) con los que cuenta el Data Center, se podría implementar adecuadamente un sistema perimetral Firewall, o considera necesaria la adquisición de nuevas herramientas para dicho fin.**

    Podría ser, solo se tendría que analizar la Topología.

11. **Como administrador del DATA CENTER que sugerencias brindaría para la implementación satisfactoria del Firewall.**

    Establecer política clara de Seguridad al momento de realizar el Nat.

12. **Que tipos y marcas de servidores existen.**

    BLADE C3000, P2000
    HP. DELL.

## ANEXO 3
## FICHA DE OBSERVACIÓN APLICADA EN EL DATA CENTER DE LA ESPAM MFL.

# FICHA DE OBSERVACIÓN

- **INSTRUCCIONES**

Lea detenidamente y seleccione la(s) respuesta(s) que correspondan

- **OBJETIVO**

Conocer los tipos de sistemas que se manejan el Data Center y Establecer los niveles de seguridad del sistema perimetral firewall.

1. **Se utilizan servidores locales o virtuales.**
   Local X virtual ✓
2. **Que marcas de servidores utilizan en el Data Center de la ESPAM MFL.**
   DELL X HP X IBM ___ otros X
   COMPAQ ___ LG ___ LENOVO ___
3. **Qué tipo de procesadores utilizan los servidores.**
   ATOM ___ CELERON ___ PENTIUM ___
   CORE ___ XEON X
4. **Cuál es la capacidad de memoria RAM que tienen los servidores.**
   30 GB
5. **Cuál es la capacidad de almacenamiento de los Discos Duros.**
   Storas Arreglos de Discos
6. **Que proveedor de Internet tienen contratado en la ESPAM MFL.**
   PUNTONET CNT NETLIFE
   TELCONET IPLANET TELECOM
7. **Que ancho de banda manejan en los servidores?**
   100 mb dedicado de subida y bajada
8. **Que cantidad de usuarios tiene acceso diario al Data Center?**
   255 al dia (Informatica 3000 mil (Universidad
9. **Los equipos del Data Center se encuentran en condiciones climáticas óptimas.**
   SI X NO ___
10. **La ESPAM-MFL cuenta con un canal dedicado de acceso a internet.**
    SI X NO ___
11. **Qué tipo de sistemas operativos utilizan los servidores del Data Center.**
    LINUX X UNIX ___ WINDOWS X APPLE ___ OTROS ___
12. **Qué nivel de seguridad considera que tiene el Data Center.**
    ALTO ___ MEDIO X ALTO ___
13. **Cuentan con un sistema perimetral firewall.**
    SI ___ NO X
14. **Cree que sería satisfactorio implementar un sistema perimetral Firewall.**
    SI X NO ___
15. **El cuarto donde esta ubicado el Data Center es el adecuado?**
    SI X NO ___

# ANEXO 4
# ENCUESTA APLICADA A DOCENTES Y PERSONAL ADMINISTRATIVO DE LA ESPAM MFL.

## ENCUESTA PARA EL PERSONAL ADMINISTRATIVO Y DOCENTE DE LA ESPAM-MFL

**El objetivo de la siguiente encuesta es conocer el nivel de seguridad que tiene el Data Center de la ESPAM-MFL y obtener información para la implantación de un Sistema Perimetral Firewall.**

**Un firewall (Cortafuegos) es un sistema informático que permite bloquear accesos no autorizadas a una red de equipos computacionales y mejorar la seguridad de la información.**

1. **Con que frecuencia accede a los servicios del DataCenter (Centros de Datos) de la ESPAM-MFL.**
   Diariamente X
   Día por medio ___
   Una vez por semana ___
   Mensualmente ___
   Nunca accede ___

2. **Considera que las aplicaciones de la ESPAM MFL (página web, aula virtual, etc.) se ejecutan de manera rápida?**
   Si ___
   No X

3. **Considera que las aplicaciones de la ESPAM MFL (página web, aula virtual, etc.) se ejecutan de forma Segura?**
   Si ___
   No X

4. **Cree usted que se debe mejorar la seguridad de los servicios que ofrece el DataCenter de la ESPAM?**
   Si X
   No ___

5. **Ha tenido algún problema o inconveniente de seguridad al momento de utilizar los servicios del DataCenter (página web, aula virtual, etc.).**
   Si X
   No ___

