



**INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE  
TECNOLOGÍA**

**PROYECTO DE GRADO A LA OBTENCIÓN DEL TÍTULO DE  
TECNOLOGÍA EN ANÁLISIS DE SISTEMAS**

**TEMA:**

IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL ADMINISTRADO  
POR EL SOFTWARE PFSENSE COMMUNITY EDITION PARA LA  
SEGURIDAD INFORMÁTICA DEL HOTEL CONTINENTAL DE LA  
CIUDAD DE GUAYAQUIL EN EL 2019.

**AUTOR:**

JAVIER MESIAS GUIRACOCCHA CUADRA

**TUTOR**

PHD. TAPIA BASTIDAS TATIANA YEOBANKA

**GUAYAQUIL, ECUADOR**

**2019**

## **DEDICATORIA**

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darnos fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí.

A mis hermanas (os) por estar siempre presentes, acompañándome y por el apoyo moral, que me brindaron a lo largo de esta etapa de mi vida.

A todas las personas que nos han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

Y por último y no menos importante: A mi Esposa Katherine y a mis hijos Michael y Mathías, esto es por ustedes.

**Javier Mesías Guiracocha Cuadra**

## **AGRADECIMIENTO**

Agradezco a Dios por bendecirme en mi vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mis padres: Jesús e Isabel; a mi esposa Katherine; mis hijos: Michael y Mathías por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

Agradezco al Instituto Tecnológico Bolivariano de Tecnología por la aceptación y curso de mi carrera, a mis distinguidos docentes por haber compartido sus conocimientos a lo largo de la preparación de mi profesión, de manera especial, a la PhD. Tapia Bastidas Tatiana Yeobanka tutora de mi proyecto, quien ha compartido su conocimiento y guiado con su paciencia durante el desarrollo del presente trabajo.

Mi agradecimiento también va dirigido al Ing. Manuel Cevallos Castillo – Jefe Departamental de Informática del Hotel Continental por su apertura y aceptación a mi petición de realizar mi tesis.

**Javier Mesías Guiracocha Cuadra**

# **INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA**

## **UNIDAD ACADEMICA DE CIENCIAS COMERCIALES, ADMINISTRATIVAS Y CIENCIAS**

**Proyecto previo a la obtención del título de:  
Tecnólogo en Análisis de Sistemas.**

### **Tema**

**“Implementación de un servidor firewall administrado por el software  
PfSense community edition para la seguridad informática del hotel  
continental de la ciudad de Guayaquil en el 2019”**

**Autor:** Javier Mesías Guiracocha Cuadra

**Tutor:** PH. D. Tatiana Tapia

## **RESUMEN**

El presente trabajo tiene como objetivo principal la implementación de un servidor firewall de tipo open source en Continental Hotel S.A. luego de estudio realizado mediante las diferentes técnicas de investigación entre ellas la observación la cual ayudó al levantamiento de información de su infraestructura de red, se pudieron determinar también las necesidades con respecto al uso del servicio de internet, correo electrónico, vpn, servidor web, entre otros.

El actual software de tipo firewall Microsoft TMG 2010 con el que contaban en la institución demostraba vulnerabilidades como la falta de soporte directo por el fabricante, paquetes de servicio, parches de seguridad, actualizaciones de categorización de filtrado web y licenciamiento provocó que dicho servidor se encuentre vulnerable y limitado en sus características.

Debido a esto y contando con la capacitación respectiva se procedió con la implementación paso a paso de la solución propuesta en este trabajo, con esto se consigue la disminución de vulnerabilidades y se cuenta con un software actualizado y robusto capaz de brindar seguridad a los usuarios de la red. PfSense Community edition es un software basado en linux pudiendo personalizarse gracias a la instalación de paquetes y servicios como lo son el squid proxy server, el squidguard, dns server y open vpn, configuración basada en interface gráfica. Gracias a la tecnología de virtualización se logra adema contar con la contingencia adecuada en caso de daño o trabajos de mantenimiento. Hasta la realización de este trabajo el servidor firewall PfSense ha demostrado estabilidad en todo su funcionamiento.

# **INSTITUTO SUPERIOR TECNOLÓGICO BOLIVARIANO DE TECNOLOGÍA**

## **UNIDAD ACADÉMICA DE CIENCIAS COMERCIALES, ADMINISTRATIVAS Y CIENCIAS**

**Proyecto previo a la obtención del título de:  
Tecnólogo en Análisis de Sistemas.**

### **Tema**

“Implementación de un servidor firewall administrado por el software PfSense community edition para la seguridad informática del hotel continental de la ciudad de Guayaquil en el 2019”

**Autor:** Javier Mesías Guiracocha Cuadra

**Tutor:** PH. D. Tatiana Tapia

### **ABSTRACT**

This work has as main objective the implementation of an open source firewall server in Continental Hotel S.A. After a study carried out through the different research techniques, including observation, which helped to gather information on its network infrastructure, it was also possible to determine the needs regarding the use of the internet, email, vpn, web server, among others.

The current Microsoft TMG 2010 firewall-type software that they had in the institution-demonstrated vulnerabilities such as the lack of direct support by the manufacturer, service packages, security patches, web filtering categorization updates and licensing caused that server find vulnerable and limited in its characteristics.

Due to this and with the respective training, the step-by-step implementation of the solution proposed in this work was carried out, with this the vulnerability reduction is achieved and there is an updated and robust software capable of providing security to the users of the net. PfSense Community edition is a Linux-based software that can be customized thanks to the installation of packages and services such as the squid proxy server, the squidguard, dns server and open vpn, based on a graphic interface. Thanks to virtualization technology, it is also possible to have adequate contingency in case of damage or maintenance work. Until the completion of this work, the PfSense firewall server has demonstrated stability throughout its operation.

## INDICE GENERAL

### Páginas

CARATULA.....	i
DEDICATORIA .....	ii
AGRADECIMIENTO .....	iii
CERTIFICACIÓN DE LA ACEPTACIÓN DEL TUTOR .....	iv
CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN.....	v
CERTIFICACIÓN DE ACEPTACIÓN DEL CEGESCIT.....	vi
RESUMEN .....	vii
ABSTRACT.....	ix
INDICE GENERAL.....	xi
1 PLANTEAMIENTO DEL PROBLEMA .....	17
1.1 Diagnóstico .....	17
1.2 Ubicación en su contexto.....	18
1.3 Situación.....	20
1.4 Factibilidad de la implementación .....	21
1.5 Delimitación .....	22
1.5.1 Campo.....	22
1.5.2 Áreas.....	22
1.5.3 Aspectos .....	22
1.5.4 Tiempo .....	22
1.6 Formulación .....	22
1.7 Definición de variables.....	22
1.7.1 Independiente .....	22
1.7.2 Dependiente .....	22
1.8 Objetivos.....	22
1.8.1 Objetivo General .....	22
1.8.2 Objetivos específicos .....	22
1.9 Conveniencia .....	23
1.10 Relevancia social.....	23
1.11 Implicaciones prácticas.....	23



2	MARCO REFERENCIAL.....	25
2.1	Fundamentación teórica .....	25
2.1.1	Antecedentes históricos .....	25
2.2	Antecedentes del problema .....	25
2.3	Antecedentes referenciales .....	26
2.4	Que es un firewall .....	28
2.5	Generación de Firewall .....	29
2.5.1	Primera generación – Filtro de paquetes .....	29
2.5.2	Segunda generación – Filtros de sesión Estado .....	29
2.5.3	Tercera Generación - Application Gateway.....	30
2.5.4	Cuarta Generación y posterior .....	30
2.6	Características de PfSense .....	31
2.7	Fundamentación legal.....	33
3	METODOLOGÍA.....	35
3.1	Diseño de la Investigación .....	35
3.2	Tipos de Investigación .....	35
3.2.1	Investigación exploratoria.....	35
3.2.2	Investigación descriptiva .....	36
3.2.3	Investigación de Campo.....	38
3.2.4	Investigación bibliográfica-documental.....	39
3.3	Técnicas e instrumentos de la Investigación .....	41
3.3.1	La observación.....	41
3.3.2	Observación Directa e Indirecta .....	42
3.4	Población y muestra .....	42
3.4.1	Muestra .....	43
3.5	Entrevista.....	44
3.5.1	Entrevista con el Ing. Manuel Cevallos Castillo.....	44
3.5.2	Encuesta .....	45
3.6	Análisis de resultados de la encuesta.....	45
3.6.1	Comentarios finales sobre los resultados de la encuesta ...	55
3.7	Presupuesto económico .....	56
4	LA PROPUESTA.....	58
4.1	Procedimiento.....	58

4.1.1	Fase 1: Interpretar.....	58
4.1.2	Fase 2. Estudio in situ.....	58
4.1.3	Fase 3. Planteamiento.....	59
4.1.4	Fase 4: Pruebas de laboratorio e implementación.....	59
4.1.5	Fase 5: Seguimiento.....	59
4.2	Proceso de Instalación.....	60
4.2.1	Preparación del equipo virtual.....	60
4.2.2	Configuración del equipo virtual.....	65
4.2.3	Instalación de PfSense Community Edition.....	68
4.2.4	PfSense Community Edition-Primeros pasos.....	76
4.3	Instalación de paquetes adicionales en PfSense Community Edition	81
4.4	Interfaces de red.....	83
4.5	Configuración de NAT – Port forward.....	84
4.6	Reglas de Acceso.....	86
4.6.1	Reglas aplicadas a la red LAN.....	88
4.6.2	Reglas aplicadas a la red DMZ.....	89
4.6.3	Reglas aplicadas a la red VPN.....	89
4.7	Configuración del Servicio de Bind (DNS Server).....	90
4.7.1	Configuración de la Zona DNS.....	90
4.8	Configuración de NTP cliente.....	92
4.9	Unir servidor firewall al dominio local.....	93
4.10	Configuración de Squid Proxy.....	94
4.10.1	Services/Squid Proxy Server/Antivirus.....	95
4.11	Configuración de SquidGuard Proxy Filter.....	97
4.12	Configuración del servicio de OpenVPN.....	106
4.12.1	Creación del Certificado de Autorización.....	106
4.12.2	Configuración del Tunnel.....	108
4.12.3	Configuración avanzada de cliente.....	108
4.12.4	Creación de usuarios para la VPN.....	109
4.13	Configuración de archivo WPAD.....	110
4.14	Pruebas de ejecución.....	113
4.14.1	Pruebas de acceso a internet.....	113

4.14.2	Prueba del servidor de correo electrónico.....	121
4.14.3	Ingreso a sitio de facturación electrónica clientes .....	122
4.14.4	Pruebas de acceso al servidor FTP .....	123
4.14.5	Pruebas de conexión remota mediante OpenVPN.....	124
5	CONCLUSIONES Y RECOMENDACIONES .....	127
5.1	Conclusiones .....	127
5.2	Recomendaciones .....	128
6	ANEXOS .....	129
6.1	Anexo 1.....	129
6.2	Anexo 2.....	131
7	BIBLIOGRAFÍA .....	133

# CAPITULO I

## 1 PLANTEAMIENTO DEL PROBLEMA

### 1.1 Diagnóstico

CONTINENTAL HOTEL S.A. es una empresa de tipo hotelero fundada en la ciudad de Guayaquil por el año 1979, la misma que desde sus inicios ha venido utilizando diferentes tipos de tecnologías acorde al mercado y la época. Desde el año 2000 con la aparición de los servicios de comunicación vía radio y el internet en servicios como el web y correo electrónico se vio muy necesario contar con sistemas de seguridad que puedan proteger la información de la organización entrante, saliente y en sitio.

Con el paso de los años se han implementado sistemas de seguridad tipo firewall de la firma de Microsoft tal como el ISA server en su versión 2004 y desde el año 2010 la versión de Microsoft Threat Management Gateway 2010 la misma que ha se ha venido utilizando hasta fines de año 2018.

La problemática surgió con el software antes mencionado que hasta el año 2015 el fabricante decide darle fin al soporte estándar del producto ocasionando que el producto no reciba las actualizaciones de:

- Definiciones de virus
- Service pack
- Licencia de categorización de filtrado web

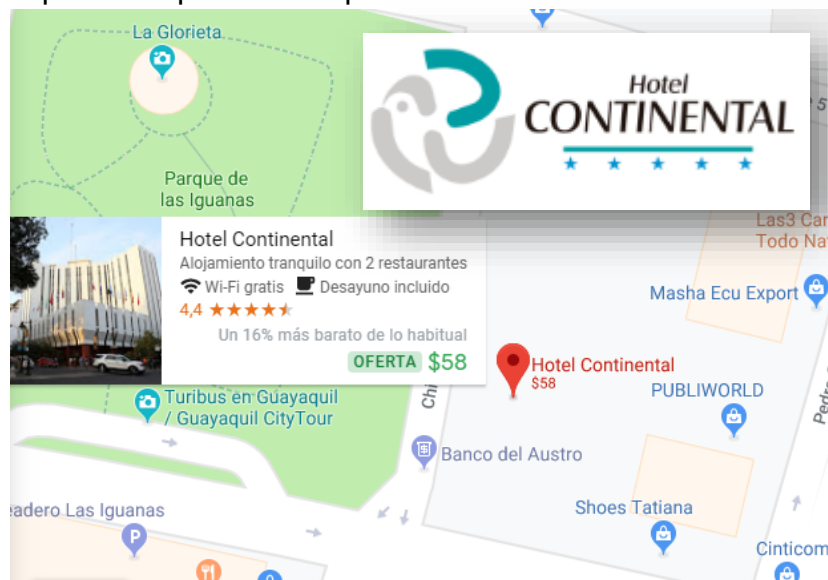
A esto se añade la poca eficiencia al momento de categorizar correctamente los sitios bloqueados direcciones (url) del mismo sitio que contienen subdominios, direcciones IP públicas de sitios que contienen certificados de acceso y objetos webs. Todas estas casuísticas crearon que la organización se encuentre en un estado de vulnerabilidad en los servicios de red hacia el mundo teniendo un alto porcentaje de probabilidad de ser víctimas de ataques y fraudes informáticos por parte de ciberdelincuentes.

## 1.2 Ubicación en su contexto

CONTINENTAL HOTEL S.A. es el producto de una larga ilusión de un inmigrante italiano y la continuidad profesional de sus hijos. Emilio Bruzzone, el mayor de seis hermanos se educó en Italia, en una Escuela Hotelera en la Ciudad de Génova y se graduó en 1960. Llegó a Guayaquil con 21 años de edad, seis más que su padre cuando llegó a Guayaquil en 1923.

Para fines de los años 60, su padre Francisco, impulsado por la iniciativa de su hijo, adquirió en propiedad tres solares sobre los que luego se proyectaría un hotel de 400 habitaciones, diseñado por Morris Lapidus, de Miami, Florida, famoso arquitecto especialista en hoteles y renombrado por sus proyectos en los EEUU y en el Caribe. Ese primer proyecto no pudo realizarse, por los múltiples inconvenientes, obra de los competidores de aquellos años, que veían en los grandes peligros para sus hoteles.

Finalmente, en los años 70, estimulado por el interés manifiesto por la Corporación Financiera Nacional, quienes se proponían dotar a Guayaquil de un nuevo hotel, financiaron la obra del CONTINENTAL HOTEL S.A., producto de un replanteamiento arquitectónico total, redimensionamiento adecuado de su capacidad y un tamaño de inversión prudente para esas épocas.



En octubre de 1974 se inauguró el CONTINENTAL HOTEL S.A., con 91 habitaciones y unos servicios de alimentos y bebidas realmente innovadores para el mercado de ese tiempo. Nadie podrá olvidar el sentimiento colectivo de alegría y satisfacción que predominaba entre los guayaquileños que comenzaron a disfrutar de los servicios de un moderno hotel de cinco estrellas.

No pasó mucho tiempo y los salones de eventos “Los Candelabros” fueron el centro de las celebraciones más elegantes y novedosas de la sociedad de la Ciudad; en ese salón se presentaron artistas internacionales y sus famosos espectáculos, brindándole a Guayaquil, a nivel sudamericano, una envidiable posición de preponderancia cultural; por cientos fueron las parejas que se casaron y las jovencitas que celebraron sus quince años en esos salones.

El Fortín, el restaurante de corte mediterráneo, ha servido alimentos de la cocina tradicional europea y durante 36 años se ha distinguido por su nivel de calidad y servicio. Unos años después de su inauguración se abrió el Santa Ana (1984), una sala de música donde se presentaron, por 25 años consecutivos, los más destacados artistas nacionales, conjuntos y solistas que hoy adornan el repertorio musical de Guayaquil.

Y la joya de la corona del CONTINENTAL HOTEL S.A.: “La Canoa”, una cafetería ambientada en el sabor criollo, con lo mejor de la cocina vernácula, típica, folklórica, aquella que es muy difícil que hoy se la prepare en casa.

La Canoa, es el reducto de la tradición gastronómica de la Ciudad y goza de la aceptación de propios y extraños por la consistencia de su calidad. Desde su inicio la Canoa ofreció servicio 24 horas, lo que fue la mayor innovación en los servicios de la Ciudad; no ha cerrado sus puertas en 37 años consecutivos e ininterrumpidamente. Cálculos conservadores hablan de que La Canoa ha sido visitada por 11 millones de clientes a la fecha.

Más de treinta y siete años han transcurrido y el CONTINENTAL HOTEL S.A. continúa siendo visitado con el mismo interés, para orgullo de sus administradores.

Don Francisco Bruzzone murió el 2007, de 99 años de edad, y lo suceden sus hijos Emilio y Aldo, este último funge de Gerente General del Hotel.

Actualmente en el hotel laboran cerca de 200 personas entre las diferentes áreas tales como:

- Frontdesk
- Cafetería
- Restaurante
- Costos
- Contabilidad
- Personal
- Informática
- Auditoria
- Cobranzas
- Ama de llaves
- Mercadeo
- Banquetes y eventos
- Seguridad
- Caja
- Almacén
- Mantenimiento
- Lavandería

### **1.3 Situación**

Con la solución de firewall actual si bien es cierto luego de su lanzamiento en el año 2010 por parte de Microsoft el cual reemplazó a ISA Server 2004, fue conocido como uno de los mejores en su categoría sobre todo por la integración que ofrecía en entornos de

productos Microsoft en el cual la administración fue muy amigable sin embargo con el paso de los años surgieron los siguientes problemas:

- Fin al soporte estándar del producto (asistencia por especialistas del producto).
- Negativa por parte de Microsoft en el desarrollo del producto para versiones posteriores.
- Fin de actualizaciones de definiciones de virus.
- No contar con service pack vuelve a la organización vulnerable frente a los ataques del exterior.
- Actualización y licencia de categorización de filtrado web no disponible para la venta.
- Inestabilidad al momento de aplicar filtrado web a los sitios visitados por los usuarios.
- Poca eficacia en el filtrado de sitios web https.

Adicionalmente, el software ya presentaba problemas en la categorización de los diferentes accesos a internet y no permitía discernir entre aquellos que son permitidos o no en el ambiente laboral, como también restringir los accesos no deseados lo que generaba vulnerabilidades a la organización.

#### **1.4 Factibilidad de la implementación**

CONTINENTAL HOTEL S.A. actualmente trabaja sobre entornos virtualizados donde a finales del año 2018 se realizó la actualización del hardware a cada uno de sus servidores lo que da fundamento a que este tipo de implementación cuente con el hardware necesario para su funcionamiento.

Adicional cabe recalcar que este proyecto fue presentado a la Gerencia General la misma que estuvo dispuesta en financiar y aprobar el alcance del mismo.



El área de IT mantuvo capacitación para la instalación e implementación de la solución, por lo que el proyecto se lo califica como factible en todos sus ámbitos.

## **1.5 Delimitación**

### **1.5.1 Campo**

Firewall Open Source, FreeBSD, Hyper V Server

### **1.5.2 Áreas**

Seguridad informática

### **1.5.3 Aspectos**

Implementación servidor firewall

### **1.5.4 Tiempo**

2019

## **1.6 Formulación**

¿Cómo influye la instalación de una solución en seguridad robusta en la disminución de vulnerabilidades en servicios de red de la empresa CONTINENTAL HOTEL S.A. en el periodo 2019?

## **1.7 Definición de variables**

### **1.7.1 Independiente**

Solución en seguridad

### **1.7.2 Dependiente**

Disminución de vulnerabilidades

## **1.8 Objetivos**

### **1.8.1 Objetivo General**

Implementar un servidor firewall administrado por el software PFSENSE community edition para la seguridad informática del CONTINENTAL HOTEL S.A. de la ciudad de Guayaquil en el 2019.

### **1.8.2 Objetivos específicos**

- Identificar la información científica disponible con respecto a la implementación de la solución de una plataforma firewall administrado por el software PFSENSE community edition
- Diagnosticar el estado actual de la falta de una solución en seguridad robusta en la disminución de vulnerabilidades basadas en servicios de red de la empresa.
- Implementar la solución firewall administrado por el software PFSENSE community edition para la disminución y el control eficiente de acceso a servicios de red por parte de los usuarios y equipos de la empresa CONTINENTAL HOTEL S.A.

### **1.9 Conveniencia**

Es relevante la implementación de una solución de tipo firewall que pueda monitorear y controlar las conexiones entrantes y salientes al utilizar los servicios de red del CONTINENTAL HOTEL S.A., el control de acceso que tienen los usuarios en servicios como el internet, correo electrónico y acceso remoto busca mantener la integridad de la información que viaja a través de estos canales y retener los ataques que diariamente realizan ciberdelincuentes a las diferentes entidades.

### **1.10 Relevancia social**

Este tipo de solución se podrá implementar tanto en pequeñas, medianas y grandes empresas ya que su funcionalidad es robusta y confiable y se adapta a las necesidades de cada entidad que buscan herramientas confiables, eficaces y seguras para controlar el acceso a los servicios de red entrantes y salientes por parte de los usuarios y equipos.

### **1.11 Implicaciones prácticas**

La ventaja es que al contar con una herramienta de tipo firewall actualizada y que en la actualidad cuenta con soporte especializado provee la confianza necesaria a la hora de implementarlo como solución para el CONTINENTAL HOTEL S.A.

Ayudará al departamento de IT a administrar la red y reducir significativamente el riesgo de ser vulnerables a los ataques de ciberdelincuentes, virus, malware y acceso a sitios no autorizados y considerados de alta peligrosidad.

## **CAPITULO II**

### **2 MARCO REFERENCIAL**

#### **2.1 Fundamentación teórica**

##### **2.1.1 Antecedentes históricos**

Antes de hablar de Firewalls debemos remontarnos al nacimiento de la INTERNET, este gran avance surge como la Red de Agencia de Proyectos de Investigación Avanzada (ARPANET), hasta ese entonces tan sólo era una pequeña comunidad cerrada donde todos se conocían entre sí, pero luego el dos de noviembre de 1988 Peter Yee en el Centro de Investigación Ames de la NASA informa a la comunidad por medio de correo electrónico que han sido atacados por un virus llamado Gusano Morris y es ahí cuando los creadores y organizaciones afiliadas se percatan de que la red no era tan cerrada ni tan segura como ellos pensaban.

A partir de este momento los investigadores comienzan a compartir información sobre sus prácticas con el fin de evitar futuras intrusiones. Algunos de los resultados de esta perturbación fue el aumento en las listas de correo dedicado a la seguridad y el seguimiento de errores. Gracias al Gusano Morris y demás incidentes que se presentaron en aquella época es que las personas empiezan a preocuparse por asegurar la red y a tomar conciencia por la protección de la información, en este punto se habla por primera vez del surgimiento de una herramienta que proteja a las redes de intrusiones desde otras redes.

#### **2.2 Antecedentes del problema**

CONTINENTAL HOTEL S.A., desde los años 90 ha venido incorporando tecnología a los diferentes departamentos administrativos y operativos, una de las adquisiciones fue el servicio

de internet banda ancha y junto con ello la implementación de firewall basado en hardware y luego en software, un ejemplo de ella fue la adquisición del ISA 2004 de la compañía Microsoft el cual basado en la época cumplía con todo lo requerido para proteger a la compañía de los ataques externos al estar conectado con el mundo, con el paso del tiempo se adquirió la actualización del producto a TMG 2010, éste se basaba en licenciamiento anual para poder utilizar el filtrado web por categorías, sin embargo con el paso de los años se anunció por parte de Microsoft que el mencionado software se encontraba en proceso de descontinuado y que no iban a salir al mercado futuras versiones o actualizaciones del producto, ya para esto TMG 2010 presentaba problemas al momento de categorizar sitios webs, permitía el acceso a sitios https a pesar de que estos estén bloqueados para ciertos usuarios y en el año 2018 los partners o socios dejaron de licenciar este producto es decir TMG 2010, al no estar licenciado el motor de filtrado web por categorías dejó de funcionar. La infraestructura tecnológica de CONTINENTAL HOTEL S.A. se encontraba expuesto a ataques externos comprometiendo así la información comercial y administrativa que se almacena en servidores y estaciones de trabajo.

### **2.3 Antecedentes referenciales**

Un primero trabajo corresponde se basa en el diseño de un servidor firewall de tipo open source llamado **PfSense versión 2.4** en el centro de salud San José de la provincia de Santa Elena, la misma que tenían como problemática el control de acceso a páginas webs y otros servicios de internet por parte de los usuarios, todo esto basado en un análisis del centro de salud y cumpliendo con los estándares tecnológicos se logró cumplir a cabalidad el diseño implementación de la solución (Dominguez, 2016, p. 77).

El segundo ejemplo basó su trabajo en: Tecnología VPN y Firewall de Check Point implementada para establecer seguridad en comunicaciones remotas en El Grupo MDM que es el encargado de administrar y gerenciar una franquicia compuesta por tres hoteles de la corporación Marriott, y tiene la necesidad de protegerse de ataques con una herramienta donde el costo beneficio sea un punto importante pero donde el punto más susceptible y decisivo es resguardar de manera confiable la seguridad de su información. Es importante que los usuarios remotos sean capaces de conectarse a la red interna de la organización desde cualquier parte del mundo sin ningún inconveniente. Con estos requisitos, Firewall-1VPN-1, de Check Point, fue seleccionado entre varios productos que ofrecen protección sobre equipos y aplicaciones que trabajan expuestos al Internet, para ser implementado por los administradores de red del Grupo MDM. Como resultado de la implementación se tiene un sistema seguro y confiable que brinda facilidad de administrar las diferentes redes, equipos y usuarios, donde se puede aislar un equipo afectado ocasionado por un tipo de ataque malicioso (García Vélez, 2007, p. 55).

Como tercer ejemplo quiero mencionar a Esparza Morocho (2013) el cual basó su trabajo en:

la Implementación de un Firewall sobre plataforma Linux en la empresa de contabilidad Armas & Asociados la misma que es una mediana empresa creada con el fin de proporcionar servicios de Contabilidad, Auditoría y Tributación a diferentes empresas de forma independiente, ubicada en Quito, su infraestructura consta de varios computadores con conexión a internet, cuenta una sola oficina matriz, la problemática consistía en que al tener una conexión directa a Internet sin

restricciones, se tiene el riesgo de sufrir intromisiones de virus y ataques informáticos que pondrían en riesgo la integridad del software y la información confidencial y los datos confidenciales de los clientes de la empresa a quienes se les debe brindar un servicio de calidad y seguridad (p.78).

Como cuarto y último ejemplo menciono al Instituto Superior Bolivariano de Tecnología en cuya infraestructura la cual es extensa debido a las numerosas estaciones de trabajo en diferentes sedes (laboratorios, salas, oficinas administrativas, ciber, cctv, puntos de acceso, servidores, centrales IP. Etc.) utiliza como firewall el producto Hillstone Networks' Enterprise Security el cual es de tipo hardware, cuenta con protección basada en la nube, para centro de datos, gestión de la seguridad y detección de brechas.

Por lo tanto, luego de la etapa de evaluación de diferentes firewalls basados en hardware y software se optó por factibilidad implementar uno de tipo open source llamado Fedora en su versión 12.0 donde mediante consola fue configurado el servicio de firewall y luego de las pruebas de funcionamiento queda implementado ofreciendo seguridad a los usuarios en su trabajo diario.

## **2.4 Que es un firewall**

El término Firewall o cortafuegos no se originó con la Internet, ya que los cortafuegos en si son barreras que se utilizan para contener un incendio hasta que los bomberos lleguen a apagarlo, para la industria automotriz se considera cortafuegos a una lámina que separa el compartimiento de los pasajeros con el motor, es decir que en tecnología llamamos Firewall o cortafuegos a un dispositivo o sistema de información que restringe el acceso entre dos o más redes (Forero Gandur, 2013, p.2).

La necesidad de utilizar firewall se debe al hecho de restringir el acceso a las redes mediante el uso de internet y esto surgió desde los años 80 cuando a nivel gubernamental y académico las redes iban en constante crecimiento dando como resultado lo que hoy conocemos como el internet, de igual forma el avance de la tecnología en los computadores personales hizo que nacieran las primeras comunidades de hackers.

## **2.5 Generación de Firewall**

Así como los computadores, los firewalls informáticos también tuvieron generaciones en la cual con el paso de tiempo su tecnología en constante desarrollo fue tomando su lugar en el mercado, a continuación, se detallan las 4 generaciones:

### **2.5.1 Primera generación – Filtro de paquetes**

La tecnología se dio a conocer en diciembre de 1988, fruto de la investigación de Bill Cheswick y Steve Bellovin de AT&T quienes propusieron un modelo de filtrado de paquetes donde se evalúa un conjunto de protocolos TCP/IP, esto quiere decir que se restringe el tráfico basándose en las direcciones IP de origen, destino y a través de la puerta del servicio (puerto) (Forero Gandur, 2013, p.2)

### **2.5.2 Segunda generación – Filtros de sesión Estado**

Se conocen en la década de los 90`s por los laboratorios Bell y fueron llamados cortafuegos circuito. Estos tomaron las restricciones de los Firewalls que se tenían en la primera generación y adicionalmente a eso agregaron restricción de tráfico a principios de



conexiones, el tráfico de paquetes que se inició desde la red protegida y restringía los paquetes que tenían número de secuencia correcta. Estos cortafuegos guardan el estado de las conexiones y filtros basados en ese estado, los cuales son conocidos como: NUEVO para nuevas conexiones, ESTABLECIDO para conexiones establecidas y RELACIONADO para las conexiones a otros existentes relacionados. (Forero Gandur, 2013, p.2)

### **2.5.3 Tercera Generación - Application Gateway**

Fue esta la generación que lanzó el primer producto comercial el 13 de junio de 1991 y se hizo popular en los años 90. Se conoce con este nombre por la aplicación del concepto de representación y control de acceso en un solo dispositivo, es decir, es capaz de recibir un sistema de conexión, protocolos de decodificación en la capa de aplicación e interceptar la comunicación entre cliente / servidor para así aplicar las reglas de acceso. Se caracteriza porque implementó todas las reglas de las anteriores generaciones, restringió el acceso FTP a los usuarios anónimos a portales de entretenimiento y a protocolos desconocidos en el puerto 443. (Forero Gandur, 2013, p.2)

### **2.5.4 Cuarta Generación y posterior**

Se consolida como una solución para redes de comunicación TCP / IP para inspeccionar paquetes y tráfico de datos en base a las características de cada aplicación, la información asociada con todas las capas

del modelo OSI y el estado de las conexiones activas y las sesiones, prevención de intrusiones con el propósito de identificar el abuso de los protocolos TCP / IP, inspección profunda de paquetes donde se combina la inspección de estado con las técnicas de los dispositivos IPS. (Forero Gandur, 2013, p.2)

Desde el año 2000, la tecnología del Firewall ha ido en constante mejora para su aplicación a las estaciones de trabajo y computadores de tipo doméstico, además de la incorporación de soluciones Firewall para servidores.

