Universidad Michoacana de San Nicolas de Hidalgo

Facultad de Ciencias Físico Matemáticas

Mat. Luis Manuel Rivera Gutiérrez

Diseño, implementación y documentación de un firewall de alta disponibilidad

Tesis
Para obtener el título de
Licenciado en ciencias Físico Matemáticas

PRESENTA
Lorena Peña García

ASESOR
Edgardo Morales Ontiveros

Morelia, Mich. Septiembre 2009

Índice general

Índice de figuras

Capítulo 1

Introducción

Las sociedades avanzadas de principios de este siglo son denominadas con frecuencia *"sociedades de la información"*, pues el volumen de datos que es procesado, almacenado y transmitido es incomparablemente mayor que en cualquier época pretérita.

Además la importancia de esta información es imprecindible para el desarrollo económico y social. Las organizaciones consideran que la información es un bien más de sus activos y, en muchos casos, prioritario sobre los restantes.

Así mismo todo lo que conlleva almacenar, procesar y enviar esa información, como son los medios de comunicación, las respectivas aplicaciones que se utilizan y los medios físicos de los que se valen comúnmente las llamadas tecnologías de información, adquieren la misma relevancia que la información misma, ya que no existiría una sin las demás.

No hay que dejar de mencionar el inminente crecimiento de Internet, y el impacto social que está causando en nuestra vida diaria, está cambiando la forma de vida de las sociedades, todo es más práctico y las distancias no parecen existir, haciendo nuestra vida más sencilla y práctica, quitando la limitante económica que significaba trasladarse a otros lugares. En estos tiempos es muy sencillo desde comprar un artículo seminuevo a algún desconocido en Argentina, hasta estudiar una carrera profesional a distancia en instituciones internacionales. Un problema de seguridad real, son los virus, los cuales pueden destruir información en los sistemas basados en Windows, para lo cual existe una diversa cantidad de antivirus en el mercado, sin embargo en ocasiones, el costo de licencias es elevado impidiendo a los usuarios acceder facilmente a actualizaciones. Por otro lado la evolución de virus sobrepasa la efectividad de los antivirus, es decir, diariamente aparecen variaciones o mutaciones que son indetectables por las versiones más recientes de antivirus.

Un aspecto en contra a todas las posibilidades que nos oferta Internet, es la seguridad de la información, por un lado no existe garantía de que la información que es enviada a algun sitio web (información confidencial de los clientes de una institución Bancaria) viaje por un medio seguro, y por otro lado no podemos confiar ciegamente en que la información que descargamos, provenga de una fuente confiable. En ambos casos existe el peligro latente de ver comprometida la integridad de la información. Es aquí donde la Seguridad Informática tiene su campo de acción para ayudar a proteger de ataques a la información, perpetrados por terceras personas o sistemas externos. En la actualidad la seguridad de los sistemas de información es de vital importan-

cia. Ya que en muchas ocasiones, la pérdida de información motiva a la instalación de esquemas más robustos en la infraestructura de red de cómputo. La Seguridad de los Sistemas de Información (SSI) está relacionada con la disponibilidad, confidencialidad e integridad de la información (veáse la figura 1.1)) manejada por los computadoras y las redes de comunicación. Se usan comúnmente otros términos que en esencia tienen el mismo significado, tales como la seguridad de la información, seguridad de las computadoras y seguridad de datos o protección de la información, pero se orientan a la Seguridad de los Sistemas de Información, como un todo, hardware, software y usuarios.

Figura 1.1: Disponibilidad, confidencialidad e integridad de la información

Dentro del amplio horizonte que abarca el tema de la seguridad informática, los firewalls (cortafuegos) toman una importancia relevante, ya que son el recurso de seguridad que protege de ataques, por lo tanto debe ser aplicado en todo tipo de entorno, principalmente en servidores, así que es fundamental contar con este tipo de protección y saber cómo manejarla.

Existen cortafuegos de basados software libre (0 pesos) que a veces son dificiles de instalar, sin embargo no existe suficiente documentación sobre su funcionamiento, lo cual resolver alguna situacion en particular podria tomar tiempo en resolverla. Por otro lado los firewalls comerciales son costosos ya que se requiere comprar accesorios especificos de ese fabricante, su instalación es realizada por personal ajeno, y en caso de que se requiera soporte técnico es necesario nuevamente realizar el pago de una licencia.

Este proyecto está organizado de la siguiente manera: En el capítulo 2, se presentan los conceptos básicos como de la comunicación en los equipos de una red, los orígenes del sistema operativo en el que está basado el firewall, características y ventajas de tener un firewall instalado, las diferencias entre firewalls comerciales y de licencia libre. La instalación y configuración esta descrita en el capítulo 3, aquí se mencionan los aspectos generales sobre la instalación estándar. El capítulo 4 trata de la configuración de las reglas del firewall y algunas características particulares. Para proporcionar un mayor ancho de banda, redundancia de conexión hablamos de balanceo de carga en el capítulo 5. Para proporcionar un acceso seguro y acceso a la red de la organización remotamente mediante OpenVPN, además de otros elementos de autenticación se mencionan en el capítulo 6. En el capítulo 7 se describe la tolerancia y redundancia en los servidores de red. Y el caso de estudio de la problemática de la red de una organización (Facultad de Cs. Físico Matemáticas, UMSNH)

así como las soluciones propuestas se presentan en el capítulo 8. Finalmente en el capítulo 9 se presentan los resultados y conclusiones de dicho proyecto.

Los objetivos de este proyecto son comparar en funcionamiento los firewalls comerciales contra los firewalls basados en software libre de código abierto, además se incluye documentación sobre la administración y configuración de un firewall como solución al problema de seguridad informática y administración en una organización.

Se espera que la conjunción del análisis e implantación de éste proyecto, motive a otros administradores a utilizar software libre en lugar de su contraparte comercial.

Capítulo 2

Conceptos básicos

2.1. Tecnología

Actualmente las tecnologías de red se basan en los siguientes estándares:

El cable coaxial es utilizado para transportar señales eléctricas de alta frecuencia, que posee dos conductores concéntricos, uno central, llamado positivo o vivo, encargado de llevar la información, y uno exterior (de aspecto tubular), llamado malla o blindaje que sirve como referencia de tierra y retorno de las corrientes.

La fibra óptica es un medio de transmisión inmune a las interferencias, ampliamente utilizada en redes locales, transmisión de datos y transmisión de video a grandes distancias (superando los 50 kilómetros) a mayor velocidad que con un cable y por radio. Una posible desventaja es su precio elevado.

El Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos, ambas se diferencian en uno de los campos de la trama de datos (las tramas Ethernet y IEEE 802.3 pueden coexistir en la misma red).

Ethernet Giga bit también conocida como GibE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE2) que consigue una capacidad de transmisión de 1 giga bit por segundo que en la práctica se convierte en unos 100 mega bytes útiles, funciona sobre cables de cobre (par trenzado) del tipo UTP y categoría 6, y fibra óptica. La última especificación IEEE para 10 Giga bit Ethernet (8023an), también conocido como el estándar 10GBASE-T3 10GBASE-T3 de par trenzado sin blindaje de categoría 6 de cableado de cobre. Todas las razones para el uso de iSCSI4 iSCSI especialmente de bajo costo y simplicidad se ven reforzadas por el nuevo pliego de condiciones, rendimiento a velocidades de hasta 10Gbit/seg.

2.2. Plan para la comunicación de la información

La comunicación se lleva a cabo por protocolos, y se han desarrollado varias herramientas para ayudar a los diseñadores de protocolos a entender las partes del problema de comunicación y planear la familia de protocolos. Una de las herramientas más importantes se llama modelo de capas, esta es una manera de

dividir el problema de la comunicación en partes llamadas capas. La familia de protocolos puede diseñarse especificando un protocolo que corresponda a cada capa.

2.2.1. Capas y protocolos TCP/IP

El modelo TCP/IP es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permite la transmisión de datos entre redes de computadoras. En ocasiones se la denomina conjunto de protocolos TCP/IP. (veáse la tabla 2.1), en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia.

Aplicación
Transportación
Internet
Enlace
Física

Tabla 2.1: Capas del modelo TCP/IP

Cuatro de las capas del modelo de referencia TCP/IP corresponden a una o más capas del modelo de referencia ISO. Sin embargo, éste modelo no tiene una capa de Internet. A continuación se describen las capas del modelo TCP/IP.

1. *Física*. La capa uno corresponde al hardware básico de red, igual que la capa uno del modelo de referencia de siete capas de la ISO.

2. *Enlace*. Los protocolos de esta capa especifican como son transportados los paquetes sobre la capa física incluyendo los delimitadores (patrones de bits concretos que marcan el comienzo y el fin de cada envío de datos).

3. *Internet*. Los protocolos de esta capa indican el formato de los paquetes enviados por una red sencilla, así como el mecanismo para reenviar paquetes del transmisor, por medio de los enrutadores, a su destino final.

4. *Transportación*. Los protocolos de ésta como los de la misma capa del modelo ISO, especifican la manera de asegurar una transferencia confiable.

5. *Aplicación*. Ésta capa corresponde a las capas 6 y 7 del modelo ISO, los protocolos de esta capa definen la manera en que las aplicaciones usan el Internet.

Los protocolos TCP/IP se organizan en cinco capas conceptuales, aunque algunas capas del modelo de referencia TCP/IP corresponden a las capas del modelo de referencia ISO, el esquema de capas ISO no tiene una capa que corresponda a la capa de Internet de TCP/IP.

2.2.2. Capas y protocolos ISO

En los albores de la historia de la conectividad, la Organización Internacional de Normalización (ISO) definió un modelo de referencia de siete capas (veáse la tabla 2.2).

Aplicación
Presentación
Sesión
Transportación
Red
Enlace de datos
Física

Tabla 2.2: Modelo de capas de las ISO

Aunque los conceptos sobre el diseño de protocolos han cambiado en los 20 años transcurridos desde el desarrollo del modelo ISO, existen muchos protocolos modernos que no encajan en el modelo anterior.

El modelo ISO es conocido porque ofrece una explicación sencilla de la relación entre los complejos componentes de hardware y de protocolo de la red. En este modelo la capa inferior corresponde al hardware y las capas sucesivas al software que usa la red. A continuación se describen las capas de la ISO:

1. *Física*. Esta capa corresponde al hardware de red básico.
2. *Enlace de datos*. Especifica la manera de organizar los datos en paquetes y su transmisión por la red. Por ejemplo, los estudios sobre los formatos de cuadros, relleno de bits o bytes y cálculo de cifras de comprobación.
3. *Red*. Los protocolos de esta capa especifican la asignación de las direcciones y el reenvío de paquetes de un extremo de la red al otro.
4. *Transportación*. Los protocolos de esta capa que especifican los detalles de la transferencia confiable, son de los más complicados.
5. *Sesión*. Indican cómo establecer sesiones de comunicación con un sistema remoto. Por ejemplo, cómo establecer una sesión con una computadora de tiempo compartido remota. La especificación de detalles de seguridad como la validación de identificación mediante contraseñas pertenece a esta capa.
6. *Presentación*. Los protocolos de la capa 6 especifican la manera de representar los datos. Tales protocolos son necesarios porque las diferentes marcas de computadoras usan distintas representaciones internas para los enteros y los caracteres. Por lo tanto los protocolos de esta capa son necesarios para traducir de la representación de una computadora a la representación de la otra.
7. *Aplicación*. Cada protocolo de esta capa especifica cómo usa la red una aplicación particular. El protocolo especifica los detalles sobre cómo hace una solicitud el programa de aplicación de una máquina, por ejemplo, cómo especificar el nombre del archivo deseado, y cómo responde la otra máquina.

2.3. Firewall

Un firewall es un elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas. Puede ser un conjunto de dispositivos (hardware y software) situados entre un equipo o una red pública, o bien entre dos redes. Para proteger la red de un atacante, todo el tráfico desde el interior hacia el exterior, y viceversa, debe pasar a través del firewall. Sólo el tráfico autorizado se le permitirá pasar. A diferencia de un router, un firewall enruta paquetes en base a unas reglas definidas por el administrador.

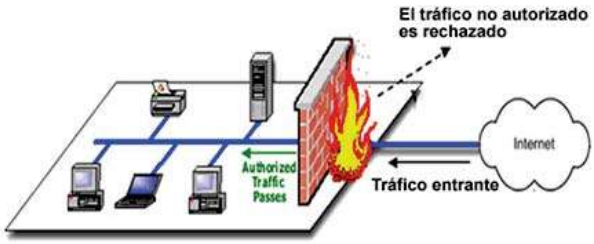

Figura 2.1: Firewall protegiendo una red local

Existen 2 tipos de firewall, los basados en hardware y los basados en software.

2.3.1. Firewalls basados en hardware

Son aquellos diseñados específicamente para diseñar funciones de enrutado y filtrado de paquetes y para establecer comunicaciones VPN. Generalmente se usan para unir sedes de grandes infraestructuras, a través de redes públicas. Suelen tener un rendimiento muy superior, sin embargo requieren licencias de mantenimiento de un costo elevado.

2.3.2. Firewalls basados en software

Se tienen dos tipos de usuarios (administradores de sistemas y usuarios comunes), los usuarios comunes al comprar un equipo tienen integrado en su sistema operativo (Linux, Windows, Mac) un firewall, que tiene capacidades mínimas, su función es únicamente proteger el equipo, en ocasiones llega a ser bastante tedioso de configurar, que termina siendo inútil. Existen aplicaciones externas enfocadas a mejorar las funcionalidades del firewall. El costo de los firewalls basados en software se reduce significativamente comparado con los firewalls basados en hardware. Existe una multitud de productos, tanto implementados con software libre, como propietario.

A continuación se listan las funciones principales de un firewall.

- Bloquea el tráfico no deseado.
- Registra el tráfico desde y hacia la red local.

- Enruta paquetes a una red de entrada y salida.
- Crea un punto centralizado desde en el cual se controlan las decisiones de seguridad.
- Limita su exposición.
- Oculta la infraestructura, dejando ver sólo los servicios bajo reglas.

Funciones que no puede hacer un firewall:

- Proteger contra aquellos ataques que se efectúen fuera de su punto de operación.
- Proteger de empleados malintencionados.
- Proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software.
- Prohibir que se copien datos corporativos en disquetes o memorias portátiles.

De esta forma, un firewall centraliza el control de acceso, los usuarios pueden acceder a la red interna de forma controlada y segura, pasando a través del firewall.

2.4. Algunos firewalls bajo licencia comercial

Los firewalls comerciales son soluciones para cualquier organización (empresas, escuelas, casas, bibliotecas, agencias de publicidad, etc.) su instalación y configuración, en la mayoría de las ocasiones se incluye con el precio de venta.

2.4.1. Ejemplos de firewalls basados en hardware de licencia comercial

3Com Embedded Cortafuegos. Funciona con las 3Com 10/100 Secure Network Interface Cards (familia 3CR990). Esta solución permite extender la protección del firewall perimetral, brindando una seguridad resistente a sabotajes a todas las computadoras de escritorio y servidores que se encuentran en riesgo, ya que éstos son los puntos de entrada más comunes para los atacantes potenciales. El 3Com Embedded firewall controla el acceso de los usuarios y filtra todo tipo de tráfico, sin importar si se origina dentro de la LAN corporativa o en Internet. Los precios de obtener su licencia son de 500 dólares por 10 licencias, 2 mil 250 dólares por 50 licencias y 8 mil dólares por 200 licencias.

FortiManager. El sistema FortiManager es una herramienta de gestión integrada de monitorización que permite a empresas y proveedores de servicios automatizar el despliegue y la gestión de decenas, cientos y miles de FortiGate™ Antivirus Cortafuegoss en múltiples instalaciones dispersas por todo el mundo. Las herramientas de la familia de productos FortiGate emplean el exclusivo chip de procesamiento de contenidos FortiASIC™ y el potente sistema operativo FortiOS™ creado por Fortinet, para ofrecer una óptima relación calidad-precio.

2.4.2. Ejemplos de firewalls basados en software comercial

Sygate Personal Cortafuegos 5.6.2808. Es una herramienta para administrar el sistema de seguridad de su PC, protegiéndola de ataques externos (intrusos y accesos no autorizados). Es un software gratuito para uso personal. Te ofrece funciones de protección de acceso compartido a Internet y efectúa un análisis a nivel de protocolos; esto le permite perimetrar finamente las reglas de acceso por aplicación, puerto y dirección IP.

ZoneAlarm 7.0.483. ZoneAlarm es un poderoso firewall el cual protege la PC de intrusiones. Existe una versión gratis del programa la cual funciona perfectamente. Se puede configurar para que funcione de la manera que se quiera, incluso podrá cerrar el acceso a Internet, puede trabajar con cualquier programa de descarga, hasta podrá decidir cuáles son sus aplicaciones de confianza. También protegerá su correo, de manera que todas las posibles entradas de malware queden controladas y pueda hacer uso seguro de Internet. La versión comercial cuesta alrededor de 200 dólares, pero no puede ser usada en servidores.

2.5. Firewalls basados en software libre

Al ser software libre, se libera el pago de licencias, sin embargo su instalación puede llegar a ser sumamente complicada, y por otro lado no se cuenta con suficiente soporte técnico en caso de dificultades en su operación.

2.5.1. IPCop

IPCop es una de las opciones a valorar especialmente por el hecho de que es la distribución que se estaba utilizando hasta la realización de este proyecto. Se trata de una distribución basada en RedHat Linux (por tanto es software libre) con una interfaz gráfica por web. Utiliza iptables como software de enrutado / filtrado de paquetes (figura2.2).

Figura 2.2: Consola web de administración de IPCop

Como puntos a favor tiene el hecho de que es conocida por ser la utilizada hasta ahora. Además, tiene un sistema de respaldo muy completo que permite desde la propia instalación una restauración completa del sistema. También es destacable la cantidad de desarrolladores que tiene detrás, programando paquetes para funciones específicas, como un filtro para tráfico P2P. No existe mucha documentación sobre su instalación / funcionamiento. Como puntos en contra tiene que el definir las reglas es muy complejo, ya que se debe hacer editando el fichero de reglas (no desde la interfaz web de administración) y no tiene ninguna funcionalidad de Portal Captivo (para la validación de la red inalámbrica). [9]

2.5.2. mOnOwall

mOnOwall es un sistema operativo derivado de FreeBSD, dedicado para la implementación de firewalls corporativos. Al estar basado en FreeBSD, se trata de software libre.

Se trata de un sistema diseñado para sistemas embebidos. Estos sistemas son equipos que tienen todos los componentes montados en una placa de tamaño pequeño. Se suelen utilizar para aplicaciones a medida (controladores de robots, sistemas de adquisición de datos, etc.) y con la extensión de los firewalls, se utilizan estos equipos adaptados con varias tarjetas de red y de gran ancho de banda. El almacenamiento suele ser en una tarjeta de memoria y las especificaciones del hardware, no son muy elevadas (para las funciones que están diseñados, tampoco se necesitan).

Los sistemas embebidos para redes, se suelen montar en cajas de tamaño estándar de los armarios de comunicaciones y con los conectores por la parte delantera para que tengan una integración sencilla con los equipos de comunicaciones (switches, routers, etc.).

Los puntos a favor de mOnOwall son una interfaz de administración web muy completa y atractiva y una gran cantidad de funcionalidades (veáse la figura 2.3), como la creación de reglas desde la interfaz, Portal Captivo y servidor de Wake-on-LAN. Además la documentación disponible sobre mOnOwall es excelente y los foros de soporte son muy activos.