6. **Conoce acerca de algún tipo Sistema Perimetral Firewall (SI - salte 7, 8, NO salte a la 9)**
   Si X
   No ___

7. **Cree Ud. que es necesario la implementación de un sistema perimetral Firewall?**
   Si X
   No ___

8. **Cree Ud. que con la implementación del Sistema Firewall mejorará la seguridad de los datos?**
   Si X
   No ___

9. **Considera usted que las aplicaciones basadas en código libre son eficientes?**
   Si X

## ANEXO 5
## ENCUESTA APLICADA A ESTUDIANTES DE LA ESPAM MFL.

# ENCUESTA PARA ESTUDIANTES DE LA ESPAM MFL

**El objetivo de la siguiente encuesta es conocer el nivel de seguridad que tiene el Data Center de la ESPAM-MFL y obtener información para la implantación de un Sistema Perimetral Firewall.**

**Un firewall (Cortafuegos) es un sistema informático que permite bloquear accesos no autorizadas a una red de equipos computacionales y mejorar la seguridad de la información.**

1. **Con que frecuencia accede a los servicios del DataCenter (Centros de Datos) de la ESPAM-MFL.**
   Diariamente ___ Día por medio ____
   Una vez por semana ___ Mensualmente ____
   Nunca accede ____

2. **Considera que las aplicaciones de la ESPAM MFL (página web, aula virtual, etc.) se ejecutan de manera rápida?**
   Si ___
   No ___

3. **Considera que las aplicaciones de la ESPAM MFL (página web, aula virtual, etc.) se ejecutan de forma Segura?**
   Si ___
   No ___

4. **Cree usted que se debe mejorar la seguridad de los servicios que ofrece el DataCenter de la ESPAM?**
   Si ___
   No___

5. **Ha tenido algún problema o inconveniente de seguridad al momento de utilizar los servicios del DataCenter (página web, aula virtual, etc.).**
   Si ___
   No ___

6. **Conoce acerca de algún tipo Sistema Perimetral Firewall (SI - salte 7, 8, NO salte a la 9)**
   Si ___
   No ___

7. **Cree Ud. que es necesario la implementación de un sistema perimetral Firewall?**
   Si ___
   No ___

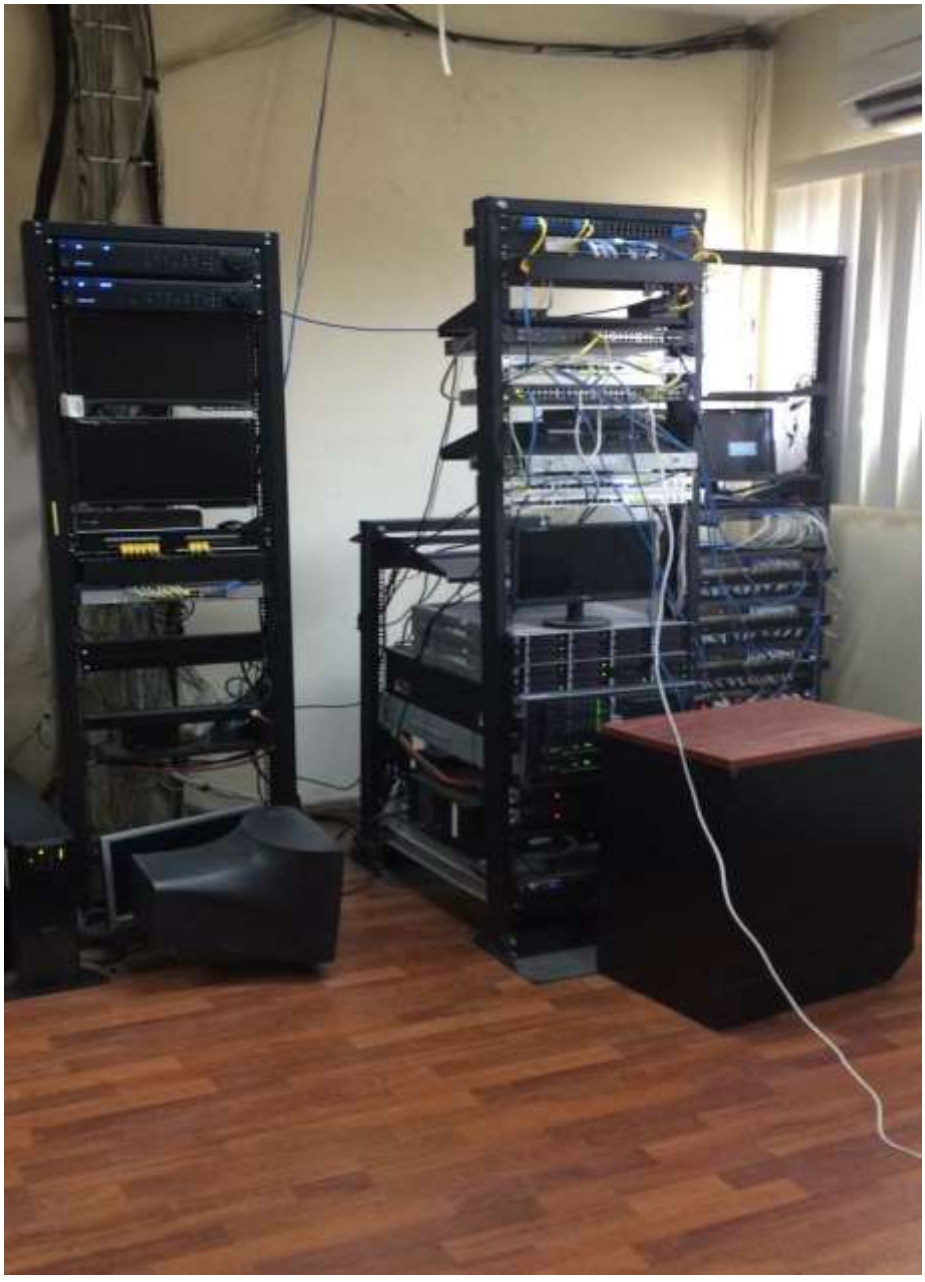
8. **Cree Ud. que con la implementación del Sistema Firewall mejorará la seguridad de los datos?**
   Si ___
   No ___