## **2.6 Características de PfSense**

Basado en estos antecedentes en el año 2018 se procede a la capacitación de administración e implementación del software llamado PfSense Community Edition cuya finalidad es reemplazar al firewall existente para este efecto a continuación sus principales características:

Según (Netgate, Netgate Solutions, 2019) las características de PfSense son las siguientes:

- Firewall and ruteador
- Anti-Spoofing
- Reglas basadas en tiempo
- Soporta IPv4 y IPv6
- NAT (entrada/salida)
- VLAN
- Ruteo estático
- Servidor DHCP
- Servidor DNS
- IPsec y OpenVPN
- Multi-WAN balanceo

- Failover automático
- Radius y Ldap autenticación
- HTTP and HTTPS proxy
- Domain/URL filtering
- Anti-virus filtering
- Reportes diario, semanal y mensual
- Interfaz basada en web
- Soporte multi-idioma
- Actualizaciones
- Registro del log
- Monitoreo en tiempo real con gráficos

(Netgate, Netgate Solutions, 2019) indica que:

El software PfSense es una distribución personalizada, gratuita y de código abierto de FreeBSD diseñada específicamente para su uso como firewall y enrutador que se gestiona por completo a través de la interfaz web. Además de ser una plataforma de enrutamiento y cortafuegos flexible y potente, incluye una larga lista de características relacionadas y un sistema de paquetes que permite una mayor capacidad de expansión sin agregar posibles vulnerabilidades de seguridad a la distribución base. Puede ser instalado en una gran variedad de ordenadores (p.1).

Además para (Hardware, 2019) “PfSense es un proyecto abundantemente probado, cuenta con más de 1.000.000 descargas e innumerables instalaciones en todo el mundo, desde el uso casero hasta las grandes empresas, autoridades públicas, ministerios y universidades”(p.1).

Asimismo (Netgate, Netgate Docs, 2019) “Indica los requerimientos mínimos son los siguientes: CPU 600Mhz o

superior, RAM 512 MB o mayor, 4GB de espacio en disco (HDD,SSD), DVD o USB booteable (p.1).

Basado en lo anterior expuesto, el autor de esta investigación vio una oportunidad para brindar una posible solución al problema descrito del CONTINENTAL HOTEL S.A. y cubrir sus necesidades de protección cibernética.

## **2.7 Fundamentación legal**

El Expresidente Rafael Correa Delgado mediante decreto ejecutivo número 1014 con registro oficial 322 fechado 23 de abril del 2008 bajo el título: Utilización de software libre (open source) en la administración pública (Informática, 2009) decreta :

Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos, esto con el fin de alcanzar la soberanía tecnológica y ahorro en recursos públicos, además se establece la migración de software propietario a software previa su evaluación y recurso técnico disponible (p.24).

El servicio ecuatoriano de normalización (INEN) en el mes de abril del año 2017 implementa la norma técnica ecuatoriana INEN-ISO/IEC 27002 TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN donde menciona que:

Esta norma nacional está diseñada para que las organizaciones la usen como referencia a la hora de seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 o bien como documento

guía para organizaciones que implementen controles de seguridad de la información comúnmente aceptados. Esta norma está pensada también para usarse en el desarrollo de directrices de gestión de seguridad de la información en industrias y organizaciones específicas, teniendo en cuenta sus entornos específicos de riesgo de seguridad de la información. (INEN, 2017, p.12)

Es importante recalcar que las existen organizaciones de todo tipo y tamaño tanto del sector público y privado, comercial y sin ánimo de lucro que recogen, procesan, almacenan y transmiten información de muchas formas que incluyen medios electrónicos, físicos y verbales.

Asimismo mediante Acuerdo Ministerial No. 166, publicado en el Registro Oficial No. 88 del 25 de septiembre de 2013, (Peñaherrera, 2013) dispone:

La implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), en todas las entidades de la Administración Pública Central, (APC); donde se establece 126 hitos o controles, basadas en la norma técnica ecuatoriana INEN ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”, cuya implementación debe ser prioritaria para las entidades públicas (fase I) y la implementación de la fase II del EGSI se realizará en cada institución de acuerdo al ámbito de acción. Estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la información (p.3).

## CAPÍTULO III

### 3 METODOLOGÍA

#### 3.1 Diseño de la Investigación

En este capítulo se detalla la metodología que será utilizada para realizar la propuesta que conlleva a la implementación de un firewall de tipo open source para la disminución de las vulnerabilidades en el Hotel Continental.

Sobre la metodología, se ha utilizado una metodología de investigación mixta, como son la exploratoria, descriptiva, de campo y bibliográfica. Aporta además a los estudios exploratorios de documentos, búsqueda, revisión bibliográfica, y notas de campo para entender los conceptos claves e ideas sobre la información obtenida, esto partiendo de la información bibliográfica y del conocimiento y experiencia de expertos en la materia.

A fin de obtener conceptos amplios de las metodologías de investigación utilizadas en este trabajo se detallan a continuación las siguientes:

#### 3.2 Tipos de Investigación

##### 3.2.1 Investigación exploratoria

Para (Cazau, INTRODUCCIÓN A LA INVESTIGACIÓN, 2006) “La investigación exploratoria, también llamada formulativa permite conocer y ampliar el conocimiento sobre un fenómeno para precisar mejor el problema a investigar. Puede o no partir de hipótesis previas” (p.17).

Así también (Cazau, INTRODUCCIÓN A LA INVESTIGACIÓN, 2006) “Indica que en la investigación

exploratoria se estudian qué variables o factores podrían estar relacionados con el fenómeno en cuestión, y termina cuando uno ya tiene una idea de las variables que juzga relevantes, es decir, cuando ya conoce bien el tema” (p.17).

Por otro lado (Paneque, 1998) explica que “En estudios exploratorios se abordan campos poco conocidos donde el problema, necesita ser aclarado y delimitado. Esto último constituye precisamente el objetivo de una investigación de tipo exploratorio. Las investigaciones exploratorias suelen incluir amplias revisiones de literatura y consultas con especialistas” (p.21)

La investigación exploratoria según lo afirma Sabino (Sabino, 1992) “esta investigación, exigen del investigador una extraordinaria creatividad y capacidad de improvisación, ya que implica la ausencia de guías teóricas que faciliten la comprensión del tema de estudio, aparte de la incertidumbre respecto a los resultados que seguramente provocará” (p.44).

### **3.2.2 Investigación descriptiva**

La investigación descriptiva se considera como lo afirma (Salkind, 1998):

Se reseña las características de un fenómeno existente, así como también referente a ésta investigación indica que la investigación descriptiva no sólo puede ser autosuficiente, como demuestran los ejemplos, sino también puede servir como base para otros tipos de investigaciones, porque a menudo es preciso describir las características de un grupo antes de poder abordar la significatividad de cualesquier diferencias observadas (p.37).

Por otro lado (Odón, 2012) indica que “La investigación descriptiva consiste en la caracterización de un hecho o fenómeno, individuo o grupo con el fin de establecer su estructura o comportamiento” (p.17).

Según (Frank, 2012) :

El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son meros tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento (p.62).

Asimismo, la investigación descriptiva consta de las siguientes etapas:

1. El estudio de las propiedades del problema.
2. La definición y la formulación de las hipótesis.
3. Se seleccionan temas y sus fuentes.
4. La selección de técnicas para la recolección de datos.
5. Las observaciones deben ser de tipo objetivo y puntuales.
6. Descripción, análisis y la interpretación de los datos obtenidos, en base a términos claros y específicos.



### 3.2.3 Investigación de Campo

Para (Arias, 2012):

La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental (p.31).

Además (Arias, 2012) también sostiene que:

En una investigación de campo también se emplean datos secundarios, sobre todo los provenientes de fuentes bibliográficas, a partir de los cuales se elabora el marco teórico.

No obstante, son los datos primarios obtenidos a través del diseño de campo, los esenciales para el logro de los objetivos y la solución del problema planteado.

La investigación de campo, al igual que la documental, se puede realizar a nivel exploratorio, descriptivo y explicativo (p.31).

Según (Ramirez, 2010), “La investigación de campo puede ser extensiva, cuando se realiza en muestras y en poblaciones enteras (censos); e intensiva cuando se concentra en casos particulares, sin la posibilidad de generalizar los resultados”

Para (Sabino, 1992) en su libro titulado El proceso de la investigación afirma que:

En los diseños de campo los datos de interés se recogen en forma directa de la realidad, mediante el trabajo concreto del investigador y su equipo. Estos datos, obtenidos directamente de la experiencia empírica, son llamados primarios, denominación que alude al hecho de que son datos de primera mano, originales, producto de la investigación en curso sin intermediación de ninguna naturaleza. Cuando, a diferencia de lo anterior, los datos a emplear han sido ya recolectados en otras investigaciones y son conocidos mediante los informes correspondientes nos referimos a datos secundarios, porque han sido obtenidos por otros y nos llegan elaborados y procesados de acuerdo con los fines de quienes inicialmente los obtuvieron y manipularon. Como estas informaciones proceden siempre de documentos escritos, pues esa es la forma uniforme en que se emiten los informes científicos, damos a estos diseños el nombre de bibliográficos (p.79)

#### **3.2.4 Investigación bibliográfica-documental**

Para (Arias, 2012):

La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos (p.27).

Sin embargo, es necesario entender los conceptos de dato, fuente y documento.

### **Dato**

Corresponde a la unidad de información que se consigue en la ejecución de la investigación. En base a su procedencia, los datos pueden ser primarios, cuando éstos son recabados originalmente por el investigador; también son de tipo secundarios, en caso sean extraídos de documentos de terceros investigadores.

### **Fuente**

Es todo lo que facilita los datos e información.

### **Documento**

Llámesese así al soporte físico, esto es papel, madera, tela, cinta magnética) o dispositivo digital donde se registra y a su vez almacena la información.

Por su parte (Arias, 2012) en su libro El proyecto de la investigación nos sugiere las siguientes etapas para una investigación documental:

1. Búsqueda de fuentes: impresas y electrónicas (Internet).
2. Lectura inicial de los documentos disponibles.
3. Elaboración del esquema preliminar o tentativo.
4. Recolección de datos mediante lectura evaluativa y elaboración de resúmenes.
5. Análisis e interpretación de la información recolectada en función del esquema preliminar.
6. Formulación del esquema definitivo y desarrollo de los capítulos.

7. Redacción de la introducción y conclusiones.
8. Revisión y presentación del informe final.

Así también (Cazau, 2006) nos indica que la investigación bibliográfica permite:

“Entre otras cosas, apoyar la investigación que se desea realizar, evitar emprender investigaciones ya realizadas, tomar conocimiento de experimentos ya hechos para repetirlos cuando sea necesario, continuar investigaciones interrumpidas o incompletas, buscar información sugerente, seleccionar un marco teórico, etc.” (p.152)

### **3.3 Técnicas e instrumentos de la Investigación**

#### **3.3.1 La observación**

(Sanjuan, 2011) define a la observación como “Un elemento fundamental de todo proceso de investigación; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación” (p.5)

Por su parte (Bravo, 1984) la define como “La inspección y estudio realizado por el investigador, mediante el empleo de sus propios sentidos, con o sin ayuda de aparatos técnicos, de las cosas o hechos de interés social, tal como son o tienen lugar espontáneamente”.

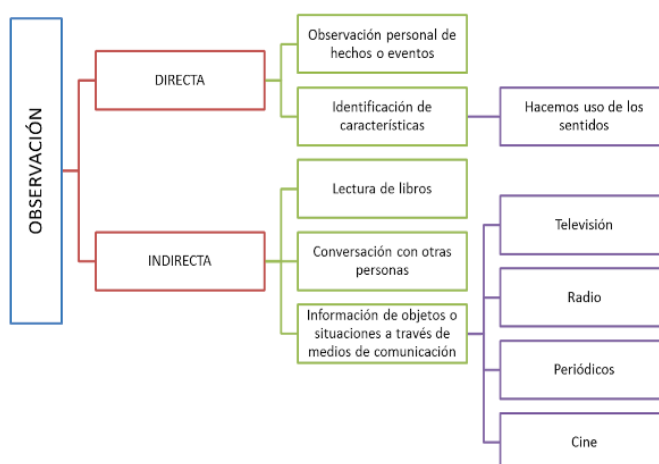
Mientras que (William, 1981) “Considera que la observación juega un papel muy importante en toda investigación porque le proporciona uno de sus elementos fundamentales; los hechos”.

### 3.3.2 Observación Directa e Indirecta

(Sanjuan, 2011) sostiene que:

La observación directa sucede cuando el investigador se pone en contacto personalmente con el hecho o fenómeno que trata de investigar.

Mientras que la investigación indirecta tiene sus bases cuando el investigador entra en conocimiento del hecho o fenómeno observado a través de las observaciones realizadas anteriormente por otra persona (p.8).



### 3.4 Población y muestra

Para (Rienzo, 2009) una población es “Un conjunto de elementos acotados en un tiempo y en un espacio determinados, con alguna característica común observable o medible”(p.2).

Así (Rienzo, 2009) también lo define como “El conjunto de individuos, objetos, elementos o fenómenos en los cuales puede presentarse determinada característica susceptible de ser estudiada(p.2)”.

En CONTINENTAL HOTEL S.A podemos detallar a la población basado en la siguiente tabla:

<b>DEPARTAMENTOS</b>	<b>CANTIDAD</b>
Personal	3
Cafetería	80
Almacén	10
Seguridad	7
Caja	12
Lavandería	10
Mantenimiento	15
Recepción	10
Banquetes y Eventos	15
Auditoría	5
Contabilidad	5
Mercadeo	3
Informática	3
Gerencia	2
Sub-Gerencia	3
Habitaciones	10
Cobranzas	4
<b>TOTAL</b>	<b>197</b>

### 3.4.1 Muestra

Según (Rienzo, 2009) se entiende por muestra: “A todo subconjunto de elementos de la población. También podemos definir a la muestra como un subgrupo o subconjunto representativo de la población, extraída seleccionada por algún método de muestreo. La muestra siempre es una parte de la población” (p2).

Realizado previamente los conceptos de población muestra, hay que entender que existe un solo tipo de muestreo el cual se basa en la cantidad de personal administrativo y operativo que tiene el hotel, por ello se aplicará la siguiente fórmula para calcular del muestreo de una población:

$$n = \frac{m}{e^2 (m-1)+1}$$

En dónde:

**m** = Es el tamaño de la población (197)

**e** = Error máximo permitido para la media muestra = 0.06

**n** = Es el tamaño de la muestra

Obtendremos como muestra:

$$n = 115$$

### **3.5 Entrevista**

Con ayuda de ésta técnica de investigación se logró obtener mayor información en cuanto a la problemática referente al actual firewall implementado en el hotel y de la necesidad de poder reemplazarlo por otra solución cuyas características beneficien a la seguridad de la información de la empresa.

#### **3.5.1 Entrevista con el Ing. Manuel Cevallos Castillo**

Uno de los puntos clave de la entrevista fue el deficiente funcionamiento que tienen el actual firewall ya que según menciona debido a la antigüedad del mismo adolece soporte alguno de parte del fabricante, adicional a ello

también el producto adolece de paquetes de servicio (service pack) con el cual se contribuya a la seguridad, también otro factor importante es que el fabricante dejó de liberar el licenciamiento anual, la categorización de filtrado web y la actualización de definiciones del antivirus y por último un bajo desempeño de performance. Añadió adicionalmente problemas con permisos de sitios con protocolo https y bloqueo de sitios que si están permitidos.

Uno de los puntos a favor es la pre disposición de reemplazar y utilizar otra solución de firewall en este caso se tiende a optar por una de tipo open source. El software de tipo open source ya es conocido en el departamento de informática ya que actualmente utilizan FreeNas que es utilizado como almacenamiento de red y años anteriores se realizó un laboratorio con el servidor de correo Zimbra community con sistema operativo de Open Suse Server.

Asimismo, se tiene en cuenta que el costo en el que se infringe es mucho menor comparado con software de marcas reconocidas, por tanto, es una buena oportunidad para optar por una alternativa open source eso sí, implementado de forma responsable.

### **3.5.2 Encuesta**

De acuerdo con el objetivo propuesto se realizó la encuesta a un total de 115 personas pertenecientes a los diferentes departamentos administrativos y operativos del hotel, con el fin de obtener retroalimentación acerca de la necesidad de implementar un sistema firewall actualizado y robusto.

## **3.6 Análisis de resultados de la encuesta**

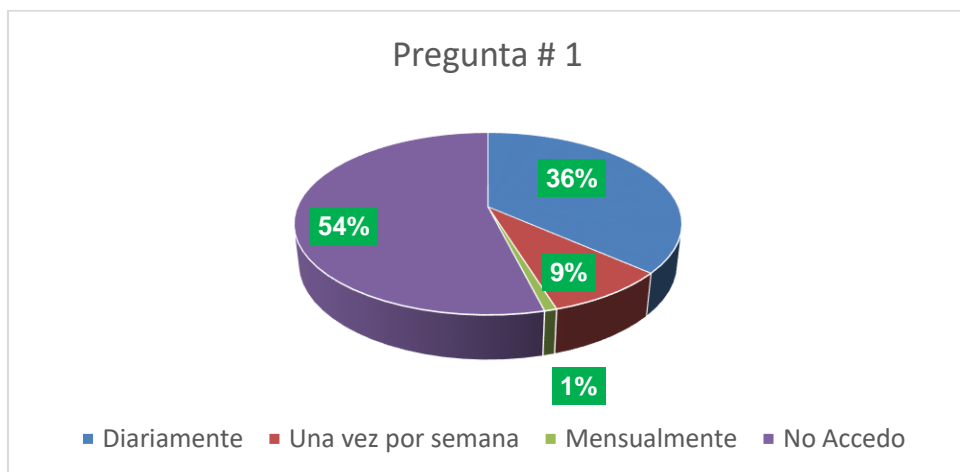


A continuación, se presenta un análisis de los datos de la encuesta desarrollada al personal administrativo de CONTINENTAL HOTEL S.A, sin embargo, tener en cuenta que la mayoría del personal que labora es de tipo operativo.

**Pregunta 1: ¿Con que frecuencia utiliza los servicios a través del internet?**

**Resultados**

Diariamente	42	36 %
Una vez por semana	10	9 %
Mensualmente	1	1 %
No accedo	62	54 %
<b>TOTAL</b>	<b>115</b>	<b>100 %</b>

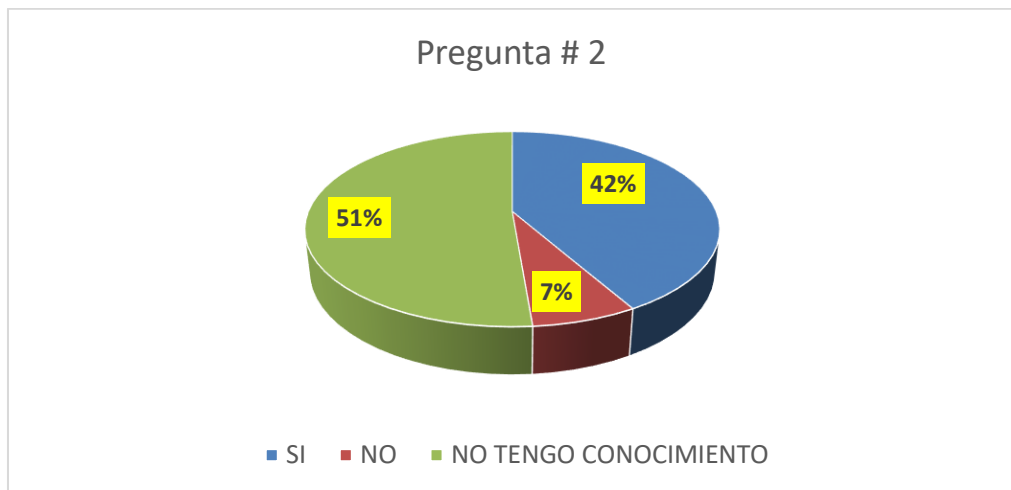


Podemos notar que más de la mitad del personal no utiliza servicios de internet y esto es porque la mayoría del personal es operativo por tanto los mismos a pesar de tener acceso a los computadores no utilizan estos servicios. Sin embargo, para el resto de la muestra queda en evidencia de que actualmente los usos de los servicios de internet son necesarios en la vida laboral diaria para que cada colaborador pueda realizar su trabajo de forma ágil.

**Pregunta 2: ¿Considera que el acceso a internet y otros servicios los utiliza de forma segura?**

**Resultados**

SI	48	42 %
NO	8	7%
NO TENGO CONOCIMIENTO	59	51%
<b>TOTAL</b>	<b>115</b>	<b>100%</b>



Existe un pequeño número de colaboradores que no se siente seguro del acceso a sitios web y la recepción de correo electrónico ya que muy probablemente hayan experimentado algún tipo de problema el cual se haya convertido en una mala experiencia.

**Pregunta 3: ¿Qué tan importante es para usted mejorar la seguridad de los servicios a través de internet?**

**Resultados**

MUY IMPORTANTE	90	78%
NADA IMPORTANTE	0	0%

NO TENGO CONOCIMIENTO	25	22 %
<b>TOTAL</b>	<b>115</b>	<b>100%</b>



El resultado de esta pregunta recalca la importancia de estar actualizado y contar con lo último en soporte para brindar seguridad dentro de la empresa.

**Pregunta 4: ¿Ha tenido algún problema o inconveniente de seguridad al momento de utilizar los servicios a través del internet?**

**Resultados**

SI	3	5 %
NO	60	44 %
NO TENGO CONOCIMIENTO	52	51 %
<b>TOTAL</b>	<b>115</b>	<b>100%</b>

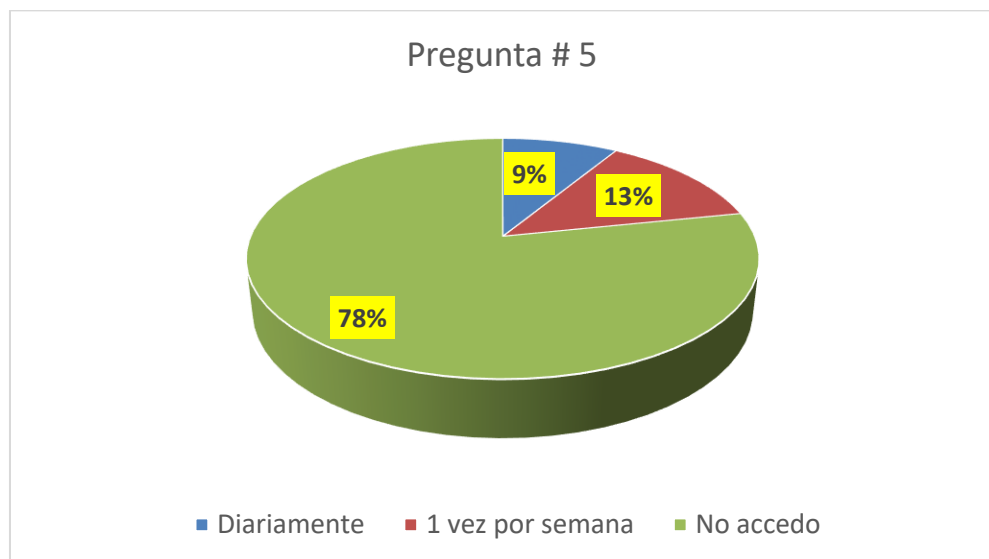


Basado en la pregunta 3, existen usuarios que actualmente hayan incurrido en problemas en la cual se haya comprometido la seguridad de su estación de trabajo.

**Pregunta 5: ¿Con que frecuencia se conecta desde el exterior a su computador de trabajo de forma remota?**

**Resultados**

DIARIAMENTE	10	9 %
1 VEZ POR SEMANA	15	13 %
NO ACCEDO	90	78 %
<b>TOTAL</b>	<b>115</b>	<b>100 %</b>

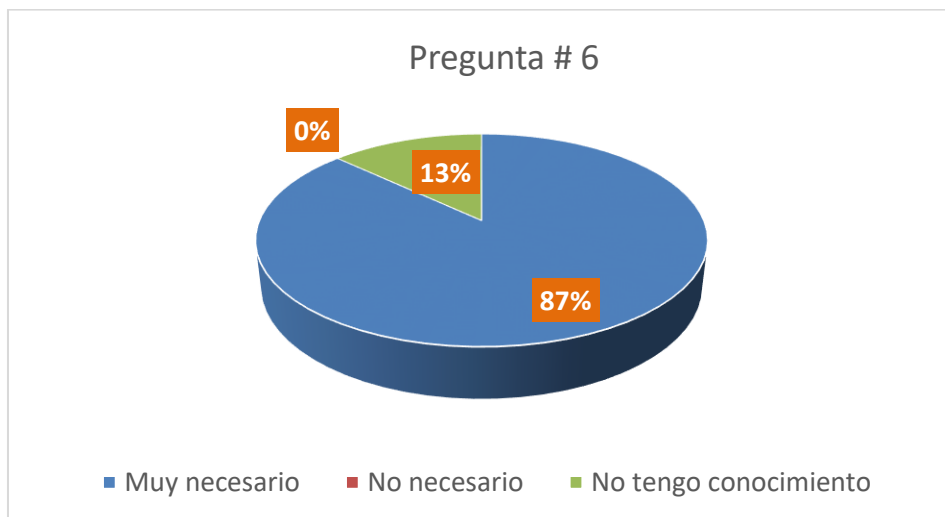


Dentro de las facilidades que ofrece la empresa se encuentra el acceso remoto con el fin de que los usuarios puedan realizar sus trabajos de forma externa, por lo que también se quiere seguridad para las conexiones entrantes.

**Pregunta 6: ¿Cree usted que es necesario mantenerse actualizado en lo que respecta a seguridad informática?**

**Resultados**

MUY NECESARIO	100	87 %
NO NECESARIO	0	0 %
NO TENGO CONOCIMIENTO	15	13 %
<b>TOTAL</b>	<b>115</b>	<b>100 %</b>

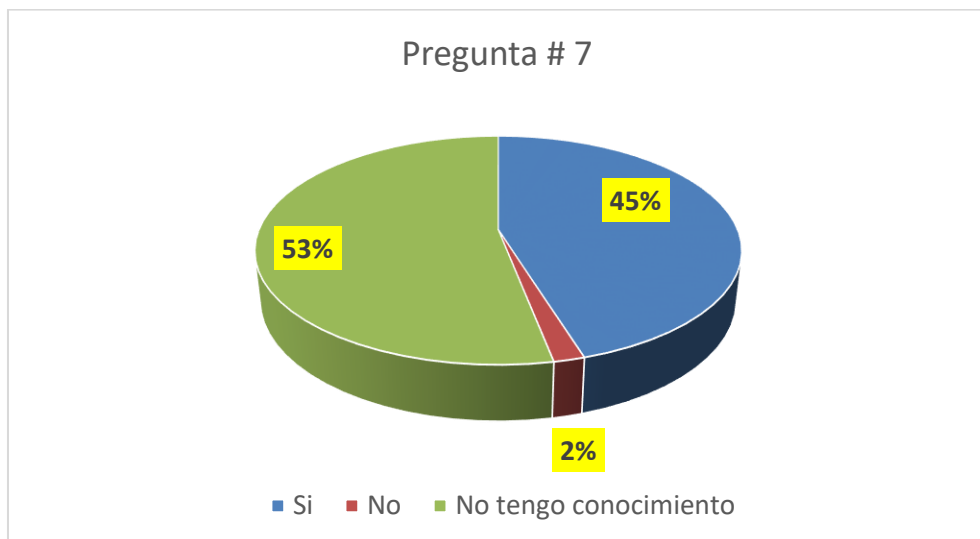


El criterio de mantenerse actualizado en temas de seguridad informática es importante ya que contribuye a que los usuarios puedan realizar su trabajo de forma permanente mediante conexiones externas.

**Pregunta 7 ¿Cree usted que la implementación de un nuevo firewall ayudará a mejorar la seguridad dentro de la empresa?**

**Resultados**

SI	52	45 %
NO	2	2 %
NO TENGO CONOCIMIENTO	61	53 %
<b>TOTAL</b>	<b>115</b>	<b>100 %</b>

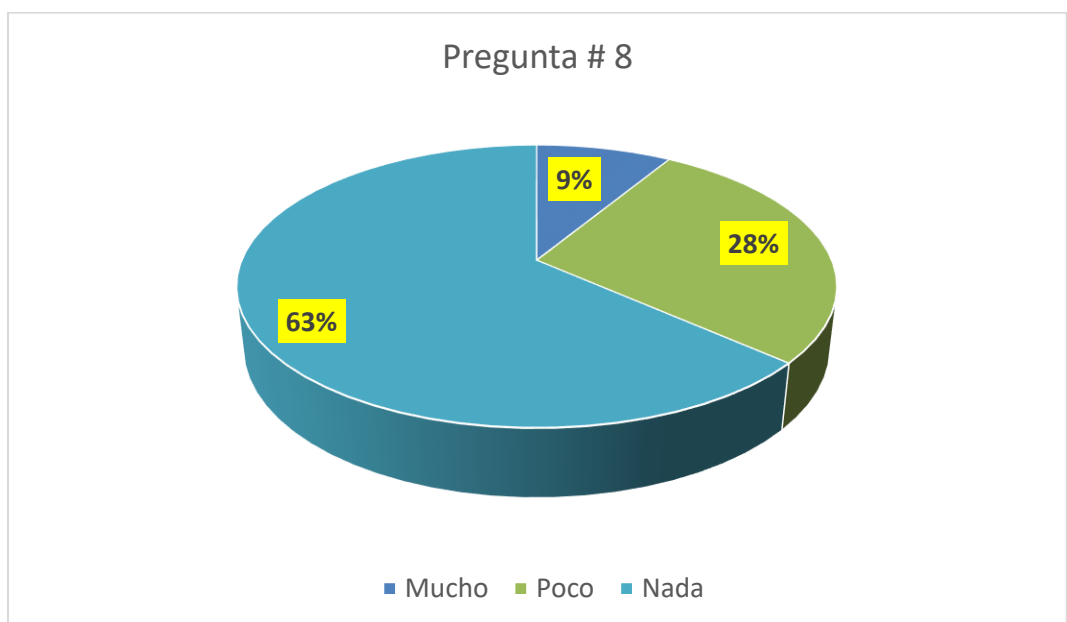


Como se aprecia los colaboradores que mantiene contacto con la tecnología están de acuerdo en el ingreso de nueva tecnología que contribuye al desarrollo de sus actividades.