En cuanto a los puntos negativos, básicamente es que está orientado a una arquitectura de equipos que no son estándar. De hecho, actualmente no es sencillo conseguir un equipo compatible totalmente con el sistema, lo que hace que, en caso de haber hardware se puedan producir problemas importantes. Tampoco dispone de un sistema de redundancia activa ni la posibilidad de implementar en la misma máquina un sistema de detección de intrusos, debido a las limitaciones de hardware. [11]

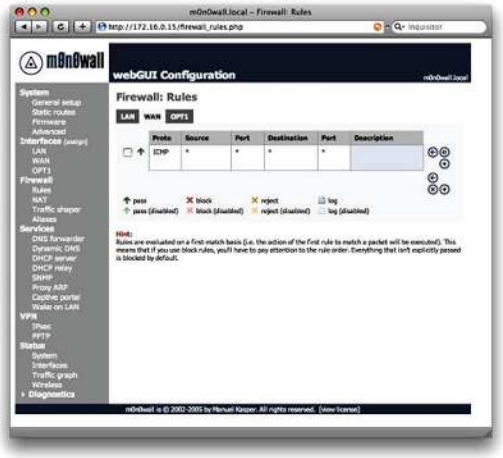

Figura 2.3: Interfaz web de administración de mOnOwall. Reglas del firewall.

2.5.3. SmoothWall

SmoothWall Express es una distribución FreeBSD, con licencia GNU, creada por la impresa SmoothWall Limited. La empresa está especializada en firewalls y es un derivado del producto comercial de la compañía. Sus puntos fuertes son que es un sistema muy estándar y es mucho más completo que otras distribuciones Linux para firewalls (como IPCop, por ejemplo). Es totalmente administrable desde la interfaz web, que es muy completa. (figura 2.4). Tiene soporte de hardware bastante amplio.

En cuanto a sus puntos en contra están que no tiene Portal Captivo para red inalámbrica, ni dispone de un sistema de redundancia activa (la distribución comercial si la tiene). Además, el hecho de que sea mantenida por una empresa privada, puede provocar que pase a ser un producto de software privativo. [15]

Figura 2.4: Interfaz web de administración de SmoothWall Express

2.5.4. OpenBSD

Las siglas BSD significan *"Berkeley Software Distributions"*. Este software de Berkeley fue realizado por el grupo de desarrolladores de la Universidad de California de Berkeley, aparte de la colaboración del grupo de AT&T y de los laboratorios Bell. OpenBSD es un sistema operativo libre tipo Unix, multiplataforma, basado en 4.4BSD, su mayor interés está centrado en la corrección de código así como la portabilidad, la seguridad proactiva y criptografía integrada. OpenBSD nació en 1995 en razón de expulsión de Theo de Raadt del grupo de desarrollo de NetBSD, a finales de 1994.

Dejando aparte el hecho de que la seguridad sea la principal razón para que Open BSD exista, el proyecto también tiene como meta mantener el espíritu del copyright original Berkeley Unix, que permitía una fuente de distribución relativamente libre de restricciones, siendo un descendiente de NetBSD, en un sistema operativo muy portable y el seguro del mercado.

OpenBSD ha hecho importantes avances: de especial interés es el desarrollo de OpenSSH, basado en el paquete SSH (Secure Shell) original y desarrollado por el equipo OpenBSD. Apareció por primera vez en OpenBSD 2.6, actualmente es la implementación sencilla de SSH más extendida, disponible como estándar o como opción en muchos sistemas operativos.

Después, un colaborador de OpenBSD , Daniel Hartmeier, comenzó a elaborar un nuevo filtro de paquetes que fue incorporado en la versión 3.0. Este nuevo filtro fue nombrado como PF *(Packet Filter)*, el cual ha impactado a muchos por la rápida incorporación de código para permitir Balanceo de Carga y la posibilidad de controlar ancho de banda, a través de las reglas de este software.

La filosofía de OpenBSD puede ser reducida a 3 palabras *Free, Functional and Secure* (Libre, Funcional y Seguro). Libre hace referencia a su licencia, funcional se refiere al estado en el cual se decide finalizar el versionado de los programas, y seguro por su extrema revisión y supervisión del código incluido en sus versiones. Debido a todas estas características, OpenBSD se usa mucho en el sector de seguridad informática como sistema operativo para firewalls y sistemas de detección de intrusos. El filtro de paquetes de OpenBSD (pf), es un potente firewall desarrollado a causa de problemas con la licencia de ipf. OpenBSD fue el primer sistema operativo libre que se distribuyó con un sistema de filtrado de paquetes incorporado.

2.5.5. Objetivos de OpenBSD

- Proporcionar una buena plataforma de desarrollo. Dar acceso a las fuentes tanto a desarrolladores como a usuarios, permitiendo observar los cambios directamente del sistema de control de versiones o *Concurrent Versions System (CVS)*.
- Integrar código de cualquier fuente siempre y cuando sea lo suficientemente bueno y posea un derecho de autor no muy restringido.
- Se pretende que el código fuente esté disponible para cualquiera y para cualquier propósito.
- Prestar especial atención en los problemas de seguridad y tratar de solucionarlos antes que ningún otro, de esta manera se intenta que sea el sistema operativo más seguro.
- Gran interacción de software orientado a criptografía. Tal que como: IPSec o Ipv6.

- Motores de claves como Kerberos, free-AFS entre otras.
- Seguir e implementar estándares ANSI, POSIX, partes de X/Open, entre otros.
- Trabajar en un código lo más independientemente posible de la máquina, de esta manera brindar soporte a tantos sistemas como hardware disponible exista.
- Tener una política lo más libre posible.
- No dejar ningún problema sin solucionar.

2.5.6. Modelo de seguridad de OpenBSD

Como ya se ha comentado antes, el desarrollo de OpenBSD está en evolución y se publica una nueva versión cada 6 meses, además del desarrollo en sí del proyecto, una parte de los desarrolladores se encarga únicamente de auditar el código, como el que se va portando de versión en versión. Esta auditoría es llevada por diferentes desarrolladores a lo largo de la vida del proyecto. Todo lo antes mencionado es una de las grandes razones por las que OpenBSD fue el sistema operativo indicado para incluirlo dentro de este proyecto de tesis.

2.5.7. Orígenes de pfSense

PfSense es una distribución basada en FreeBSD, derivada de mOnOwall. Su objetivo es tener un firewall fácilmente configurable a través de una interfaz web e instalable en cualquier PC. PfSense es un proyecto destinado a crear un completo paquete de software, que cuando se utiliza con una PC ofrece todas las características importantes de las cajas de un firewall comercial (incluyendo la facilidad de uso) a una fracción del precio (software libre).

PfSense se basa en una versión básica de FreeBSD, junto con un servidor web, PHP y algunos otros servicios públicos. Toda la configuración del sistema se almacena en un único archivo de texto en XML. mOnOwall es probablemente el primer sistema UNIX que tiene su tiempo de arranque de configuración realizado en PHP, en lugar de los usuales *scripts de Shell*, y que tiene todo el sistema configurado almacenado en formato XML.

2.5.8. Características de pfSense

PfSense incluye todas las características de los firewalls comerciales. Más adelante se enunciará una lista de características disponibles en la actualidad en el pfSense versión 1.2. Todas éstas son posibles en la interfaz web, sin usar línea de comandos. A continuación se enuncian algunas características de pfSense.

- Filtraje por IP origen y destino, protocolo IP, puerto origen y destino para tráfico TCP y UDP.
- Capaz de limitar conexiones simultaneas en base a una por regla.
- Opción a registrar o no el tráfico dependiendo de cada regla.

- Opción de alias, éstos permiten agrupación y renombramiento de IPs, redes y puertos, lo cual ayuda a mantener su reglamento del firewall y fácil de entender, especialmente en entornos con múltiples IPs públicas y numerosos servidores.
- Alta flexibilidad en las políticas de ruteo mediante la selección de la puerta con base a una per-regla (para el balance de carga, failover, múltiples WAN, etc.)
- Normalización de Paquetes. Descripción de la documentación pf scrub *"Scrubbing"* es la normalización de paquetes, para que no halla ambigüedades en interpretación por medio del destino final del paquete. La directiva *scrub* también reensambla paquetes fragmentados, protegiendo algunos sistemas operativos de algunas formas de ataque e ignora paquetes TCP que tengan combinaciones de flags invalidas.
    1. Activado en pfSense por defecto *default*.
    2. Puede desactivarse si es necesario. Esta opción causa problemas en algunas implementaciones NFS, pero es seguro y debería dejarse activado en la mayoría de las instalaciones.
- Sin filtraje opcional. Se puede apagar el filtro del firewall completamente si se desea convertir el pfSense en un simple ruteador.

La mayoría de los servidores de seguridad carecen de la capacidad de controlar su estado finamente. PfSense tiene numerosas características que permiten el control de su estado, gracias a las capacidades de PF *(Packet Filter)*. Además de las características, hay limitaciones del sistema en la que somos conscientes. Desde nuestra experiencia y la contribución de miles de experiencias de los usuarios, se entiende muy bien lo que el software puede o no puede hacer. PfSense tiene la desventaja de que al ser una distribución muy joven y activa, sin embargo, el sistema no tiene buena documentación.

Capítulo 3

Instalación del firewall

En este capítulo se describen los pasos necesarios y requisitos para la instalación y administración de pfSense, los pasos de instalación son claros para que su instalación sea fácil y segura, y así pueda acceder a la interfaz de administración y hacer la configuración necesaria.

3.1. Requisitos de instalación de pfSense

Para instalar pfSense se necesita una computadora de propósito general basada en arquitectura Intel con al menos unidad de CD-ROM, una unidad de disco duro tipo IDE (en caso de una instalación permanente), 512 MB de RAM y al menos dos tarjetas de red en su máquina. No instalar ningún hardware innecesario como un módem, ya que pfSense no puede usarlo. El hardware compatible por ejemplo DELL, HP, IBM, etc. lo puede encontrar en la siguiente página web del proyecto FreeBSD [7]:

3.2. Guía de instalación de pfSense 1.2

A continuación se describen los pasos para instalar pfSense detallando los pasos necesarios para la configuración inicial del firewall.

3.2.1. Disco de instalación

Se debe descargar de la página web oficial www.pfsense.org, la última versión estable, en este caso la versión 1.2. Pfsense es distribuido en una imagen ISO que ocupa aproximadamente 250MB. Una vez descargado, se graba en un CD ROM con el que hará la instalación.

Una vez preparado el disco de instalación se procede a iniciar el sistema arrancando desde el CD ROM, si todo va bien aparecerá el menú de arranque, en este menú salvo en casos excepcionales como problemas con una instalación anterior, o en equipos que no sean de las características mínimas, se selecciona la primera opción: arranque normal, como se muestra en la figura 3.1.

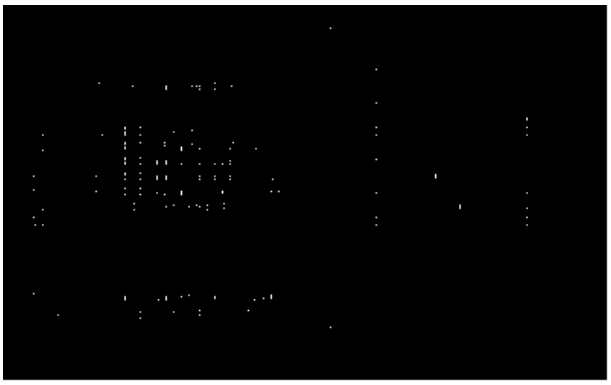

Figura 3.1: Menú de arranque

Enseguida empezará a detectar el hardware del equipo y a configurar los controladores de dispositivos, iniciará preguntandole si desea utilizar soporte para VLAN como se muestra en la figura 3.2. Para decidir activar la opción de soporte VLAN, es necesario contar con un *switch* que sea compatible con 801Q, ver el apéndice para entender el funcionamiento de las VLAN.

Figura 3.2: Detección del hardware del equipo y configuración de los controladores

3.2.2. Interfases de red

El siguiente paso es la configuración de los dispositivos de red. PfSense mostrará las interfases de red disponibles que tienen la posibilidad de soportar VLAN, si cuenta con un conmutador *(switch)* que soporta VLAN deberá habilitar esta opción (para más información sobre VLAN en el apéndice A el manual del *switch Nortel)*, de esta manera aparecen las interfases de red.

Nota: Al seleccionar la interfaz LAN, los nombres de las interfases en BSD vienen dados según el fabricante, por ejemplo para la tarjeta *Broadcom Giga bit* se llamara bg0, las de *chipset Realtek* aparecerán como le0, etc.

3.2.3. Seleccionar interfases de red

Si el firewall contara con más de 2 interfases de red, estas serán opcionales y deberán ser asignadas de la misma manera que para el caso de la LAN o WAN y aparecen como OPT. En la figura 3.3 se seleccionan

las tarjetas de red correspondientes a las interfases, de acuerdo como usted lo desee. Ya seleccionado cuál va a ser la interfaz y si no hay más interfases por agregar, presiona retorno *(enter)* para continuar.

Figura 3.3: Selección de la interfases LAN y WAN

La figura 3.4 muestra como quedaron seleccionadas las interfases y el programa de instalación, le preguntará si desea seguir con la instalación, da la opción de *y/n*, donde la *y* = sí y *n* = no. Se debe contestar *y*.

Figura 3.4: Proceder con la selección

3.2.4. Guardar la configuración

Aparecerá el menú de la consola de configuración (veáse la figura 3.5):

```
  pfSense consola setup
0)Logout (SSH only) (Desconectarse (SSH solamente))
1)Assign interfaces (Asignación de las interfases)
2)Set LAN IP address (Establecer la dirección IP LAN)
3)Reset WebConfigurator (Restablecer WebConfigurator)
4)Reset to factory defaults (Restablecer los valores predeterminados de fá-
  brica)
5)Reboot system (Reinicie el sistema)
6)Halt system (Detener sistema)
7)Ping host (Se hace uso de la herramienta ping)
8)Shell
```

```
9)PFtop
10)Filter Logs (Filtro de registros)
11)Restar WebConfigurator
99)Install pfSense to a hard drive/memory drive, etc. (Instalación de
   pfSense a una unidad de disco duro / unidad de memoria, etc.
```

Se selecciona la opción 99, que le permite instalar pfSense en un disco duro, memoria USB u otro dispositivo de almacenamiento. Nota: El dispositivo de almacenamiento seleccionado será borrado permanentemente por lo cual sea cuidadoso.

Figura 3.5: Consola de configuración de pfSense

En la figura 3.6 se dan las siguientes opciones:

```
<Change video font (default)> (Cambio de fuente de video)
<Change ScreenMap (default)> (Cambio)
<Change keymap (default)> (Cambiar mapa de teclado)
<Accept these Settings> (Aceptar esta configuración)
```

En este caso se elige Cambio de fuente de video, significa cambiar el tamaño de letra, que se mostrará en la consola de administración.

Figura 3.6: Menú de opciones de teclado

Enseguida le pide que elija una de las siguientes tareas a realizar:

<Install pfSense> (Instalar pfSense)
<Reboot> (Reiniciar)
<Exit> (Salir)

Para iniciar la instalación del programa debe eligir instalar pfSense (veáse la figura 3.7).

Figura 3.7: Selección de tareas

3.2.5. Particionamiento

Ahora se iniciará un proceso para dar formato al disco duro, particionando y copia de archivos. En la figura 3.8 le pedira seleccionar un disco para instalar pfsense. Las opciones en esta figura son las siguientes:

<da0: VMware, VMware Virtual S 1.0> Fixed Direct Access SCSI-2 device.
(VMware, VMware Virtual S 1.0. Fija el acceso directo al dispositivo SCSI-2).
<Return to Select Task> (Volver a la Selección de tareas).

Figura 3.8: Selección de disco duro

Una vez seleccionado el disco duro se procede al formato de este disco, y se borrará todo el contenido del mismo. Ahora el programa de instalación le pregunta si desea dar formato a este disco, debe formatear el disco si es nuevo, o si desea comenzar de nuevo puede borrar su información, pero no debe formatear el disco si contiene información que desee conservar. (veáse la figura 3.9). Las opciones son las siguientes:

<Format this Disk> (Formatear este disco)

<Skip this step> (Omitir este paso)
<Retunr to Select Disk> (Volver a Selección de disco)

Figura 3.9: Selección formato del disco

En la mayoría de los casos la geometría del disco duro es correcta, para evitar problemas de instalación, el BIOS deberá tener la opción de acceso DMA, el acceso UDMA no tiene compatibilidad con BSD. En la figura 3.10 el sistema informa que la geometría en da0 es de 391 cilindros, 255 heands, 63 sectores. Esta geometría permite que arranque desde este disco, entonces se recomienda usarla para continuar. Las opciones son las siguientes:

<Use this geometry> (Utilice esta geometría)
<Return to Select Disk> (Volver a Selección de disco)

Figura 3.10: Selección de la geometría del disco

En la figura 3.11 advierte que todos los datos de todas las particiones estan en el disco, y le pregunta por última vez si desea seguir adelante o si desea cancelar.

<Format da0> (Formato da0)
<Return to Select disk> (Volver a Selección de disco)

Figura 3.11: Formato al disco

Ahora puede particionar el disco si lo desea (veáse la figura 3.12). Si formatea el disco, puede instalar varios sistemas operativos en el mismo, como también reservar una parte del disco para cada una de éstos y así crear varias particiones, una para cada sistema operativo. Si el disco ya tiene sistemas operativos en lo que se desea mantener, usted debe tener cuidado de no cambiar las particiones que son en el caso de elegir particionar el disco. El sistema o programa de instalación en la opción *Partition Disk* da opciones para realizar las siguientes tareas:

```
<Partition Disk> (Particionar disco)
<Skip this Step> (Omitir este paso)
<Return to Format> (Regresar a formatear disco)
```

Si se desea particionar el disco, deberá seleccionarse la opción *Partition Disk* (veáse la figura 3.12). Luego le solicitará particionar el disco, esto es para instalar el sistema operativo FreeBSD.

Figura 3.12: Particionar el disco

3.2.6. Sistema de archivos (File System)

Por defecto el formato utilizado es FreeBSD, pero se pueden seleccionar otros sistemas de archivos (NetBSD, OpenBSD, BSDOS, etc.). (Veáse la figura 3.13). Ahora se debe seleccionar la partición donde se intalará el sistema operativo (las particiones reciben el nombre de ”slice”) que quiere tener en este disco. Introduzca un tamaño de sectores (1 GB = 2097152 setores) o un solo ′*′ para indicar que use el espacio restante en el disco.

<Accept y create> (Aceptar y crear)
<Return a formato Disk> (Volver al formato del disco)
<Revert De partición en Disk> (Volver a particionar el disco)

Figura 3.13: Selección del sistema de archivo

Ahora si ya tiene instalado un gestor de arranque puede omitir este paso, pero si no, tiene que configurar su gestor de arranque por separado. Puede que ahora desea instalar *bootblocks* en uno o más de un disco (veáse la figura 3.14). Enseguida le pregunta si desea instalar *Bootblocks*, y las opciones de respuesta son:

<Accept and Install Bootblocks> (Aceptar e instalar Bootblocks)
<Skip this Step> (Omitir este paso)
<Return to Partition Disk> (Volver a la partición del disco)

Si la primera opción fue su respuesta, se va a instalar el sector de inicio en el disco duro.

Figura 3.14: Instalación del sector de inicio en el disco duro

El la figura 3.15 se selecciona la partición primaria de da0 (también conocida como un ”trozo” de la tradición BSD) en la cual se va a instalar pfsense.