9. **Considera usted que las aplicaciones basadas en código libre son eficientes?**
   Si ___
   No ___

# ANEXO 6
# CHECKLIST APLICADO PARA REALIZAR EL ESTUDIO COMPARATIVO DE LOS FIREWALS IPFIRE, PFSENSE Y UNTANGLE.

| CHECKLIST | | | |
|---|---|---|---|
| **1. IDENTIFICACIÓN DE LA EVALUACIÓN** | | | |
| **PROPÓSITO: ESTUDIO COMPARATIVO DE LOS SISTEMAS FIREWALLS IPFIRE, PFSENSE Y UNTANGLE** | | | |
| **PROYECTO:** SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL. | **SOFTWARE A EVALUAR** ☐ IpFire ☐ PfSense ☐ Untangle | | |
| **2. AUTORES** | | | |
| **NOMBRES:** DELGADO ZAMBRANO PABLO RICARDO , LOOR LOOR LUIS ANTONIO | | | |
| **E-MAIL:** ricky020694@hotmail.com; luis_all25@hotmail.com | **FONO:** | | |
| **3. CHECKLIST** | | **SI** | **NO** |
| ¿EL FIREWALL SE INSTALA COMO UN SISTEMA INDPENDIENTE? | | | |
| ¿EL FIREWALL REQUIERE GRAN CANTIDAD DE RECURSOS EN HARDWARE? | | | |
| ¿EL FIREWALL CONFIGURACIÓN PERSONALIZADA? | | | |
| ¿EL FIREWALL CUENTA UN ENTORNO WEB DE ADMINISTRACIÓN? | | | |
| ¿EL FIREWALL PUEDE SER INSTALADO COMO SERVIDOR VIRTUAL? | | | |
| ¿EL FIREWALL ES COMPATIBLE CON EL SISTEMA VMWARE? | | | |
| FILTRADO WEB | | | |
| INTERFAZ GRÁFICA AMIGABLE | | | |
| CONTROL DE INTRUSOS | | | |
| ANTISPAM | | | |
| ANTIVIRUS | | | |
| ANTIPHISHING | | | |
| CONTROL DE USUARIOS | | | |
| PERMITE REALIZAR BALANCEO DE CARGA | | | |
| PERMITE CONFIGURAR 2 CORTAFUEGOS DENTRO DEL MISMO (REDUNDANCIA) | | | |
| TABAL DE ESTADOS DE CONEXIONES ABIERTAS | | | |
| SERVIDOR STREAMING | | | |
| SERVIDOR DHCP | | | |
| SERVIDOR PPPoE | | | |
| SERVIDOR VPN | | | |
| SERVIDOR DNS | | | |
| SERVIDOR GRABADOR DE VIDEO | | | |
| SERVIDOR PARA CENTRAL VOIP | | | |
| SERVIDOR PROXY | | | |
| PORTAL CAUTIVO | | | |
| ENRUTAMIENTO ESTÁTICO | | | |
| CACHÉ DE NOMBRES DE NOMINIOS | | | |