**Pregunta 8: ¿Tiene usted conocimiento acerca de las vulnerabilidades que existen al utilizar los servicios a través del internet?**

**Resultados**

MUCHO	10	9 %
POCO	32	28 %
NADA	73	63 %
<b>TOTAL</b>	<b>115</b>	<b>100 %</b>



Esta pregunta es necesaria para obtener una idea del conocimiento que tienen los usuarios acerca de las vulnerabilidades que existen en el medio, para así en futuras actividades poder abordar el tema.



**Pregunta 9: ¿Cree usted que es necesario se realicen capacitaciones sobre seguridad informática?**

**Resultados**

SI	115	100%
NO	0	0%
<b>TOTAL</b>	<b>115</b>	<b>100%</b>

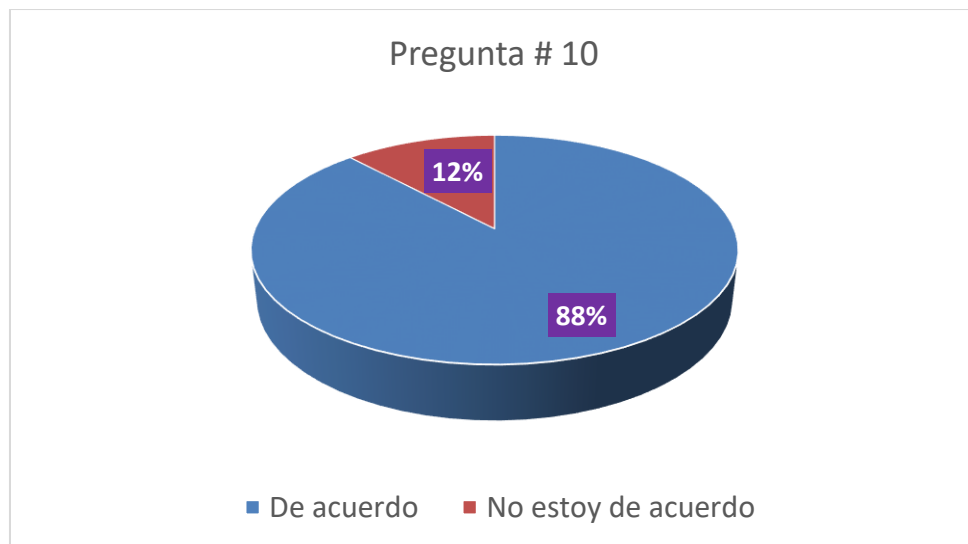


Junto con la pregunta 8, se debe abordar el tema de charlas y capacitaciones acerca de tema, el objetivo es crear conciencia acerca de la seguridad informática, de los peligros y los beneficios de la misma.

**Pregunta 10: ¿Está usted de acuerdo en que el acceso a los servicios que se utilizan a través del internet sean debidamente controlados por un firewall?**

**Resultados**

DE ACUERDO	97	88%
NO ESTOY DE ACUERDO	18	12%
<b>TOTAL</b>	<b>115</b>	<b>100%</b>



Es una tarea imperiosa de que los usuarios deben estar respaldados y protegidos de cualquier vulnerabilidad y ésta debe estar controlada desde la “puerta” centralizada.

**3.6.1 Comentarios finales sobre los resultados de la encuesta**

Mediante la encuesta fue posible recabar la información oportuna acerca primeramente de lo que esperan los usuarios de departamento de informática en la implementación de sistemas de seguridad en este caso de un firewall que se encuentre actualizado, esto con el fin de complementar el trabajo y desarrollo de las actividades de la

empresa. Asimismo, como la planificación futura acerca de las vulnerabilidades que existen en el medio de la seguridad informática. Existe además usuarios que trabajan desde lugares externos hacia sus estaciones de trabajo dentro de la empresa por tanto es imperioso que este tipo de conexiones sean permanentes y sobretodo seguras teniendo en cuenta que CONTINENTAL HOTEL S.A. al ser un negocio hotelero debe mantener su actividad las 24 horas del día los 365 días del año.

Es responsabilidad del departamento de informática dotar de las herramientas necesarias y que el usuario pueda tener la seguridad de que su trabajo lo realiza con plena seguridad.

### 3.7 Presupuesto económico

El presupuesto económico para la implementación del servidor firewall PfSense Comunity Edition, cumplen con características de protección, esto considerando los costos no elevados con el fin de mantener una red segura la cual cumple con los estándares y satisface las necesidades de CONTINENTAL HOTEL S.A.

A continuación, la tabla de costos de implementación de la solución la cual fue aceptada y aprobada:

RECURSO	DETALLE	CANTIDAD	PRECIOS
<b>Suministros</b>	Bolígrafos	2	\$0.50
	Hojas A4 Resmas	1	\$4.00
	Anillados	2	\$10.00
<b>TOTAL SUMINISTROS</b>			<b>\$14.50</b>
<b>Viáticos</b>	Movilización y alimentación		\$20.00

<b>TOTAL VIATICOS</b>			<b>\$20.00</b>
<b>Software</b>	PfSense Open Source Firewall	1	\$0.00
	Microsoft Hyper V Server 2016 R2	1	\$0.00
<b>TOTAL SOFTWARE</b>			<b>\$ 0.00</b>
<b>Infraestructura</b>	Actualización de hardware para servidor Dell R710	1	\$ 1,400.00
	<ul style="list-style-type: none"> <li>• Almacenamiento</li> <li>• Controladora de discos</li> <li>• Cables de controladora,</li> <li>• Memoria RAM,</li> <li>• Batería de controladora</li> <li>• Unidad de DVD-RW</li> </ul>		
<b>TOTAL INFRAESTRUCTURA</b>			<b>\$ 1,400.00</b>
<b>Capacitación</b>	Curso de capacitación para instalación e implementación	1	\$400.00
<b>TOTAL CAPACITACIÓN</b>			<b>\$400.00</b>
<b>TOTAL GENERAL</b>			<b>\$1,834.50</b>

## **CAPITULO IV**

### **4 LA PROPUESTA**

#### **4.1 Procedimiento**

Se procederá con el estudio de la infraestructura a la empresa CONTINENTAL HOTEL S.A. ubicada en la ciudad de Guayaquil, el correspondiente análisis con el fin de poner en evidencia la condición actual en lo que respecta a la seguridad del firewall.

Se realizará un registro de la información observada, posterior a ello su interpretación y finalmente la elaboración de las conclusiones conforme al análisis de la información recabada.

Basado en los problemas identificados, los cuales no permiten los niveles de seguridad adecuados, se planteará la implementación de un firewall basado en open source que ayude y proporcione seguridad a la empresa.

Esta investigación se divide en 5 fases:

##### **4.1.1 Fase 1: Interpretar**

Para el levantamiento de la información se inicia con el análisis de lo siguiente:

- Situar la problemática actual basado en la seguridad.
- Aprendizaje en cuanto a un firewall.
- Investigación del software PfSense Community Edition: requerimientos de hardware, software y casos de éxito.

##### **4.1.2 Fase 2. Estudio in situ**

- Basado en el levantamiento de la información y el estudio de la topología de red.
- Estudio visual del estado físico de la red de la empresa.

- Estudio de los elementos positivos de la red de la empresa CONTINENTAL HOTEL S.A.
- Análisis de los requerimientos de integración con servidores de autenticación.
- Conclusiones acerca del estado de la red de la empresa.
- Capacitación en cuanto a la funcionalidad e implementación de firewall PfSense community edition.
- Estudio de compatibilidad con estaciones de trabajo, servicios y servidores.

#### **4.1.3 Fase 3. Planteamiento**

Ofrecer una solución de firewall que contribuya a fortalecer la seguridad informática de la red de la empresa basado en la definición de reglas de control de acceso al Internet, control de categorización de sitios webs a usuarios, servicios de VPN server y cliente.

#### **4.1.4 Fase 4: Pruebas de laboratorio e implementación**

Realizar las diferentes pruebas en ambiente de laboratorio utilizando la virtualización para medir el funcionamiento e integración del software firewall PfSense community edition, posteriormente se realizará la implementación en ambiente de producción paso a paso finalizando con las pruebas de funcionamiento de cada servicio del firewall.

#### **4.1.5 Fase 5: Seguimiento**

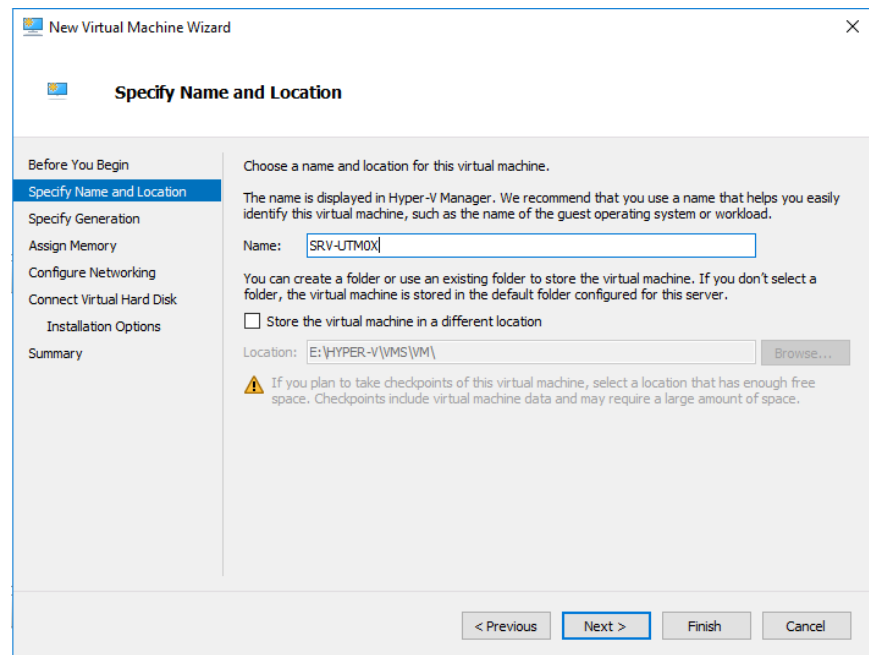
Posterior a la implementación, se procede con el monitoreo de cada uno de los servicios del firewall, reglas de acceso, control y usabilidad por parte del usuario final.

## 4.2 Proceso de Instalación

### 4.2.1 Preparación del equipo virtual

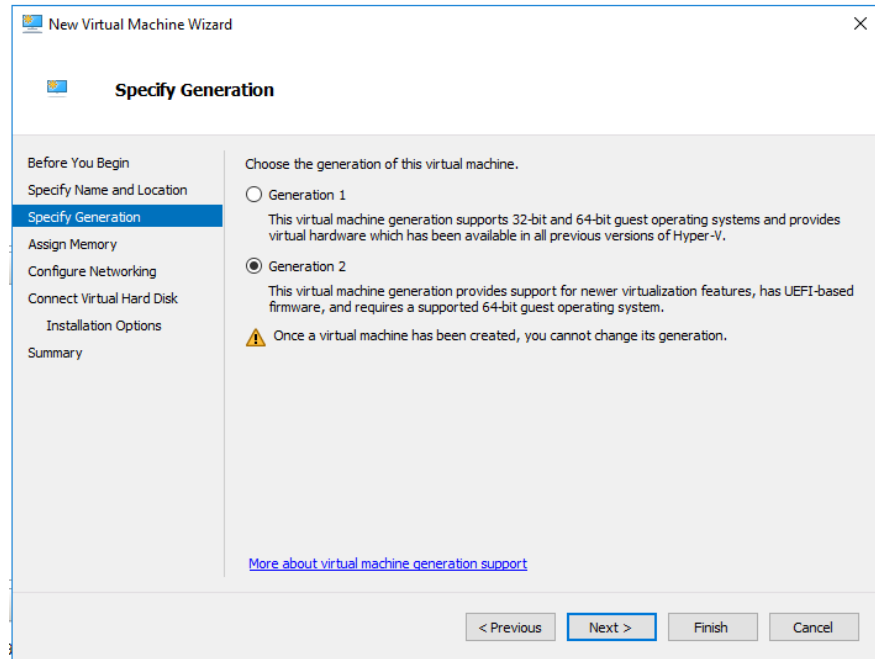
Se procede a la ejecución del asistente para crear un nuevo equipo virtual con ayuda del HyperVisor el cual viene integrado en versiones de Windows 10 o Windows Server 2012 R2.

En esta ventana del asistente se coloca en el nombre del equipo virtual con el cual será identificado dentro del administrador de equipos virtuales



Una vez se haya escrito el nombre del equipo virtual dar clic con el mouse en el botón **Next**.

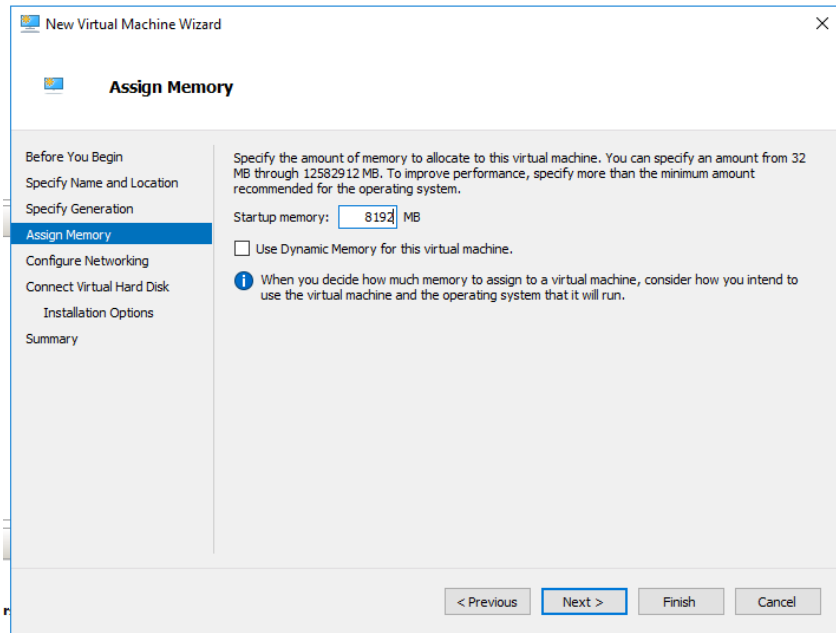
Escoger **Generation 2** ya que el sistema operativo que utiliza PfSense funciona bajo UEFI en una plataforma de 64 bits.



Hacer clic con el botón del mouse en el botón **Next**

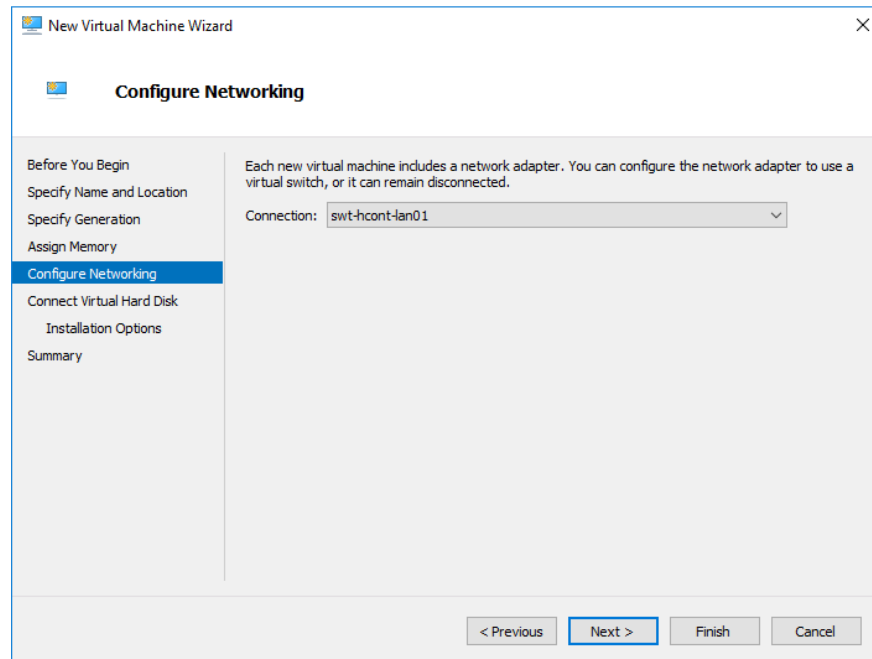
La asignación de memoria RAM dependerá del número de paquetes a instalar (más adelante) y el número de usuarios que pasarán a través del firewall, para este caso el equipo utilizará la cantidad de 8 GB de memoria RAM.





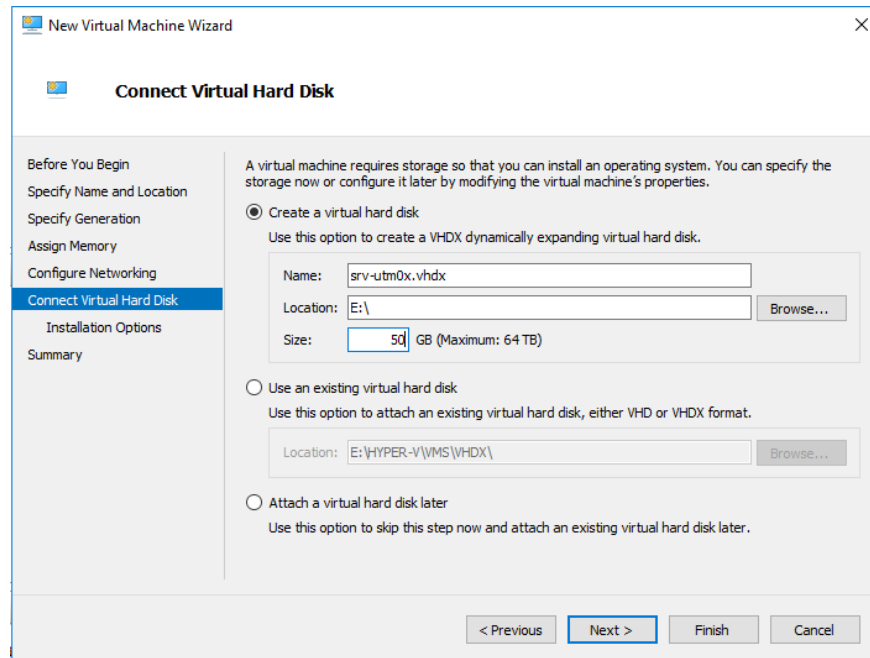
Hacer clic con el botón del mouse en el botón **Next**

En este siguiente paso se seleccionará una interface de red para el equipo, se escoge la interface de red que comunica con la red privada, más adelante se añadirán otra interface.



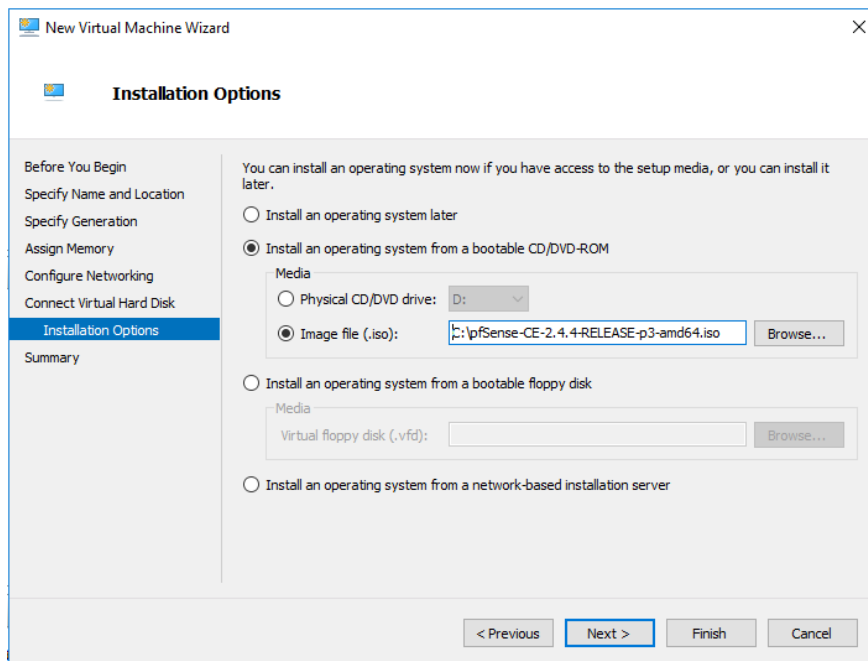
Hacer clic con el botón del mouse en el botón **Next**

En esta ventana se coloca la cantidad de espacio de almacenamiento de disco que utilizará el equipo virtual, como en este proyecto se va a utilizar reportes se requiere almacenamiento para los archivos logs, por tanto, se asigna la cantidad de 50 GB.



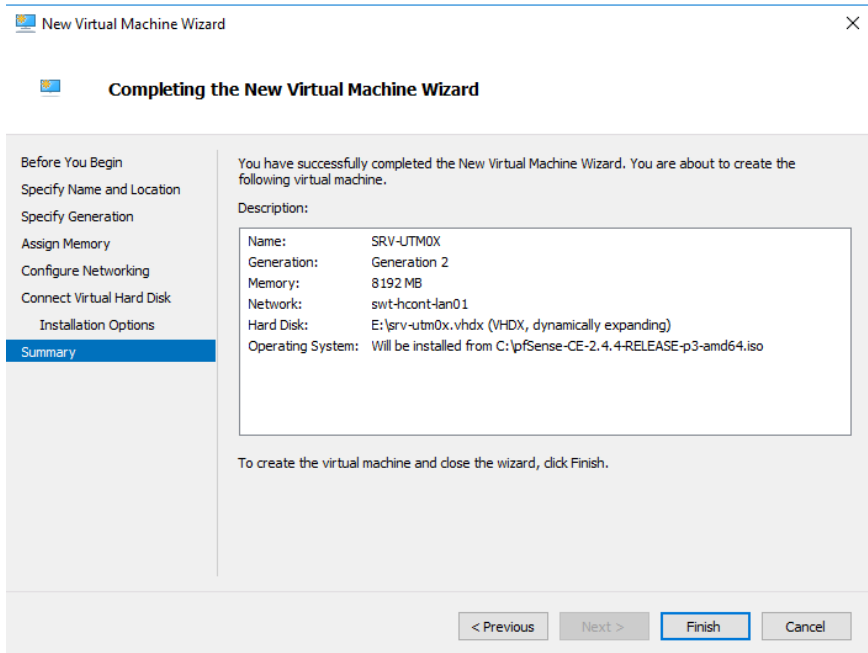
Hacer clic con el botón del mouse en el botón **Next**

En esta ventana, se puede asignar en medio de inicio, como la unidad de DVD o archivo en formato ISO que se utilizará como medio de instalación, en este caso se ha seleccionado el archivo ISO de instalación de PfSense.



Hacer clic con el botón del mouse en el botón **Next**

Al finalizar el asistente nos presentará un resumen de las características básicas del equipo virtual creado.

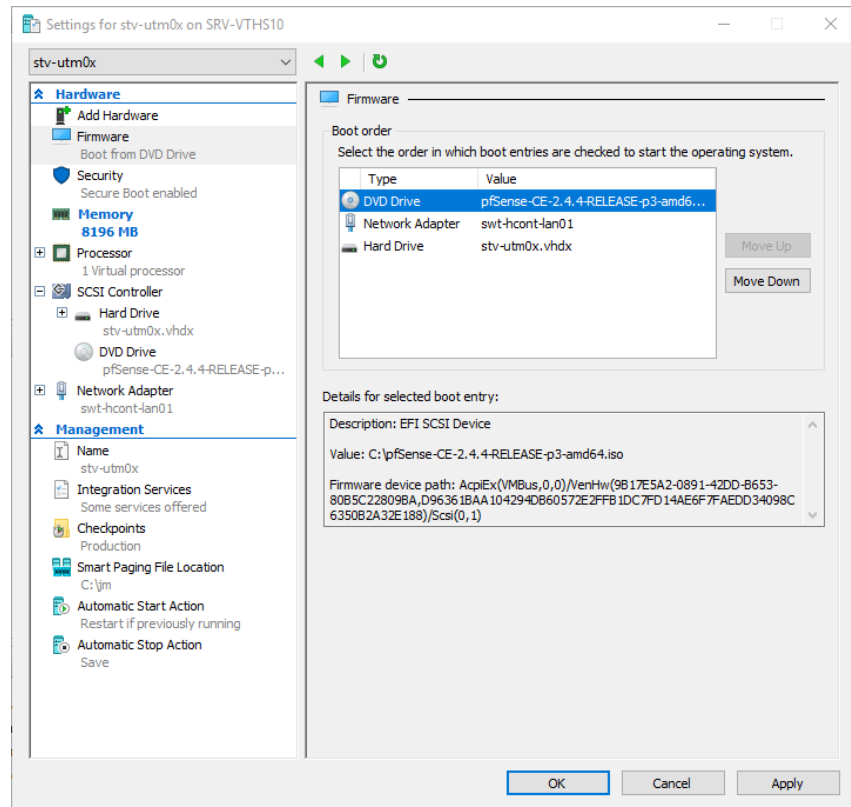


Hacer clic con el botón del mouse en el botón **Finish**.

## 4.2.2 Configuración del equipo virtual

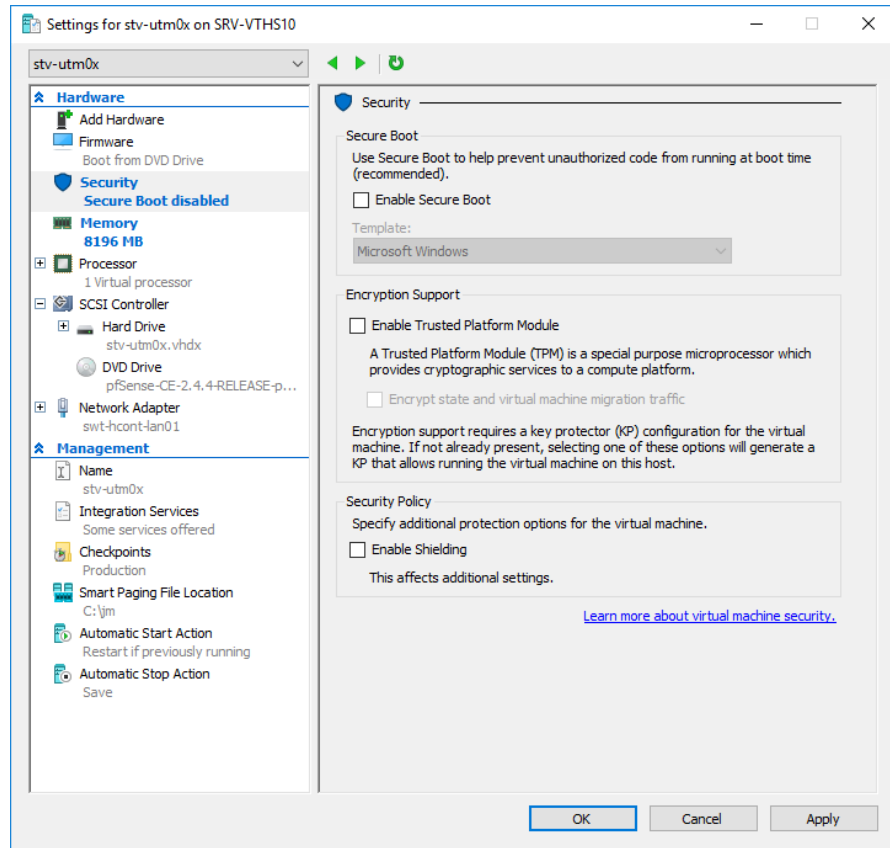
Se procede con la configuración del equipo virtual con el fin de afinar detalles que se deben tener en cuenta.

En esta ventana se debe confirmar que el equipo debe iniciar desde la unidad de DVD.



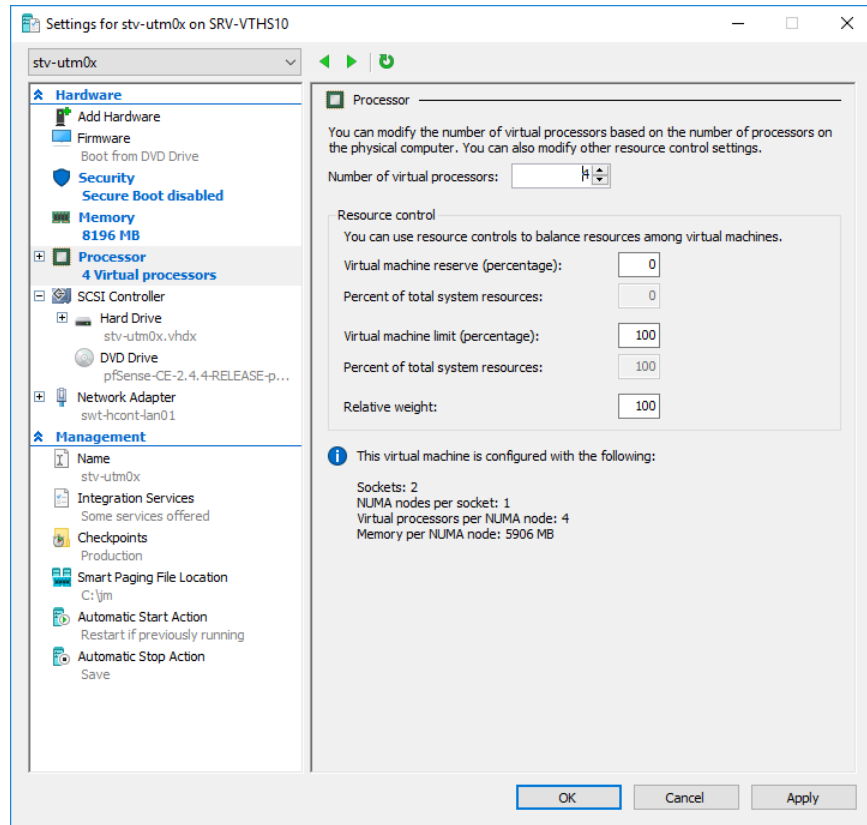
Hacer clic con el botón del mouse en el botón **Apply**.

En la opción de Security: Se debe deshabilitar el Secure Boot



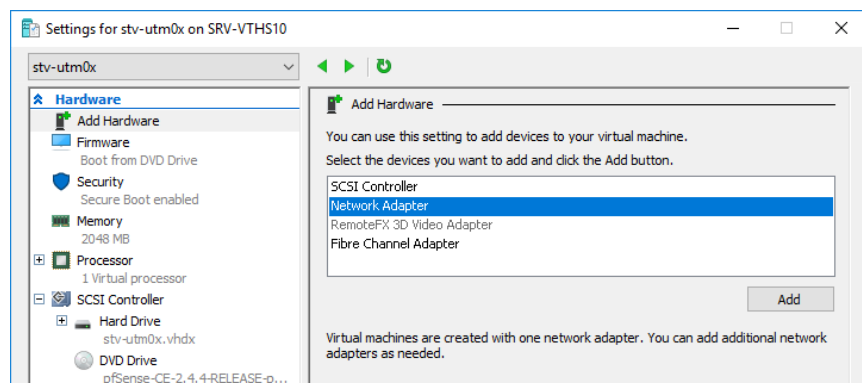
Hacer clic con el botón del mouse en el botón **Apply**.