<1: 1.99G (63-6281415) id = 165>
<Return to install Bootblocks> (Volver a instalar Bootblocks>

Figura 3.15: Selección de la partición a instalar

Ahora debera configurar las particiones, la capacidad que se va a utilizar será ”M” para indicar megabytes, ′G′ para indicar gigabytes, o un ′*′ para indicar que ”utilizar el espacio restante en la partición primaria”, osea que tomará todo el espacio disponible en el disco. También se indica la capacidad de montaje. (Veáse la figura 3.16).

<Accept and create> (Aceptar crear AHD)
<Return to Select Partitions> (Volver a Seleccione Partición)
<Switch to Expert Mode> (Cambiar al modo experto)

Figura 3.16: Configuración de particiones

Finalmente se copian los archivos al disco, tardará algunos minutos. (Veáse la figura 3.17).

Figura 3.17: Copia de los archivos al disco

Ahora la máquina está a punto de ser apagada. Después de que la máquina llegue a cerrar su estado, usted puede retirar el CD de la unidad de CD-ROM. y precione *Reboot* para iniciar el sistema desde el disco duro. (Veáse la figura 3.18)

```
<Reboot> (Reiniciar)
<Return to Select Task> (Volver a seleccionar tarea)
```

Figura 3.18: Reiniciar la máquina

3.3. Acceso a la interfaz de administración

Por defecto la interfaz LAN utiliza la dirección IP 192.168.1.1, se deberá cambiar la IP de la máquina cliente a 192.168.1.x (donde x es cualquier número entre 2 y 250), la máscara de red deberá ser 255.255.255.0 para así acceder a la interfaz de configuración. Es debido a que el servidor DHCP no está habilitado. Desde la máquina cliente se accede a través de un navegador web a la dirección de la 192.168.1.1 (LAN del firewall). La primera pantalla es como la que aparece en la figura 3.19, que hace la solicitud de usuario y contraseña, donde el usuario será *admin* y la contraseña *pfSense*.

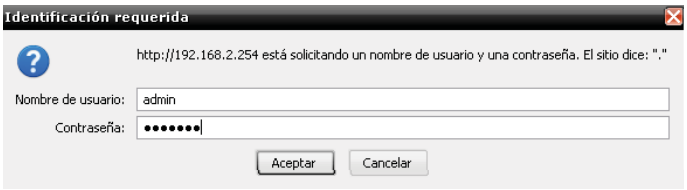

Figura 3.19: Pantalla de solicitud de usuario y contraseña

El asistente de configuración *setup wizard*, que se encuentra en el menú *System* permite personalizar su firewall pfSense, donde se define la ubicación, zona horaria mundial, dirección IP del servidor DNS de su ISP, contraseña del sistema, IP LAN (Se recomienda dejar establecido como predeterminado). Debe dar click en *next* para personalizar su firewall. (Veáse la figura 3.20). Es recomendable planear con anticipación qué rangos de direcciones IP va a utilizar.

Figura 3.20: Asistente de configuración

Una vez personalizado su firewall pfSense, al entrar a su sistema aparecera una pantalla como la figura 3.21 que muestra un resumen de la configuración inicial.

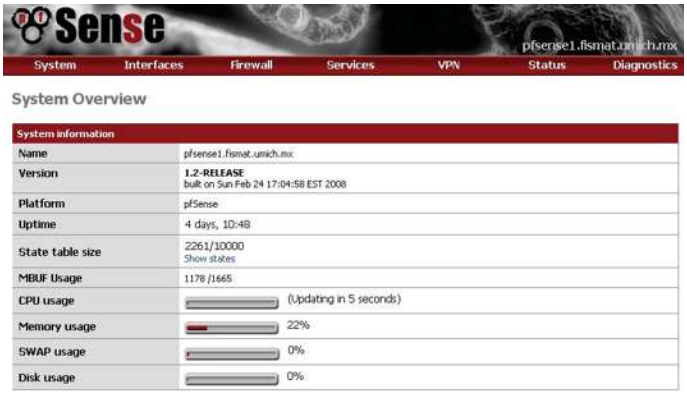

Figura 3.21: Pantalla de resumen de pfSense

Los campos de la pantalla de configuración general de parámetros dela figura 3.22 son los siguientes:

- Nombre de la máquina anfitrión (Hostname): Es un nombre que usted le puede dar a su pfSense, por ejemplo mi servidor, pfSense1, etc.
- Dominio (Domain): Es el nombre asignado por el servidor de nombres (DNS).

- Servidor DNS Primario (Primary DNS Server): Aquí se introduce la dirección IP del DNS primario.
- Servidor DNS Secundario (Secondary DNS Server): Aquí se introduce la dirección IP del DNS secundario (en el caso que se cuente con dos proveedores de Internet).

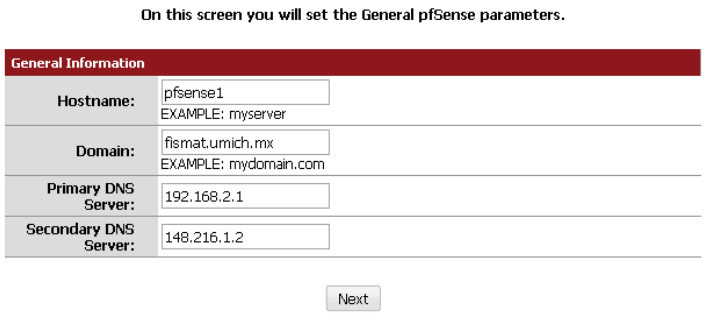

Figura 3.22: Pantalla de configuración general de parámetros

Ahora se deben configurar cada una de las interfases de red que se dispongan, los campos de configuración para las interfases de red que se muestran en la figura 3.23 son:

- Tipo (Type): En esta opción debo elegir si va a ser de manera estática o dinámica.
- Mac Address: Este campo se puede utilizar para modificar (”falso”) la dirección MAC de la interfaz WAN (puede ser necesario con algunas conexiones de cable). Se puede introducir una dirección MAC en el siguiente formato: xx: xx: xx: xx: xx: xx o dejar en blanco.
- MTU: Si introduce un valor en este campo y, a continuación, los SMS de sujeción de las conexiones TCP con el valor ingresado, menos 40 (TCP / IP de tamaño cabecera) será, en efecto. Si deja este campo en blanco, una MTU de 1492 bytes para el protocolo PPPoE y 1500 bytes para todos los demás tipos de conexión se asumirá.
- Dirección IP (IP Address): Se trata de la dirección IP asignada, según su red local.
- Puerta de enlace (Gateway): Es por donde se dará salida a los paquetes, esto es útil si se quiere utilizar pfSense solo como direccionador *(router)*, sin filtrado.

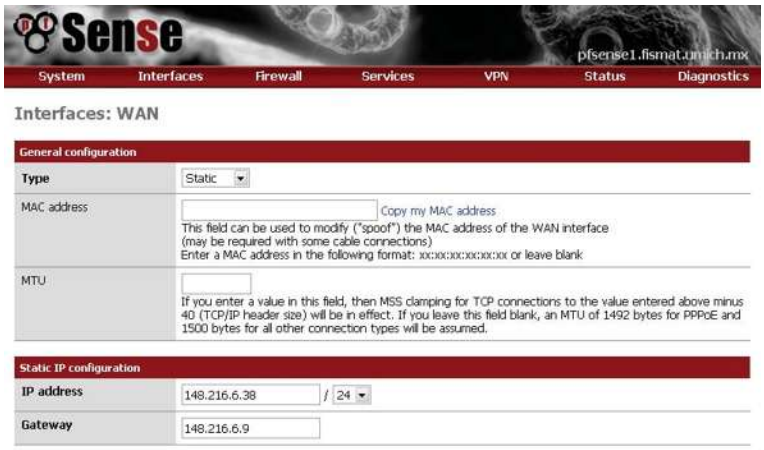

Figura 3.23: Configuración de la interfaz WAN

3.3.1. Servicios: Servidor DHCP: LAN

Para configurar el servidor DHCP en pfSense debe seleccionar *Services: DHCP Server* y seleccionar la pestaña correspondiente a la interfaz de red donde se habilitará el servidor de DHCP. La figura 3.24 muestra una pantalla configuración del servidor DHCP y los campos de configuración se describen a detalle en el capítulo 5.

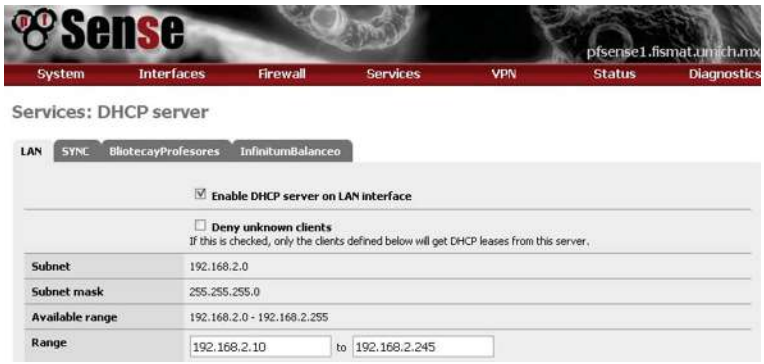

Figura 3.24: Pantalla de Servicios: Servicio DHCP

De esta manera queda instalado su sistema *OpenBSD* y listo para usarse como firewall, por lo que es necesario reiniciarlo.

Capítulo 4

Reglas del firewall

En este capítulo se describirá brevemente la configuración de reglas del firewall, como las opciones que incorpora pfSense (*Schedules*, *Traffic Shaper* e *IP Virtuales*) que hacen que sea un firewall completo e implementado de alta disponibilidad. El menú Firewall de pfSense contiene características importantes que nos ayudan a proteger nuestra red, además de ser uno de los servicios más importantes en pfSense, en esta parte es donde se configuran y administran las reglas de entrada y salida de paquetes y tráfico, que se requiera al administrador.

4.1. Reglas

La función de la reglas es decidir cuales conexiones se permiten y cuáles no, además de realizar ruteo de paquetes. Si se cuenta con más de una interfaz de red, cada una tendrá sus reglas, que se ejecutarán según el orden de prioridad. Cuando un paquete entra al firewall, éste revisa las reglas de una en una y la que cumpla con las características del paquete, se ejecutará la acción definida en ella. Si se tiene un paquete que ha pasado por todas las reglas y no cumple las condiciones, el paquete simplemente no pasa, si no hay regla el paquete será bloqueado.

Las reglas son una serie de acciones, asignadas a unas condiciones determinadas. Las acciones son 3:

- Aceptar (pass): El paquete cumple las condiciones, así que se acepta y el firewall lo enruta hacia su destino.
- Bloquear (block): El paquete se desecha, sin realizar ninguna acción.
- Rechazar (reject): El paquete se desecha, pero se le envía al emisor un paquete comunicando que su petición ha sido rechazada.

En la figura 4.1 se puede ver una captura de pantalla de las opciones de creación de una regla en pfSense.

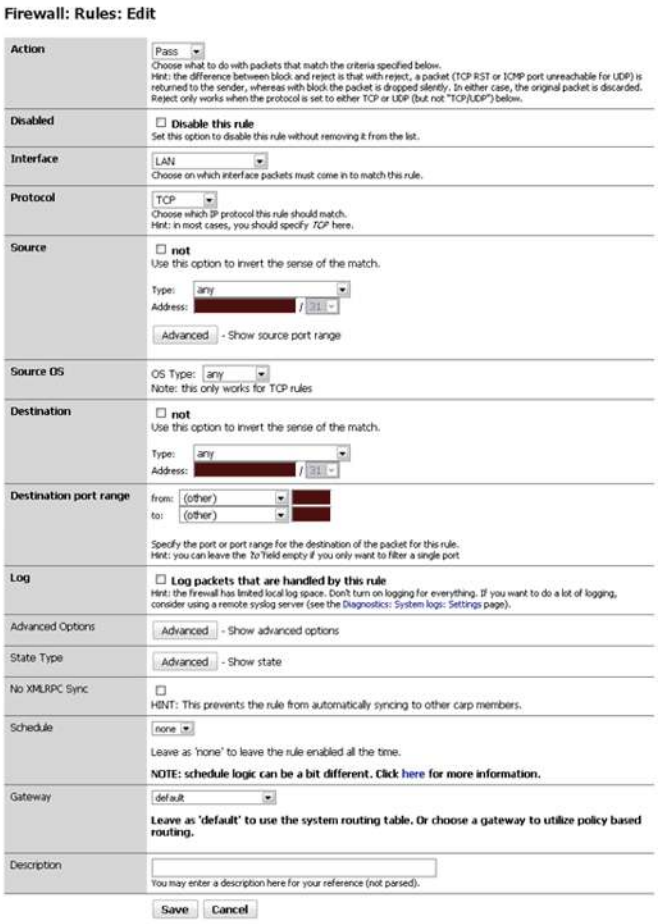

Figura 4.1: Pantalla de creación de una regla de filtrado en pfSense

Generalmente si no desea permitir tráfico, se bloquean los paquetes, sin dar más explicación al emisor. En cuanto a las condiciones que se aplican a una regla, son muchas y dependen de los resultados esperados. En pfSense se pueden desactivar reglas. Las reglas desactivadas se ven ”difuminadas” en la lista de reglas.

Existen reglas básicas de seguridad que son necesarias para apoyar el acceso de la interfaz LAN a Internet, como también existen las reglas que se necesitan para apoyar el acceso entrante de Internet a las máquinas de la interfaz LAN, esto incluye la forma de prestar apoyo a las aplicaciones.

4.2. Configuración de reglas

Los campos de la página de configuración de reglas son los siguientes:

- Acción (Action): Se selecciona si se deja pasar, bloquear o rechazar un determinado paquete.
- Deshabilitada (Disabled): Se selecciona esta opción para desactivar la regla sin quitarla de la lista.

- Interfaz (Interface): Interfaz de red sobre la que se aplicará la regla.
- Protocolo (Protocol): Protocolo por el que se verificarán las condiciones. El más típico suele ser TCP o UDT, aunque parecen otros como ICMP ICMP, IGMP, etc.
- Origen (Source): Condición de origen del campo de direcciones del protocolo. Esto se puede aplicar sobre una dirección IP, sobre una subred, o sobre un alias definido anteriormente (que pueden ser direcciones individuales o grupos de direcciones).
- Puerto de origen (Source OS): Corresponde con el puerto origen que genera la transmisión. Sólo es aplicable al protocolo TCPIP y sirve para diferenciar el tipo de tráfico, aunque generalmente el puerto origen no es significativo. Se puede aplicar sobre puertos individuales, rangos o alias (que pueden agrupar varios puertos).
- Destino (Destination): Igual que el origen pero con direcciones de origen.
- Puerto de destino (Destination port range): Los puertos de destino definen el tipo de tráfico (por ejemplo, TCP puerto 80 suele ser tráfico web) con lo que es ideal para filtrar tipos de tráfico. Crear alias con grupo de puertos que identifique servicios es muy común y muy útil (por ejemplo, tráfico web, que engloba http, puerto 80 y http2, puerto 445).
- Opción de registrar evento: En el caso de que se cumpla la regla se genera una entrada en el registro de eventos del sistema (log) con los datos del paquete y la acción realizada.
- Opciones avanzadas (Advanced Options): Limita muchas conexiones, como conexiones simultaneas de cliente, máximo de entradas por el estado anfitrión, máximo de nuevas conexiones / por segundo y estado del tiempo en segundos.
- Tipo de estado (State Type): Aplica la regla en función de los estados del paquete. Por ejemplo, no es lo mismo un paquete de petición que uno de respuesta a una petición, etc.
- Sincronización con otros firewalls (No XMLRPC Sync): Este es en caso redundancia.
- Horario (Schedule): Es la hora sobre la que se aplica la regla.
- Puerta de enlace (Gateway): Es por donde se dará salida a los paquetes, esto es útil si se quiere utilizar pfSense solo como direccionador *(router)*, sin filtrado. Y cuando se tiene balanceo de carga o un proveedor de Internet, si no se selecciona ninguna puerta de enlace en particular, entonces saldrá por defecto *(default)*.
- Descripción de la regla (Description): Texto identificativo.

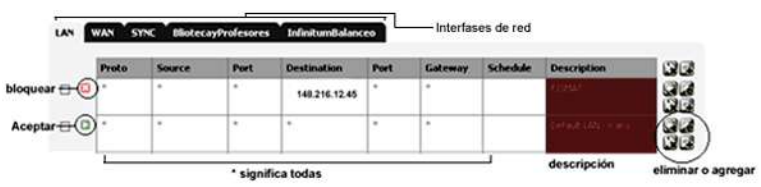

Figura 4.2: Pantalla de una regla LAN

La lista de reglas se ejecuta según su creación, de manera que cuando se cumplan todas las condiciones de una regla se aplica la acción a realizar y se salta al siguiente paquete. Así pues, el orden en que se aplican las reglas es muy importante. De hecho, un firewall con las reglas ordenadas de manera óptima será mucho más eficiente que uno que no las tenga bien ordenadas.

4.3. Alias

Un concepto que simplifica la administración, son los grupos. En este caso, pfSense los denomina como alias. Un alias es un identificador de uno o varios objetos, de tres tipos: direcciones, redes y puertos. Si se definen alias correctamente, el número de reglas será menor y la administración más sencilla. Para definirlos, se accede a través de la consola web en el menú *Firewall: Aliases*. En esta parte le aparecerá la figura 4.3, que es la pantalla de configuración de una alias.

Figura 4.3: Pantalla de configuración de un alias

Los campos de la página de configuración de los alias son los siguientes:

- Nombre (Name): Se debe añadir un nombre que contenga los caracteres de la a-z, A-Z y 0-9.
- Descripción (Description): Una descripción de referencia si lo desea.
- Tipo (Type): Debe seleccionar si se trata de un host, de una red o de un puerto (s), y añade una dirección IP del usuario o máquina que desee añadirle el alias y una breve descripción, además si se trata de un grupo se añaden todos (host, red o puerto).

4.4. NAT

NAT (Network Address Translation) traducción de dirección de red, es un mecanismo utilizado por direccionadores *(routers)* IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de

direcciones dentro de la conversación del protocolo, un uso común es permitir utilizar direcciones privadas, si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada, para que solo puedan salir a Internet con una sóla dirección IP.

Estas traducciones de dirección son almacenada en una tabla, para saber qué dirección y puerto le corresponde a cada dispositivo cliente y así saber a donde se deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es eliminado. Con este comportamiento se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web.

Tenemos dos tipos de NAT estático y dinámico, el dinámico es un tipo de NAT en el que una dirección IP privada se traduce a una pública y siempre es la misma, para que así un host tenga una dirección IP de red privada pero visible en Internet como un servidor web. Y el estático es un tipo de NAT en que una dirección IP se mapea a una IP pública basándose en una tabla de direcciones IP públicas registradas, el direccionador NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el ruteador elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada, esto permite aumentar la seguridad de una red dado que se enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública.

En pfSense, NAT tiene tres secciones que son: *Outbound, 1:1 y Port Forward*.

4.4.1. Firewall: NAT: Outbound

Si está usando direcciones IP públicas en cualquiera de las interfases en su pfSense (con la excepción de las interfases de puente) es necesario cambiar el comportamiento del NAT avanzados permitiendo salida NAT. Ahora en el caso tener una subred privada deberá introducir sus propias asignaciones NAT, por ejemplo si se tiene una red local con la subred 192.168.1.0/24 y con direcciones IP públicas, tendrá que habilitar NAT avanzados de salida, y añadir un NAT de la red LAN. Y debe agregar una regla para la interfaz WAN, que tenga de fuente 192.168.1.0/24, que vaya a cualquier destino, y por último escribir una descripción de su elección.