## ANEXO 7
## EQUIPOS CON LOS QUE CUENTA EL DATA CENTER DE LA ESPAM MFL.



**ANEXO 8**
**AUTORES DEL TRABAJO INSTALANDO LOS COMPONENTES FÍSICOS DEL SERVIDOR FIREWALL EN EL DATA CENTER DE LA ESPAM MFL.**

# ANEXO 9
# AUTORES DEL TRABAJO CONFIGURANDO EL SERVIDOR FIREWALL EN EL DATA CENTER DE LA ESPAM MFL.

**ANEXO 10**
**MÁQUINA DONDE SE ECUENTRA FUNCIONANDO EL SERVIDOR FIREWALL.**

## ANEXO 11
## DATA CENTER DE LA ESPAMMFL, CON CLIMATIZACIÓN ADECUADA, CON ACCESO DE PERSONAL AUTORIZADO, LIBRE DE HUMEDAD Y DE AGENTES NOCIVOS.

## ANEXO 12
## AVAL DE CULMINACIÓN DE INSTALACIÓN Y CONFIGURACIÓN DEL FIREWALL, FIRMADO POR EL ADMINISTRADOR DEL DATA CENTER.

**Oficio No: 009-CAMZ-DC-CUT**
**Calceta 06 de Julio del 2016**

**Ing.**
Ricardo Chica Cepeda
**TUTOR DE TESIS**
**En su Despacho.**

De mi consideración:

El presente es para informarle que el Sr. Luis Antonio Loor Loor con cedula de ciudadanía 1314291269, y el Sr. Pablo Ricardo Delgado Zambrano con cedula de ciudadanía 1315708931, realizaron la instalación y configuración de un servidor firewall para el DMZ del Data Center de la ESPAM MFL, como proyecto de titulación denominado: SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL.

Es todo lo que puedo certificar en honor a la verdad.

Por la presente me suscribo de usted.

Atentamente,

**Ing. Cesar Moreira Zambrano. MSC.**
**ADMINISTRADOR DATA CENTER ESPAM MFL**
**E-mail**: cmoreira@espam.edu.ec
**Tele: 0969659578**

**C. c** Archivo

12-07-2016

## ANEXO 13
## AVAL ENVIADO POR PARTE DEL TUTOR DE TESIS AL PRESIDENTE DEL TRIBUNAL DE APLICACIONES INFORMÁTICAS.

ESPAMMFL

ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FELIX LÓPEZ

Calceta, 25 de Agosto 2016

**Ingeniero**
Luis Cedeño Valarezo
**PRESIDENTE DEL TRIBUNAL DE SOLUCIONES DE SOFTWARE**
En su despacho.-

De mi consideración

Me dirijo a usted deseándole el mayor de los éxitos en cada una de sus labores diarias, de igual forma me permito comunicarle que el grupo conformado por los estudiantes **Delgado Zambrano Pablo Ricardo** y **Loor Loor Luis Antonio,** de la Carrera de Computación, cuya tesis de pregrado se titula: ***"SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL"***, ha finalizado con los objetivos propuestos de forma satisfactoria.

Para los fines pertinentes, me suscribo de usted.

Atentamente,

**Ing. Ricardo Chica Cepeda, MBA.**
**Docente - Tutor**

Recibido!
25-08-16
17:37

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

Calceta, 8 de noviembre 2016

**Ingeniero**
Luis Cedeño Valarezo
**PRESIDENTE DEL TRIBUNAL DE APLICACIONES INFORMÁTICAS**
En su despacho.-

De mi consideración

Me dirijo a usted deseándole el mayor de los éxitos en cada una de sus labores diarias, de igual forma me permito comunicarle que el grupo conformado por los estudiantes **Delgado Zambrano Pablo Ricardo** y **Loor Loor Luis Antonio,** de la Carrera de Computación, cuya tesis de pregrado se titula: ***"SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL"***, ha incorporando las observaciones efectuadas oportunamente, finalizando con los objetivos propuestos de forma satisfactoria.