En la opción de Processor: Configurar el número de procesadores virtuales, en ésta ocasión se coloca el número de 4.

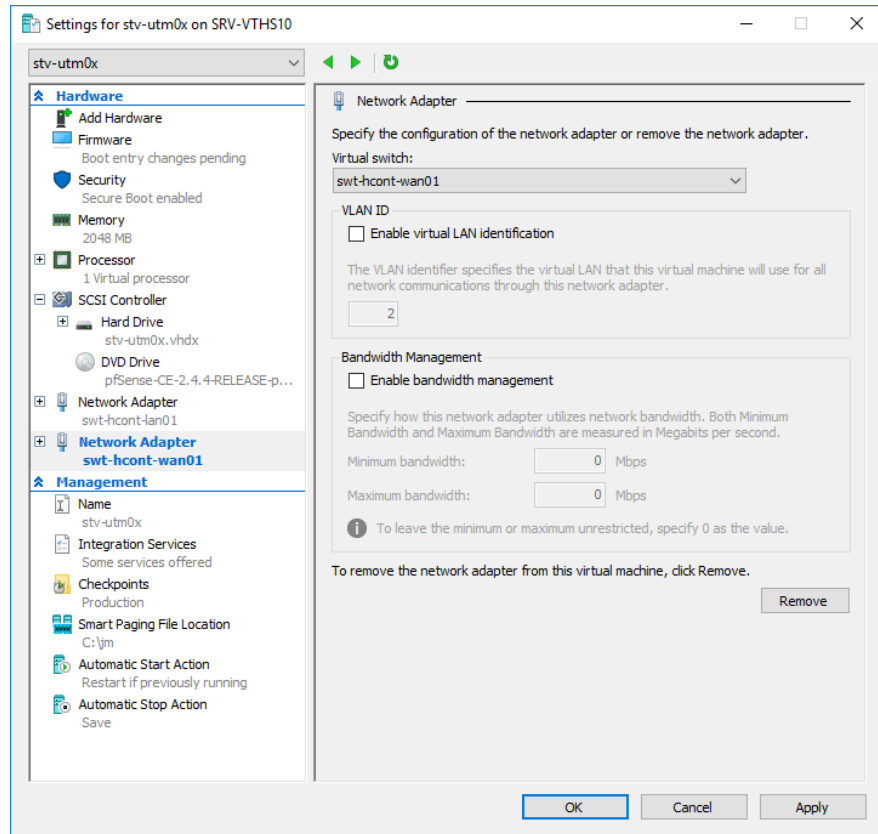


Hacer clic con el botón del mouse en el botón **Apply**.

En la opción de Network Adapter: Añadir una segunda interface de red la cual provee el servicio de internet.



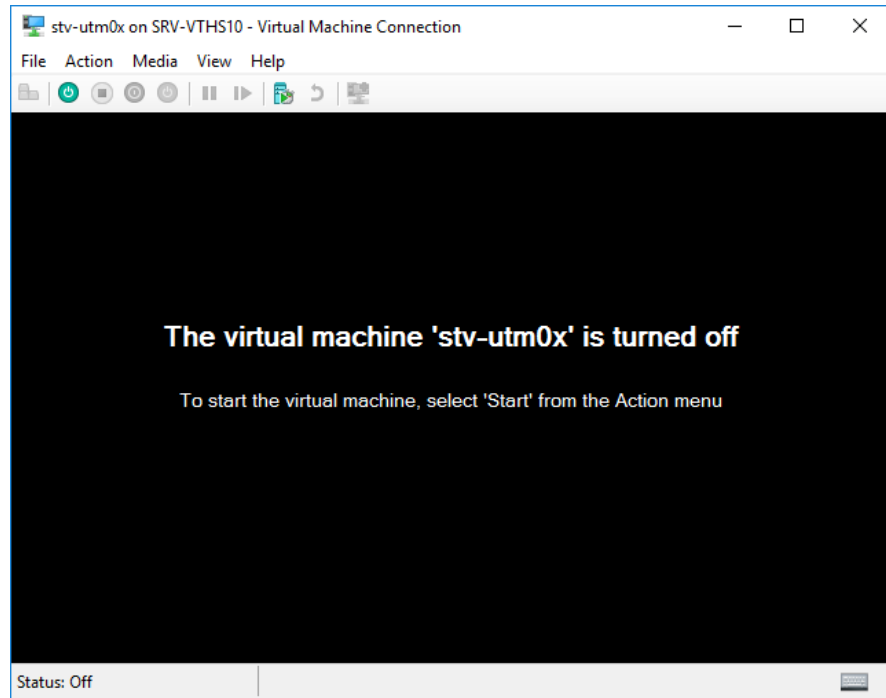
Una vez añadida la interface confirmar que en el panel del lazo izquierdo aparezca la segunda interface.



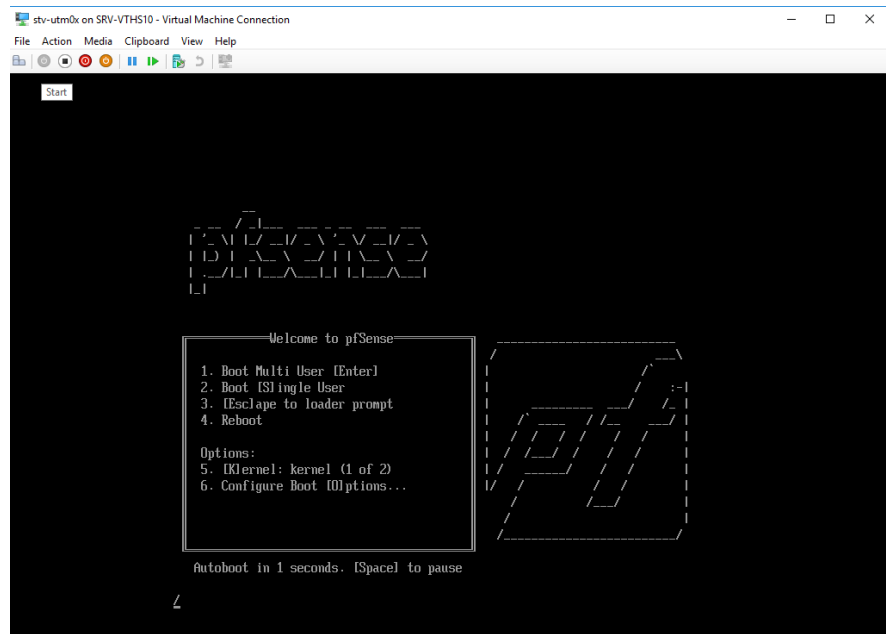
Hacer clic con el botón del mouse en el botón **Apply** y finalmente hacer clic con el botón del mouse en **OK**

### 4.2.3 Instalación de PfSense Community Edition

Una vez el equipo virtual se encuentra configurado, se procede a encenderlo utilizando el botón de **Power**.



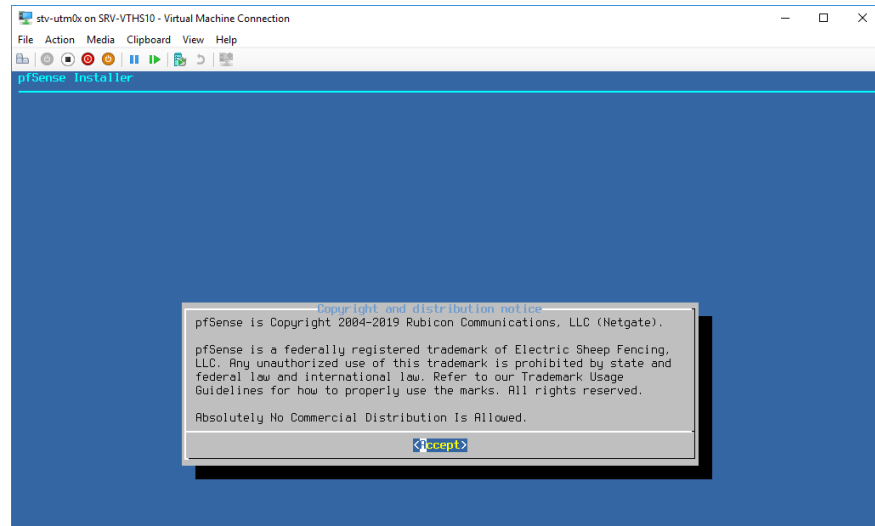
Aparecerá la ventana de inicio de programa de instalación de PfSense con diferentes opciones.



Presionar la tecla **Enter** para continuar.

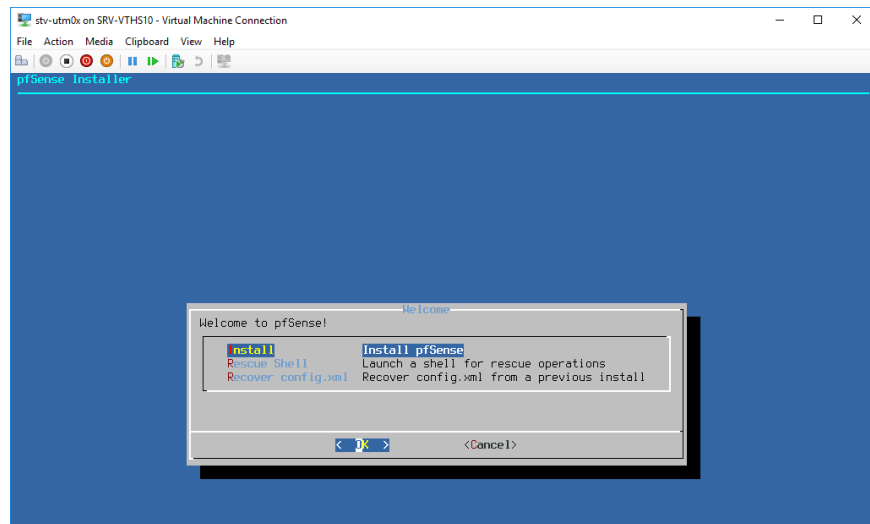


## Aceptar los términos y acuerdo de uso del software



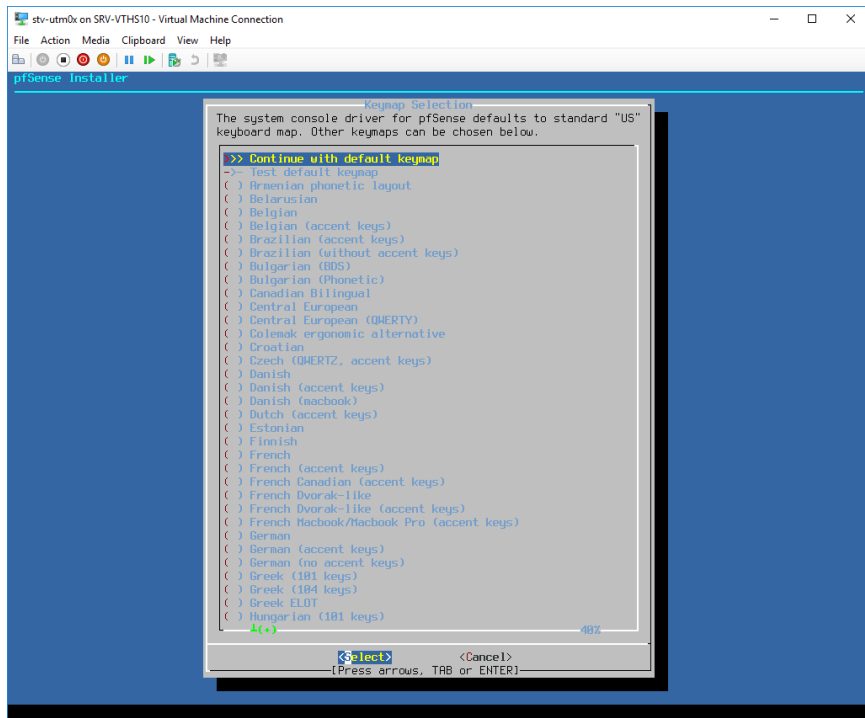
Con el teclado, presionar **Enter** sobre el botón de **Accept**.

En ésta pantalla de bienvenida a la instalación de PfSense, entre las 3 opciones que muestra se debe escoger la opción de **Install**.



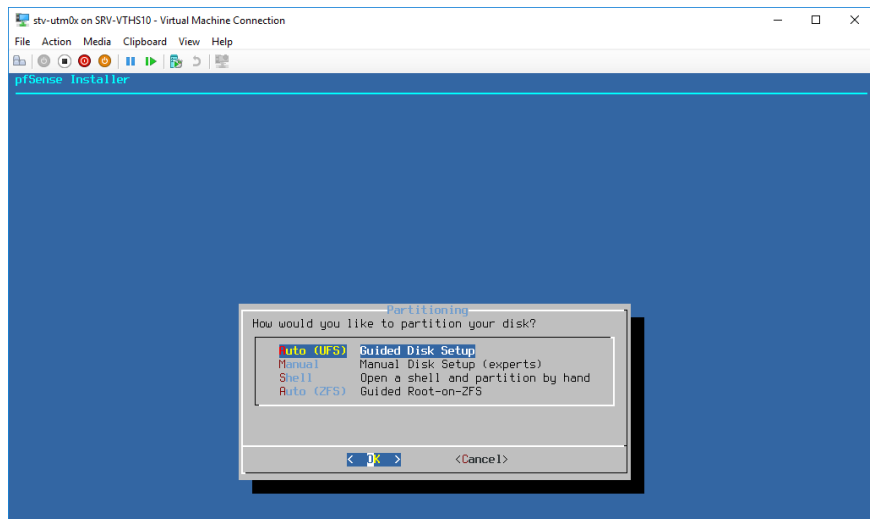
Con el teclado, presionar **Enter** sobre el botón de **OK**.

En ésta siguiente ventana se muestran los diferentes mapas de caracteres, escoger el default **keymap**



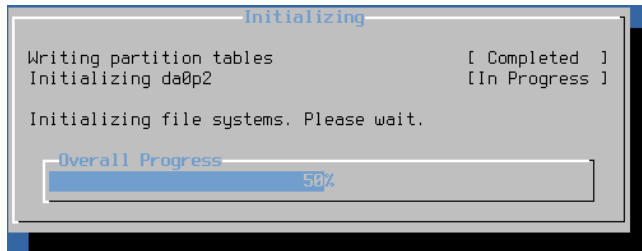
Con el teclado, presionar **Enter** sobre el botón de **Select**.

A continuación, se muestra las opciones de particionado de disco, para este caso escoger la opción de Auto (UFS) con esto se consigue que el asistente de instalación realice cada una de las particiones según el espacio disponible.

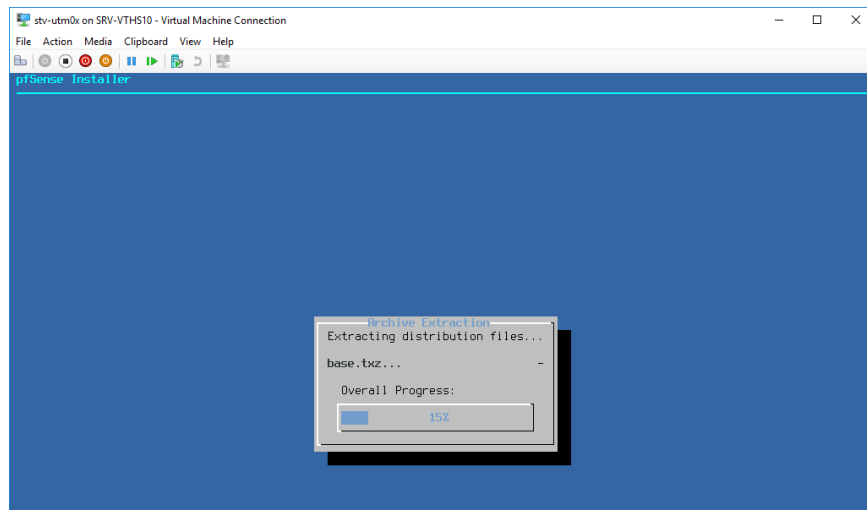


Con el teclado, presionar **Enter** sobre el botón de **OK**.

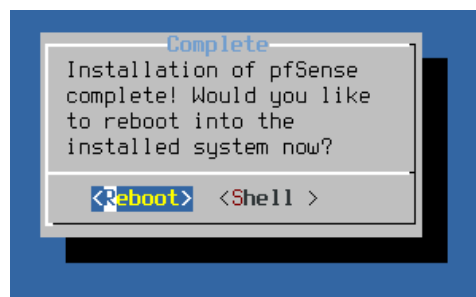
### Progreso del proceso de particionado de disco



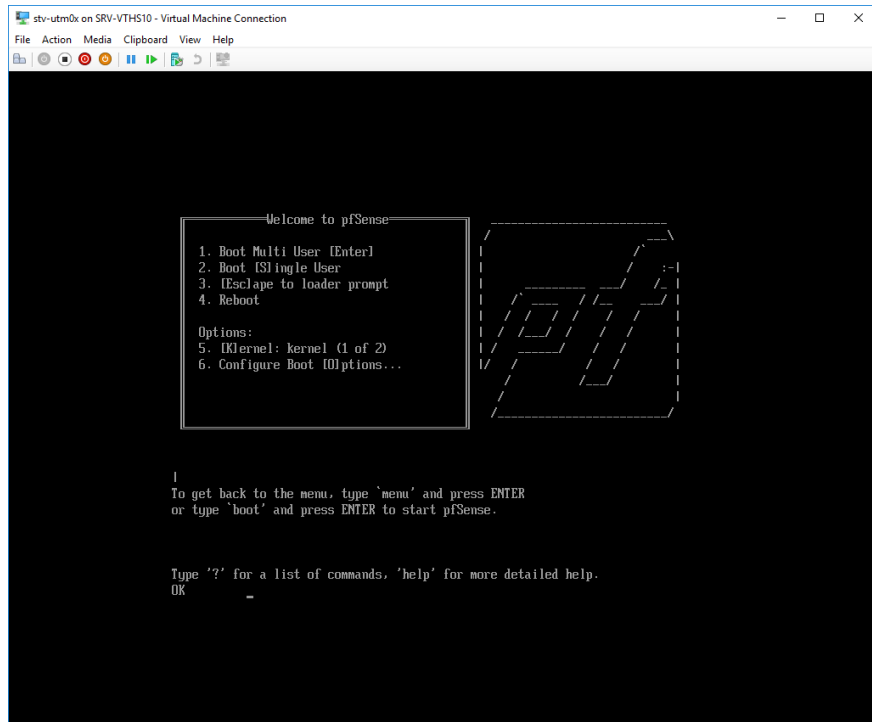
En esta ventana nos muestra el progreso de la instalación de PfSense



Una vez concluida la instalación, con el teclado, presionar **Enter** sobre el botón de **Reboot**.



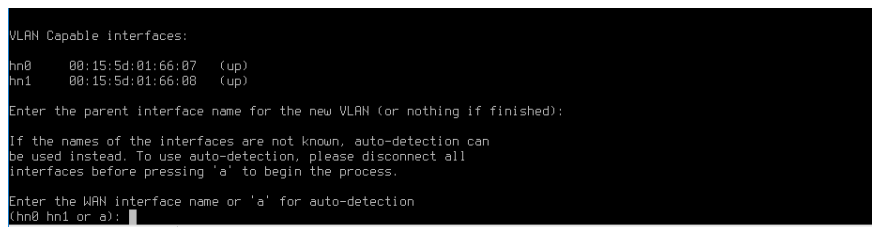
Luego de reinicio del equipo virtual, aparecerá la pantalla de inicio de PfSense, en este caso no presionamos ninguna tecla ya que el inicio es automático.



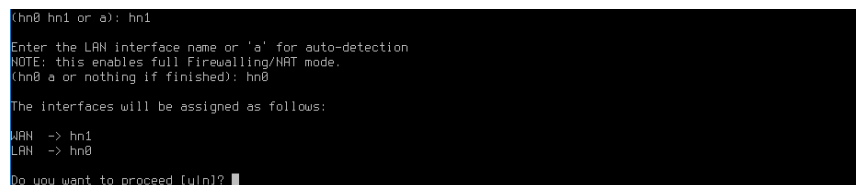
Como parte de la configuración inicial, se debe especificar la interface WAN y LAN respectivamente.

hn0 = WAN

hn1 = LAN

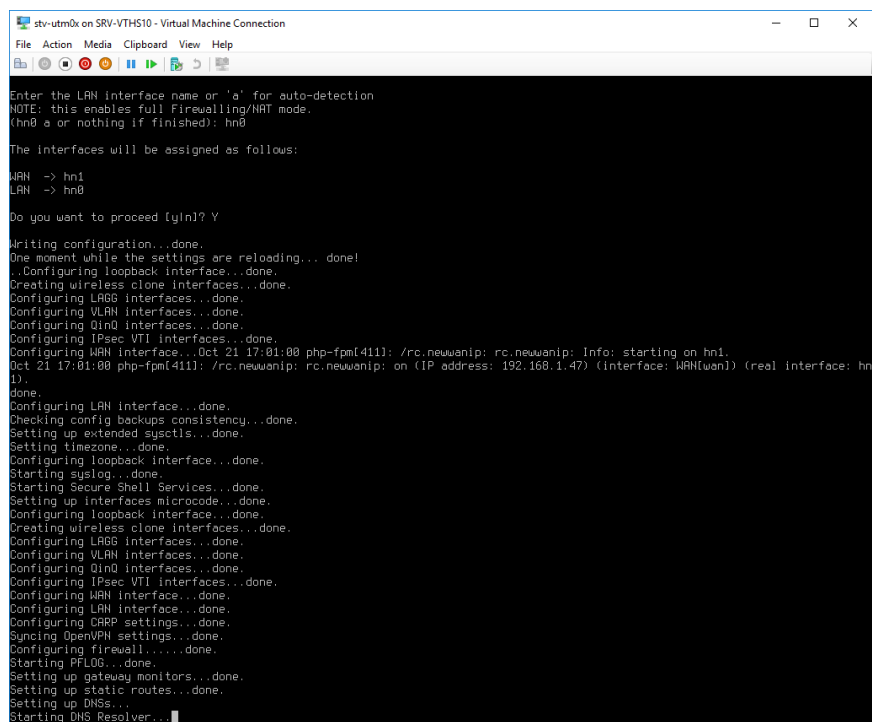


A continuación, se solicita la confirmación para proceder a aplicar los cambios en la asignación de las interfaces.



Con el teclado presionar la tecla **y**, luego presionar la tecla **Enter**, luego de ello se requerirá que ingresemos la dirección IP y la máscara de subred que tendrá tanto la interface LAN, así como la WAN.

En esta pantalla nos muestra cada uno de los servicios que se encuentran iniciando en consola, es importante estar pendiente de que no existan errores.



```
str-utm0x on SRV-VTHS10 - Virtual Machine Connection
File Action Media Clipboard View Help
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn0 a or nothing if finished): hn0

The interfaces will be assigned as follows:

WAN -> hn1
LAN -> hn0

Do you want to proceed [y/n]? Y
Writing configuration...done.
One moment while the settings are reloading... done!
..Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAGB interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring IPsec VTI interfaces...done.
Configuring WAN interface...Oct 21 17:01:00 php-fpm[411]: /rc.newwanip: rc.newwanip: Info: starting on hn1.
Oct 21 17:01:00 php-fpm[411]: /rc.newwanip: rc.newwanip: on (IP address: 192.168.1.47) (interface: WAN(wan)) (real interface: hn
1).
done.
Configuring LAN interface...done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting suslog...done.
Starting Secure Shell Services...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAGB interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring IPsec VTI interfaces...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Configuring ARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall...done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...
```

A continuación, se nos preguntará si deseamos habilitar el servicio de DHCP server en la interface LAN, en este caso no aplica ya que dentro de la infraestructura existe ya un equipo dentro de la red que provee el servicio de DHCP.

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 130.100.1.253/24
You can now access the webConfigurator by opening the following URL in your web browser:
http://130.100.1.253/

Press <ENTER> to continue.
```

Con el teclado presionar la tecla **n** y luego presionar la tecla **Enter**.

Para finalizar con el inicio del servidor firewall PfSense, nos muestra la pantalla de inicio con las diferentes opciones.

```
Press <ENTER> to continue.
Hyper-V Virtual Machine - Netgate Device ID: 0c37a1237a2faae8970a

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

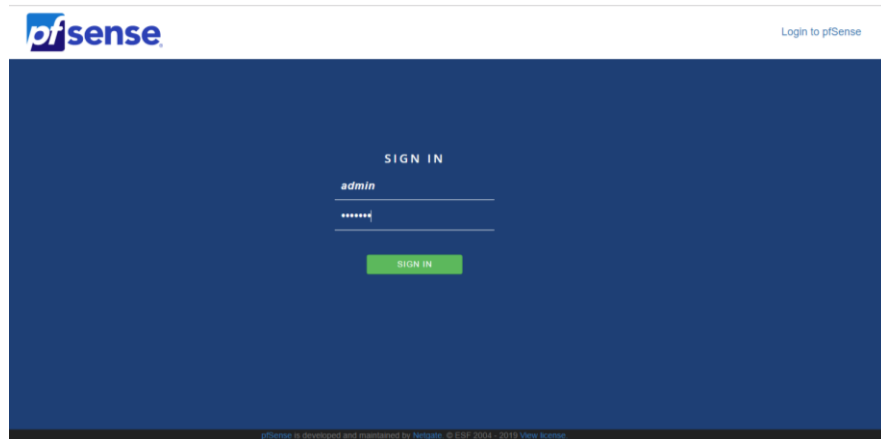
WAN (wan)      -> hn1      -> v4/DHCP4: 192.168.1.47/22
LAN (lan)      -> hn0      -> v4: 130.100.1.253/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

Una vez llegado a este punto las siguientes configuraciones a realizar se harán a través del **Web Configurator** de PfSense.

#### 4.2.4 PfSense Community Edition-Primeros pasos

Para ingresar al Web Configurator ingresamos en el navegador web la dirección IP que le asignamos a la interface LAN al momento de la instalación.



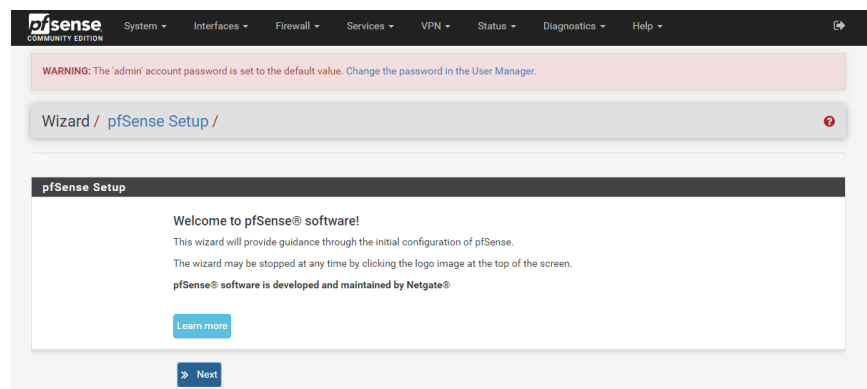
Por defecto las credenciales locales son las siguientes:

Usuario: admin

Contraseña: pfsense

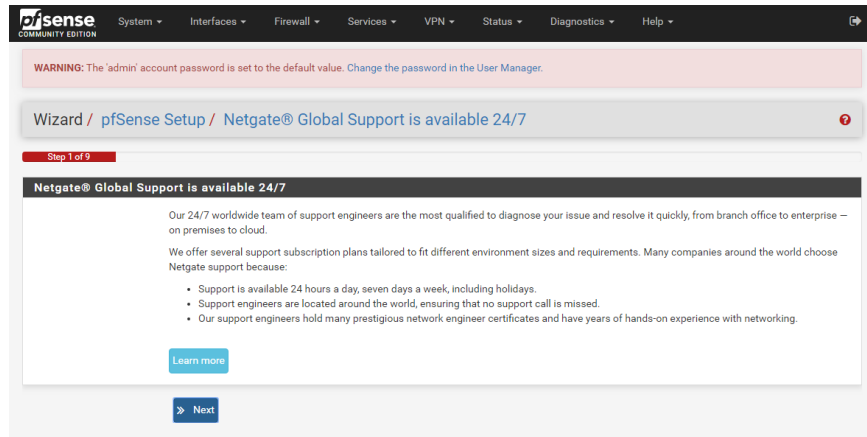
Presionar con el mouse en el botón **SIGN IN**

A continuación, aparecerá el asistente de configuración (wizard) en la cual nos requerirá cierta información adicional.



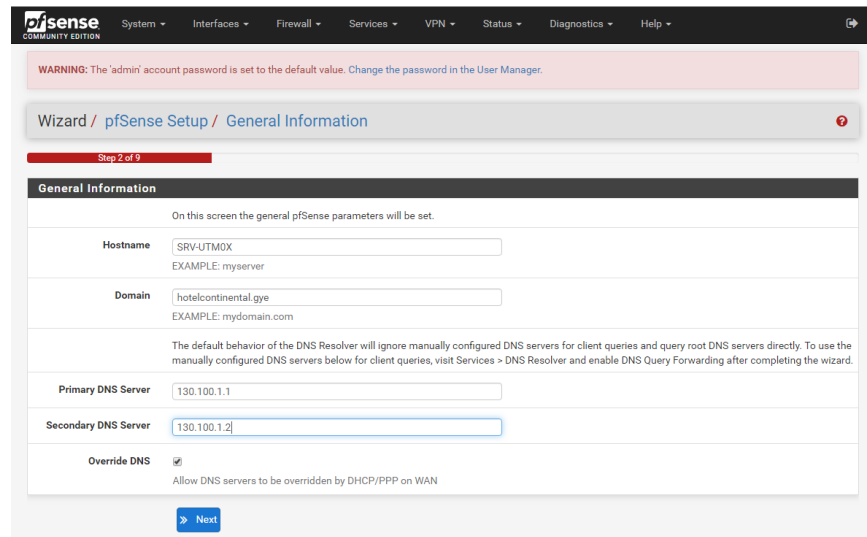
Presionar con el mouse en el botón **Next**

En la siguiente pantalla nos comunica acerca de soporte de PfSense a través de Netgate y se nos invita a leer más acerca del servicio.



Presionar con el mouse en el botón **Next**

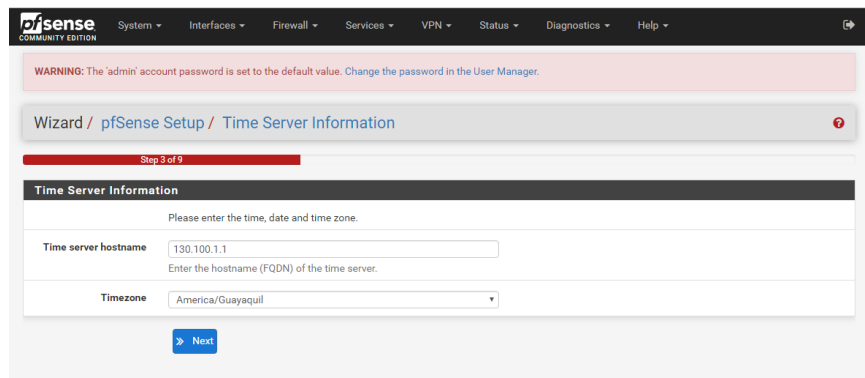
En el siguiente paso se debe ingresar el nombre del servidor (Hostname), el dominio y la dirección IP de los servidores DNS tanto primario como secundario.