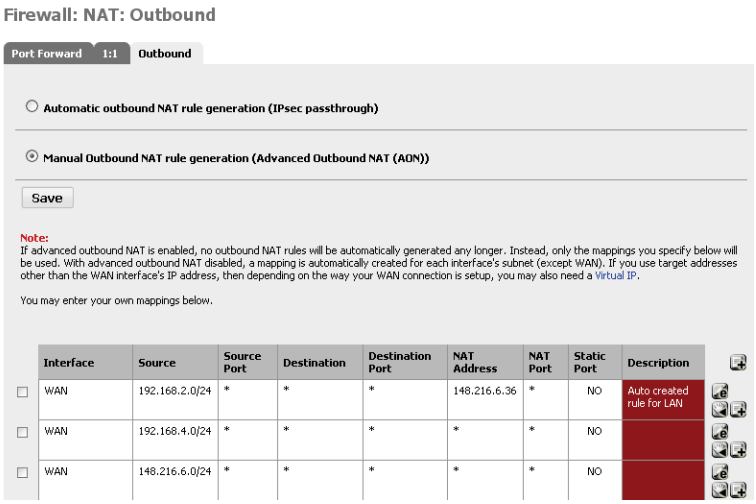

Figura 4.4: Reglas de NAT salida

4.4.2. Firewall: NAT: 1:1

En esta sección se mapea una dirección IP pública a una dirección IP privada por la especificación de un /32 de subred. Esto significa tener dos equipos con direcciones IP 148.216.6.38 y 148.216.6.36, una de ellas pertenece a pfSense y la otra se asigna a un equipo a través de la LAN, lo que se logra con el NAT: 1:1 que es una petición es enviada a la dirección de red 148.216.6.36, pfSense no la filtra simplemente reenviará el tráfico a la IP asignada.

4.4.3. Firewall: NAT: Port Forward

El reenvío de puertos se define como el acto de la transmisión de un puerto de red de un nodo de red a otro. Esta técnica puede permitir a un usuario externo llegar a un puerto de una dirección IP privada (dentro de una LAN) desde el exterior a través de un router NAT activado. Además se permiten reglas de filtrado.

El reenvío de puertos permite qué ordenadores remotos (por ejemplo, máquinas públicas en Internet) se conecten a un equipo específico dentro de una LAN privada. Por ejemplo:

- Reenvío el puerto 80 para ejecutar un servidor web HTTP en Internet desde la LAN privada.
- Reenvío del puerto 22 (Secure Shell) permite el acceso privado a un servidor desde Internet.

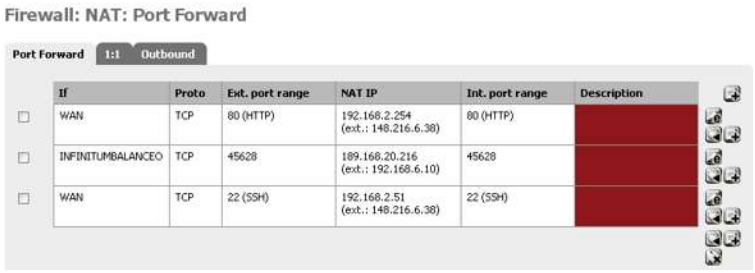

Figura 4.5: Reglas de NAT Reenvío de puertos

4.4.4. Agendas (Schedules)

Las agendas funcionan para activar y desactivar reglas en el firewall, pueden crearse en cada una de las interfases de red que se tengan. Dicho de otra manera, usted tiene la libertad de activar y desactivar reglas siempre y cuando exista una agenda para cada una de éstas, usted elige la fecha y hora arbitraria de acuerdo a las necesidades que se tengan. La configuración se muestra en la figura 4.6:

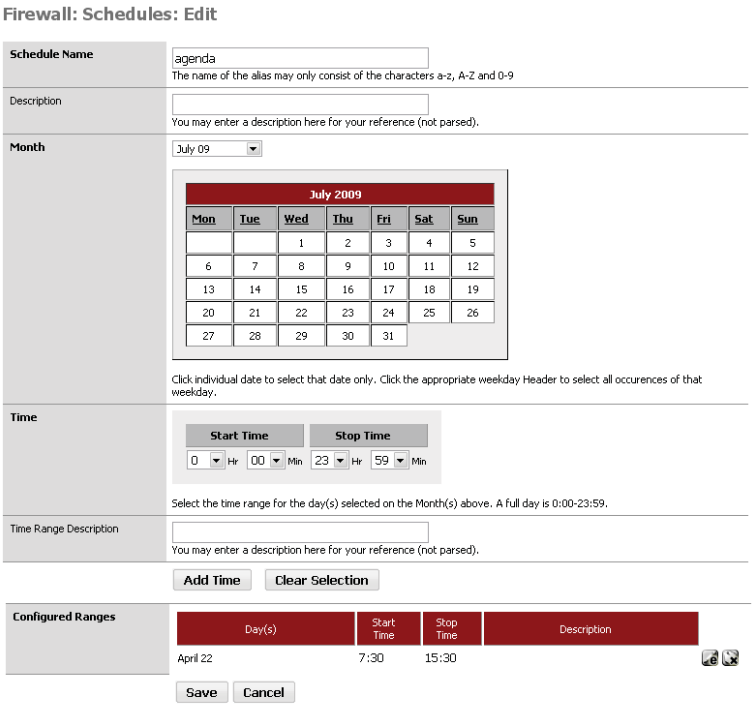

Figura 4.6: Configuración de una agenda

Los campos de la página de configuración de las agendas son los siguientes:

- Nombre de la agenda (Schedule Name): Se le añade un nombre a la agenda que se va a crear, podrá utilizar los caracteres a-z, A-Z y 0-9.
- Descripción: Puede introducir una descripción para su consulta (no analizada).

- Mes (Month): Haga click en cada fecha para seleccionar sólo esa fecha. También seleccione el día de la semana.
- Tiempo (Time): Seleccione el rango de tiempo para el día (s) seleccionado en el mes (s) anterior. Un día completo es 0:00-23:59.
- Rango de Tiempo Descripción (Time Range Description): Puede introducir una descripción para su consulta.
- Configured Ranges: En esta parte le aparecerá el o los rangos configurados.

4.4.5. Control de tráfico (Traffic Shaper)

En el menú de firewall también se encuentra *Traffic Shaper*, que es recomendado utilizarse para ajustar el caudal de tráfico y así crear un conjunto de reglas que den prioridad al tráfico (tráfico de descarga y tráfico VoIP). *Traffic Shaper* proporciona un asistente que le guiará en el proceso de la creación de reglas de control de caudal, el asistente le permite activar opciones para controlar el tráfico VoIP, el P2P, juegos en red y clientes de mensajería.

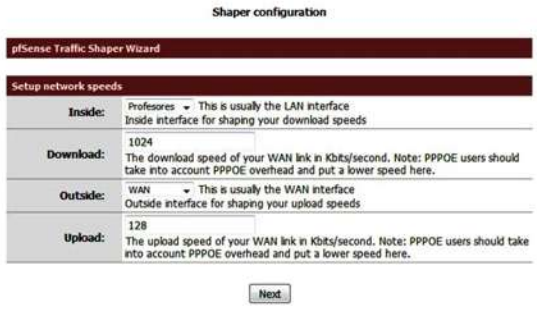

Figura 4.7: Parámetros del ancho de banda de la red

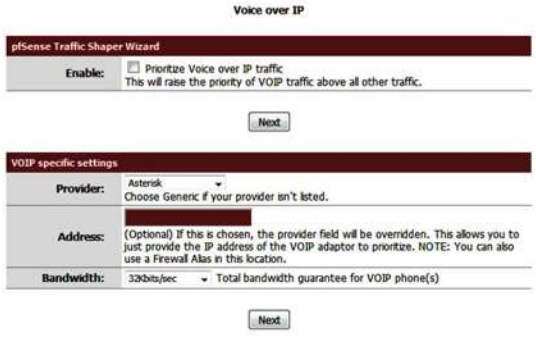

Figura 4.8: Ancho de banda asignado al VoIP

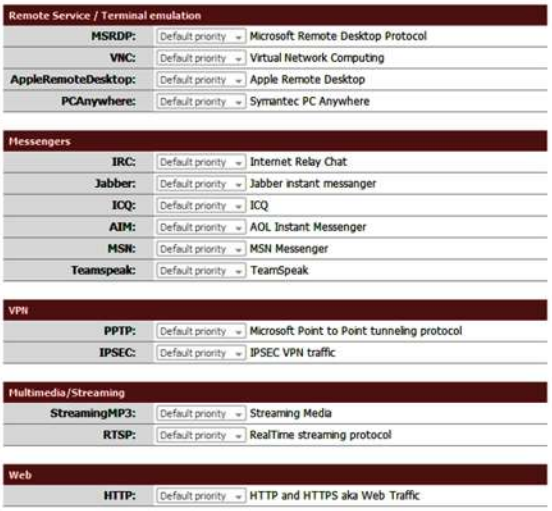

Figura 4.9: Ancho de banda asignado a los clientes de mensajería

Como ejemplo, se tiene la configuración de tráfico VoIP. Suponiendo que utiliza el asistente, habrá *qPenaltyUp* y *qPenaltyDown* (aquí *q* abrevia queue) ya creado. Cuando inicia una aplicación VoIP VoIP, se debe ver el tráfico en estas colas. Estas están diseñados para transportar la mayor parte del tráfico VoIP, que normalmente ralentiza la conexión abajo. Otros tipos de tráfico pueden ser, como páginas web HTTP, correo electrónico, IM, VoIP, etc. Los cuales irán en otras colas.

Inicialmente, el asistente establece todas las colas hasta el 1 % del ancho de banda. Esto no es suficiente. En particular, la cola *qwanacks* (es la cola de acude de recibo ACK) sin duda necesita más ancho de banda que si lo hace una pila de descarga. En primer lugar, una breve nota acerca de los paquetes ACK.

Cuando se descarga, el equipo tiene que enviar (subir) los paquetes ACK. Estos son, básicamente, decir ”Sí, tengo la parte de la descarga Aceptar”. Si el equipo que está descargando de un ACK detecta que no se ha recibido, se supone que los datos no se han recibido y lo reenvía de nuevo. La velocidad a la que se envían los ACK de regreso también se utiliza para ayudar a determinar la velocidad máxima a la que pueden descargar los datos, por lo que es importante obtener el ACK enviado tan pronto como sea posible y no se redujo con el fin de mantener sus descargas esto tiene una velocidad aceptable. Si se reducen puede resultar en ACK conexiones, página web con tiempos de espera, muy altos.

Usted debe asegurarse de que la cola *qwanacks* tiene suficiente ancho de banda para mantener sus descargas. Para calcular cuánto ancho de banda se necesita, hay dos opciones. Podría simplemente experimentar, estando pendiente de la cola mientras que tan rápido va la descarga si su conexión se lo permite, o podría tratar de solucionarlo. Como punto de partida, una conexión por cable DSL 1Mb/128Kb necesidades 125-128Kb/sec acerca de los paquetes ACK para descargar a la máxima velocidad. La figura 4.10 muestra una pantalla de *Queues* creadas con las condiciones mensionadas anteriormente.

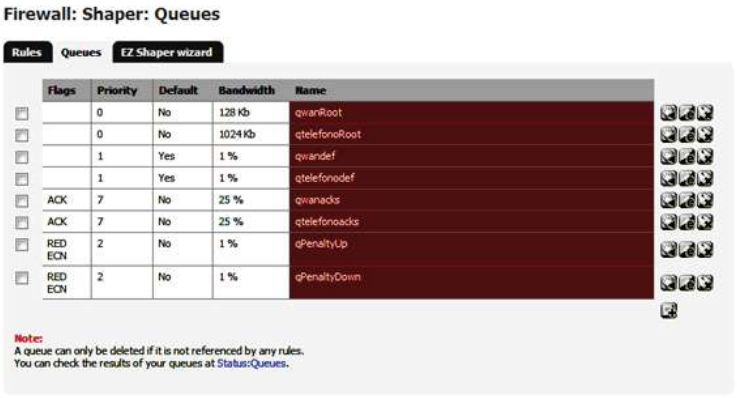

Figura 4.10: Pantalla de Queues creadas

Tomando el ejemplo anterior, en la figura 4.10, podemos ver que ACK puede consumir el 25 % de la carga del ancho de banda disponible. Por lo tanto, *qwanacks* debe tener al menos el 25 % del ancho de banda disponible. Si establece *qwanacks*, no debe ver que todo cae en cola. Sin embargo, usted verá mucho, pero que está bien. VoIP de carga a granel son los paquetes de tráfico, no es realmente importante por lo que no afecta si se desprende un poco. *qPenaltyUp* ahora se utiliza lo que queda de la subida de ancho de banda disponible, después de *qwanacks* ha utilizado hasta un 25 % de la misma. Usted probablemente querrá asignar un ancho de banda fijo para telefonía ya que no queremos que las llamadas se escuchen con eco o las conversaciones sean inaudibles. Por lo que asignaremos 25 kb de subida en la cola. Se han creado dos colas, una para la descarga otra para en el *qPenaltyUp* y 26 kb para la descarga en la que definimos como *qPenaltyDown*.

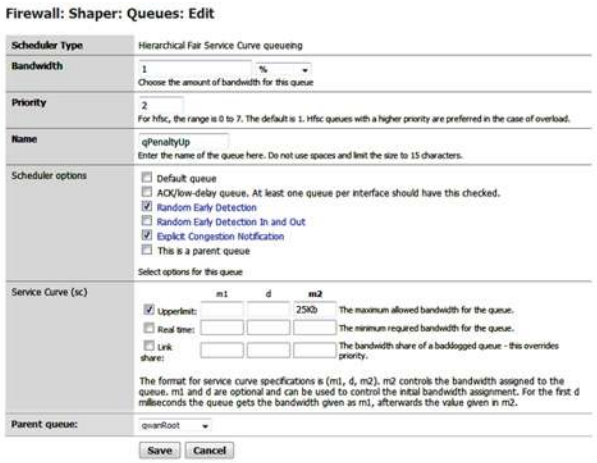

Figura 4.11: Configuración de Queues

4.4.6. IP Virtuales

Las IP virtuales sirven para crear sudredes y se definen como una dirección IP que no está conectada a un ordenador o tarjeta de interfaz de red en un equipo. Los paquetes se envían a la dirección VIP (IP virtual), pero todos los paquetes viajan a través de la interfaz de red real. En pfSense una IP virtual se define en el

menú Firewall, una pantalla de configuración se muestra en la figura 4.12 y las opciones de configuración son las siguientes:

- Tipo (Type): Se trata del tipo IP virtual. Lo estándar es “ProxyARP” que es una tecnología mediante la cual el firewall responde a todas las peticiones ARP de esa dirección, con lo que recibe los paquetes. “CARP” se utiliza para implementar un sistema con redundancia (básicamente son varias máquinas que comparten una dirección), mientras que la opción “other” se usa para opciones avanzadas que mezclan características de “proxyARP” y “CARP”(CARP se verá en el capítulo 7).
- Interfaz (Interface): La interfaz sobre la que se pública la IP.
- Dirección IP (IP Address): Se trata de la dirección o grupo de direcciones que el firewall capturará como copias.
- Las opciones *Virtual IP Password, VHID Group y Advertising Frequency* son descritas con detalle en el capítulo 7.
- Descripción: texto identificativo de la entrada Virtual IP.

Figura 4.12: Pantalla de configuración de una dirección IP Virtual

Una vez configurada la IP virtual, el siguiente paso es crear reglas correspondientes del NAT para las direcciones IP virtuales, seleccione Firewall, después en el submenú seleccione NAT y añada una nueva regla. (Veáse la figura 4.13).

En el campo seleccione la opción la interfaz WAN, después seleccione una de las direcciones IP virtuales que ha creado anteriormente, el tipo de protocolo NAT que desea (TCP, UDP, TCP/UDP, etc.), el rango de puerto externo (puede seleccionar otro si desea, como una web personalizada o un puerto del servidor, etc.) En el campo NAT IP, introduzca la dirección interna del servidor que desea ruta / NAT para el tráfico, después en el puerto local hay que especificar el puerto en la que la aplicación va a enviar el tráfico. Finalmente introduzca una descripción para identificar esta regla, asegúrese de que está marcada la opción de auto-añadir una regla de firewall para permitir el tráfico y guarde. Recuerde aplicar los cambios para sean activados.

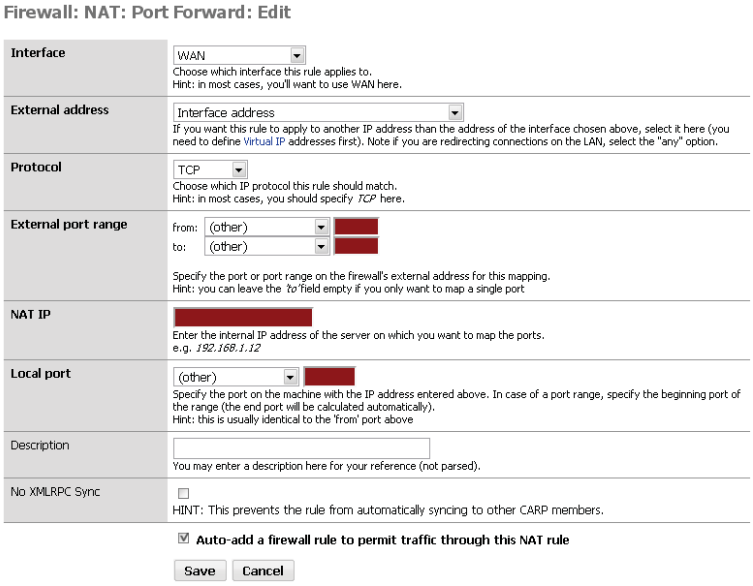

Figura 4.13: Pantalla de creación de una regla NAT salida

Capítulo 5

Balanceo de carga

En este capítulo describiremos uno de los servicios más importantes de pfSense, el balanceo de carga, sin embargo este menú cuenta con algunas otras opciones que no se cubriran en esta documentación (por encontrarse en fase de desarrollo y no garantizamos resultados satisfactorios) y su descripción será incluida en versiones futuras de este documento, nos referimos a las opciones: *OLSR, PPPoE Server, UPnP y RIP*. PfSense en el menú *System* en la opción *Packages*, lista algunos de los servicios opcionales que pueden ser instalados.

Más comúnmente, el término se refiere al equilibrio de carga mediante la distribución de las peticiones HTTP a través de los servidores web en un conjunto de servidores, para evitar una sobrecarga en cualquier servidor. Ya que el equilibrio de carga distribuye las solicitudes sobre la base de carga real en cada servidor, que es excelente para garantizar la disponibilidad y la defensa contra ataques de denegación de servicio .

En redes, el balanceo de carga es una técnica para distribuir el trabajo entre dos o más ordenadores, conexiones de red, CPU, discos duros, u otros recursos, a fin de obtener una óptima utilización de los recursos, maximizar el rendimiento y minimizar el tiempo de respuesta. Utilizando múltiples componentes con equilibrio de carga, en lugar de un único componente, se puede aumentar la fiabilidad mediante la redundancia de equipos. El equilibrio entre el servicio suele ser proporcionado por un programa dedicado o dispositivo de hardware como un conmutador *(switch)*. En general, el equilibrio de carga es un método uniforme para la transformación o distribución de las solicitudes de servicio a través de dispositivos en una red.