Para los fines pertinentes, suscribo de usted.

Atentamente,

08/11/2016
19H08

**Lcdo. Pabelco Y. Zambrano Moreira, MGTR.**
**Docente - Tutor**

## ANEXO 14
## AVAL ENVIADO POR PARTE DELTRIBUNAL DE TESIS AL TUTOR DE TESIS DE HABERSE REALIZADO LA PRE DEFENSA

ESPAMMFL

***ESCUELA SUPERIOR POLITECNICA AGROPECUARIA DE MANABI***

Carrera de COMPUTACIÓN

Calceta, 30 de enero de 2016

Lic. Pabelco Zambrano Moreira.
TUTOR DE TESIS

Ciudad.-

De nuestra consideración.

Por medio de la presente quienes conformamos el tribunal especializado de tesis de la línea de investigación Aplicaciones Informáticas de la Carrera de Computación, tenemos a bien indicar que luego de haber realizado la pre defensa de la tesis "SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL" de los postulantes: Delgado Zambrano Pablo Ricardo y Loor Loor Luis Antonio, manifiestan que la tesis antes mencionada se encuentra habilitada para continuar con los tramites de sustentación.

Particular que comunico a usted para los fines pertinentes.

Atentamente:

CC. Postulante de Tesis

Ing. Luis Cedeño Valarezo Mgs.
**PRESIDENTE DEL TRIBUNAL**

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABI MANUEL FÉLIX LÓPEZ
TRIBUNAL DE APLICACIONES DE SOFTWARE

## ANEXO 15
## AVAL ENVIADO POR PARTE DE LOS AUTORES AL PRESIDENTE DEL TRIBUNAL DE APLICACIONES INFORMÁTICAS

ESPAMMFL

**ESCUELA SUPERIOR POLITECNICA AGROPECUARIA DE MAN[illegible]**
**Carrera de Computación**
***TRIBUNAL DE TESIS***

Carrera de COMPUTACIÓN

Calceta, 24 de abril del 2017

Señores

Pablo Ricardo Delgado Zambrano y Luis Antonio Loor Loor

POSTULANTES

De nuestras consideraciones:

Los miembros del Tribunal, después de revisar las correcciones al Artículo Científico cuyo tema es: **"SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD EN EL DATA CENTER DE LA ESPAM MFL"**, presentando por ustedes, les informamos que luego de haber comprobado su cumplimiento y realizado los correctivos del caso, en la sesión correspondiente, se determinó que ha sido aprobada por la unanimidad en su contenido y forma, de acuerdo al Art. 2 del reglamento de tesis y la viabilidad técnica y económica.

Atentamente:

Ing. Luis Cedeño Valarezo
**PRESIDENTE DEL TRIBUNAL**

Lic. José Intriago Cedeño
**MIEMBRO DEL TRIBUNAL**

Ing. Hirania Santana Cedeño
**SECRETARIO DEL TRIBUNAL**

**ANEXO 16**
**AVAL ENVIADO POR PARTE DE LA DIRECCION DE REVISTA ESPAMCIENCIA**

REPÚBLICA DEL ECUADOR

ESPAM MFL
ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

VICERRECTORADO ACADÉMICO

COORDINACIÓN GENERAL DE INVESTIGACIÓN

DIRECCIÓN DE REVISTA ESPAMCIENCIA

Calceta, 15 de mayo de 2017
No 035-C.RE-17

# CERTIFICACIÓN

Por medio del presente tengo a bien certificar que los Sres. Luis Antonio Loor Loor, con cédula de identidad 131429126-9 y Pablo Ricardo Delgado Zambrano, con cédula de identidad 131570893-1 postulantes de la carrera de Computación han presentado en el correo electrónico de la Revista ESPAMCIENCIA el artículo científico **"SISTEMA PERIMETRAL FIREWALL Y FORTALECIMIENTO DE LA SEGURIDAD DEL DATA CENTER DE LA ESPAM MFL"**, de acuerdo a normativa institucional.

Particular que informo para los fines legales pertinentes.

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
DIRECCIÓN DE REVISTA ESPAM MFL

Ing. Ángel Guzmán Cedeño, Ph.D.
**DIRECTOR**

# ANEXO 17
# MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL FIREWALL PFSENSE