Presionar con el mouse en el botón **Next**



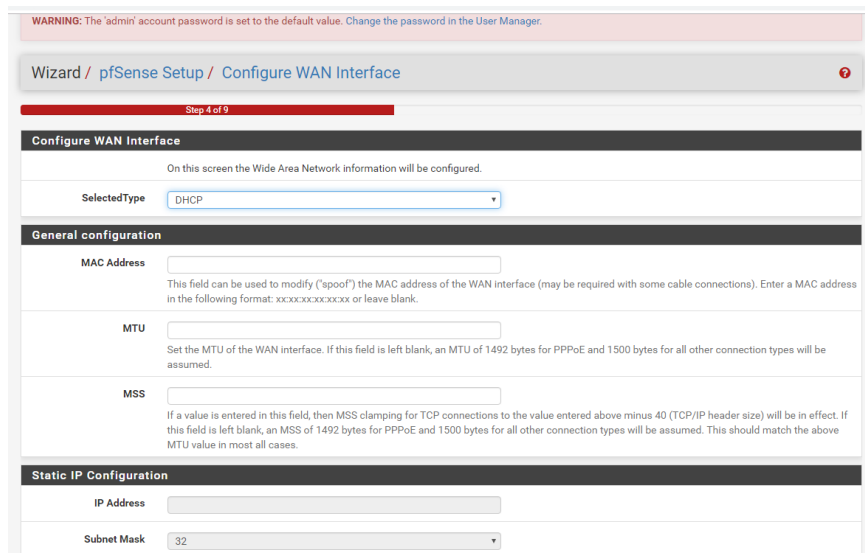
Como siguiente paso solicita la dirección IP del equipo que provea servicios de NTP (Network Time Protocol).



The screenshot shows the pfSense web interface at the 'Time Server Information' step of the setup wizard. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The breadcrumb trail reads 'Wizard / pfSense Setup / Time Server Information'. A progress bar indicates 'Step 3 of 9'. The main heading is 'Time Server Information' with a sub-heading 'Please enter the time, date and time zone.' The form contains three fields: 'Time server hostname' with the value '130.100.1.1', 'Timezone' with a dropdown menu set to 'America/Guayaquil', and a 'Next' button at the bottom.

Una vez ingresado lo requerido, presionar con el mouse en el botón **Next**

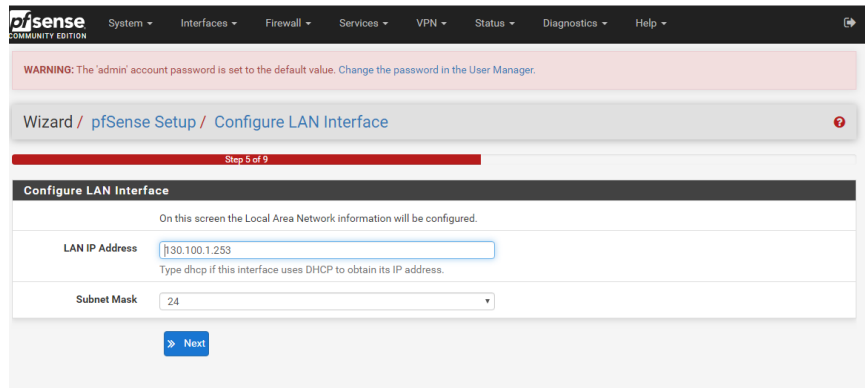
En este paso se requerirá confirmar la dirección IP de la interface WAN, en caso de que existan cambios, entonces realizarlo en esta pantalla.



The screenshot shows the pfSense web interface at the 'Configure WAN Interface' step of the setup wizard. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the menu is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The breadcrumb trail reads 'Wizard / pfSense Setup / Configure WAN Interface'. A progress bar indicates 'Step 4 of 9'. The main heading is 'Configure WAN Interface' with a sub-heading 'On this screen the Wide Area Network information will be configured.' The form contains several sections: 'SelectedType' with a dropdown menu set to 'DHCP', 'General configuration' with fields for 'MAC Address', 'MTU', and 'MSS', and 'Static IP Configuration' with fields for 'IP Address' and 'Subnet Mask' set to '32'.

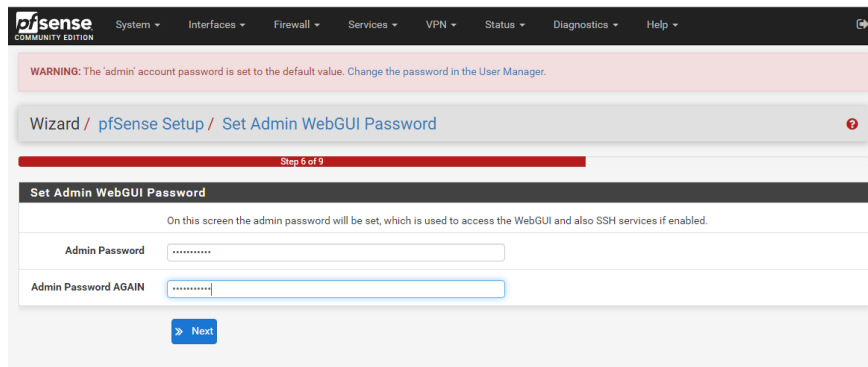
Presionar con el mouse en el botón **Next**

En el siguiente paso asimismo se nos pide confirmar la dirección IP de la interface LAN, en caso de que existan cambios, entonces realizarlo en esta pantalla.



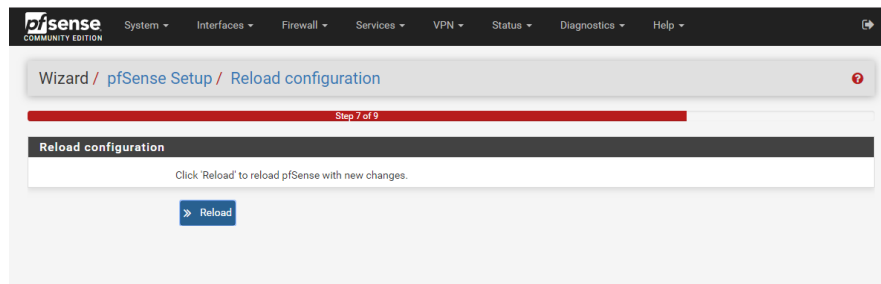
Presionar con el mouse en el botón **Next**

En el siguiente paso se requiere de forma obligatoria cambiar la contraseña de administrador por defecto por una nueva.

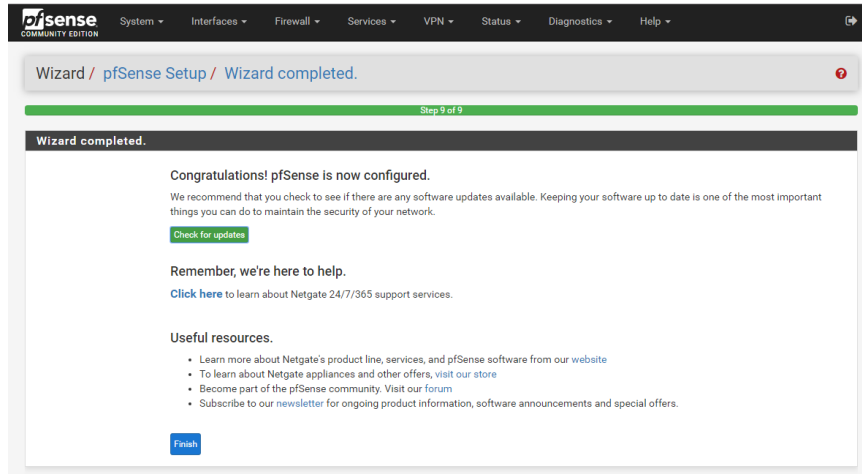


Presionar con el mouse en el botón **Next**

Presionar con el mouse en el botón de **Reload**.

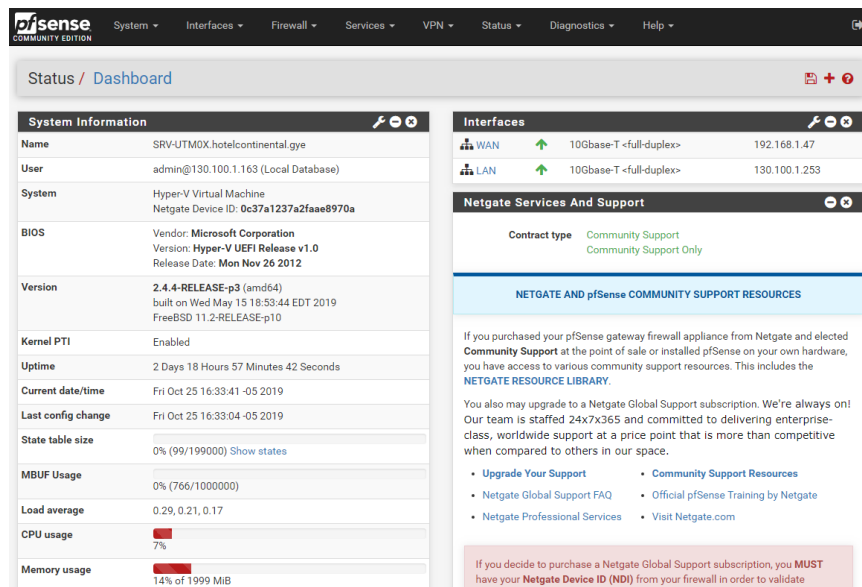


Es recomendable realizar un **check for updates** con el fin de instalar las últimas correcciones o mejoras.



Presionar con el mouse en el botón de **Finish**.

Una vez finalizado el asistente inicial se muestra la página web de inicio de PfSense de tipo **Dashboard**.

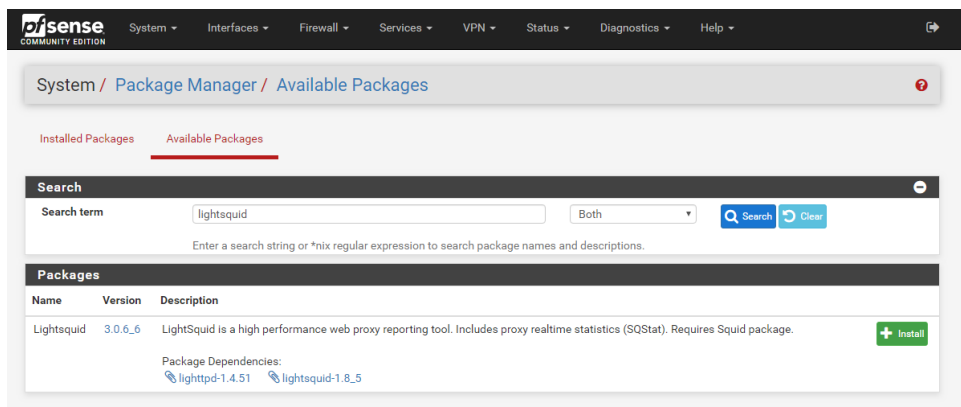


### 4.3 Instalación de paquetes adicionales en PfSense Community Edition

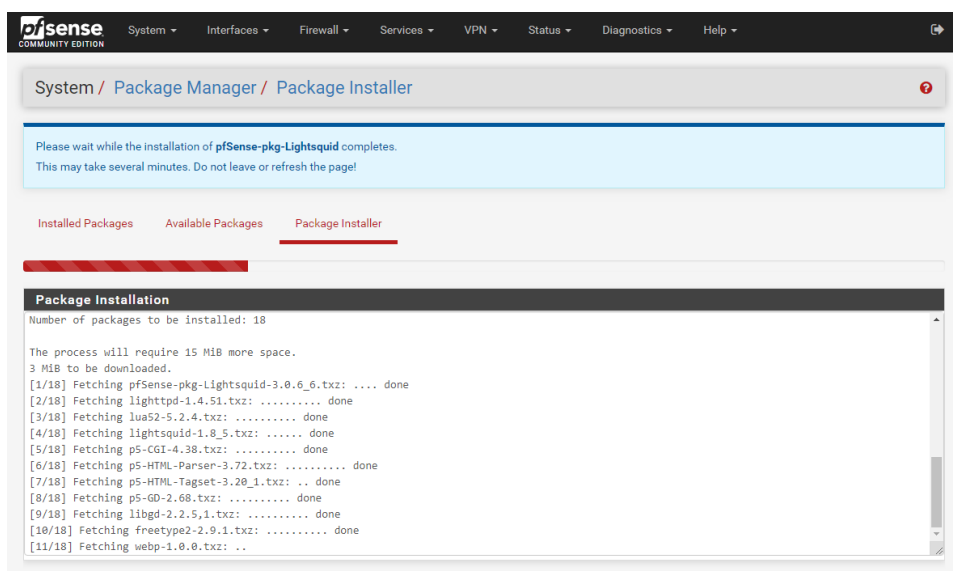
PfSense community edition requiere paquetes adicionales según las necesidades que requiera la red a controlar.

El primer paquete a instalar es el Lightsquid el cual sirve para reportes de uso del servicio de internet por parte de los usuarios.

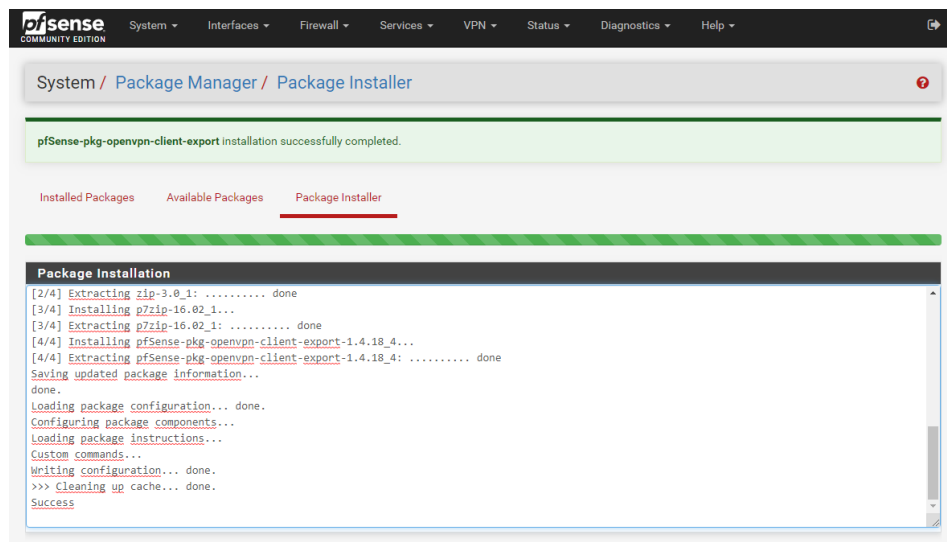
La ruta para realizar este paso es ir al menú de **SYSTEM>PACKAGE MANAGER>AVAILABLEPACKAGES**, escribir en el campo de search term el nombre del paquete y realizar la búsqueda.



Con el mouse hacer clic en el botón **Install** y a continuación aparece el progreso de instalación del paquete.



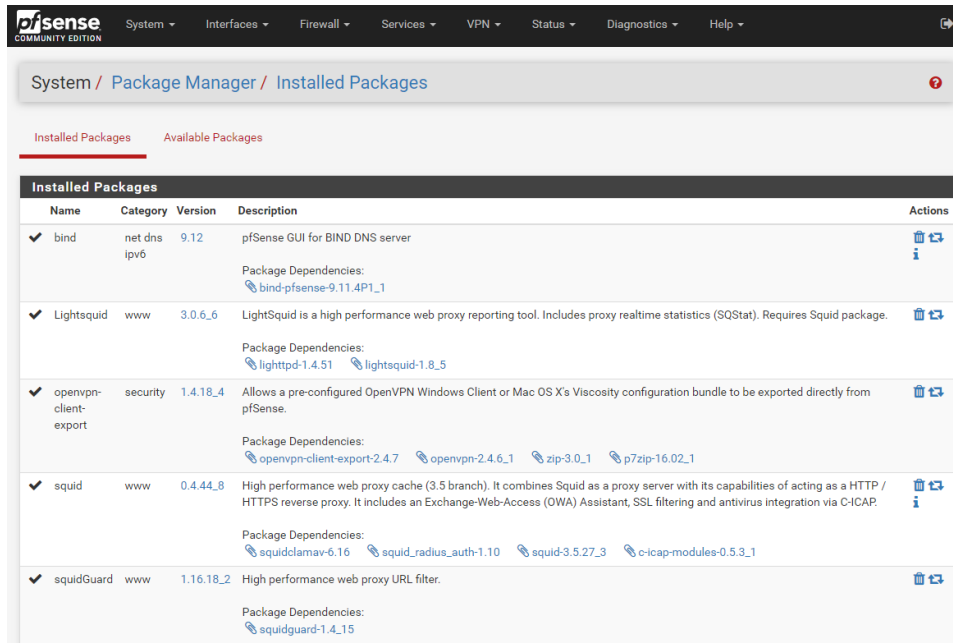
Una vez finalizada la instalación del paquete debe aparecer en la última línea del detalle de instalación la palabra **Success**



Adicionalmente se debe instalar los siguientes paquetes:

- Squid
- SquidGuard
- Openvpn-client-export
- Bind

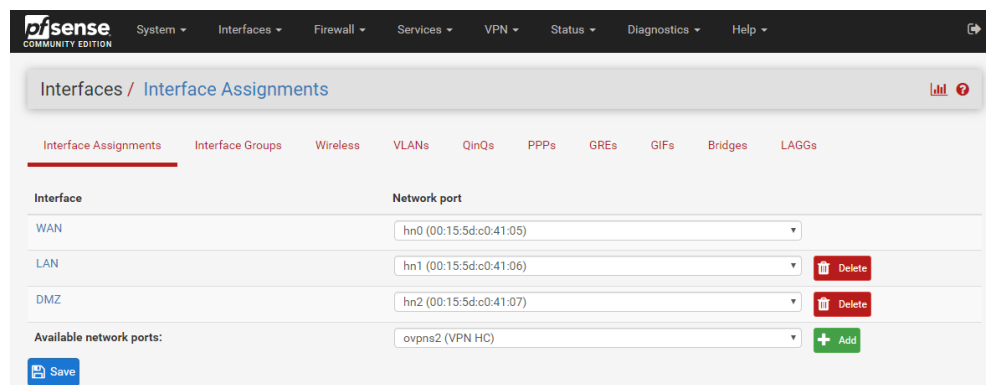
Una vez finalizada la instalación de los paquetes requeridos, se debe mostrar como la siguiente pantalla la instalación de los mismos en la pestaña de **Installed Packages**.



## 4.4 Interfaces de red

Anteriormente ya se ha ingresado el direccionamiento IP de la interface WAN y LAN sin embargo se ha añadido una interface adicional cuyo nombre es DMZ que significa zona desmilitarizada. CONTINENTAL HOTEL S.A. tiene en su zona desmilitarizada un equipo virtual con servicios web donde se encuentra publicada el sitio de facturación electrónica para clientes y además un servidor FTP.

Se ingresa en el menú de **Interfaces>Interface Assignments** Como se ha agregado la interface DMZ se la asocia con la tarjeta de red de nombre **hn2**.



En el menú de **Interfaces>DMZ** se procede con la configuración de la dirección IP y máscara

Interfaces / DMZ (hn2)

**General Configuration**

Enable  Enable interface

Description DMZ  
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxxxx  
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxx:xxx:xxx:xxx:xxx:xxx or leave blank.

MTU  
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS  
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)  
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

IPv4 Address 130.100.3.2 / 29

#### 4.5 Configuración de NAT – Port forward

Como parte de la infraestructura de red CONTINENTAL HOTEL S.A. posee de parte del ISP (Proveedor de internet) un segmento de direcciones IP's públicas con el fin de publicar los diferentes servicios tales como correo electrónico, web, ftp, VPN. A continuación, se muestra el procedimiento para realizar NAT.

En el menú nos dirigimos a: **Firewall/NATPort/Forward**

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

**Rules**

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
-----------	----------	----------------	--------------	---------------	-------------	--------	-----------	-------------	---------

Add Add Delete Save Separator

Hacemos clic con el mouse sobre el botón **Add**.

Ingresamos los datos solicitados en el siguiente formulario.

Firewall / NAT / Port Forward / Edit

### Edit Redirect Entry

**Disabled**  Disable this rule

**No RDR (NOT)**  Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface** WAN  
Choose which interface this rule applies to. In most cases "WAN" is specified.

**Protocol** TCP  
Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source** [Display Advanced](#)

**Destination**  Invert match. WAN address  
Type: Address/mask

**Destination port range** Other From port Custom To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP**  
Enter the internal IP address of the server on which to map the ports.  
e.g.: 192.168.1.12

**Redirect target port** Other Port Custom  
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be

**Description**  
A description may be entered here for administrative reference (not parsed).

**No XMLRPC Sync**  Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection** Use system default

**Filter rule association** Add associated filter rule  
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

[Save](#)

Para finalizar hacer clic con el mouse sobre el botón de **Save**

**Nota: Este procedimiento se repite para cada servicio a publicar.**

Una vez ingresados todo lo requerido quedaría como lo muestra la siguiente imagen.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	192.168.1.12	prtFtp	130.100.3.6	prtFtp	ftp hcont	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	*	*	192.168.1.12	80 (HTTP)	130.100.3.5	80 (HTTP)	Facelect to dmz	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	LAN net	*	*	80 (HTTP)	130.100.1.254	3128	Redirect http to proxy	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.30.1	80 (HTTP)	Wan to Web Server	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	21 (FTP)	10.10.30.1	21 (FTP)	Wan to FTP Server	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	*	*	192.168.1.12	443 (HTTPS)	130.100.1.13	443 (HTTPS)	Servidor de Microsoft Exchange	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/>	WAN	TCP	*	*	192.168.1.12	25 (SMTP)	130.100.1.13	25 (SMTP)	Mail SMTP Exchange Server	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

Legend  
▶ Pass  
🔗 Linked rule

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)



**Nota: Por privacidad, en este documento se ha marcado con rojo las direcciones IP's publicas utilizadas.**

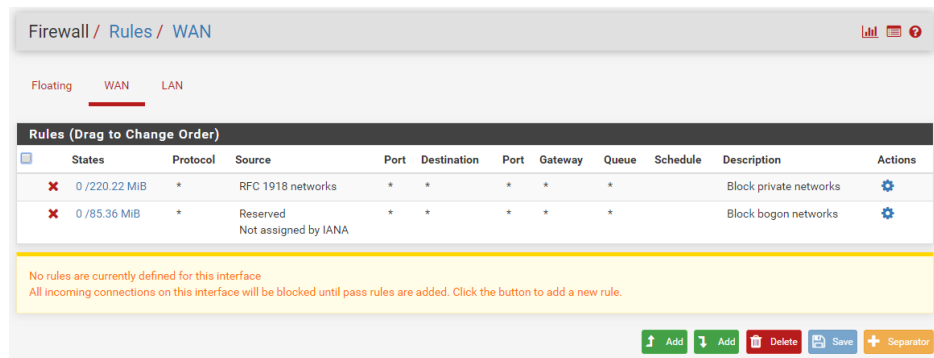
## 4.6 Reglas de Acceso

En PfSense las reglas se acceso se dividen en 4 apartados:

Las reglas aplicadas a la red WAN, las que aplican a la red LAN, a la DMZ y por ultimo las reglas de acceso de la VPN.

La opción a utilizar es en el menú: **FIREWALL\RULES\WAN**

### Reglas aplicadas a la red WAN



Firewall / Rules / WAN

Floating **WAN** LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 /220.22 MiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
0 /85.36 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑ Add ↓ Add 🗑️ Delete 💾 Save ➕ Separator

Hacer clic con el mouse sobre el botón **Add**.

En el siguiente formulario se solicita información sobre la interface, protocolo, dirección IP /host de origen con su respectivo puerto, IP/host de destino con su respectivo puerto y una descripción en la cual se explique el motivo de la regla.

Firewall / Rules / Edit

### Edit Firewall Rule

**Action**    
 Choose what to do with packets that match the criteria specified below.   
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule   
 Set this option to disable this rule without removing it from the list.

**Interface**    
 Choose the interface from which packets must come to match this rule.

**Address Family**    
 Select the Internet Protocol version this rule applies to.

**Protocol**    
 Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match.   /

[Display Advanced](#)   
 The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination**

**Destination**  Invert match.   /

**Destination Port Range**       
 From Custom To Custom   
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log**  Log packets that are handled by this rule   
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

[Save](#)

Al finalizar con el botón de mouse hacer clic sobre el botón **Save**.  
 Para el caso de la infraestructura de CONTINENTAL HOTEL S.A. se han agregado las siguientes reglas en la interface WAN.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN DMZ OpenVPN

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0 / 0 B	IPv4 TCP	LAN net	*	130.100.1.254	3128	*	none		NAT Redirect http to proxy	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 2 / 102.17 GiB	IPv4 TCP	*	*	130.100.1.13	443 (HTTPS)	*	none		NAT Servidor de Microsoft Exchange	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 5 / 33.47 GiB	IPv4 TCP	*	*	130.100.1.13	25 (SMTP)	*	none		NAT Mail SMTP Exchange Server	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 0 / 161.85 MiB	IPv4 UDP	*	*	WAN address	53 (DNS)	*	none		Consultas al DNS desde Internet	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 0 / 1.85 GiB	IPv4 TCP	*	*	130.100.3.5	80 (HTTP)	*	none		NAT Facelect to dmz	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 0 / 37.75 MiB	IPv4 TCP	*	*	130.100.3.6	prtFtp	*	none		NAT ftp hcont	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>
<input type="checkbox"/> ✓ 0 / 31.97 GiB	IPv4 UDP	*	*	WAN net	1195	*	none		OpenVPN VPN del Hotel Continental wizard	<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

## 4.6.1 Reglas aplicadas a la red LAN

Basado en lo anterior, el procedimiento para crear cada regla es el mismo, solo que ésta vez aplicada a la red **LAN**.

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
4 / 1.62 GiB	*	*	*	LAN Address	80 22	*	*	*	Anti-Lockout Rule		
0 / 976.43 MiB	IPv4 TCP/UDP	*	*	WebBolivariano	80 - 443	*	none	*	bolivariano		
0 / 1.49 GiB	IPv4 TCP/UDP	*	*	Bguay	*	*	none	*	bankguay		
52 / 222.91 GiB	IPv4 TCP/UDP	Out_Total	*	*	*	*	none	*	Internet Out-Total		
0 / 1.20 GiB	IPv4 TCP	e_rec_040	*	*	Spotify_ ports	*	none	*	Computador de recepción - música ambiental la canoa		
0 / 0 B	IPv4 UDP	LAN net	*	This Firewall	53 (DNS)	*	none	*	Consultas al DNS del PFSENSE		
190 / 704.94 GiB	IPv4 TCP	LAN net	*	This Firewall	3128	*	none	*	Lan to ProxyFilter		
0 / 1.05 MiB	IPv4 ICMP	*	*	*	*	*	none	*	Ping en lan		
0 / 1.05 MiB	IPv4 ICMP	*	*	*	*	*	none	*	Ping en lan		
90 / 2.28 GiB	IPv4 UDP	130.100.1.1	*	*	53 (DNS)	*	none	*	Salida a consultas DNS		
0 / 0 B	IPv4 TCP	LAN net	*	This Firewall	7445	*	none	*	ProxyReport		
0 / 0 B	IPv4 TCP	LAN net	*	This Firewall	23 (Telnet)	*	none	*	Lan to TelNet		
0 / 57.07 MiB	IPv4 *	LAN net	*	130.100.2.0/24	*	*	none	*	Acceso total Hotel Bodesur		
Reglas Servidores											
0 / 0 B	IPv4 TCP	epoServer	*	McAfee	*	*	none	*	Actualizacion de Epo Server		
0 / 192 KiB	IPv4 UDP	Ip_DVR	*	*	123 (NTP)	*	none	*	Sincroniza tiempo DVR		
12 / 95.24 GiB	IPv4 TCP	130.100.1.13	*	*	25 (SMTP)	*	none	*	Salida smtp srv-mail04		
31 / 1.05 GiB	IPv4 UDP	DC_internal	*	*	53 (DNS)	*	none	*	Dns from DC		
0 / 38 KiB	IPv4 UDP	DC_internal	*	*	123 (NTP)	*	none	*	Ntp sync from dc		
0 / 123.87 MiB	IPv4 TCP	LAN net	*	DMZ net	80 (HTTP)	*	none	*	lan to dmz		
Excepciones para usuarios											

## 4.6.2 Reglas aplicadas a la red DMZ

Al tratarse de una zona desmilitarizada se aplicarán reglas de acceso entre la red DMZ y la red LAN sólo para servidores y estaciones con puertos específicos tales como el 53 (DNS), 21 (ftp), 80 (http), 1433 (SQL server) y 3389 (RDP).

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	IPv4 TCP/UDP	DMZ net	*	*	*	*	none			
0 / 0 B	IPv4 TCP/UDP	SRV_WWW	*	DATOS_LAN	DMZ_LAN_PORTS	*	none		Acceso a consultas de Servidores Internos TCP	
0 / 8.33 MiB	IPv4 UDP	SRV_WWW	*	DC_internal	53 (DNS)	*	none		Acceso a consultas de Servidores Internos DNS	
0 / 0 B	IPv4 TCP	DMZ net	*	LAN net	*	*	none		DMZ to LAN	

## 4.6.3 Reglas aplicadas a la red VPN

PfSense utiliza como cliente VPN a OpenVPN Client basado en open source el cual como se vio en el apartado de instalación de paquetes es parte de esta implementación. El procedimiento para añadir las reglas es el mismo ya visto anteriormente, por lo que para esta implementación quedaría de la siguiente manera:

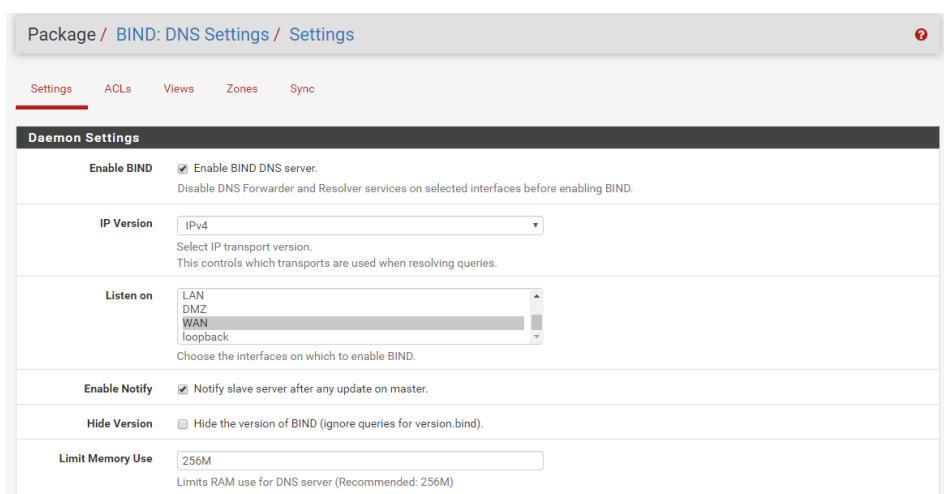
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	IPv4 TCP/UDP	*	*	LAN net	*	*	none		Kerberos protocol	
0 / 0 B	IPv4 ICMP	*	*	*	*	*	none		Ping a todos los lugares	
0 / 4.35 MiB	IPv4 TCP	*	*	*	prtWeb	*	none		Para protocolo http	
0 / 8.04 GiB	IPv4 TCP	*	*	LAN net	3389 (MS RDP)	*	none		Solo escritorio remoto	
0 / 0 B	IPv4 TCP/UDP	*	*	LAN net	prtSQL	*	none		SQL server access to lan	
0 / 42.74 MiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Resolucion de nombres red interna	
0 / 3.92 MiB	IPv4 TCP	*	*	LAN net	3128	*	none		Proxy	
0 / 4.97 MiB	IPv4 TCP	*	*	LAN net	5900 (VNC)	*	none		Para vnc soporte	
0 / 0 B	IPv4 TCP	*	*	*	22 (SSH)	*	none		Al SSH	

Con esto se concluye la configuración de reglas de acceso en este servidor.