5.1. Balanceo de carga

Es el equilibrio de carga para distribuir las solicitudes de los servidores en la capa de trasporte, como TCP, UDP y el protocolo de transporte; el balanceador de carga distribuye las conexiones de red de los clientes que conocen una única dirección IP para un servicio, a un conjunto de servidores que realmente realizan el trabajo. Dado que la conexión se debe establecer entre el cliente y el servidor en relación orientada hacia el transporte, antes de enviar la solicitud del contenido, el balanceador de carga por lo general selecciona un servidor sin tener en cuenta el contenido de la solicitud. El balanceo de carga es también conocido como agregación de enlaces, usando dos o más enlaces en una sola, de mayor ancho de banda. Los enlaces agregados también proporcionan redundancia y tolerancia a fallos, si cada uno de los enlaces agregados sigue un camino distinto.

La agregación de enlaces puede utilizarse para mejorar el acceso a las redes públicas y líneas ADSL digitales. En la actualidad para automentar el ancho de banda en una red DSL, es mucho más costeable contratar varios módems DSL que utilizar uno con mayor ancho de banda. El equilibrio de carga consiste en la distribución de una tarea a un conjunto de equipos o periféricos para:

- Nivelar el tráfico de la red, es decir, distribuir la carga total en diferentes equipos.
- Asegurar la disponibilidad de equipos enviando datos sólo a aquellos equipos que puedan manejarlos o a los que tengan el mejor tiempo de respuesta.

La Capa 4 de equilibrio de carga también se puede usar para equilibrar el tráfico de acceso a Internet en múltiples vínculos, a fin de aumentar la velocidad de acceso a Internet. La Capa 7 de balanceo de carga, también conocida como el nivel de aplicación de balanceo de carga, es para analizar las solicitudes en la capa de aplicación y distribución de las solicitudes a los servidores basados en diferentes tipos de contenido de la solicitud, a fin de que pueda proporcionar la calidad de los servicios necesarios para los diferentes tipos de contenidos y mejorar el rendimiento global de grupo. Analizar la sobrecarga de solicitudes en la capa de aplicación es alto, por lo tanto su escalabilidad es limitada, en comparación con la capa 4 de balanceo de carga.

Ahora se presentaran las instrucciones para configurar el balanceo de carga y los procedimientos de salida del tráfico de Internet. Es conveniente comprobar si hay actualizaciones actuales y aplicarlas antes de configurar pfSense.

Primero debe ir al menú *Services* y seleccionar *Load Balancer*. Cree su *Load Balance Pool* (grupo de conexiones) que es una técnica, se abrirá la ventana de la figura 5.1.

Figura 5.1: Configuración del balanceo de carga

Los campos de configuración para la creación de un balanceador de carga son los siguientes:

- Nombre (Name): Es el nombre identificativo para el balanceador de carga.
- Descripción (Description): Texto identificativo del balanceador de carga.
- Tipo (Type): Se trata de tipo Gateway.
- Comportamiento (Behaviour): Se activa balanceador de carga.

- Puerto (Port): Este es el puerto de los servidores que están escuchando.
- Monitor: Protocolos usados para monitorear.
- Monitor IP: Dirección IP del equipo que será monitoreado.
- Nombre de la interfaz (Interface Name): Se refiere al nombre de la interfaz que se utilizará para equilibrar la carga de salida.
- Lista (List): Son las interfases que pertenecen al *pool*.

Para el caso del tipo Gateway, si se poseen dos proveedores de Internet, deberán aparecer ambos en la lista, el comportamiento en el balanceo de carga se obtendrá una velocidad de dos descargas equivalentes a la sumas de las velocidades de ambos proveedores, es decir, si la velocidad del proveedor1 = 1024kb y del proveedor2 = 1024kb, entonces la velocidad de descarga será 2048kb.

5.1.1. Balanceo de carga basado en DNS

El equilibrio basado en DNS consiste en distribuir las peticiones entre los diferentes servidores, todos en conjunto tienen una única dirección IP. Al recibir una petición el DNS resuelve un servidor, el cual cambia al recibir la siguiente petición esto se conoce como *round-robin*.

El balanceador de carga tiene algunas características especiales, de hardware y software.

- Carga asimétrica: Una relación puede ser asignada manualmente a causa de algunos servidores, para obtener una mayor proporción de la carga de trabajo que otros.
- Prioridad y activación: Cuando el número de servidores disponibles cae por debajo de un cierto número, o la carga es demasiado alta, los servidores de espera puestos en línea.
- Aceleración y descarga de SSL: Las SSL aplicaciones son una carga pesada sobre los recursos de un servidor web, especialmente en el CPU y los usuarios pueden ver una lentitud en la respuesta, o por lo menos los servidores están gastando una gran cantidad de ciclos de hacer las cosas que no fueron diseñados para hacer. Para resolver este tipo de cuestiones, un distribuidor de carga capaz de manejar SSL especializados en hardware puede ser usado, y así la carga de los servidores de la web se reduce y el rendimiento para los usuarios en estándar.
- HTTP caché: El balanceador de carga puede almacenar contenidos, para que algunas solicitudes se puedan manejar sin ponerse en contacto con los servidores web.
- Filtrado de contenido: Algunos balanceadores de carga pueden modificar arbitrariamente el tráfico en el camino.
- HTTP seguridad: Algunos balanceadores de carga pueden ocultar las páginas de error HTTP, eliminan la identificación de las cabeceras HTTP de respuestas, y encriptar *cookies* para los usuarios que no puedan eliminarlo.

Generalmente se encontraran tres tipos de tráfico permitidos, y son:

1. Tráfico que puede ser de carga equilibrada de modo que la velocidad de conexión, sea el resultado de sumar las velocidades de diferentes proveedores de Internet.
2. Tráfico en el caso de que una conexión falle, se tiene una conexión alterna.
3. Tráfico que tiene que ir a una conexión específica, es decir, el tráfico es enviado a una determinada ruta.

5.2. Conmutación por error (Failover)

La conmutación por error o *Failover* es un modo de funcionamiento en el que las funciones de un componente del sistema (como un procesador, un servicio de red o una base de datos) son asumidos por los componentes del sistema secundario, cuando el componente principal no está disponible, ya sea por un error o tiempo previsto, se utiliza para hacer los sistemas tolerantes a fallos. El procedimiento implica automáticamente descarga de tareas a un componente del sistema de reserva a fin de que el procedimiento sea transparente como sea posible para el usuario final. La conmutación por error puede aplicarse a cualquier aspecto de un sistema, en una PC por ejemplo, en caso de fallo puede ser un mecanismo para proteger contra un fallo del procesador; dentro de una red, en caso de fallo se puede aplicar a cualquier sistema o componente de red de los componentes, puede ser un dispositivo de almacenamiento o servidor web.

La conmutación por error en pfSense funciona de la misma manera que el comportamiento de equilibrio de carga, creando un pool (grupo de conexiones), pero las interfases son seleccionadas de una lista ordenada, una a una hasta que el sistema pueda restablecer la conexión.

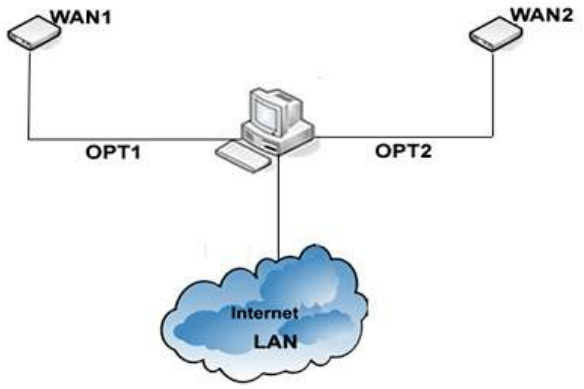

Figura 5.2: Diagrama de conmutación por error

En la figura tenemos que si WAN1 falla entonces la puerta de enlace utilizará a WAN2, hasta que WAN1 vuelva a estar disponible. De la misma manera que con el balanceo de carga el monitoreo se realiza usando ICMP o algún protocolo. Si deseamos monitorear más de una conexión, es necesario agregar un *pool failover* para cada conexión. Ejemplo: De la figura 5.3 agregamos un conmutador por error para la interfaz WAN1 monitoreando a 148.216.6.9.

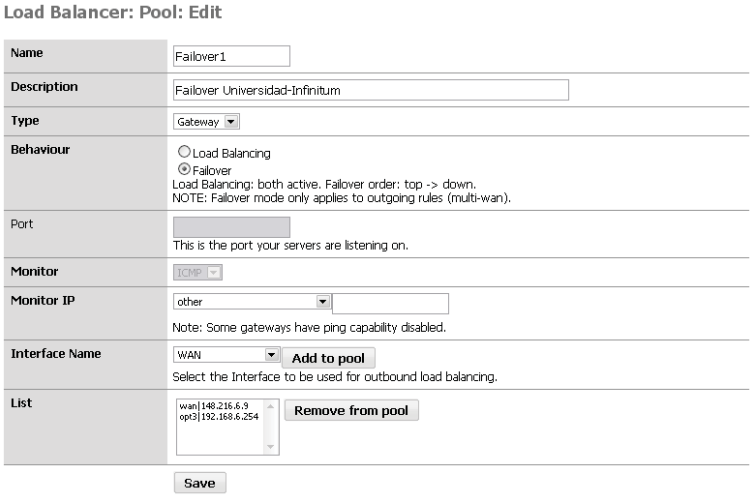

Figura 5.3: Configuración de conmutación por error1

De la misma manera se agrega un *failover* para WAN2

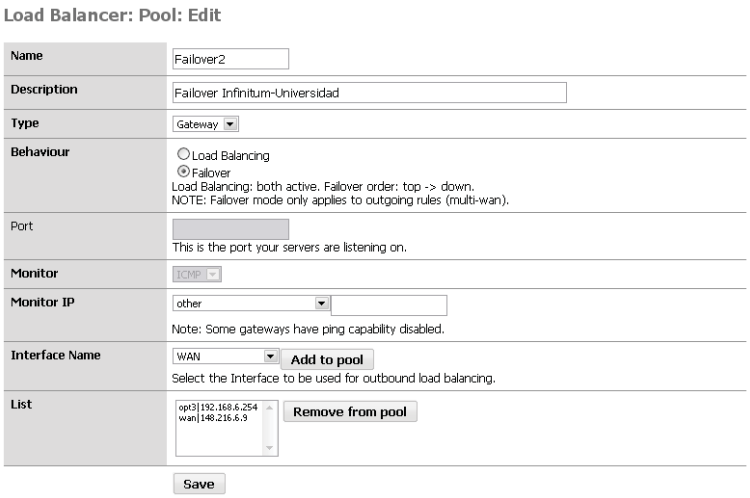

Figura 5.4: Configuración de conmutación por error2

5.3. Servicios adicionales

5.3.1. DNS forwarder

Es una base de datos que permite almacenar información de nombres de dominio en redes como Internet. El uso más común que se le da es permitir la asignación de un nombre de domino de Internet a un ordenador con dirección IP. Esto permite conectarse con la máquina en cuestión sin necesidad de tener que rastrear las direcciones IP. La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio de http:/google.com es 74.125.47.103, la mayoría

de los usuarios llegan a su equipo especificando http:/google.com y no la dirección IP, además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre. El DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet.

El DNS *forwarder* es un mecanismo para crear un servidor DNS en los clientes DHCP de una red local, de tal manera que los nombres de los equipos podrán ser accesibles de la misma manera que servidores de Internet. Existe una lista donde se asocian IP y nombres, para ello deberá seleccionar DNS *forwarder* en el menú *Services*, donde se mostrará una pantalla como la figura 5.5.

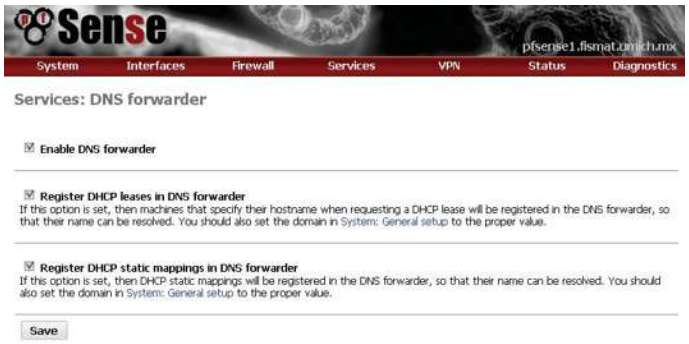

Figura 5.5: Pantalla de Services, DNS forwarder

También se dice que es un servidor de nombres limitado pero muy rápido, que recurrirá a los servidores de nombres especificados en la configuración básica del firewall cuando no pueda resolver un nombre. Al emplear el DHCP de pfSense, las máquinas verán el firewall como su servidor de nombres y puerta de enlace. Además, podemos indicar nombres de máquinas (incluido su dominio) para forzar la resolución del nombre de máquina hacia una determinada IP. Esto nos permite asignar IP locales a nombres de máquina del tipo nombremaquina.dominio.ejemplo, los usuarios podrán ver un servicio (web, correo) con el mismo nombre tanto si están en la red local como si se conectan desde Internet (desde casa, desde una biblioteca, desde un ciber, etc.) Resulta ideal poner en esta lista de nombres de máquina todas las máquinas que den servicio a la red (servidores e impresoras). De esta forma la resolución de nombres para los servicios será eficaz. Eventualmente también se puede emplear esta asignación para bloquear o redireccionar el acceso a alguna dirección de Internet que no interese que esté disponible. No conviene abusar de esta funcionalidad. Si lo que pretendemos es filtrar contenidos, es mejor pensar en un servidor proxy como, por ejemplo, *Squid*.

La figura 5.6 muestra la edición de un host y sus campos de configuración son los siguientes:

- Host: Nombre del host, sin parte de dominio, por ejemplo, myhost.
- Dominio (Domain): Dominio de la acogida, por ejemplo, blah.com.
- Dirección IP (IP address): Dirección IP del anfitrión, por ejemplo, 192.168.100.100.
- Descripción (Description): Puede introducir aquí una descripción para su consulta (no analizada).

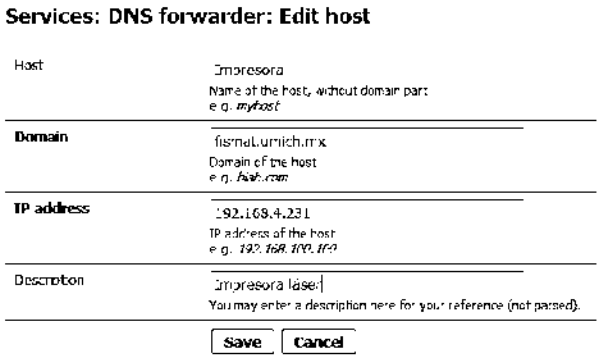

Figura 5.6: Edición de un Host

5.3.2. DHCP

Protocolo Dinámico de Configuración de Anfitrión, es un protocolo de red de tipo cliente/servidor el cual posee una lista de direcciones IP, que se encarga de asignar direcciones IP a los clientes conforme estos van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Algunas de las ventajas de tener configurado el DHCP son:

- Configuración automática de las conexiones de red de cada dispositivo (ordenador, punto de acceso, impresora, etc.)
- La posibilidad de asignar direcciones IP “estáticas” en función de la dirección MAC del dispositivo.
- La posibilidad de “capturar” fácilmente las direcciones MAC, sin tener que introducirlas manualmente.
- La posibilidad de “cerrar” la lista de direcciones MAC, impidiendo la conexión de dispositivos “no conocidos”.
- Poder “despertar” dispositivos de la red para tareas de mantenimiento remoto.
- Tener una pantalla donde tienes relacionados todos los equipos de una red.
- Eventual movilidad de equipos entre redes.

Capítulo 6

Autenticación de clientes

En este capítulo se habla del paquete *OpenVPN* que incorpora pfSense, el cual permite crear redes privadas virtuales (VPN). Con *OpenVPN* se puede extender la red a cualquier lugar del mundo, haciendo que la identificación y la comunicación sean seguras. Antes de tener instalado en su servidor pfSense, el administrador de la red se conectaba al escritorio de uno de los servidores de su red por RDP, desde una IP fija. Al usar una IP fija se podía controlar con las reglas de uno de los routers ADSL el acceso a este servicio. Ahora, con *OpenVPN* el administrador entra directamente en la red local, sin necesidad de que ningún ordenador le haga de puente. Y lo hace desde una IP dinámica, autentificándose en base a certificados SSL. La figura 6.1 muestra una estructura de autenticación de clientes.

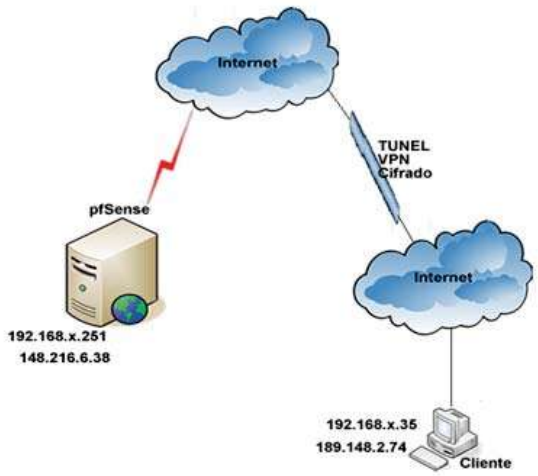

Figura 6.1: Estructura de autenticación de clientes

6.1. Instalación de OpenVPN

La instalación de *OpenVPN* tiene 3 fases:

- Creación de los certificados, que se realizará en una estación de trabajo con Windows XP.
- Configuración del servidor, a través de la consola web de administración de pfSense.
- Configuración de los clientes *OpenVPN*.

El primer paso se realizará desde una estación de trabajo convencional, el *OpenVPN* para Windows XP es compatible con la mayoría de los firewalls . Descargamos de www.openvpn.se la última versión de *OpenVPN* para Windows (es de código libre) con driver TAP de tarjeta de red virtual incluido: http:/openvpn.se/files/install_ packageavpn-2.0.9-gui-1.0.3-install.exe Desde el panel de control en conexiones de red, encontrará una nueva tarjeta de red. Se le sugiere cambiar el nombre que tiene por el de TAP, puede aprovechar también para ponerle a la tarjeta real el nombre de LAN. Esto con el fin de identificar de manera amigable las interfases de red (veáse la figura 6.2).

Figura 6.2: Interfases de red

Enseguida se darán una serie de pasos para la configuración de *OpenVPN*.

- Seleccione o vaya a la carpeta: `C:\Archivos de programa\OpenVPN\config` y cree un archivo de texto de nombre dominio.ejemplo.ovpn con el siguiente contenido:

```
float port 1194
dev tun
dev-node TAP
proto tcp-client
remote RRR RRR RRR RRR 1194
ping 10
persist-tun
persist-key
tls-client
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
# comp-lzo
Pull
Verb 4
```

Siendo RRR RRR RRR RRR la IP pública del sitio al que quiera conectarse. La línea comp-lzo está comentada (símbolo #) para poder hacer las primeras pruebas sin comprensión en las comunicaciones.

6.1.1. Generación de llaves y certificados (entidad certificadora, servidor y cliente)

Abra una ventana de órdenes MS-DOS (cmd.exe) y teclee:

```
cd \c:\Archivos de programa\OpenVPN\easy-rsa"
init-config
edit vars.bat
```

Ahora edite vars.bat, poniendo sus datos en las últimas líneas:

set KEY_COUNTRY = ES
set KEY_PROVINCE = Provincia
set KEY_CITY = Población
set KEY_ORG = El nombre de la organización
set KEY_ EMAIL = Administrador @ dominio.ejemplo

- De nuevo en la ventana del intérprete de órdenes MS-DOS, haga lo siguiente:

```
vars
clean-all
build-ca
```

El último comando (build-ca) generará el certificado CA a través del comando openssl. Se mostrarán los datos por defecto, los cuales sólo tendrá que confirmar. En el nombre del servidor tendrá que poner dominio.ejemplo ya que este proceso generará ca.key (llave privada de la entidad certificadora, para el servidor) y ca.crt (certificado-raíz en la entidad certificadora, para el servidor y para todos los clientes).

```
Build-key-server server
```

Este proceso genera la llave privada y el certificado (server.key y server.crt) para un servidor OpenVPN. Aquí tendremos que indicar cortafuegos.dominio.ejemplo como el nombre de la máquina.

```
Build-key client
```

Este proceso genera la llave privada y el certificado (client.key y client.crt) para un cliente OpenVPN. Indica como nombre de máquina cliente.dominio.ejemplo: A las dos preguntas finales de confirmación sólo se tiene que contestar *y (yes)*. En caso de conectar más de un cliente cada uno de ellos tiene que tener su propia llave y certificado de cliente. Los certificados de cliente pueden ser revocados y de esta manera un cliente deja de estar autorizado para conectarse.

```
Build-dh
```

Como paso final se tienen que generar los parámetros *Diffie Hellman* para el servidor *OpenVPN*, lo que requiere un cierto tiempo en la máquina: Se obtendrá con ello un archivo para el servidor llamado dh1024.pem.

6.1.2. Instalación de la llave y de los certificados en el cliente Windows XP

Copie los archivos ca.crt, client.key y client.crt que se tiene en:
`c:\Archivos de programa\OpenVPN\easy-rsakeys` (generados en el apartado anterior) a
`c:\Archivos de programa\OpenVPN\config` del ordenador cliente.

6.2. Configuración de OpenVPN en pfSense

Seleccione VPN: OpenVPN: Server: Edit y añade un servidor VPN. Elija el protocolo TCP, active *Dinamic IP*, añada el puerto 1194, en el campo en *Address pool* se tiene que poner una red que no coincida con ninguna de las ya existentes para diferenciarla con las redes internas. Recuerde añadir la máscara de red correspondiente. Si usted no desea que el servidor le asigne de manera automática una dirección IP, entonces active la casilla *Use static IPs*. De la misma manera debe activar Client-to-client VPN, y se procede a pegar el contenido del certificado de CA en formato X.509, en el campo CA certificate.

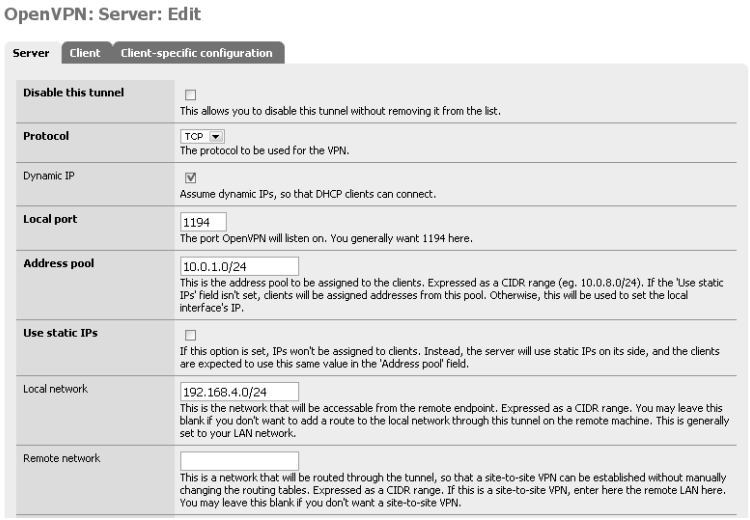

Figura 6.3: Pantalla de configuración de OpenVPN

De la misma manera se pegan los contenidos de los archivos: server.crt, server.key en el campo server key y por último el archivo dh1024.pem en el campo DH parameters. (veáse la figura 6.4).

Figura 6.4: Pantalla de configuración de archivos

Ahora se debe activar “LZO compression” para obtener mayor rendimiento y las opciones que le convengan para la configuración de la red. Se recomienda que la primera vez se haga sin comprensión.

Figura 6.5: Pantalla de configuración de OpenVPN

Ya está todo a punto para la primera conexión. En el cliente en la barra de tarea se tienen 2 iconos, el de OpenVPN GUI (interfaz gráfica) y el de TAP, que nos dice que esta desconectada:

Figura 6.6: Iconos en la barra de tarea

Si hace doble click sobre el icono de OpenVPN GUI, verá una pantalla como la siguiente figura:

Donde se informan los pasos que hace la conexión. Si todo ha ido bien, esta ventana se cerrará y verá que el icono TAP cambia:

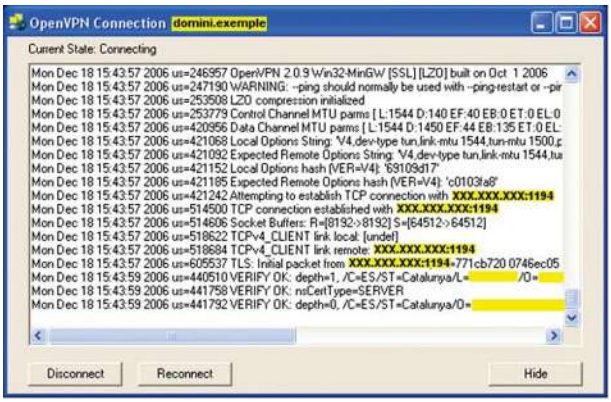

Figura 6.7: Datos administrados

Figura 6.8: Conexión de la interfaz TAP

Con esto ahora está usted en la red gestionada por pfSense como una máquina más. Pruebe si puede acceder a recursos que estén en las redes 192.168.2.0, 192.168.4.0. Por ejemplo a la propia administración web de pfSense. Recuerde que si ha hecho las primeras pruebas sin comprensión LZO hay que activarla, tanto en el servidor como en el cliente (ya comentado anteriormente). Con estos pasos ya se tiene configurada la VPN, falta crear una regla en el firewall que abra el puerto 1194 para dar acceso a la conexión desde el exterior. En la siguiente figura se ve la imagen de la regla, en el conjunto de reglas de entrada de WAN. Se ha establecido el registro de los eventos de esa regla, para poder monitorear el acceso por VPN.

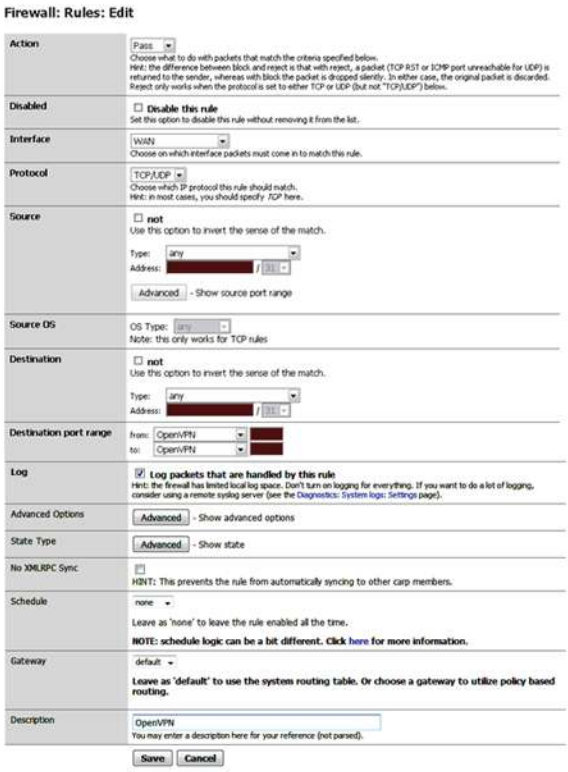

Figura 6.9: Pantalla de creación de una regla de OpenVPN

Una vez que pulse “guardar” debe aplicarse.

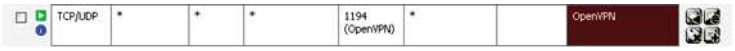

Figura 6.10: Pantalla de la regla creada de OpenVPN

Después debe ir a *Firewall: NAT: Outbound*, deberá estar activada la opción *Manual Outbound NAT rule generation*. Agregue una regla de salida en función de la dirección de la red VPN, pulse guardar.

Figura 6.11: Regla NAT de salida

6.3. Portal Captivo

En este punto, el firewall está configurado y debería ser plenamente operativo. El siguiente paso es configurar el Portal Captivo *(Captive Portal)* en la red inalámbrica, de manera que se pueda regular el acceso. Hasta ahora, el acceso a la red inalámbrica se controlaba mediante una clave configurada en los puntos de acceso con encriptación wep. Esta clave estaba compartida en una unidad de red, de manera que se limitaba el acceso al personal de la facultad. Este sistema de seguridad es muy débil ya que el hecho de compartir la clave no asegura

el sistema, y al no ser pública evita que todos los usuarios puedan acceder. Mediante el portal captivo, la red es abierta y cualquiera tiene acceso. En cuanto se conecta un usuario e intenta acceder a través de un navegador a un servicio de red, se abre una página web donde se solicita validación basándose en credenciales. En el caso de tener una autentificación correcta se le redirige a la página solicitada, en caso contrario se le niega el acceso. PfSense permite validación de usuarios del portal captivo con una base de datos local o a través de un servidor RADIUS, (sistema de validación de aplicaciones de Internet).

6.3.1. Configuración del sistema de Portal Captivo para la red inalámbrica

A continuación se muestran los pasos necesarios para configurar el sistema de validación mediante Portal Captivo, que se usará en las redes inalámbricas. Es requisito tener implementado de manera totalmente funcional el firewall, con el comportamiento deseado en cuánto a reglas y servicios. Para configurar Portal Captivo se debe acceder a la pestaña de *Services: Captive Portal* desde la consola de administración de pfSense como se ve en la figura 6.13.

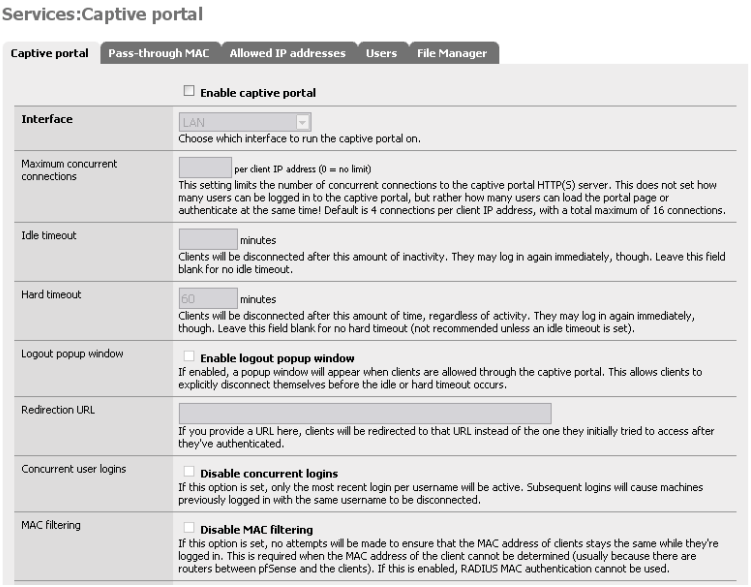

Figura 6.12: Pantalla de configuración de Portal Captivo

Los parámetros que se pueden configurar son:

- Tiempo de inactividad (Idle Timeout): Indica el tiempo que el sistema tarda en cerrar una sesión sin actividad. En ese caso vuelve a aparecer la página de validación y el usuario pueda volver a conectarse introduciendo sus credenciales.
- Tiempo duro (Hard Timeout): Fija el tiempo máximo de conexión. Al cerrarse la conexión aparece la ventana de validación otra vez.
- Cerrar sesión ventana (Logout popup window): Se trata que al validarse en el sistema, se abra una ventana emergente en el navegador, con el botón para salir del sistema. La mayoría de los navegadores modernos

bloquean las ventanas emergentes, con lo que muchas veces no aparecerá. En este caso, se desconectará la sesión mediante los sistemas de Timeout.

- Redirección de URL (Redirection URL): Dirección de la página a la que se enviará al navegador después de una conexión autentificada.
- Inicios de sesión de usuario concurrente (Concurrent user logins): Se trata de permitir o no más de una sesión para un solo usuario. En el caso de ser deshabilitado (disable), se podrá conectar desde la última máquina donde se haya validado.
- Filtrado de MAC (MAC filtering): El sistema de Portal Captivo permite crear una lista de direcciones desde las que se dará acceso sin tener que introducir siempre usuario y contraseña. En el caso de que se seleccioné esta opción, esa lista será ignorada.

La última parte de la página de configuración permite rellenar las opciones de la página de conexión que aparecerá para llenar los datos. De las opciones de la página, es importante comentar que se puede hacer que la validación sea por https, protocolo por encriptación, en vez de http. En este caso se debe dar los datos de los certificados necesarios, así como sus claves asociadas. Por último se puede adjuntar un fichero HTML con el contenido de la página que mostrará el sistema para la validación y en caso de error en las credenciales. Se puede añadir referencias a imagines u otros documentos que se hayan subido previamente al servidor, utilizando la pestaña Upload. Respecto al tema de la autentificación, en el caso de seleccionar *Local User Authentication*, se deben crear los usuarios bajo la pestaña *Users* de la consola web de administración de pfSense, en el apartado de Portal Captivo. El sistema nos pedirá los datos de usuario, contraseña y descripción.

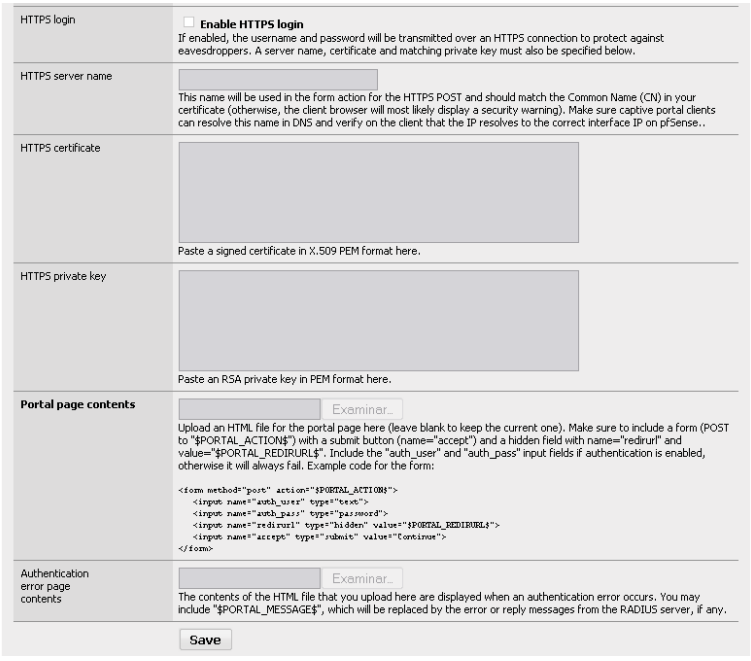

Figura 6.13: Pantalla de la última parte de la configuración del Portal Captivo

Capítulo 7

Replicación del servidor

En esté capítulo se presenta una creación de servidores de seguridad redundante, es decir, se tiene un grupo de host usando CARP es un llamado ”grupo de redundancia”, dentro de este grupo uno equipo es designado como maestro, los demás son llamados esclavos. El maestro es el que toma la dirección IP y responde a todo el tráfico o petición presentada. Cada host puede pertenecer a varios grupos de la redundancia. Cabe señalar que cada host debe tener una segunda dirección IP única. Toda configuración de CARP se puede hacer desde la propia consola web de administración y el requisito es que se debe tener una interfaz de red en cada equipo que se quiera redundar. De esta manera se tendrá un servicio de redundancia completo y seguro.

7.1. CARP

CARP es Common Address Redundancy Protocol (protocolo de redundancia de dirección común) es un protocolo que permite que múltiples máquinas de la misma red local puedan compartir un conjunto de direcciones IP. Su principal propósito es proporcionar redundancia en caso de fallo. El sistema se basa en varios equipos que compartan una dirección de red, de manera que cuando el sistema principal (maestro) no responda, el secundario (esclavo) realice la función de éste.

En el IETF a fines de 1990 se comenzó a trabajar sobre una solución para el problema de la IP compartida. En 1997, CISCO les informó de que éste ya estaba cubierto por las patentes de CISCO. Éste informó a los desarrolladores de OpenBSD que deberían hacer valer los patentes de HSRP. Una implementación libre de VRRP (Virtual Router Redundancy Protocol) no se podía realizar, entonces los desarrolladores de OpenBSD dieron una alternativa a los patentes de VRRP, según los términos de la licencia. Para evitar todo esto, se garantizó que su idea para el CARP era fundamentalmente diferente, siendo diseñado para seguridad y usando criptografía, además de que está disponible completamente gratis desde 2003 y se ha integrado a FreeBSD y NetBSD .

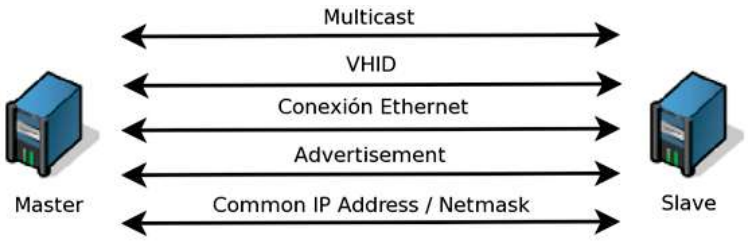

Figura 7.1: Protocolo CARP

Entonces se puede resumir que CARP nace como alternativa libre (no-propietaria) de VRRP de CISCO, el cual hace casi, pero no del todo, lo mismo que hace CARP, solo que su uso es especialmente para ruteadores y firewalls de CISCO o asociados, a los cuales agregarle soporte de VRRP suele ser muy caro, en cambio con CARP solo necesitas tener OpenBSD corriendo, y como se mencionó no solo le da redundancia al acceso a la red, si no a casi cualquier tipo de servicio que esté sobre IP, ya que al ser OpenBSD es un Unix, y al ser un Unix se le puede ejecutar varios servicios, a los cuales les podría servir esta redundancia de direcciones.

En la figura 7.2 muestra una imagen de una estructura de red de CARP.

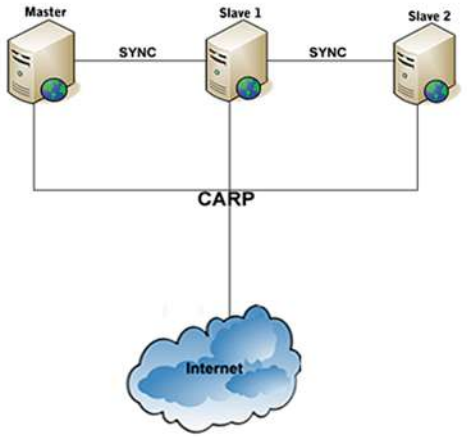

Figura 7.2: Estructura del protocolo CARP

CARP se ubica en la capa 3 del modelo OSI, y tiene cierta presencia en la capa 2 forma, CARP hace esto si tienes una máquina con cierta dirección IP, la cual es la dirección a la que los clientes se conecten se le llamará maestro, que está expuesto a los usuarios, y dentro del mismo segmento de red estarían otras máquinas, las cuales serían los esclavos, que están esperando que el maestro falle, el maestro en un cierto intervalo de tiempo manda mensajes a sus esclavos, estos mensajes llamados *advertises*, o avisos (pueden estar protegidos por diferentes medios de encriptación), si el esclavo deja de recibir mensajes en un periodo de tiempo definido, entonces se considerará que el maestro no está funcionando, por lo que otro equipo actuando como esclavo tomará su lugar, claro que quien será el nuevo maestro dependerá de las prioridades que le hayan establecido. Tomado el lugar del maestro avisa a los esclavos que él es el que hará todas las funciones ahora, y estos esclavos estarán pendientes para cuando éste falle, si el primer maestro se activa, de nuevo tomará su lugar, y debido a prioridades los esclavos obedecerán al maestro.