## 4.7 Configuración del Servicio de Bind (DNS Server)

Para acceder seleccionar en el menú: **SERVICES\BIND DNS SERVICES**

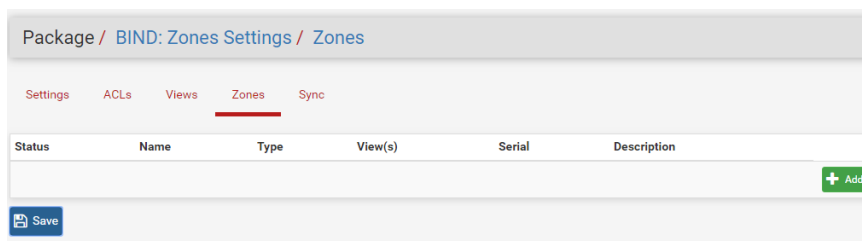
En la primera pestaña se configuran la activación del servicio y los parámetros con los cuales funcionará el servidor tales como la versión IP, selección de la IP que escucha y notificaciones. Tal como muestra la siguiente imagen.



Una vez terminado con el mouse hacer clic sobre el botón **Save**.

### 4.7.1 Configuración de la Zona DNS

Seleccionar la pestaña de Zones y con el mouse hacer clic sobre el botón **Add**.



Luego se procede con el ingreso de la información solicitada para crear la zona

Domain Zone Configuration	
<b>Disable This Zone</b>	<input checked="" type="checkbox"/> Do not include this zone in BIND config files.
<b>Zone Name</b>	<input type="text" value="hotelcontinental.com.ec"/> Enter the name for this zone (e.g. example.com) For reverse zones, include zone IP in reverse order. (e.g. 1.168.192) <b>Note: IN-ADDR.ARPA will be automatically included in config files when reverse zone option is checked.</b>
<b>Description</b>	<input type="text" value="Zona autoritativa del Hotel Continental"/> Enter a description for this zone.
<b>Zone Type</b>	<input type="text" value="Master"/> Select zone type.
<b>View</b>	<input type="text" value="hotelcontinental.com.ec"/> Select (CTRL+click) the views that this zone will belong to.
<b>Reverse Zone</b>	<input type="checkbox"/> Check if this is a reverse zone.
<b>IPv6 Reverse Zone</b>	<input type="checkbox"/> Check if this is an IPv6 reverse zone. Reverse Zone must also be enabled.
<b>Response Policy Zone</b>	<input type="checkbox"/> Check if this zone is used in a response policy.
<b>Custom Option</b>	<input type="text"/> You can put your own custom options here.

<b>Name Server</b>	<input type="text" value="ns1.hotelcontinental.com.ec"/> Enter nameserver for this zone.
<b>Base Domain IP</b>	<input type="text" value="52.48.185.213"/> Enter IP address for base domain lookup. (Meaning, what IP should nslookup mydomain.com return.)
<b>Mail Admin Zone</b>	<input type="text" value="it.hotelcontinental.com.ec"/> Enter mail admin zone.
<b>Serial</b>	<input type="text" value="2011052097"/> Parsed value for the slave to update the DNS zone.
<b>Refresh</b>	<input type="text" value="1d"/> Slave refresh (Default: 1 day)
<b>Retry</b>	<input type="text" value="2h"/> Slave retry time in case of a problem (Default: 2 hours)
<b>Expire</b>	<input type="text" value="4w"/> Slave expiration time (Default: 4 weeks)
<b>Minimum</b>	<input type="text" value="1h"/> Maximum caching time in case of failed lookups (Default: 1 hour)
<b>allow-update</b>	<input type="text" value="any"/> none any localhost localnets Select(CTRL+click) who is allowed to send updates to this zone. The allow-update statement defines a match list of IP address(es) that are allowed to submit dynamic updates for 'master' zones - i.e., it enables Dynamic DNS (DDNS).

Continuando con la configuración de la zona ahora se ingresan los registros de dominio.

Zone Domain records				
Record	Type	Priority	Alias or IP address	
ns1	A		186.3.54.60	Delete
@	NS		nic.ec.mars.orderbox-dn	Delete
@	MX	10	mail.hotelcontinental.co	Delete
hotelcontinental.com.ec	TXT		*v=spf1 mx ip4:186.3.54	Delete
mail	A		186.3.54.60	Delete
autodiscover	CNAME		mail.hotelcontinental.co	Delete
legacy	CNAME		mail.hotelcontinental.co	Delete
bodesur	A		40.112.187.7	Delete
e	A		186.3.54.62	Delete
ftp	A		186.3.54.59	Delete
rds	A		186.3.54.200	Delete
www	CNAME		d3fybqbjkerk.cloudfor	Delete
vpn	A		186.3.54.60	Delete
_DMARC	TXT		*v=DMARC1;p=quaranti	Delete
8732eb16-b87e-4734-91	CNAME		dkim.infusionmail.com	Delete

## 4.8 Configuración de NTP cliente

Continuando con la configuración de nuestro servidor firewall se procede a ingresar los parámetros para sincronizar la fecha y la hora.

En el menú de **SERVICES/NTP/SEETINGS** se declaran las interfaces y los servidores que proveen el servicio de NTP, en este caso se utilizan dos equipos que proveen el servicio.

Services / NTP / Settings

Settings **ACLs** Serial GPS PPS

**NTP Server Configuration**

Interface:   
Interfaces without an IP address will not be shown.  
 Selecting no interfaces will listen on all interfaces with a wildcard.  
 Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers:

srv-dc01.hotelcontinental.gye	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete
	Prefer	No Select	Is a Pool	
srv-dc02.hotelcontinental.gye	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete
	Prefer	No Select	Is a Pool	

Una vez ingresado los parámetros hacer clic con el mouse sobre el botón **Save**.

## 4.9 Unir servidor firewall al dominio local.

Este procedimiento es muy importante ya que mediante la autenticación del servidor con active directory se podrá autenticar a los usuarios del dominio con los servicios de squid y squidguard. En el menú **SAMBA\ACTIVE DIRECTORY COMPATIBLE DOMAIN CONTROLLER\ GENERAL SETTINGS.**

Ingresar los parámetros como listen interface, el Active Directory Type, Domain, Workgroup y las credenciales de un usuario del dominio que tenga privilegios para añadir el servidor firewall al dominio.

The screenshot shows the configuration page for Samba as an Active Directory compatible Domain Controller. The breadcrumb trail is "Package / Samba is a Active Directory compatible Domain Controller / General Settings". The "General Settings" section is highlighted. Under "General Options", the "Enable" checkbox for "Enable Samba service" is checked. The "Listen interface" dropdown menu is open, showing options: LAN, DMZ, WAN, and loopback. Below it, a note states "The interface(s) the Samba service will bind to." The "Active Directory Type" dropdown is set to "Windows 2008 +". The "Domain Member Settings" section includes: "Domain" (hotelcontinental.gye), "Workgroup" (CONTINENTAL), "Username Administrator" (pfsense), and "Password" (masked with dots). A "Save" button is located at the bottom.

Una vez finalizado hacer clic con el mouse en el botón **Save**.

**Nota: Una vez aplicado este cambio, se debe verificar en el servidor controlador de dominio que el equipo haya sido agregado al mismo.**

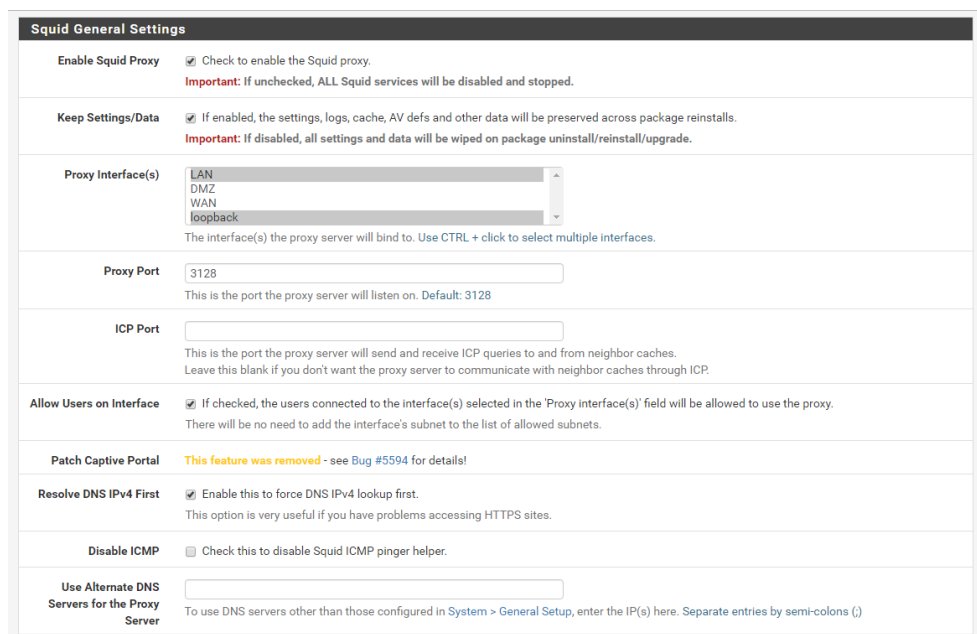


## 4.10 Configuración de Squid Proxy

Squid es un programa que te permite realizar un proxy/caché con una gran variedad de configuraciones y usos. Al usar una caché también consigue reducir el ancho de banda y los tiempos de respuesta gracias a su caché, y reutilizando las páginas web solicitadas con más frecuencia.

Con Squid puedes conseguir control de acceso, y es excelente para acelerar un servidor, ya que funciona como caché de las páginas que ofrece el servidor.

Continuando con la configuración en PfSense community edition, en el menú: **SERVICES/SQUID PROXY SERVER/GENERAL**



The screenshot shows the 'Squid General Settings' configuration page. The settings are as follows:

- Enable Squid Proxy:**  Check to enable the Squid proxy. **Important:** If unchecked, ALL Squid services will be disabled and stopped.
- Keep Settings/Data:**  If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. **Important:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
- Proxy Interface(s):** A dropdown menu with 'LAN' selected. Other options include DMZ, WAN, and loopback. Below the menu, it says: 'The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.'
- Proxy Port:** A text input field containing '3128'. Below it, it says: 'This is the port the proxy server will listen on. Default: 3128'
- ICP Port:** An empty text input field. Below it, it says: 'This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.'
- Allow Users on Interface:**  If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
- Patch Captive Portal:** **This feature was removed - see Bug #5594 for details!**
- Resolve DNS IPv4 First:**  Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
- Disable ICMP:**  Check this to disable Squid ICMP pinger helper.
- Use Alternate DNS Servers for the Proxy Server:** An empty text input field. Below it, it says: 'To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (,)'

Se debe habilitar el servicio, la interface que en este caso es LAN con puerto 3128 que es por defecto y configurar la ruta de los archivos de log y los días que estarán disponibles.

Logging Settings	
<b>Enable Access Logging</b>	<input checked="" type="checkbox"/> This will enable the access log. <b>Warning:</b> Do NOT enable if available disk space is low.
<b>Log Store Directory</b>	<input type="text" value="/var/squid/logs"/> The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs <b>Important:</b> Do NOT include the trailing / when setting a custom location.
<b>Rotate Logs</b>	<input type="text" value="15"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
<b>Log Pages Denied by SquidGuard</b>	<input checked="" type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions. <a href="#">i</a>

Hacer clic con el mouse en el botón **Save**.

#### 4.10.1 Services/Squid Proxy Server/Antivirus

Se debe habilitar el antivirus que acompaña a squid proxy como una capa más de protección a la navegación web, habilitar Google Safe Browsing y la frecuencia de actualización de la base de virus la cual por defecto es de cada hora.

ClamAV Anti-Virus Integration Using C-ICAP	
<b>Enable AV</b>	<input checked="" type="checkbox"/> Enable Squid antivirus check using ClamAV.
<b>Client Forward Options</b>	<input type="text" value="Send both client username and IP info (Default)"/> Select what client info to forward to ClamAV.
<b>Enable Manual Configuration</b>	<input type="text" value="disabled"/> <b>Warning: Only enable this if you know what you are doing.</b> <a href="#">i</a> When enabled, the options below no longer have any effect. You must edit the configuration files directly in the 'Advanced Features'. After enabling manual configuration, click the button below <b>once</b> to load default configuration files. To disable manual configuration again, select 'disabled' and click 'Save'. <input type="button" value="Load Advanced"/>
<b>Redirect URL</b>	<input type="text"/> When a virus is found then redirect the user to this URL. Example: http://proxy.example.com/blocked.html Leave empty to use the default Squid/pfSense WebGUI URL.
<b>Google Safe Browsing</b>	<input checked="" type="checkbox"/> Enables Google Safe Browsing support. Google Safe Browsing database includes information about websites that may be phishing sites or possible sources of malware. <b>Warning:</b> This option consumes significant amount of RAM.
<b>Exclude Audio/Video Streams</b>	<input checked="" type="checkbox"/> This option disables antivirus scanning of streamed video and audio.
<b>ClamAV Database Update</b>	<input type="text" value="every 1 hour"/> Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here. <a href="#">i</a> <b>Important:</b> Set to 'every 1 hour' if you want to use Google Safe Browsing feature. Click the button below <b>once</b> to force the update of AV databases immediately. <b>Note:</b> This will take a while. Check freshclam log on the 'Real Time' tab for progress information. <input type="button" value="Update AV"/>

Hacer clic con el mouse en el botón **Save**.

#### Menú: SERVICES/SQUID PROXY SERVER/ACL

Basado en los sitios webs a los que acceden los diferentes usuarios departamentales en los cuales utilizan puertos diferentes a 80 y 443, en esta opción se debe ingresar los puertos adicionales tanto en http como https.

Squid Allowed Ports	
ACL SafePorts	<input type="text"/> <small>This is a space-separated list of "safe ports" in addition to the predefined default list.            Default list: 21 70 80 210 280 443 488 563 591 631 777 901 1025-65535</small>
ACL SSLPorts	<input type="text" value="444 4443 5038 81 8181 8443 9443 4070 8082 80"/> <small>This is a space-separated list of ports to allow SSL "CONNECT" to in addition to the predefined default list.            Default list: 443 563</small>

Menú: **SERVICES/SQUID** **PROXY**  
**SERVER/AUTENTICACION**

El servidor proxy utilizará la autenticación con Active Directory a través del protocolo LDAP, para esto se utiliza como método Winbind NTLM, la dirección IP del servidor de autenticación con puertos por default el 389.

Squid Authentication General Settings	
Authentication Method	<input type="text" value="Winbind NTLM"/> <small>Select an authentication method. This will allow users to be authenticated by local or external services.</small>
Authentication Server	<input type="text" value="130.100.1.1"/> <small>Enter the IP or hostname of the server that will perform the authentication here.</small>
Authentication server port	<input type="text"/> <small>Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.</small>
Authentication Prompt	<input type="text" value="Favor identifiquese"/> <small>This string will be displayed at the top of the authentication request window.</small>
Authentication Processes	<input type="text" value="10"/> <small>The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.</small>
Authentication TTL	<input type="text" value="480"/> <small>This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5</small>
Require Authentication for Unrestricted IPs	<input type="checkbox"/> If enabled, even 'Unrestricted IPs' configured on the ACLs tab are required to authenticate to use the proxy.
Subnets That Don't Need Authentication	<input type="text"/> <small>Enter subnet(s) or IP address(es) (in CIDR format) that should NOT be asked for authentication to access the proxy. Put each entry on a separate line.</small>

Se ingresará la misma cuenta de usuario que se utilizó al configurar samba, ingresando los parámetros correctamente según se lo requiere.

Squid Authentication LDAP Settings	
LDAP version	<input type="text" value="3"/> <small>Select LDAP protocol version.</small>
LDAP Server User DN	<input type="text" value="CN=PFSense,OU=INFORMATICA,OU=Usuarios,OU=1-MATRIZ,DC=hote"/> <small>Enter the user DN to use to connect to the LDAP server here.</small>
LDAP Password	<input type="password" value="....."/> <small>Enter the password to use to connect to the LDAP server here.</small>
LDAP Base Domain	<input type="text" value="DC=hotelcontinental,DC=gye"/> <small>Enter the base domain of the LDAP server here.</small>
LDAP Username DN Attribute	<input type="text" value="sAMAccountName"/> <small>Enter LDAP username DN attribute here.</small>
LDAP Search Filter	<input type="text" value="sAMAccountName=%s"/> <small>Enter LDAP search filter here.</small>

Una vez concluido hacer clic con el mouse en el botón **Save.**

Las demás opciones no se realizarán cambios ya que no se

requieren para esta implementación.

## 4.11 Configuración de SquidGuard Proxy Filter

Este sistema es uno de los más conocidos; utiliza un sistema de filtrado de re direccionamiento web y fue desarrollado como un complemento para squid.

Menú: **SERVICES/SQUIDGUARD PROXY FILTER/GENERAL**

Primeramente, se debe habilitar el servicio de squidGuard, luego configurar los parámetros de autenticación LDAP con active directory, se utilizarán las credenciales del punto anterior.

General Options	
Enable	<input checked="" type="checkbox"/> Check this option to enable squidGuard. <small>Important: Please set up at least one category on the 'Target Categories' tab before enabling. See <a href="#">this link for details</a>. The Save button at the bottom of this page must be clicked to save configuration changes. To activate squidGuard configuration changes, <b>the Apply button must be clicked.</b></small>
<input checked="" type="button" value="Apply"/>	
SquidGuard service state: <b>STARTED</b>	
LDAP Options	
Enable LDAP Filter	<input checked="" type="checkbox"/> Enable options for setup ldap connection to create filters with ldap search
LDAP DN	<input type="text" value="CN=PFSense,OU=INFORMATICA,OU=Usuarios,OU=1-MATRIZ,DC=hotel"/> <small>Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)</small>
LDAP DN Password	<input type="password" value="....."/> <small>Password must be initialize with letters (Ex: Change123), valid format: [a-zA-ZV][a-zA-Z0-9/_\-\.\ \%\!\?=&amp;]</small>
Strip NT domain name	<input type="checkbox"/> Strip NT domain name component from user names (/ or \ separated).
Strip Kerberos Realm	<input type="checkbox"/> Strip Kerberos Realm component from user names (@ separated).
LDAP Version	<input type="text" value="Version 3"/>

Marcar las opciones de log, esto servirá para seguimiento.

Logging options	
Enable GUI log	<input checked="" type="checkbox"/> Check this option to log the access to the Proxy Filter GUI.
Enable log	<input checked="" type="checkbox"/> Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation	<input checked="" type="checkbox"/> Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Asimismo, habilitar las opciones de blacklist y la url que debe ser: <http://www.shallalist.de/Downloads/shallalist.tar.gz>

Blacklist options	
Blacklist	<input checked="" type="checkbox"/> Check this option to enable blacklist <small>Do NOT enable this on NanoBSD installs!</small>
Blacklist proxy	<input type="text"/> <small>Blacklist upload proxy - enter here, or leave blank. Format: host:[port login:pass] . Default proxy port 1080. Example: '192.168.0.1:8080 user:pass'</small>
Blacklist URL	<input type="text" value="http://www.shallalist.de/Downloads/shallalist.tar.gz"/> <small>Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).</small>

Esto se utilizará para la categorización de sitios web para su filtrado de contenido.

Hacer clic con el botón del mouse sobre el botón **Save**.




### Menú: **SERVICES/SQUIDGUARD PROXY FILTER/COMMON ACL**

Esta opción se aplicará la regla por defecto para toda conexión saliente en la red que no tenga permisos de acceso a Internet o a algún sitio que se encuentre categorizado como denegado.

Hacer clic con el botón del mouse sobre el botón **Save**.

### Menú: **SERVICES/SQUIDGUARD PROXY FILTER/GROUPS ACL**

Parte de la infraestructura de CONTINENTAL HOTEL S.A son los permisos a usuarios según sus funciones, para esto en active directory se han creado 3 grupos cuyos nombres diferencian el acceso a internet que tendrá cada usuario que pertenezca a los siguientes grupos:

-  GG\_Internet\_Full
-  GG\_Internet\_Medium
-  GG\_Internet\_Social\_Media

En la opción de Groups ACL se aplicará el filtrado de contenido web a cada uno de los grupos, hacer clic en **Add** e ingresar los parámetros requeridos.

General Options	
<b>Disabled</b>	<input type="checkbox"/> Check this to disable this ACL rule.
<b>Name</b>	<input type="text" value="GG_Social_Media"/> Enter a unique name of this rule here. The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.
<b>Order</b>	<input type="text" value="----"/> Select the new position for this ACL item. ACLs are evaluated on a first-match source basis. <b>Note:</b> Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list. <b>Example:</b> ACL with single (or short range) source ip 10.0.0.15 must be placed before ACL with more large ip range 10.0.0.0/24.
<b>Client (source)</b>	<input type="text" value="ldapusersearch ldap://130.100.1.1:3268/DC=hotelcontinental,DC=gye?sAMAccountName?sub?(&amp;(sAMAccountName=%s)(memberOf=CN=GG_Internet_Social_Media%2cOU=Grupos%2cOU=1-"/> Enter client's IP address or domain or 'username' here. To separate them use space. <b>Example:</b> IP: 192.168.0.1 - Subnet: 192.168.0.0/24 or 192.168.1.0/255.255.255.0 - IP-Range: 192.168.1.1-192.168.1.10 Domain: foo.bar matches foo.bar or *.foo.bar Username: 'user1' <b>Ldap search (Ldap filter must be enabled in General Settings):</b> ldapusersearch ldap://192.168.0.100/DC=domain,DC=com?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=it%2cCN=Users%2cDC=domain%2cDC=com)) <i>Attention: these line don't have break line, all on one line</i>
<b>Time</b>	<input type="text" value="none (time not defined)"/> Select the time in which 'Target Rules' will operate or leave 'none' for rules without time restriction. If this option is set then in off-time the second ruleset will operate.

Es importante que en la opción de Client (source) se debe especificar utilizando comandos LDAP la ruta en donde se encuentra ubicado el nombre del grupo: **GG\_Social\_Media** en el active directory.

Marcar las opciones de Do not allow IP-Adresses in URL y use Safe Search engine y log, asimismo ingresar una descripción de la regla

<b>Do not allow IP-Addresses in URL</b>	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
<b>Redirect mode</b>	<input type="text" value="Int error page (enter error message)"/> Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible. Options: <a href="#">ext url err page</a> , <a href="#">ext url redirect</a> , <a href="#">ext url as move</a> , <a href="#">ext url as found</a>
<b>Redirect</b>	<input type="text"/> Enter the external redirection URL, error message or size (bytes) here.
<b>Use SafeSearch engine</b>	<input checked="" type="checkbox"/> To protect your children from adult content you can use the protected mode of search engines. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. <b>Note:</b> This option overrides 'Rewrite' setting.
<b>Rewrite</b>	<input type="text" value="none (rewrite not defined)"/> Enter the rewrite condition name for this rule or leave it blank.
<b>Rewrite for off-time</b>	<input type="text" value="none (rewrite not defined)"/> Enter the rewrite condition name for this rule or leave it blank.
<b>Description</b>	<input type="text" value="GG_Internet_Social_Media - Solo paginas de redes sociales"/> You may enter any description here for your reference.
<b>Log</b>	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.

Para finalizar se especificará el filtrado de contenido web para los usuarios que pertenezcan al grupo GG\_Social\_Media

[blk_BL_adv]	access	---	▼
[blk_BL_aggressive]	access	---	▼
[blk_BL_alcohol]	access	---	▼
[blk_BL_anonvpn]	access	---	▼
[blk_BL_automobile_bikes]	access	---	▼
[blk_BL_automobile_boats]	access	---	▼
[blk_BL_automobile_cars]	access	---	▼
[blk_BL_automobile_planes]	access	---	▼
[blk_BL_chat]	access	---	▼
[blk_BL_costtraps]	access	---	▼
[blk_BL_dating]	access	---	▼
[blk_BL_downloads]	access	---	▼
[blk_BL_drugs]	access	---	▼
[blk_BL_dynamic]	access	---	▼
[blk_BL_education_schools]	access	---	▼
[blk_BL_finance_banking]	access	---	▼
[blk_BL_finance_insurance]	access	---	▼
[blk_BL_finance_moneylending]	access	---	▼
[blk_BL_finance_other]	access	---	▼
[blk_BL_finance_realestate]	access	---	▼
[blk_BL_finance_trading]	access	---	▼
[blk_BL_fortunetelling]	access	---	▼
[blk_BL_forum]	access	---	▼
[blk_BL_gamble]	access	---	▼
[blk_BL_government]	access	---	▼
[blk_BL_hacking]	access	---	▼
[blk_BL_hobby_cooking]	access	---	▼
[blk_BL_hobby_games-misc]	access	---	▼
[blk_BL_hobby_games-online]	access	---	▼
[blk_BL_hobby_gardening]	access	---	▼
[blk_BL_hobby_pets]	access	---	▼
[blk_BL_homestyle]	access	---	▼
[blk_BL_hospitals]	access	---	▼
[blk_BL_imagehosting]	access	---	▼
[blk_BL_isp]	access	---	▼
[blk_BL_jobsearch]	access	---	▼

[blk_BL_models]	access	---	▼
[blk_BL_movies]	access	---	▼
[blk_BL_music]	access	---	▼
[blk_BL_news]	access	---	▼
[blk_BL_podcasts]	access	---	▼
[blk_BL_politics]	access	---	▼
[blk_BL_porn]	access	---	▼
[blk_BL_radiotv]	access	---	▼
[blk_BL_recreation_humor]	access	---	▼
[blk_BL_recreation_martialarts]	access	---	▼
[blk_BL_recreation_restaurants]	access	---	▼
[blk_BL_recreation_sports]	access	---	▼
[blk_BL_recreation_travel]	access	---	▼
[blk_BL_recreation_wellness]	access	---	▼
[blk_BL_redirector]	access	---	▼
[blk_BL_religion]	access	---	▼
[blk_BL_remotecontrol]	access	---	▼
[blk_BL_ringtones]	access	---	▼
[blk_BL_science_astronomy]	access	---	▼
[blk_BL_science_chemistry]	access	---	▼
[blk_BL_searchengines]	access	---	▼
[blk_BL_sex_education]	access	---	▼
[blk_BL_sex_lingerie]	access	---	▼
[blk_BL_shopping]	access	---	▼
[blk_BL_socialnet]	access	allow	▼
[blk_BL_spyware]	access	---	▼
[blk_BL_tracker]	access	---	▼
[blk_BL_updatesites]	access	---	▼
[blk_BL_urlshortener]	access	---	▼
[blk_BL_violence]	access	---	▼
[blk_BL_warez]	access	---	▼
[blk_BL_weapons]	access	---	▼
[blk_BL_webmail]	access	---	▼
[blk_BL_webphone]	access	---	▼
[blk_BL_webradio]	access	---	▼
[blk_BL_webtv]	access	---	▼
Default access [all]	access	deny	▼

Como podemos observar este grupo sólo tendrá acceso (Allow) a BL\_socialnet, la regla por default para las demás categorías es Deny

Una vez concluido hacer clic con el mouse sobre el botón **Save**.