La ventaja principal es que los clientes sigan conectados sin tener que enterarse quién dará el servicio ahora, ya que seguirán llamando a la misma dirección IP. Del mismo modo los servicios que se estén dando también deberán ser sincronizados entre los esclavos. Como desventaja el hecho de que esta sincronización provoca demasiado tráfico en ese segmento de red, lo cual no es deseable. Por ello se debe dejar una interfaz de red para la sincronización.

Capítulo 8

Caso de estudio

La Facultad de Cs. Físico-Matemáticas esta distruida en 3 edificios (B, D y L), las áreas que requieren servicios de cómputo son biblioteca, áreas adminitrivas, aulas, laboratorios y cubículos de profesores.

Los administradores de los servicios informáticos de la facultad de Físico-Matemáticas (UMSNH), se ubican en el área de servidores en el edificio "B" planta baja, y los mismos administradores se encargan de gestionar los recursos para ofrecer servicios de calidad que den soporte a las tareas propias de la facultad. Estos servicios se pueden enmarcar en dos grupos (servicio y atención al usuario).

- Servicios de acceso a la red, monitoreo, administración y actualización de la infraestructura de red (switches, cableado, etc.).
- Servicios de impresión, donde está la implementación de sistemas que permiten el trabajo colaborativo en grupo, así como el uso de recursos compartidos y los permisos adecuados.
- Atención de usuarios, entre las actividades se encuentran configuración, actualización del sistema operativo, instalación de software, reciclaje, etc.

8.1. Análisis del problema

8.1.1. Problemas actuales

1. Cableado dañado.
2. Ancho de banda insuficiente de la red. Su principal causa es la mala arquitectura que se tiene.
3. Duplicidad de direcciones IP. Con el tiempo la cantidad de direcciones IP disponibles es insuficiente, hay que contar que todos los equipos de cómputo (servidores, impresoras, etc.) cuentan con una dirección IP.
4. Infraestructura limitada, se cuenta con pocos equipos de conectividad de red (un conmutador *(switch)* administrable, un ruteador inalámbrico, etc.) por lo tanto el riesgo de que en un dado momento se presentara un problema en algún equipo, provocaría no tener servicio de red.

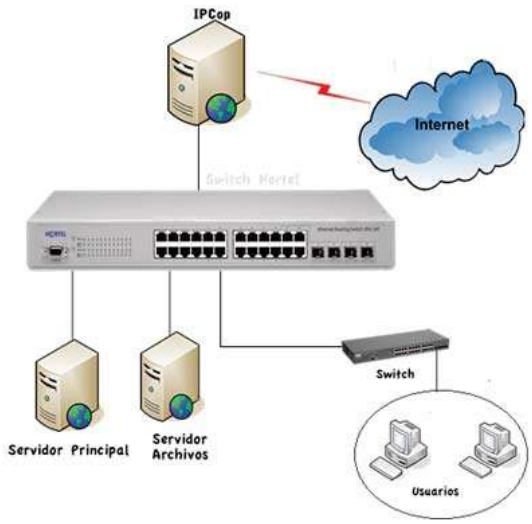

Figura 8.1: Diagrama de la red actual

5. Topología inadecuada, la figura 8.1 muestra un diagrama de la red actual.
6. Sistema de detección de intrusos activo para proteger la red local.
7. Limitaciones del software utilizado, como la imposibilidad de establecer reglas de acceso de salida, es decir todo el tráfico de la red local esta permitido hacia el exterior.
8. Imposibilidad de acceso remoto, a través de redes privadas virtuales VPN.

8.1.2. Solución

Debido a los problemas mencionados obligó a la necesidad de realizar una implementación nueva, que solucione todas estas carencias y que en medida de lo posible aporte nuevas funcionalidades de futuro a la infraestructura de red.

- Recableado. Se recableó la mayoría de los cables para tener una buena conectividad de red, así como también se etiquetaron los cables para facilitar detectar un cable.
- Se incrementó el número de puntos de acceso en la red inalámbrica.
- Diseñar una arquitectura adecuada de red que proporcione tolerancia a fallos del firewall, así como recuperar el acceso de forma sencilla y ampliar la capacidad de conexión de un gran número de equipos e identificación de las comunicaciones.
- Se dividió la red en tres subredes, de manera que los servidores e impresoras esten en una red distinta a las estaciones de trabajo, para poder filtrar y monitorizar el acceso según convenga. La segmentación de la red se basó en los tipos de usuario según su necesidad.
  En la *red LAN o red local*, están conectados los laboratorios de cómputo (aproximadamente 50 equipos de cómputo), se utilizará la subred 192.168.2.0/24 lo que permite 254 equipos.

En la *red biblioteca y profesores*, en esta red están conectados como se menciona los equipos de la biblioteca y los cubículos de los profesores (aproximadamente 33 equipos de cómputo), y la subred será 192.168.4.0/24.

Finalmente la *red balanceo* se instalaron servidores y servicios comunes (impresoras, inalámbricos, etc.) que utilizarán la subred 192.168.6.0/24.

- Administrar el conmutador *(switch)*. Se dividió la red en tres segmentos, mediante el uso de las VLAN o Redes virtuales que se usan para dividir segmentos de red a nivel del mismo conmutador, básicamente se asigna un identificador de VLAN a cada puerto del conmutador, de manera que todos los puertos que tiene el mismo identificador, actúan como si estuvieran conectados a un mismo conmutador estándar (sin VLAN), además existen puertos que están conectados a varias o a todas las VLAN. Estos puertos son llamados *trunk*.
- Reeplazar a IPcop por pfSense para contar un con software que soporte todas las necesidades antes mencionadas.

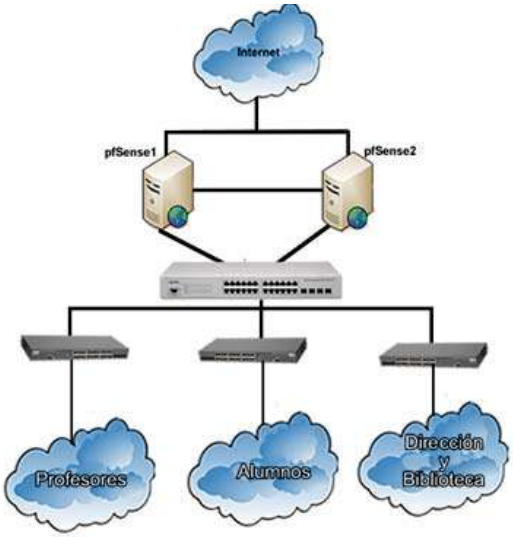

Figura 8.2: Diagrama de la red final

Esta topología cumple con las especificaciones de tolerancia a fallos del firewall, ya que en caso de algún problema, como falta de energía, quemado de discos, etc. se puede recuperar el acceso de forma sencilla, también permite ampliar la capacidad de conexión de un gran número de equipos y poder tener una identificación de las comunicaciones.

8.2. Configuración de las interfases de red

Para asignar interfases debe acceder al menú *Interfaces: Assign*, en un primer momento el sistema va denominar a las interfases que usted asigne como OPT1, OPT2, etc. después si lo desea puede cambiar el nombre para una mejor distinción.

Los campos para la configuración de una interfaz, son los siguientes:

- Para habilitar esta interfaz debe activar *Enable Optional 1 Interface*.
- Tipo (type): Se selecciona si desea que la interfaz sea estática *Static o DHCP*.
- MAC Address: En este campo se puede utilizar para modificar la dirección MAC de la interfaz asignada. (puede ser necesario con algunas conexiones de cable). Introduzca una conexión MAC en el siguiente formato: xx: xx: xx: xx: xx: xx: o dejar en blanco.
- MTU: En este campo se introduce un valor y los SMS de sujeción de las conexiones TCP con el valor ingresado, menos 40 (TCP/IP de tamaño de cabecera) será en efecto. Si deja este campo en blanco, una MTU de 1492 bytes para el protocolo PPPoE y 1500 bytes para todos los demás tipos de conexión se asumirá.
- Bridge with: Este campo es para si se desea que la interfaz haga puente con alguna interfaz ya creada o configurada.
- IP Address: Aquí se asigna una dirección IP en el caso que fue seleccionada de manera estática *(Static)*.
- Puerta de enlace (Gateway): Si tiene varias conexiones WAN, introduzca la dirección IP, en caso contrario, deje esta opción en blanco.
- FTP Helper: En este campo se deshabilita el usuario de la aplicación de proxy FTP.
- Hostname: El valor en este campo se envía como el identificador de cliente DHCP y cuando se solicite un nombre de host DHCP. Algunos proveedores de servicios de Internet pueden requerir éste (para la identificación de clientes).

8.3. Configuración de pfSense

8.3.1. Configuracion de reglas

PfSense permite organizar el tráfico para que los diferentes servidores puedan comunicarse entre sí. Si se cuenta con varios proveedores ISP es importante asegurarse que el tráfico saliente, lleva la IP correspondiente a la subred. Esto con el fin de evitar que si se tiene un servidor de correo con el ISP1 y las reglas envían el tráfico con la IP de la ISP2 y la comunicación sea rechazada.

Al crear las reglas del firewall para cada interfaz de red, las reglas que exigen una mayor prioridad están en primer lugar. Esto debido a que cada estado en la lista, tendrán prioridad por encima de los demás. Por lo tanto, si usted quiere un protocolo especial para tomar un camino específico, estos deben estar en una prioridad más alta.

Ahora se van a crear reglas para las diferentes interfases de red, las cuales son: LAN, WAN, Biblioteca y profesores y ISP1.

Para la interfaz LAN se crea la regla que se muestra en la figura 8.3 que se permite cualquier acceso a la red LAN, y se permite el acceso del protocolo ICMP, (el protocolo ICMP solamente informa de incidencias

en la entrega de paquetes o de errores en la red en general, pero no toma decisión alguna al respecto. Esto es tarea de las capas superiores).

Figura 8.3: Reglas LAN

En la interfaz WAN se crea la primera regla por defecto como se muestra en la figura 8.4, RFC 1918 networks bloquea el tráfico desde WAN hacia la LAN y viene por defecto, esta regla es para que no se pueda acceder a pfSense desde la interfaz WAN. Además de que se evita usar direcciones 192.168.x.x. en la interfaz WAN. También permite cualquier acceso a la red WAN.

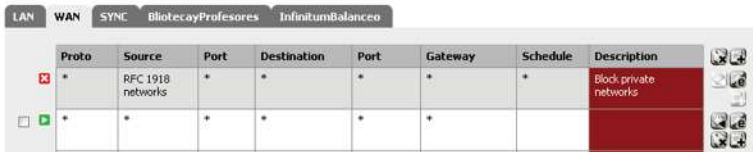

Figura 8.4: Reglas WAN

Para la interfaz de Biblioteca y profesores que fue creada en la subred 192.168.4.254, las reglas son las mismas de la interfaz LAN se permite cualquier acceso a la red Biblioteca y Profesores, como también se permite el acceso del protocolo ICMP. (Veáse la figura 8.5).

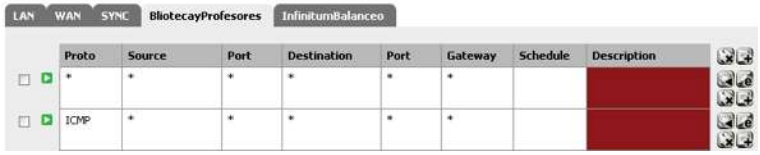

Figura 8.5: Reglas Biblioteca y Profesores

Esta interfaz ISP fue creada con la finalidad de balancear la carga junto con la interfaz WAN, por lo que también se crearon las siguientes reglas: que se permita el acceso a la red LAN, permitir el acceso del protocolo ICMP a la red LAN, permitir el acceso del protocolo TCP que venga de la dirección 192.168.2.201 del puerto 80(HTTP) con destino a la 192.168.1.254 que salga al exterior por defecto *(default)*.

8.3.2. Configuración del DHCP en pfSense

Para configurar el servidor DHCP en pfSense debe seleccionar *Services:* DHCP *Server* y seleccionar la pestaña correspondiente a la interfaz de red donde se habilitará el servidor de DHCP.

Los campos de configuración de la pantalla de servicios DHCP son los siguientes:

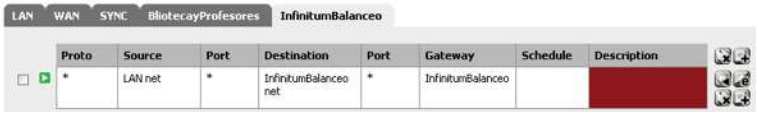

Figura 8.6: Reglas ISP

- Habilitar el servidor DHCP (Enable DHCP server on Biblioteca y Profesores interface): Esta opción habilita el DHCP en la interfaz que se este configurando, en este caso es la interfaz Biblioteca y Profesores.
- Denegar clientes desconocidos (Deny unknown clients): Si esta opción está marcada, sólo los clientes que se definen enseguida recibirán arrendamiento DHCP de este servidor.
- Subred (Subnet): Es el nombre de la subred que se esta configurando.
- Mascara de subred (Subnet mask): Es la mascara de subred de la interfaz Biblioteca y Profesores.
- Rango disponible (Available range): Es el rango disponible de las direcciones IP en la interfaz Biblioteca y Profesores.
- Rango (Range): Es el rango disponible en el que se esta configurando el DHCP.

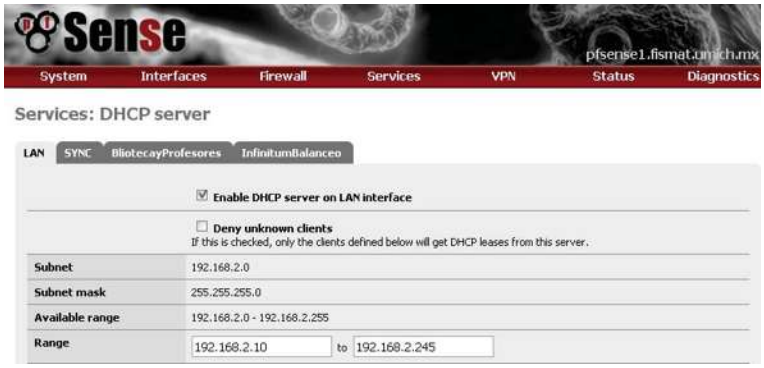

Figura 8.7: Pantalla Services, DHCP server de la interfaz LAN

En la siguiente figura 8.8 se presenta una captura de *Mac Address*, en la segunda columna se muestran las direcciones IP, en la tecera columna un *Hostname* y por último una descripción que se puede añadir. Estos datos se capturan automáticamente.

00:c0:ee:2a:d1:17	192.168.2.20		Impresora Laser Kyocera 1820
00:1e:4f:cd:c3:4e	192.168.2.35	wedgar	Workstation Edgar
00:22:64:a0:9f:5a	192.168.2.51	work	
00:1d:7e:e7:3a:ea	192.168.2.61	wfmb2	Linksys Wifi N Profesores
00:04:75:c9:77:96	192.168.2.101		
00:0f:fe:5d:15:12	192.168.2.102	lab1-102	
00:0f:fe:5a:f4:88	192.168.2.103	lab1-103	
00:0f:fe:5a:f7:f6	192.168.2.104	lab1-104	
00:0f:fe:5d:15:81	192.168.2.105	lab1-105	
00:0f:fe:5a:f7:50	192.168.2.106	lab1-106	
00:0f:fe:5d:14:d9	192.168.2.107	lab1-107	
00:0f:fe:5a:f6:3a	192.168.2.108	lab-108	
00:0f:fe:5a:f2:cc	192.168.2.109	lab1-109	
00:0f:fe:5a:f6:36	192.168.2.110	lab1-110	
00:0f:fe:5a:f1:ae	192.168.2.111	lab1-111	
00:0f:fe:5d:14:eb	192.168.2.112	lab1-112	
00:0f:fe:5d:06:3f	192.168.2.113		
00:0f:fe:5d:15:a2	192.168.2.114		
00:0f:fe:5d:0f:ba	192.168.2.115		
00:0f:fe:5a:f6:3e	192.168.2.116		
00:0f:fe:5c:73:ac	192.168.2.117		
00:0f:fe:5a:f7:e6	192.168.2.118		
00:0f:fe:5d:15:4c	192.168.2.119		lab-119
00:0f:fe:5a:f5:f2	192.168.2.120	lab1-120	
00:0f:fe:5a:f5:68	192.168.2.121	lab1-121	
00:0f:fe:5a:ee:c0	192.168.2.122	lab1-122	
00:0f:fe:74:e3:fb	192.168.2.123	lab1-123	
00:0f:fe:5a:f7:d8	192.168.2.124	lab1-124	
00:1c:10:ca:2f:9c	192.168.2.201	LynsysPap2	LinsysPap de la direccion

Figura 8.8: Captura de datos

8.4. Configuración de CARP

Primero se debe crear una nueva red para utilizarla como sincronización. Para acceder al CARP debe ir al menú *Status* y seleccionar CARP *failover*, y en la pantalla deberá habilitar CARP en todos los equipos que se usará este CARP, la configuración del CARP con pfSense que se convertirá en maestro. Y para sincronizar el estado del firewall se tiene que permitir el tráfico entre los sistemas en la interfase SYNC. Así que seleccione Firewall: Rules y la interfase SYNC y añade una regla presionando el botón añadir donde se deja pasar todo el tráfico, y guarde la regla, para configurar activo los cambios haga click en aplicar.