Para los demás grupos aplicar el mismo procedimiento, sin embargo, se detallan los permisos (Allow) para estos grupos:

### GG\_Inet\_Medium

[blk_BL_adv]	access	---	▼
[blk_BL_aggressive]	access	---	▼
[blk_BL_alcohol]	access	---	▼
[blk_BL_anonvpn]	access	deny	▼
[blk_BL_automobile_bikes]	access	---	▼
[blk_BL_automobile_boats]	access	---	▼
[blk_BL_automobile_cars]	access	---	▼
[blk_BL_automobile_planes]	access	---	▼
[blk_BL_chat]	access	allow	▼
[blk_BL_costtraps]	access	---	▼
[blk_BL_dating]	access	---	▼
[blk_BL_downloads]	access	allow	▼
[blk_BL_drugs]	access	---	▼
[blk_BL_dynamic]	access	---	▼
[blk_BL_education_schools]	access	---	▼
[blk_BL_finance_banking]	access	---	▼
[blk_BL_finance_insurance]	access	---	▼
[blk_BL_finance_moneylending]	access	---	▼
[blk_BL_finance_other]	access	---	▼
[blk_BL_finance_realestate]	access	---	▼
[blk_BL_finance_trading]	access	---	▼
[blk_BL_fortunetelling]	access	deny	▼
[blk_BL_forum]	access	deny	▼
[blk_BL_gamble]	access	deny	▼
[blk_BL_government]	access	---	▼
[blk_BL_hacking]	access	deny	▼
[blk_BL_hobby_cooking]	access	---	▼
[blk_BL_hobby_games-misc]	access	deny	▼
[blk_BL_hobby_games-online]	access	deny	▼
[blk_BL_hobby_gardening]	access	---	▼
[blk_BL_hobby_pets]	access	---	▼
[blk_BL_homestyle]	access	---	▼
[blk_BL_hospitals]	access	---	▼
[blk_BL_imagehosting]	access	---	▼
[blk_BL_isp]	access	---	▼
[blk_BL_jobsearch]	access	---	▼
[blk_BL_library]	access	---	▼

[blk_BL_models]	access	deny ▼
[blk_BL_movies]	access	deny ▼
[blk_BL_music]	access	---
[blk_BL_news]	access	deny ▼
[blk_BL_podcasts]	access	---
[blk_BL_politics]	access	---
[blk_BL_porn]	access	deny ▼
[blk_BL_radiotv]	access	deny ▼
[blk_BL_recreation_humor]	access	---
[blk_BL_recreation_martialarts]	access	---
[blk_BL_recreation_restaurants]	access	---
[blk_BL_recreation_sports]	access	---
[blk_BL_recreation_travel]	access	---
[blk_BL_recreation_wellness]	access	---
[blk_BL_redirector]	access	deny ▼
[blk_BL_religion]	access	---
[blk_BL_remotecontrol]	access	deny ▼
[blk_BL_ringtones]	access	deny ▼
[blk_BL_science_astronomy]	access	---
[blk_BL_science_chemistry]	access	---
[blk_BL_searchengines]	access	---
[blk_BL_sex_education]	access	---
[blk_BL_sex_lingerie]	access	---
[blk_BL_shopping]	access	---
[blk_BL_socialnet]	access	deny ▼
[blk_BL_spyware]	access	deny ▼
[blk_BL_tracker]	access	---
[blk_BL_updatesites]	access	---
[blk_BL_urlshortener]	access	---
[blk_BL_violence]	access	---
[blk_BL_warez]	access	deny ▼
[blk_BL_weapons]	access	deny ▼
[blk_BL_webmail]	access	allow ▼
[blk_BL_webphone]	access	---
[blk_BL_webradio]	access	deny ▼
[blk_BL_webtv]	access	deny ▼
Default access [all]	access	allow ▼

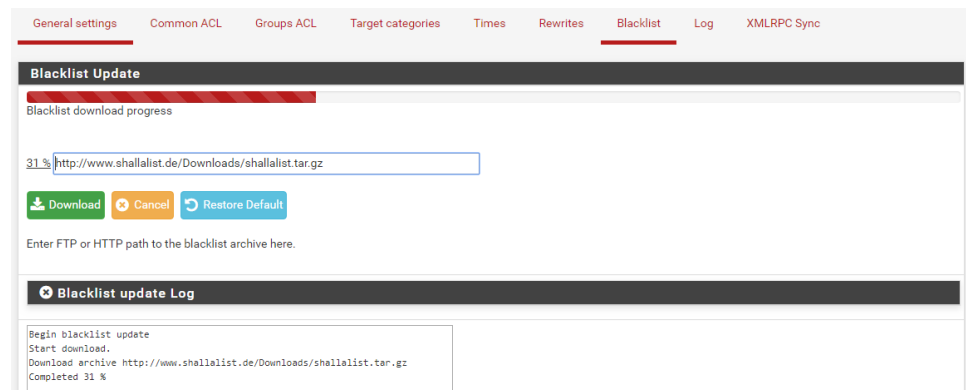
## GG\_Internet\_Full

[blk_BL_adv]	access	---	▼
[blk_BL_aggressive]	access	---	▼
[blk_BL_alcohol]	access	---	▼
[blk_BL_anonvpn]	access	---	▼
[blk_BL_automobile_bikes]	access	---	▼
[blk_BL_automobile_boats]	access	---	▼
[blk_BL_automobile_cars]	access	---	▼
[blk_BL_automobile_planes]	access	---	▼
[blk_BL_chat]	access	---	▼
[blk_BL_costtraps]	access	---	▼
[blk_BL_dating]	access	---	▼
[blk_BL_downloads]	access	---	▼
[blk_BL_drugs]	access	---	▼
[blk_BL_dynamic]	access	---	▼
[blk_BL_education_schools]	access	---	▼
[blk_BL_finance_banking]	access	---	▼
[blk_BL_finance_insurance]	access	---	▼
[blk_BL_finance_moneylending]	access	---	▼
[blk_BL_finance_other]	access	---	▼
[blk_BL_finance_realestate]	access	---	▼
[blk_BL_finance_trading]	access	---	▼
[blk_BL_fortunetelling]	access	---	▼
[blk_BL_forum]	access	---	▼
[blk_BL_gamble]	access	---	▼
[blk_BL_government]	access	---	▼
[blk_BL_hacking]	access	deny	▼
[blk_BL_hobby_cooking]	access	---	▼
[blk_BL_hobby_games-misc]	access	---	▼
[blk_BL_hobby_games-online]	access	---	▼
[blk_BL_hobby_gardening]	access	---	▼
[blk_BL_hobby_pets]	access	---	▼
[blk_BL_homestyle]	access	---	▼
[blk_BL_hospitals]	access	---	▼
[blk_BL_imagehosting]	access	---	▼
[blk_BL_isp]	access	---	▼
[blk_BL_jobsearch]	access	---	▼
[blk_BL_library]	access	---	▼

[blk_BL_models]	access	---	▼
[blk_BL_movies]	access	---	▼
[blk_BL_music]	access	---	▼
[blk_BL_news]	access	---	▼
[blk_BL_podcasts]	access	---	▼
[blk_BL_politics]	access	---	▼
[blk_BL_porn]	access	deny	▼
[blk_BL_radiotv]	access	---	▼
[blk_BL_recreation_humor]	access	---	▼
[blk_BL_recreation_martialarts]	access	---	▼
[blk_BL_recreation_restaurants]	access	---	▼
[blk_BL_recreation_sports]	access	---	▼
[blk_BL_recreation_travel]	access	---	▼
[blk_BL_recreation_wellness]	access	---	▼
[blk_BL_redirector]	access	---	▼
[blk_BL_religion]	access	---	▼
[blk_BL_remotecontrol]	access	deny	▼
[blk_BL_ringtones]	access	---	▼
[blk_BL_science_astronomy]	access	---	▼
[blk_BL_science_chemistry]	access	---	▼
[blk_BL_searchengines]	access	---	▼
[blk_BL_sex_education]	access	---	▼
[blk_BL_sex_lingerie]	access	---	▼
[blk_BL_shopping]	access	---	▼
[blk_BL_socialnet]	access	---	▼
[blk_BL_spyware]	access	deny	▼
[blk_BL_tracker]	access	---	▼
[blk_BL_updatesites]	access	---	▼
[blk_BL_urlshortener]	access	---	▼
[blk_BL_violence]	access	---	▼
[blk_BL_warez]	access	deny	▼
[blk_BL_weapons]	access	---	▼
[blk_BL_webmail]	access	---	▼
[blk_BL_webphone]	access	---	▼
[blk_BL_webradio]	access	---	▼
[blk_BL_webtv]	access	---	▼
Default access [all]	access	allow	▼

Menú: **SERVICES/SQUIDGUARD** **PROXY**  
**FILTER/BLACKLIST**

Frecuentemente es necesario actualizar la blacklist esto para mantenerse al día con la categorización de sitios webs ya que es de conocimiento común de que cada día se alojan nuevos sitios en la internet y por ende ésta lista se actualiza de forma constante.



## 4.12 Configuración del servicio de OpenVPN

Como se ha mencionado anteriormente existen usuarios que realizan su trabajo desde sitios externos al hotel por lo que es necesario otorgar el servicio de VPN y las reglas de acceso de protocolos y puertos que ya anteriormente se han definido.

### 4.12.1 Creación del Certificado de Autorización

Menú: **SYSTEM/CERTIFICATE MANAGER/CAS**

Hacer clic con el mouse sobre el botón **Add**, ingresar los datos requeridos, los mismo fueron tomados de una entidad certificadora local y hacer clic con el botón **Save**.

**Create / Edit CA**

**Descriptive name**

**Method**

---

**Existing Certificate Authority**

**Certificate data**   
Paste a certificate in X.509 PEM format here.

**Certificate Private Key (optional)**   
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

**Serial for next certificate**   
Enter a decimal number to be used as the serial number for the next certificate to be created using this CA.

## Menú: VPN/OPENVPN/SERVERS

Hacer clic con el mouse en el botón **Add** e ingresar los parámetros con los que el servidor funcionará.

**General Information**

**Disabled**  Disable this server  
Set this option to disable this server without removing it from the list.

**Server mode**

**Protocol**

**Device mode**   
\*tun\* mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
\*tap\* mode is capable of carrying 802.3 (OSI Layer 2).

**Interface**   
The interface or Virtual IP address where OpenVPN will receive client connections.

**Local port**   
The port used by OpenVPN to receive client connections.

**Description**   
A description may be entered here for administrative reference (not parsed).

---

**Cryptographic Settings**

**TLS Configuration**  Use a TLS Key  
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

**Peer Certificate Authority**

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

<b>DH Parameter Length</b>	2048 bit
	Diffie-Hellman (DH) parameter set used for key exchange. <a href="#">i</a>
<b>ECDH Curve</b>	Use Default
	The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
<b>Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)
	The Encryption Algorithm used for data channel packets when Negotiable Cryptographic Parameter (NCP) support is not available.
<b>Enable NCP</b>	<input checked="" type="checkbox"/> Enable Negotiable Cryptographic Parameters
	Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below. <a href="#">i</a>
<b>NCP Algorithms</b>	<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p>AES-128-CBC (128 bit key, 128 bit block)</p> <p>AES-128-CFB (128 bit key, 128 bit block)</p> <p>AES-128-CFB1 (128 bit key, 128 bit block)</p> <p>AES-128-CFB8 (128 bit key, 128 bit block)</p> <p>AES-128-GCM (128 bit key, 128 bit block)</p> <p>AES-128-OFB (128 bit key, 128 bit block)</p> <p>AES-192-CBC (192 bit key, 128 bit block)</p> <p>AES-192-CFB (192 bit key, 128 bit block)</p> <p>AES-192-CFB1 (192 bit key, 128 bit block)</p> <p>AES-192-CFB8 (192 bit key, 128 bit block)</p> </div> <div style="width: 35%;"> <p>AES-128-GCM</p> </div> </div> <p>Available NCP Encryption Algorithms Click to add or remove an algorithm from the list</p> <p>Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list</p> <p>The order of the selected NCP Encryption Algorithms is respected by OpenVPN. <a href="#">i</a></p>
<b>Auth digest algorithm</b>	SHA256 (256-bit)
	The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

## 4.12.2 Configuración del Tunnel

Se utilizará una red virtual propia de PfSense con servidor dhcp IPV4 la cual utilizará el segmento 10.20.20.X (por defecto) y se comunicará con el segmento 130.100.1.0 que corresponde a la red local.

Tunnel Settings	
<b>IPv4 Tunnel Network</b>	10.20.20.0/24
	This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.0.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
<b>IPv6 Tunnel Network</b>	
	This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
<b>Redirect IPv4 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<b>IPv4 Local network(s)</b>	130.100.1.0/24
	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
<b>IPv6 Local network(s)</b>	
	IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
<b>Concurrent connections</b>	
	Specify the maximum number of clients allowed to concurrently connect to this server.
<b>Compression</b>	Omit Preference (Use OpenVPN Default)
	Compress tunnel packets using the LZO algorithm. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

## 4.12.3 Configuración avanzada de cliente

Se especifica el dominio y la direcciones IP de los servidores DNS y NTP.

Advanced Client Settings	
DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	<input type="text" value="hotelcontinental.gye"/>
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	<input type="text" value="130.100.1.1"/>
DNS Server 2	<input type="text" value="130.100.1.3"/>
DNS Server 3	<input type="text"/>
DNS Server 4	<input type="text"/>
Block Outside DNS	<input type="checkbox"/> Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update	<input type="checkbox"/> Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	<input checked="" type="checkbox"/> Provide an NTP server list to clients
NTP Server 1	<input type="text" value="130.100.1.1"/>
NTP Server 2	<input type="text" value="130.100.1.3"/>
NetBIOS enable	<input checked="" type="checkbox"/> Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Para finalizar en configuración avanzada, se establece el ruteo hacia la red LAN.

Advanced Configuration	
Custom options	<input type="text" value='push "route 130.100.1.0 255.255.255.0"'/> Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"
UDP Fast I/O	<input type="checkbox"/> Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
Send/Receive Buffer	<input type="text" value="Default"/> Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.
Gateway creation	<input checked="" type="radio"/> Both <input type="radio"/> IPv4 only <input type="radio"/> IPv6 only If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Hacer clic con el mouse el botón **Save**

#### 4.12.4 Creación de usuarios para la VPN

En esta parte de la implementación se utilizará la base de datos de usuarios locales de PfSense, cada usuario contará con un certificado de autenticación que utilizará el cliente OpenVPN para realizar la conexión remota.

Menú: **SYSTEM/USER MANAGER/USERS**

Con el mouse hacer clic sobre el botón **Add** e ingresar los campos requeridos, la opción de group membership no se



la utiliza.

**User Properties**

Defined by: USER

Disabled:  This user cannot login

Username:

Password:  Confirm Password:

Full name:   
User's full name, for administrative information only

Expiration date:   
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings:  Use individual customized GUI options and dashboard layout for this user.

Group membership:    
Not member of:  Member of:

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate:  Click to create a user certificate

Activar el check de create a user certificate y añadir un nombre descriptivo.

Certificate:  Click to create a user certificate

**Create Certificate for User**

Descriptive name:

Certificate authority:

Key length:   
The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](http://keylength.com).

Lifetime:

Una vez concluido hacer clic con el mouse en el botón **Save**.

#### 4.13 Configuración de archivo WPAD

Para (Dueñas, 2016), WPAD (Web Proxy Auto-Discovery protocol) es un método utilizado por los clientes de servidores Proxy para localizar el URL de un archivo de configuración, valiéndose de métodos de descubrimiento a través de DHCP y DNS.

Los equipos clientes se descargan y ejecutan el archivo (.dat), éste utiliza un formato de auto-configuración del proxy. Para el despliegue del mencionado archivo en la red local se hará a través del siguiente método:

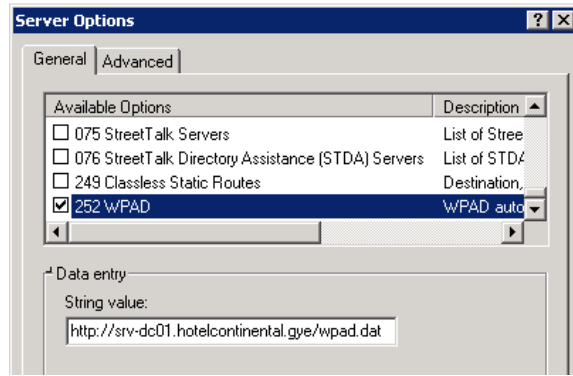
- A través de un servidor DHCP.

Basado en lo anterior y como parte de la implementación se procederá con el despliegue el archivo wpad.dat utilizando el servicio de Internet Information Server (ISS) el cual se encuentra ya instalado y configurado en el controlador de dominio bajo la siguiente ruta:

<http://srv-dc01.hotelcontinental.gye/wpad.dat>, su contenido es el siguiente:

```
function FindProxyForURL(url, host)
{
    if (
        isInNet(host, "130.100.1.0", "255.255.255.0")
        || isInNet(host, "130.100.3.0", "255.255.255.0")
        || isInNet(host, "127.0.0.0", "255.0.0.0")
        || shExpMatch(host, "130.100.*")
        || shExpMatch(host, "127.*" )
        || shExpMatch(host, "localhost")
        || isPlainHostName(host)
        || dnsDomainIs(host, ".hotelcontinental.gye")
    ) {
        return "DIRECT";
    }
    else
    {
        return "PROXY 130.100.1.254:3128";
    }
}
```

Adicional en el servidor DHCP se configura lo siguiente:



Con esto, todos los equipos de la red LAN a través del servicio de DHCP obtendrán la configuración automática del servidor proxy lo que conlleva un gran ahorro de tiempo en la administración de equipos en la red.

## 4.14 Pruebas de ejecución

Una vez implementado el servidor firewall PfSense community edition, se procederá con las diferentes pruebas de funcionalidad, para esto se ha creado un equipo virtual basado en Windows 7 Professional para pruebas de navegación, se ha creado un usuario de dominio llamado **test** el cual estará en cada uno de los grupos: **GG\_Internet\_Social\_Media**, **GG\_Internet\_Medium**, **GG\_Internet\_Full**.

Se realizarán además pruebas de salida al internet de servicios importantes como son el correo electrónico, facturación electrónica-portal de clientes, acceso a servidor FTP, y finalmente pruebas de conexión remota por OpenVPN y escritorio remoto.

### 4.14.1 Pruebas de acceso a internet

La primera prueba que se realizará con el usuario TEST es que éste no pertenezca a ningún grupo de acceso a internet, el resultado es el siguiente:

#### MICROSOFT – DENEGADO



Como se aprecia en la gráfica, a este usuario se le aplicó la regla por defecto que es impedir la salida a internet.

La segunda prueba es que el usuario test pertenezca al grupo GG\_internet\_social\_media la cual solo permite el acceso a sitios considerados como red social.

## FACEBOOK.

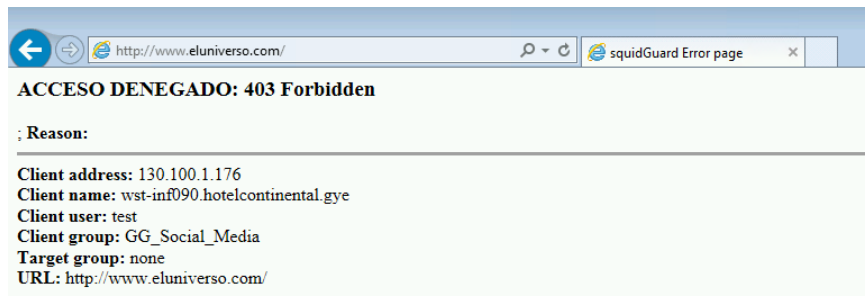
The screenshot shows the Facebook homepage in a browser. At the top, there is a navigation bar with the Facebook logo and a search bar. Below the navigation bar, there is a message: "We won't support this browser soon. For a better experience, we recommend using another browser. Más información". The main content area is split into two columns. The left column features the text "Facebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida." and a graphic of a globe with people icons connected by lines. The right column is titled "Abre una cuenta" and "Es rápido y fácil." It contains a registration form with fields for "Nombre", "Apellido", "Número de celular o correo electrónico", and "Contraseña nueva". There are also dropdown menus for "Fecha de nacimiento" (set to 6 nov 2019) and radio buttons for "Sexo" (Mujer, Hombre, Personalizado). A green "Registrarte" button is at the bottom of the form. A small disclaimer is visible below the form: "Al hacer clic en 'Registrarte', aceptas nuestras Condiciones, la Política de datos y la Política de cookies. Es posible que te enviemos notificaciones por SMS, que puedes desactivar cuando quieras."

## TWITTER

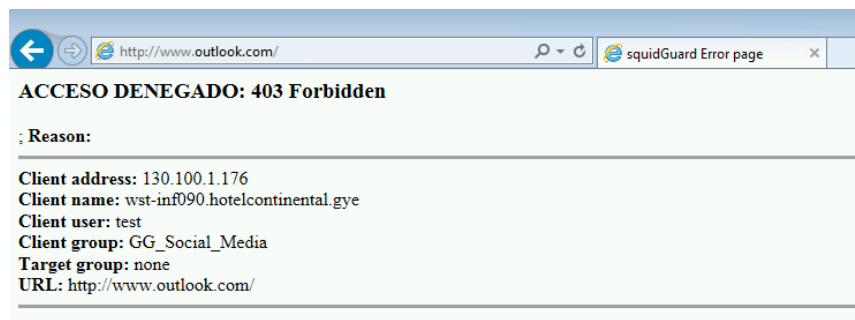
The screenshot shows the Twitter homepage in a browser. The left sidebar is blue and contains three search suggestions: "Sigue lo que te interesa.", "Entérate de lo que está hablando la gente.", and "Únete a la conversación.". The main content area is white and features the Twitter logo and the text "Descubre lo que está pasando en el mundo en este momento". Below this, there is a section titled "Únete hoy a Twitter." with a blue "Regístrate" button and a white "Iniciar sesión" button. At the top right, there is a login form with fields for "Teléfono, correo electró" and "Contraseña", and a blue "Iniciar sesión" button. A link for "¿Olvidaste tu contraseña?" is also present.

Sin embargo, al intentar ingresar a eluniverso.com y Outlook.com la solicitud fue denegada al no ser considerado como un sitio de red social.

## EL UNIVERSO – DENEGADO

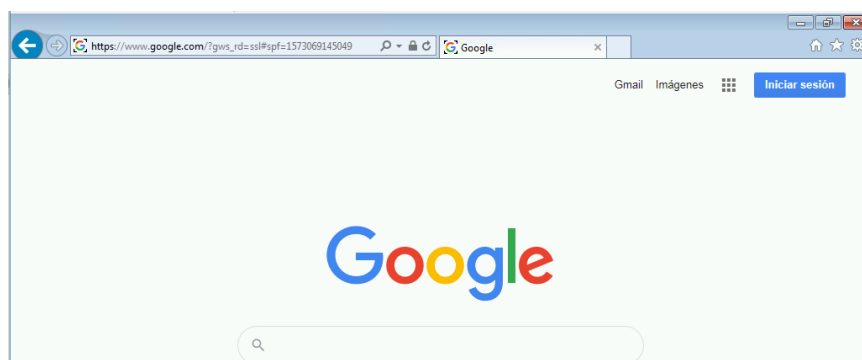


## OUTLOOK – DENEGADO

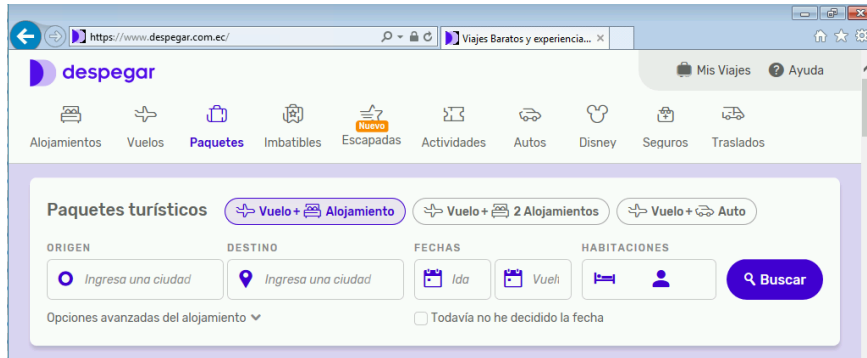


La tercera prueba es que el usuario test pertenezca al grupo GG\_internet\_Medium la cual no permite el acceso a sitios considerados tales como juegos en línea, películas, modelaje, noticias, control remoto, entre otros.

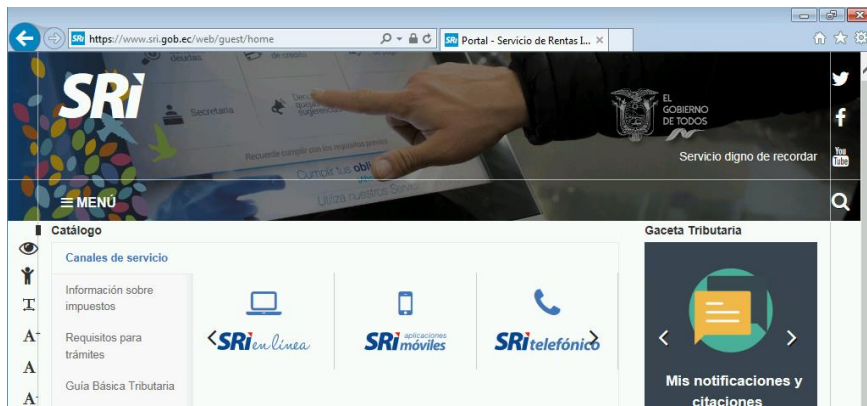
El acceso al sitio google.com se encuentra permitido



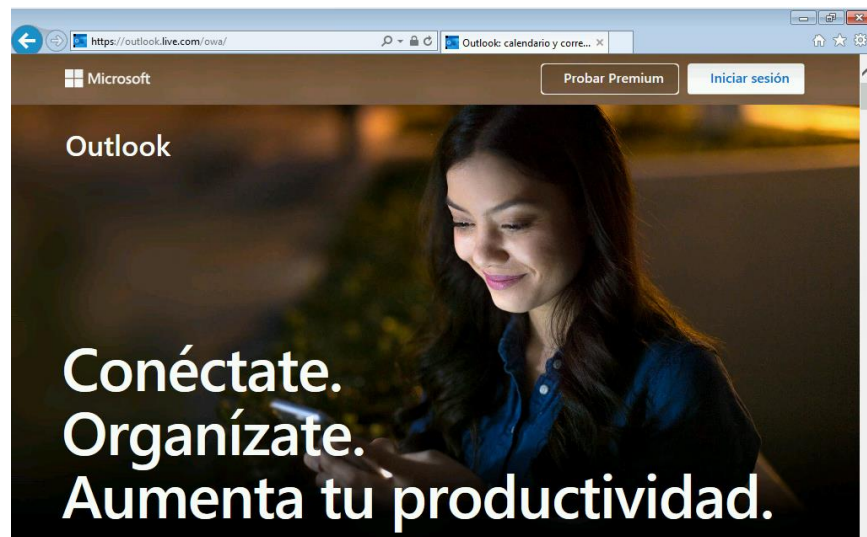
## DESPEGAR



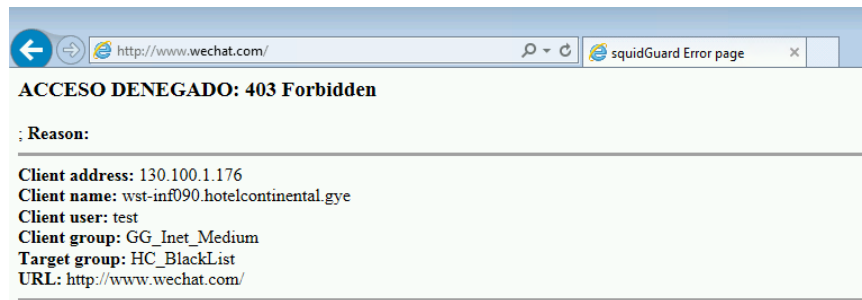
## SRI



## OUTLOOK

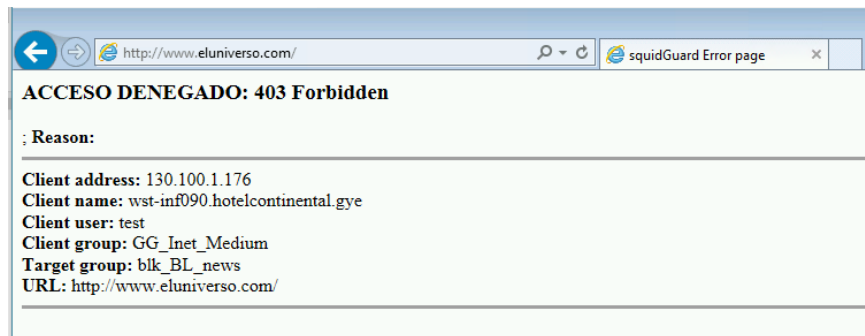


## WECHAT – DENEGADO



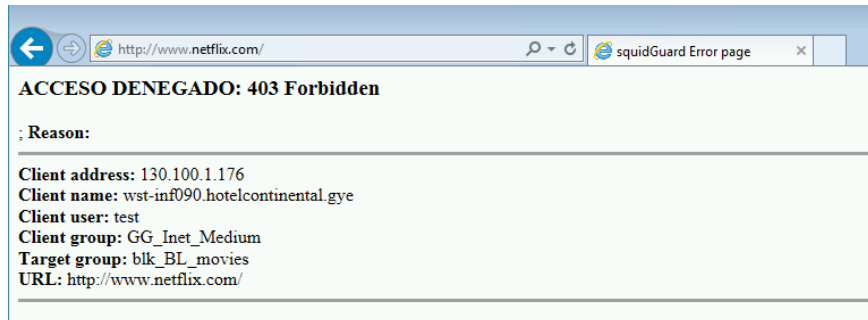
A screenshot of a web browser window showing a SquidGuard error page. The address bar contains 'http://www.wechat.com/'. The page title is 'ACCESO DENEGADO: 403 Forbidden'. Below the title, there is a section labeled ': Reason:' followed by a horizontal line. Underneath, the following details are listed: Client address: 130.100.1.176, Client name: wst-inf090.hotelcontinental.gye, Client user: test, Client group: GG\_Inet\_Medium, Target group: HC\_BlackList, and URL: http://www.wechat.com/.

## ELUNIVERSO –DENEGADO



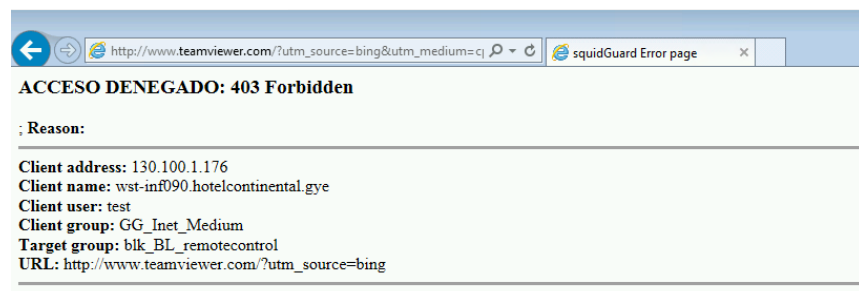
A screenshot of a web browser window showing a SquidGuard error page. The address bar contains 'http://www.eluniverso.com/'. The page title is 'ACCESO DENEGADO: 403 Forbidden'. Below the title, there is a section labeled ': Reason:' followed by a horizontal line. Underneath, the following details are listed: Client address: 130.100.1.176, Client name: wst-inf090.hotelcontinental.gye, Client user: test, Client group: GG\_Inet\_Medium, Target group: blk\_BL\_news, and URL: http://www.eluniverso.com/.

## NETFLIX – DENEGADO



A screenshot of a web browser window showing a SquidGuard error page. The address bar contains 'http://www.netflix.com/'. The page title is 'ACCESO DENEGADO: 403 Forbidden'. Below the title, there is a section labeled ': Reason:' followed by a horizontal line. Underneath, the following details are listed: Client address: 130.100.1.176, Client name: wst-inf090.hotelcontinental.gye, Client user: test, Client group: GG\_Inet\_Medium, Target group: blk\_BL\_movies, and URL: http://www.netflix.com/.

## TEAMVIEWER – DENEGADO



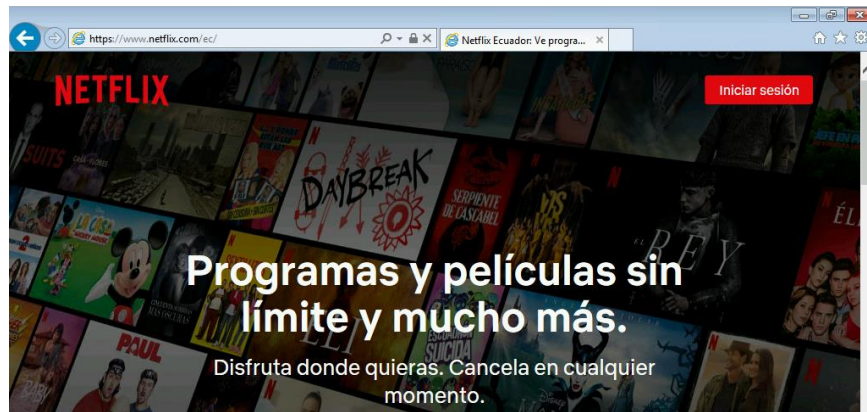
A screenshot of a web browser window showing a SquidGuard error page. The address bar contains 'http://www.teamviewer.com/?utm\_source=bing&utm\_medium=cj'. The page title is 'ACCESO DENEGADO: 403 Forbidden'. Below the title, there is a section labeled ': Reason:' followed by a horizontal line. Underneath, the following details are listed: Client address: 130.100.1.176, Client name: wst-inf090.hotelcontinental.gye, Client user: test, Client group: GG\_Inet\_Medium, Target group: blk\_BL\_remotecontrol, and URL: http://www.teamviewer.com/?utm\_source=bing.

La cuarta prueba se basa en que el usuario test pertenezca al grupo GG\_internet\_Full la cual no permite el

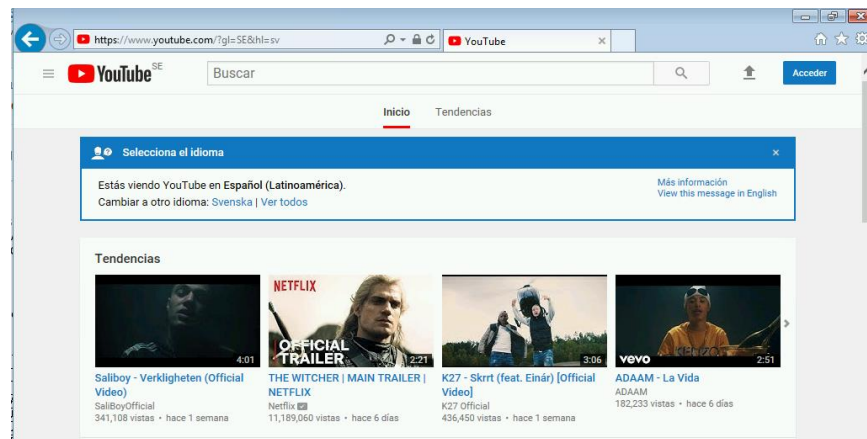


acceso a sitios considerados tales como hacking, pornografía, control remoto, warez, spyware.

## NETFLIX



## YOUTUBE



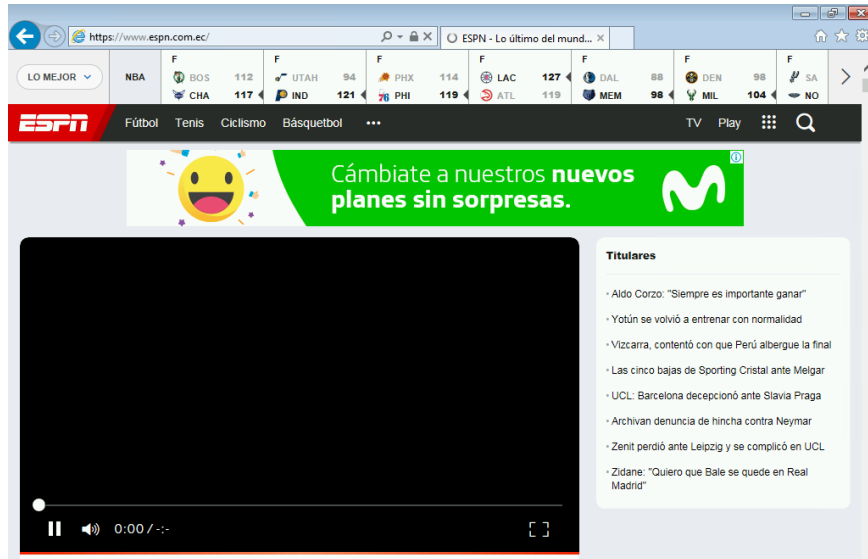
## ELUNIVERSO

The screenshot shows the homepage of the news website 'El Universo'. The browser address bar displays 'https://www.eluniverso.com/'. The main header features the site's name 'EL UNIVERSO' and a search icon. The primary headline is 'Ecuador, una 'gran autopista de la cocaína' hacia Estados Unidos y Europa, según informe internacional'. Below this headline are two sub-headers: 'Decomiso de droga cerca de Esmeraldas' and 'Hallan droga en encomienda que iba a Estados Unidos'. The page is organized into three columns of news items. The first column, under the heading 'DOCTOR TECNO', features an article titled 'Picap, la app de mototaxismo que ya está en Guayaquil' with an image of a person on a motorcycle. The second column, under 'POLÍTICA', has an article 'CIDH concluyó misión en Ecuador; informe estaría en cinco' with an image of a man speaking at a podium. The third column, also under 'POLÍTICA', features 'El exasambleísta Virgilio Hernández fue ingresado a la' with an image of a crowd of people.

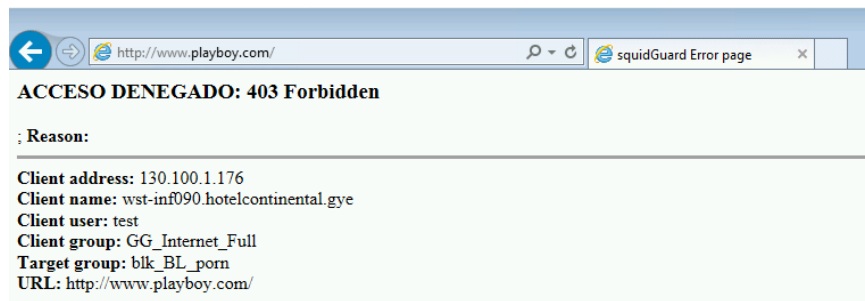
## AMAZON

The screenshot shows the homepage of the Amazon Ecuador website. The browser address bar displays 'https://www.amazon.com/'. The top navigation bar includes the Amazon logo, a search bar with 'Todos' as a dropdown, and links for 'Hola, Identificate Cuenta y Listas', 'Devoluciones y Pedidos', and 'Carrito'. Below the navigation bar, there are links for 'Enviar a Ecuador', 'Ofertas del Día', 'Ayuda', 'Listas', and 'Tarjetas de Regalo'. The main promotional banner is for 'Ofertas Navideñas' (Christmas Deals) with the tagline 'Ahorra en decoraciones, regalos y mucho más' (Save on decorations, gifts and much more). The banner features images of video game controllers, a snowflake icon, and a decorative pillow. Below the banner are three category-specific promotional tiles: 'Ofertas Navideñas' (Christmas Deals) with a pillow and game controllers, 'Ofertas Navideñas en Moda' (Christmas Deals in Fashion) with a brown coat, and 'Ofertas Navideñas en Hogar' (Christmas Deals in Home) with a white pot on a stove.

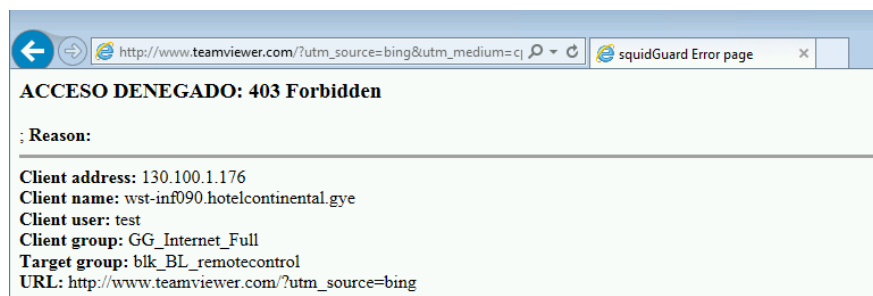
## ESPN



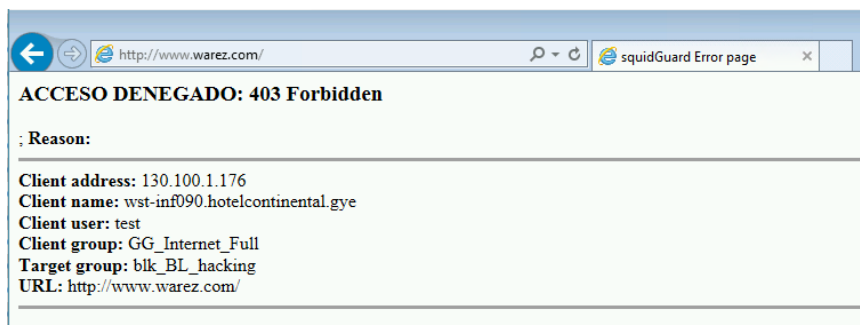
## PLAYBOY – DENEGADO



## TEAMVIEWER – DENEGADO



## WAREZ – DENEGADO



En base a las pruebas realizadas se comprueba que el servicio de squidGuard con filtrado de contenido web se encuentra funcionando correctamente.

### 4.14.2 Prueba del servidor de correo electrónico

La prueba se basará en la revisión de la regla de salida al internet por el protocolo tcp puerto 25(smtp) y 443 (owa y active sync) del servidor donde se podrá evidenciar las conexiones entrantes y salientes.

### Conexiones entrantes

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
WAN	tcp	92.118.38.54:14458 -> 130.100.1.13:25 (186.3.54.60:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	979 B / 1 KiB	
WAN	tcp	92.118.38.54:41668 -> 130.100.1.13:25 (186.3.54.62:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	979 B / 1 KiB	
WAN	tcp	141.98.80.100:39960 -> 130.100.1.13:25 (186.3.54.60:25)	FIN_WAIT_2:FIN_WAIT_2	13 / 9	750 B / 923 B	
WAN	tcp	92.118.38.38:16442 -> 130.100.1.13:25 (186.3.54.60:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	999 B / 1 KiB	
WAN	tcp	92.118.38.38:7150 -> 130.100.1.13:25 (186.3.54.59:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	999 B / 1 KiB	
WAN	tcp	46.38.144.146:8556 -> 130.100.1.13:25 (186.3.54.59:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	983 B / 1 KiB	
WAN	tcp	46.38.144.57:54796 -> 130.100.1.13:25 (186.3.54.59:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	975 B / 1 KiB	
WAN	tcp	45.227.253.140:36390 -> 130.100.1.13:25 (186.3.54.60:25)	TIME_WAIT:TIME_WAIT	13 / 9	771 B / 920 B	
WAN	tcp	45.227.253.140:31276 -> 130.100.1.13:25 (186.3.54.60:25)	TIME_WAIT:TIME_WAIT	13 / 9	739 B / 920 B	
WAN	tcp	46.38.144.32:56342 -> 130.100.1.13:25 (186.3.54.59:25)	FIN_WAIT_2:FIN_WAIT_2	16 / 13	923 B / 1 KiB	
WAN	tcp	46.38.144.17:2916 -> 130.100.1.13:25 (186.3.54.59:25)	FIN_WAIT_2:FIN_WAIT_2	17 / 12	983 B / 1 KiB	

## Conexiones salientes

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
LAN	tcp	130.100.1.13:60185 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	40 / 27	39 KiB / 3 KiB	
LAN	tcp	130.100.1.13:60187 -> 62.112.113.23:25	FIN_WAIT_2:FIN_WAIT_2	7 / 8	405 B / 622 B	
LAN	tcp	130.100.1.13:60201 -> 173.194.216.27:25	FIN_WAIT_2:FIN_WAIT_2	12 / 14	957 B / 2 KiB	
LAN	tcp	130.100.1.13:60217 -> 141.206.151.241:25	TIME_WAIT:TIME_WAIT	13 / 14	1 KiB / 4 KiB	
LAN	tcp	130.100.1.13:60227 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	128 / 77	151 KiB / 6 KiB	
LAN	tcp	130.100.1.13:60230 -> 190.57.169.119:25	CLOSED:SYN_SENT	3 / 0	152 B / 0 B	
LAN	tcp	130.100.1.13:60233 -> 62.112.113.23:25	FIN_WAIT_2:FIN_WAIT_2	7 / 8	405 B / 622 B	
LAN	tcp	130.100.1.13:60235 -> 212.92.23.162:25	TIME_WAIT:TIME_WAIT	12 / 13	925 B / 1 KiB	
LAN	tcp	130.100.1.13:60248 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	41 / 28	40 KiB / 3 KiB	
LAN	tcp	130.100.1.13:60259 -> 104.18.33.75:25	CLOSED:SYN_SENT	2 / 0	104 B / 0 B	
LAN	tcp	130.100.1.13:60262 -> 186.5.73.250:25	TIME_WAIT:TIME_WAIT	1 / 1	48 B / 40 B	

## OWA (Outlook web Access) y Active Sync

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
LAN	tcp	130.100.1.13:60185 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	40 / 27	39 KiB / 3 KiB	
LAN	tcp	130.100.1.13:60187 -> 62.112.113.23:25	FIN_WAIT_2:FIN_WAIT_2	7 / 8	405 B / 622 B	
LAN	tcp	130.100.1.13:60201 -> 173.194.216.27:25	FIN_WAIT_2:FIN_WAIT_2	12 / 14	957 B / 2 KiB	
LAN	tcp	130.100.1.13:60217 -> 141.206.151.241:25	TIME_WAIT:TIME_WAIT	13 / 14	1 KiB / 4 KiB	
LAN	tcp	130.100.1.13:60227 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	128 / 77	151 KiB / 6 KiB	
LAN	tcp	130.100.1.13:60230 -> 190.57.169.119:25	CLOSED:SYN_SENT	3 / 0	152 B / 0 B	
LAN	tcp	130.100.1.13:60233 -> 62.112.113.23:25	FIN_WAIT_2:FIN_WAIT_2	7 / 8	405 B / 622 B	
LAN	tcp	130.100.1.13:60235 -> 212.92.23.162:25	TIME_WAIT:TIME_WAIT	12 / 13	925 B / 1 KiB	
LAN	tcp	130.100.1.13:60248 -> 144.202.248.36:25	TIME_WAIT:TIME_WAIT	41 / 28	40 KiB / 3 KiB	
LAN	tcp	130.100.1.13:60259 -> 104.18.33.75:25	CLOSED:SYN_SENT	2 / 0	104 B / 0 B	
LAN	tcp	130.100.1.13:60262 -> 186.5.73.250:25	TIME_WAIT:TIME_WAIT	1 / 1	48 B / 40 B	

### 4.14.3 Ingreso a sitio de facturación electrónica clientes

Como se ha indicado anteriormente el servidor web que contiene el sitio de facturación electrónica para clientes se encuentra en una red DMZ para lo cual se han creado las reglas necesarias para su acceso mediante conexiones entrantes con protocolo TCP con puerto 80.

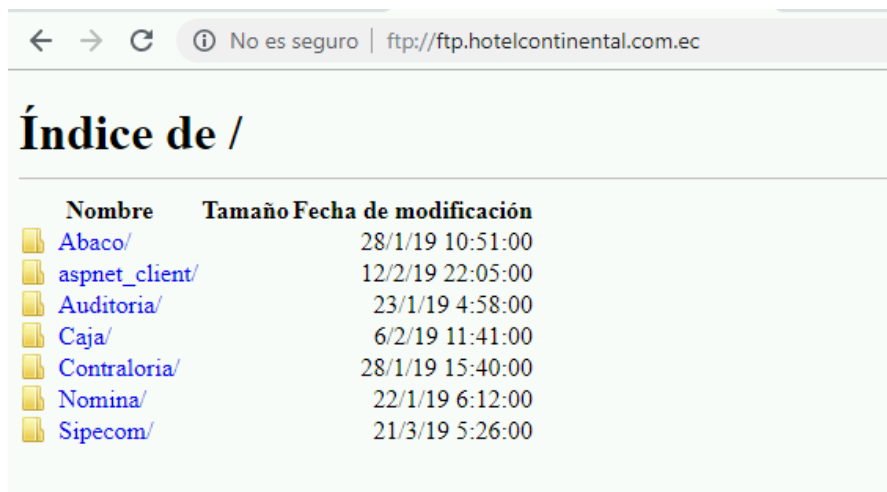
States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
WAN	tcp	181.198.6.75:53895 -> 130.100.3.5:80 (186.3.54.62:80)	FIN_WAIT_2:FIN_WAIT_2	14 / 17	4 KIB / 16 KIB	
WAN	tcp	181.198.6.75:53897 -> 130.100.3.5:80 (186.3.54.62:80)	TIME_WAIT:TIME_WAIT	3 / 2	132 B / 92 B	
WAN	tcp	181.198.6.75:53927 -> 130.100.3.5:80 (186.3.54.62:80)	FIN_WAIT_2:FIN_WAIT_2	6 / 3	1 KIB / 342 B	
WAN	tcp	181.198.6.75:53929 -> 130.100.3.5:80 (186.3.54.62:80)	FIN_WAIT_2:FIN_WAIT_2	7 / 4	2 KIB / 593 B	
WAN	tcp	181.198.6.75:53926 -> 130.100.3.5:80 (186.3.54.62:80)	FIN_WAIT_2:FIN_WAIT_2	7 / 4	2 KIB / 592 B	
WAN	tcp	181.198.6.75:53930 -> 130.100.3.5:80 (186.3.54.62:80)	FIN_WAIT_2:FIN_WAIT_2	12 / 8	6 KIB / 3 KIB	
WAN	tcp	181.198.6.75:53928 -> 130.100.3.5:80 (186.3.54.62:80)	TIME_WAIT:TIME_WAIT	3 / 2	132 B / 92 B	



#### 4.14.4 Pruebas de acceso al servidor FTP

El servidor FTP (puerto 21) se encuentra también en la red DMZ y se encuentra accesible mediante la regla ya establecidas anteriormente, en las siguientes imágenes se verifica el acceso de forma correcta.

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes	
WAN	tcp	181.198.6.75:52476 -> 130.100.3.6:21 (186.3.54.59:21)	FIN_WAIT_2:FIN_WAIT_2	15 / 15	704 B / 951 B	
WAN	tcp	181.198.6.75:52477 -> 130.100.3.6:54563 (186.3.54.59:54563)	FIN_WAIT_2:FIN_WAIT_2	4 / 4	172 B / 514 B	

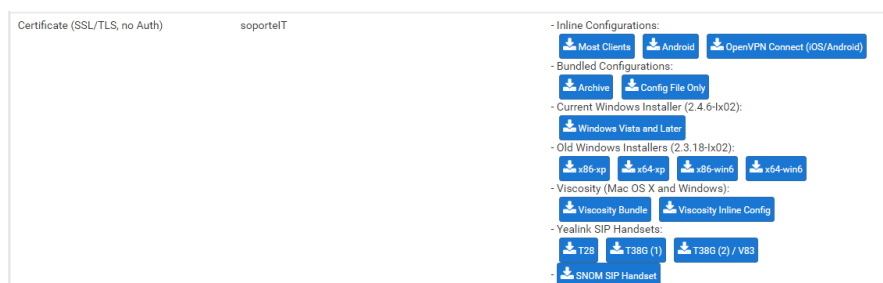


#### 4.14.5 Pruebas de conexión remota mediante OpenVPN

Para realizar las pruebas, se ha instalado el cliente OpenVPN en un computador externo a la organización, el software OpenVPN ya configurado con el certificado de autenticación se puede descargar en el sitio de configuración de PfSense como se muestra a continuación.

##### Menú VPN/OPENVPN/CLIENT EXPORT

Se ubica en el nombre de usuario creado anteriormente y se descarga el cliente OpenVPN según la plataforma, en este caso se utilizará el instalador para Windows.



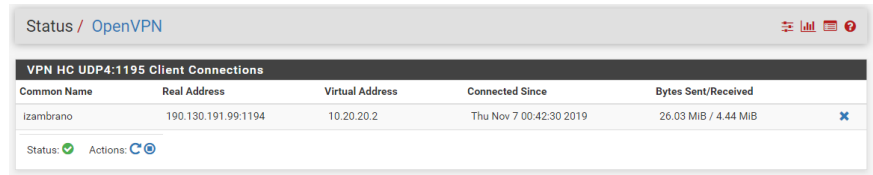
Una vez instalado en el equipo remoto se procede a la conexión remota según la siguiente imagen:

Clic con el mouse sobre **Connect**





## Menu: STATUS/OPENVPN

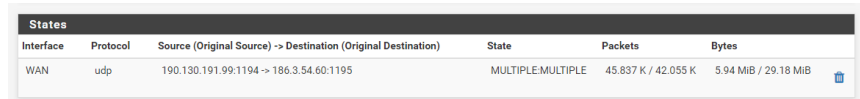


The screenshot shows the Mikrotik WinBox interface for the 'Status / OpenVPN' page. At the top, there is a breadcrumb 'Status / OpenVPN' and some utility icons. Below that is a section titled 'VPN HC UDP4:1195 Client Connections'. It contains a table with the following data:

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent/Received
izambrano	190.130.191.99:1194	10.20.20.2	Thu Nov 7 00:42:30 2019	26.03 MIB / 4.44 MIB

Below the table, the status is shown as 'Status: ✔' and 'Actions: [C](#) [E](#)'.

Y a nivel de reglas en el firewall se puede visualizar la conexión realizada.



The screenshot shows the Mikrotik WinBox 'States' page. It displays a table with the following data:

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	udp	190.130.191.99:1194 -> 186.3.54.60:1195	MULTIPLE.MULTIPLE	45.837 K / 42.055 K	5.94 MIB / 29.18 MIB

Con esto finalizan las pruebas de implementación del Firewall PfSense community edition en Continental Hotel S.A. obteniendo una plataforma estable y el haber cumplido con todo lo requerido según la infraestructura de la misma.

## CAPITULO 5

### 5 CONCLUSIONES Y RECOMENDACIONES

#### 5.1 Conclusiones

La implementación de la solución de una plataforma firewall administrado por el software PFSENSE community edition pudo ser realidad gracias a la capacitación recibida mediante un curso por parte de personal experto en el tema, asimismo mediante investigación en foros del fabricante.

Se diagnosticó el estado actual de la solución de firewall con que se contaba lo que dio pie a la falta de una solución en seguridad robusta en la disminución de vulnerabilidades en servicios de red de Continental Hotel S.A.

Se logró implementar la solución firewall administrado por el software PFSENSE community edition en CONTINENTAL HOTEL S.A. cumpliendo con lo requerido basado en la infraestructura de la empresa.

En el caso de que se presente algún daño físico en el servidor host o que éste ingrese a trabajos de mantenimiento o actualizaciones de hardware o software, se cuenta con 2 replicaciones automáticas del servidor virtual donde funciona PfSense y adicionalmente una replicación extendida hacia las bodegas del almacén, en total se cuentan con 3 respaldos en distintos lugares y horario.

## 5.2 Recomendaciones

- Mantener capacitación constante al personal del área de informática en cuanto al servidor Firewall PfSense Community Edition.
- Mantenerse al día en las actualizaciones del software actualizaciones y buenas prácticas en el uso de la herramienta.
- Mantener puntos de control en Hyper V al realizar cambios o actualizaciones y se requiera reversar.
- Realizar simulacros mediante el uso la conmutación por error de Hyper V.
- Contar con replicación del equipo virtual contratando el servicio en la nube.
- Adicional realizar copia de seguridad de la configuración actual después de cada cambio realizado.

## **6 ANEXOS**

### **6.1 Anexo 1**

#### **Preguntas para la entrevista con responsable del departamento de Informática de CONTINENTAL HOTEL S.A.**

1. ¿Cuál es su nombre y que cargo tiene en la empresa?
2. ¿Cuáles son las tareas que realiza dentro de su departamento?
3. ¿Cuántos firewalls existen dentro de su red?
4. ¿Cuál es el nombre del software que le provee servicios de firewall?
5. ¿Utilizaría otra plataforma en lugar de la implementada en la empresa?
6. ¿Cómo usted calificaría su firewall?
7. ¿Actualmente su firewall se encuentra en condiciones de brindar seguridad a su red?
8. ¿Su firewall ha experimentado algún tipo riesgos?
9. ¿No se ha planteado la posibilidad de implantar un firewall distinto del que cuenta actualmente?

10. ¿Con que tipo de problemas usted ha tenido que lidiar en lo que respecta con el uso firewall?
11. ¿Cerca de cuántos usuarios en el hotel acceden a servicios que utilizan el internet?
12. ¿Cree usted que la implementación del proyecto propuesto contribuirá en la disminución de vulnerabilidades del trafico entrante y saliente?

## 6.2 Anexo 2

### **Preguntas para la encuesta a usuarios administrativos de CONTINENTAL HOTEL S.A.**

**1. ¿Con que frecuencia utiliza los servicios a través del internet?**

- Diariamente
- Una vez por semana
- Mensualmente
- No accedo

**2. ¿Considera que el acceso a internet y otros servicios los utiliza de forma segura?**

Si\_\_\_

No\_\_\_

No tengo conocimiento\_\_\_

**3. ¿Qué tan importante es para usted mejorar la seguridad de los servicios a través de internet?**

Muy importante\_\_\_

Nada importante\_\_\_

No tengo conocimiento\_\_\_

**4. ¿Ha tenido algún problema o inconveniente de seguridad al momento de utilizar los servicios a través del internet?**

Si\_\_\_

No\_\_\_

No tengo conocimiento\_\_\_

**5. ¿Con que frecuencia se conecta desde el exterior a su computador de trabajo de forma remota?**

- Diariamente

- Una vez por semana
- No accedo

**6. ¿Cree usted que es necesario mantenerse actualizado en lo que respecta a seguridad informática?**

Muy necesario\_\_

No necesario\_\_

No tengo conocimiento\_\_

**7. ¿Cree usted que la implementación de un nuevo firewall ayudará a mejorar la seguridad dentro de la empresa?**

Si\_\_

No\_\_

No tengo conocimiento\_\_

**8. ¿Tiene usted conocimiento acerca de las vulnerabilidades que existen al utilizar los servicios a través del internet?**

Mucho\_\_

Poco\_\_

Nada\_\_

**9. ¿Cree usted que es necesario se realice una charla sobre seguridad informática?**

Si\_\_

No\_\_

**10. ¿Está usted de acuerdo en que el acceso a los servicios que se utilizan a través del internet sean debidamente controlados por un firewall?**

De acuerdo\_\_

No estoy de acuerdo\_\_

## 7 BIBLIOGRAFÍA

- Alto, P. (2012). Resumen del firewall de nueva generación . Santa Clara, California.
- Anon. (2015). Curso de Administrador de Servidores Internet.
- Arias, F. G. (2012). *El Proyecto de Investigación*. Caracas: Editorial Episteme.
- Bravo, R. S. (1984). *Ciencias sociales, epistemología, lógica y metodología*. Madrid: Parainfo.
- Cazau, P. (2006). *Introducción a la Investigación*. Buenos Aires. Obtenido de [https://www.academia.edu/28761556/La\\_investigaci%C3%B3n\\_bibliogr%C3%A1fica\\_-\\_2014?auto=download](https://www.academia.edu/28761556/La_investigaci%C3%B3n_bibliogr%C3%A1fica_-_2014?auto=download)
- Cazau, P. (2006). *INTRODUCCIÓN A LA INVESTIGACIÓN*. Buenos Aires.
- Dominguez, L. A. (2016). *Biblioteca virtual ITB*. Obtenido de <https://sga.itb.edu.ec/media/biblioteca/2017/01/03/tesis.pdf>
- Dueñas, J. B. (19 de 09 de 2016). *Alcancelibre*. Obtenido de <http://www.alcancelibre.org/staticpages/index.php/como-wpad>
- Esparza Morocho, J. P. (27 de 03 de 2013). *Repositorio Digital Institucional de la Escuela Politécnica Nacional*. Obtenido de <http://bibdigital.epn.edu.ec/handle/15000/6056>
- Forero Gandur, J. W. (2013). *Universidad Piloto de Colombia*. Obtenido de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2875/00002324.pdf?sequence=1>
- Frank, M. (2012). *Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa*. Obtenido de [http://www.academia.edu/download/34550277/Conozca\\_3\\_tipos\\_de\\_investigacion.docx](http://www.academia.edu/download/34550277/Conozca_3_tipos_de_investigacion.docx)
- García Vélez, J. J. (2007). *Repositorio Digital Universidad De Las Américas*. Obtenido de <http://dspace.udla.edu.ec/handle/33000/4031>
- Hardware, F. (2019). *Firewall Hardware*. Obtenido de <http://www.firewallhardware.es/pfsense.html>
- INEN. (04 de 2017). *Servicio Ecuatoriano de Normalización*. Obtenido de [https://181.112.149.204/buzon/normas/n-te\\_inen\\_iso\\_iec\\_27002.pdf](https://181.112.149.204/buzon/normas/n-te_inen_iso_iec_27002.pdf)
- Informática, S. d. (01 de 2009). *Gobierno Electronico*. Obtenido de [https://cti.gobiernoelectronico.gob.ec/ayuda/manual/decreto\\_1014.pdf](https://cti.gobiernoelectronico.gob.ec/ayuda/manual/decreto_1014.pdf)



- Jiménez, E. (02 de 14 de 2014). *Curso de Administrador de Servidores Internet*. Mexico, Mexico DF.
- Kaspersky. (13 de 08 de 2018). *Comunicados de prensa*. Obtenido de [https://latam.kaspersky.com/about/press-releases/2018\\_panorama-de-amenazas-phishing](https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing)
- Martínez, K. (02 de 12 de 2009). *Firewall - Linux: Una solución de seguridad informática para pymes*. Obtenido de Redalyc: <https://www.redalyc.org/pdf/5537/553756879003.pdf>
- Netgate. (2019). *Netgate Docs*. Obtenido de <https://docs.netgate.com/pfsense/en/latest/book/hardware/minimum-hardware-requirements.html>
- Netgate. (2019). *Netgate Solutions*. Obtenido de <https://www.netgate.com/solutions/pfsense/features.html>
- Netgate. (2019). *Netgate Solutions*. Obtenido de <https://www.netgate.com/solutions/pfsense/>
- Odón, F. G. (2012). *El proyecto de investigación. Introducción a la metodología científica*.
- Paneque, R. J. (1998). *METODOLOGÍA DE LA INVESTIGACIÓN*. La habana: Editorial de Ciencias Médicas.
- Pedroza, R. (12 de 04 de 2017). *SiliconWeek*. Obtenido de <https://www.siliconweek.com/software/open-source/red-hat-software-libre-crece-america-latina-79284>
- Peñaherrera, C. C. (23 de 08 de 2013). *Secretaría de planificación*. Obtenido de <https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%3%83%c2%b3n.pdf>
- Pérez, J. (20 de 06 de 2007). *Firewalls*. Obtenido de TIC: <http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf>
- Pérez, J. Á. (2011). *Firewalls*.
- Ramírez, T. (2010). *Cómo hacer un proyecto de investigación*. Caracas: Panapo.
- Rienzo, J. D. (2009). *Estadística Ciencias Agropecuarias*. Argentina: Brujas.
- Sabino, J. (1992). *El proceso de la investigación*. Caracas: Panapo.
- Salkind, N. J. (1998). *Métodos de Investigación*. México: Prentice Hall.

Sanjuan, L. D. (2011). *Universidad autónoma de Mexico*. Obtenido de [http://www.psicologia.unam.mx/documentos/pdf/publicaciones/La\\_observacion\\_Lidia\\_Diaz\\_Sanjuan\\_Texto\\_Apoyo\\_Didactico\\_Metodo\\_Clinico\\_3\\_Sem.pdf](http://www.psicologia.unam.mx/documentos/pdf/publicaciones/La_observacion_Lidia_Diaz_Sanjuan_Texto_Apoyo_Didactico_Metodo_Clinico_3_Sem.pdf)

William, V. D. (1981). *Manual de técnicas de la investigación educacional*. Barcelona: Paidós.