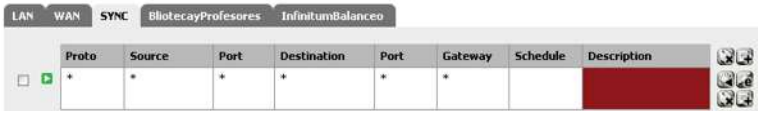

Figura 8.9: Regla de la interfaz SYNC

PfSense esclavo debe aceptar el tráfico del pfSense maestro, así que tiene que crear la misma regla. Ahora se debe ir al *Firewall: Rules*, seleccioné la pestaña de la interfaz de sincronización y pulse el botón añadir. Es exactamente la misma regla: Interfaz: SYNC, protocolo: cualquiera, puede añadir una descripción y guarde de nuevo, después aplique los cambios. Después en el maestro debe ir al *Firewall: Virtual IP* para configurar el *CARP Settings*, debe activar *Synchronize Enabled*, seleccionar la interfaz SYNC, se activan las casillas de selección que correspondan a la configuración (Sincronizar, Aliases, reglas, etc.) y en *Synchronize to IP* introduzca la dirección IP del esclavo el cual será sincronizado y la contraseña de éste mismo y guarde la

configuración (veáse la figura 8.10).
Los campos de configuración de sincronización son los siguientes:

- Sincronizar Activado (Synchronize Enabled): En este campo PFSync transfere el estado de inserción, actualización, supresión y mensajes entre los servidores de seguridad. Cada servidor de seguridad envía estos mensajes a través de multicast en una determinada interfaz, usando el protocolo PFSYNC (IP 240).
- Sincronizar la interfaz (Synchronize Interface): Se Sincroniza el estado si está activada, se utilizará esta interfaz para la comunicación. Se recomiendan las siguientes notas: Se recomienda un ajuste distinto de la interfaz LAN! Una interfaz de obras dedicado los mejores, usted debe definir una IP en cada una de las máquinas que participan en este grupo de conmutación por error y usted debe tener una dirección IP asignada a la interfaz en cualquier sincronización de nodos participantes.
- PfSync de sincronización entre iguales la propiedad intelectual (pfSync sync peer IP): Se ajuste esta opción para sincronizar la fuerza pfSync sus cuadros estables a esta dirección IP. El valor por defecto es dirigido multicast.
- Sincronizar reglas (Synchronize rules). Cuando se activa esta opción, el sistema automáticamente hace la sincronización de las reglas del firewall a los demás CARP.
- Sincronizar las listas de Firewall (Synchronize Firewall Schedules): Cuando se activa esta opción, el sistema automáticamente hace la sincronización del servidor de seguridad en los horarios de las demás CARP.
- Sincronizar alias (Synchronize aliases): Cuando se activa esta opción, el sistema automáticamente va sincronizar los alias a los demás CARP.
- Sincronizar NAT (Synchronize NAT): Cuando se activa esta opción, el sistema automáticamente hace la sincronización NAT reglas a los demás CARP.
- Sincronizar IPsec (Synchronize IPsec): Al ser activada esta opción, el sistema automáticamente sincroniza la configuración de IPsec a los demás CARP.
- Sincronizar Wake on Lan (Synchronize Wake on Lan): Cuando se activa esta opción, el sistema automáticamente hace la sincronización WOL ajustes al otro CARP.
- Sincronizar rutas estáticas (Synchronize Static Routes): Cuando esta opción está activada, este sistema de sincronización automática la configuración de la ruta al otro CARP.
- Sincronizar balanceo de carga (Synchronize Load Balancer): Cuando se activa esta opción, el sistema automáticamente sincroniza el balanceador de carga más ajustes al otro CARP.
- Sincronizar direcciones IP virtuales (Synchronize Virtual IPs): Cuando se activa esta opción, el sistema automáticamente hace la sincronización CARP virtual IP a los demás CARP.
- Sincronizar tráfico shaper (Synchronize traffic shaper): Cuando se activa esta opción, el sistema automáticamente va a sincronizar la configuración de tráfico shaper a los demás CARP.
- Sincronizar DNS reenviador (Synchronize DNS Forwarder): Cuando se activa esta opción, el sistema automáticamente va a sincronizar la configuración de DNS reenviador a los demás CARP.

- Sincronizar IP (Synchronize to IP): Introduzca la dirección IP del servidor de seguridad que se va a sincronizar.
- Sistema remoto Contraseña (Remote System Password): Introduzca la contraseña webGUI del sistema que se está sincronizando.

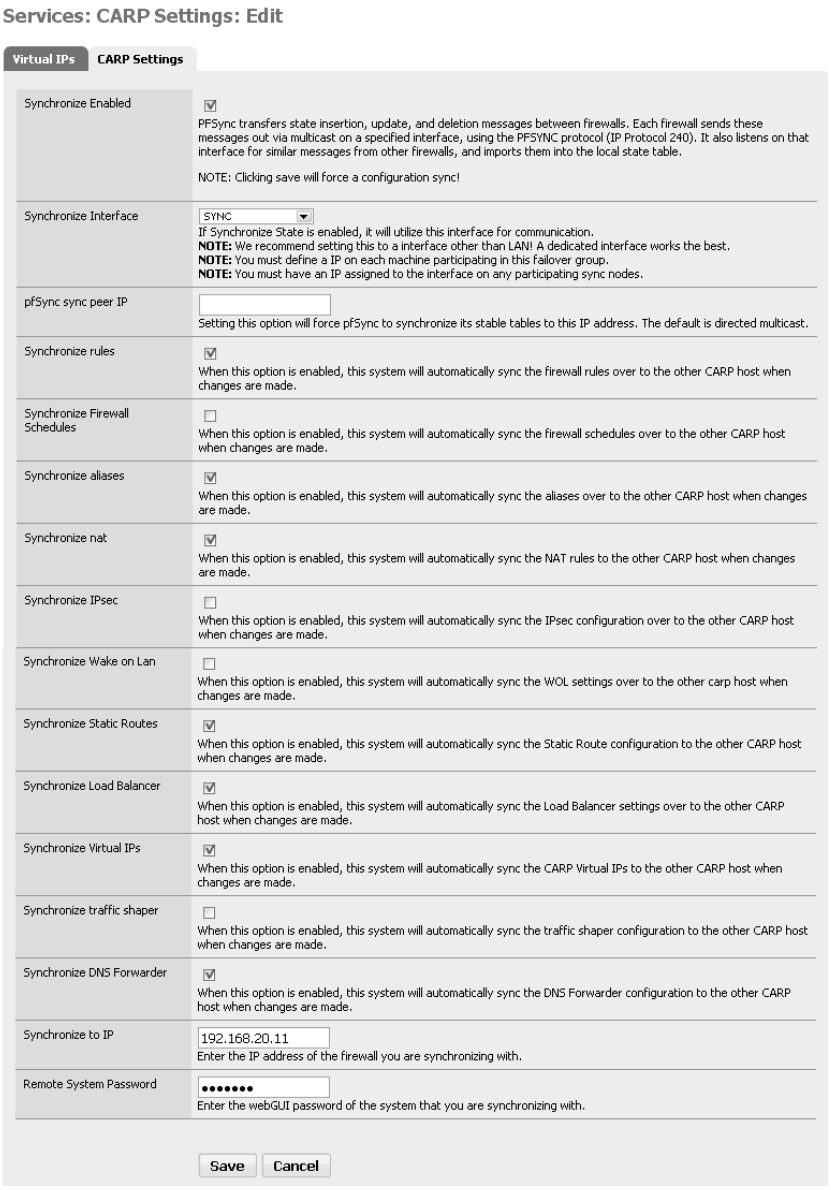

Figura 8.10: Pantalla de configuración de CARP maestro

Ahora en el CARP (pfSense esclavo) deberá activar *Synchronize Enabled*, seleccionar la interfaz SYNC y guarde (veáse la figura 8.11).

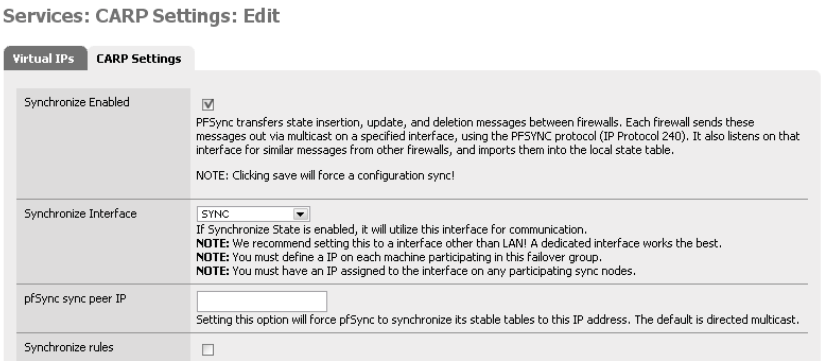

Figura 8.11: Pantalla de configuración de CARP esclavo

8.4.1. IP Virtual CARP

Enseguida se crearán las IP virtuales, se selecciona *Firewall: IP Virtual*, se requiere de al menos dos IP Virtuales (LAN y WAN), como se quiere que sean compartidas entre los sistemas, se elige de tipo CARP, y una dirección de su red WAN en el campo *IP Address* con su máscara de red/24 y se usará la IP 148.216.6.36/24. Para la comunicación entre el maestro y el esclavo se selecciona que va a ser compartida con los esclavos. El ajuste de *Advertising Frecuency* si el valor es "0" determinará que el sistema se convertirá en maestro y si es mayor, pasará a ser esclavo. Se selecciona un grupo VHID, éste deberá ser el mismo en aquellos servidores que actuarán como esclavos, además se selecciona una contraseña que será usada en todos los equipos que pertenecen al dicho grupo. Esta configuración se replica en el esclavo con un valor 1, puede poner una descripción para esta interfaz y guarde (veáse la figura 8.12).

Figura 8.12: Pantalla de configuración de IP Virtual WAN

Se repite el proceso ahora para los clientes de LAN, se agrega una IP virtual para los clientes LAN que será usada como puerta de enlace. Nuevamente se elige de tipo CARP, la interfase será LAN, se elige una contraseña y un número diferente al de la WAN. Se deberá mantener el cero para ser el maestro. Utilizando ésta como puerta de enlace, entonces pulse el botón añadir. Se elige de tipo CARP, en esta IP se activa la interfaz LAN, después tiene la libertad de poner la IP de su subred LAN, para que los clientes puedan compartir la

Máscara de red correcta. Este grupo también necesita una contraseña, se utilizará “lan”. Como es el segundo CARP le pondrá el 2 en VHID (este número es único para cada IP Virtual agregada), en la frecuencia se puede mantener el 0. Finalmente puede introducir una descripción para este grupo, guardar y aplicar cambios (veáse la figura 8.13).

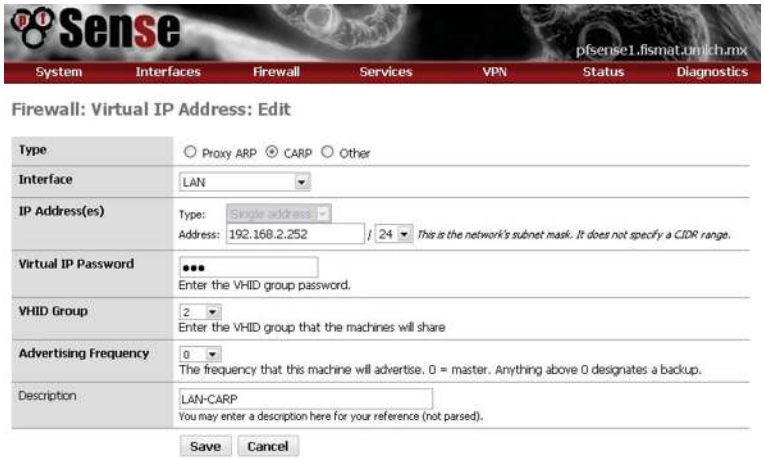

Figura 8.13: Pantalla de configuración de IP Virtual LAN

Ha creado las IP’s virtuales que necesita, sólo hay que aplicar la nueva configuración. Le quedará de la siguiente manera.

Figura 8.14: Direcciones IP virtuales creadas

Ahora puede comprobar el estado de CARP el en *failover*. En CARP tiene dos interfases con IP virtuales y de estado maestro. Esto lo puede ver selecionando en el menú *Status: CARP (failover)* como se muestra en la figura 8.15.

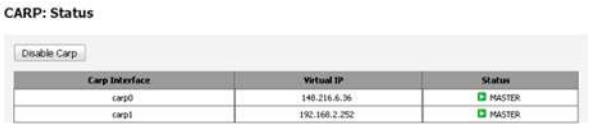

Figura 8.15: Direcciones IP en estado maestro

De la misma manera debe acceder a la opción *Status: CARP* para verificar que debe estar el sistema en estado esclavo como se muestra en la figura 8.16.

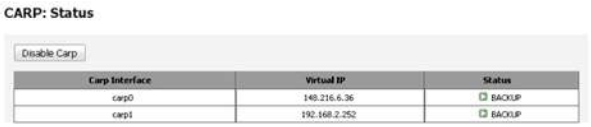

Figura 8.16: Direcciones IP en estado esclavo

Ahora debe regresar al maestro a hacer algunos ajustes finales, se quiere que la IP virtual sea utilizada por el NAT mapie, para realizar una conmutación por error de estado, en caso de que uno de el maestro falle, para esto debe seleccionar *Firewall: NAT: Outbound* (salida) y habilitar *Advanced Outbound NAT*.

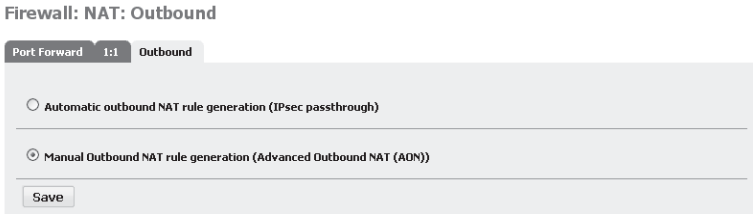

Figura 8.17: Activación de la forma manual en el NAT salida

Como puede ver, pfSense ha creado la regla por defecto, solo se tiene que modificar para que ésta funcione con las IP virtuales, puede dejar esto como esta, lo único que tiene que cambiar es el uso de la WAN IP-CARP en lugar de la verdadera interfaz IP, puede si desea modificar la descripción para reflejar los cambios, guarde y aplique. La figura 8.18 muestra la regla de NAT salida de la interfaz WAN de la IP virtual.

Figura 8.18: Regla WAN IP-CARP

En este ajuste también se sincroniza el esclavo. Para que el servidor DHCP utilize la Ip-virtual, seleccione *Services: DHCP server*, añada la puerta de enlace y DNS virtual. También puede sincronizar el servidor DHCP a la máquina esclava para proteger servicio y contra fallas.

Se cambiará el DNS y la puerta de enlace por la IP virtual LAN, y en la opción *Failover Peer IP* se agregará la IP real /LAN del equipo maestro.

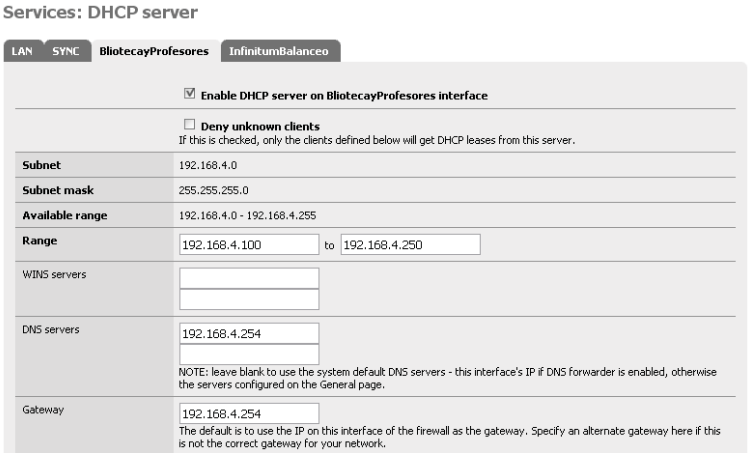

Figura 8.19: Configuración de DHCP y DNS

Capítulo 9

Resultados y Conclusiones

- **Se incrementó la seguridad y confiabilidad del sistema.**

  La infraestructura implementada en este proyecto, tiene una configuración de alta disponibilidad redundante, es decir, cuenta con dos sistemas similares (maestro y esclavo) que permiten evitar la interrupción del servicio. En caso de falla o error en el maestro, el esclavo asume todas las funciones de manera automática sin intervención. Se ha diseñado de manera que tenga una autonomía máxima y un riesgo mínimo para transmisión de datos. Tener cubierta esta necesidad es impresindible ya que aumenta la confiabilidad del sistema y beneficia de manera directa a los usuarios.

- **Incremento del ancho de banda.**
  El tráfico de entrada y salida de la interfaz WAN, inicialmente era proporcionado por un ISP con una velocidad de entrada de aproximadamente 400Kbps (veáse la figura 9.1) y de salida es en el intervalo de 60 a 128kpbs, utilizando el balanceo de carga se obtuvieron 1.71Mbps en entrada (veáse la figura 9.2), cabe mencionar que el valor de salida se obtuvo partir de los usuarios que solo enviaban datos y su descarga era casi nula. Para realizar estas pruebas utilizamos el firewall para forzar a utlizar agrupamiento de conexiones (pool) del balanceador de carga en lugar de la conexión usada normalmente (un ISP).

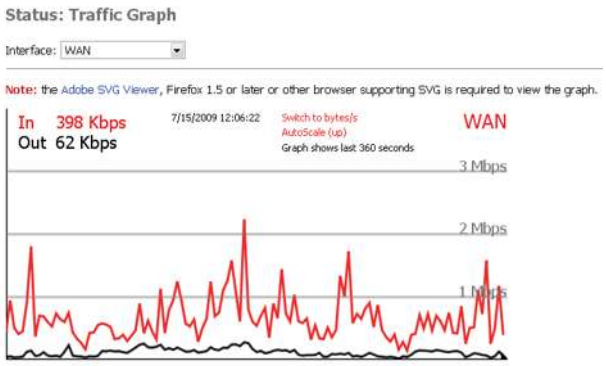

Figura 9.1: Tráfico de la interfaz WAN antes de utilizar el balanceo de carga

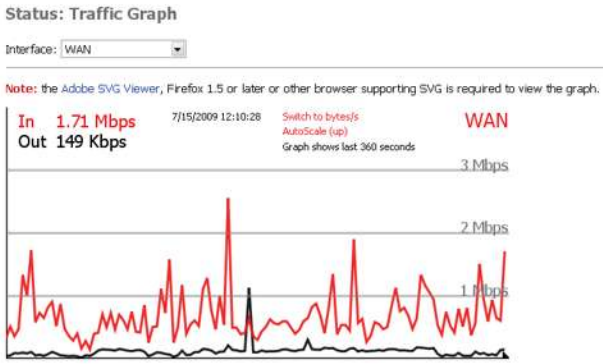

Figura 9.2: Tráfico de la interfaz WAN utilizando balanceo de carga

- **Transparencia en el funcionamiento del firewall.**

  Este proyecto presenta una solución basada en software libre de código abierto, donde se incluye la documentación de cada paso de la instalación, configuración y administración del firewall. El beneficio de contar con documentación ofrece la posibilidad de replicar este sistema en otros departamentos permitiendo que cualquier persona pueda realizarla con éxito. Debido a la flexibilidad es posible instalar este sistema en computadoras de propósito específico, tales como ruteadores inalámbricos para aumentar la funcionalidad de los mismos.

- Soporte del crecimiento de la infraestructura gracias a la nueva arquitectura de red, la cual permite un crecimiento ordenado con facilidad de administración.

9.1. Trabajo futuro

En el caso de estudio el servidor principal de datos se encuentra fuera del rango de acción del firewall, una posibilidad sería colocar el servidor principal detras del firewall para así tener control de filtrar el tráfico de entrada y salida, esto le proporcionaría alta disponibilidad a los servicios ofrecidos por este servidor.

PfSense ofrece la posibilidad de crear servidores virtuales, los cuales crean pools de conexiones, lo que incrementa la capacidad de servicio de un equipo o equipos permitiendo atender una gran cantidad de peticiones, en este proyecto no hubo la manera de utilizar esta posibilidad, dado que no hubo la manera de probarlo. La implementación, configuración y uso de un proxy para controlar el acceso a algunos contenidos quedo fuera de la investigacion de esre proyecto, dada la gran cantidad de archivos de configuración y complejidad. El beneficio del proxy impactaria de manera directa el consumo en el ancho de banda. La autenticación de clientes inalámbricos se realiza usando radius, sin embargo combinando este con LDAP se puede disponer de un control más fino y preciso de los usuarios y sus perfiles. PfSense puede ser instalado en una plataforma embebida, es decir, una computadora de capacidades mínimas, con el fin de tener un equipo profesional en un dispositivo accesible y además economiza energía.

Utilizar una plataforma embedida diseñada para manejar a pfsense como un sistema integrada.

Este proyecto ha mostrado las ventajas de contar con documentación confiable tanto de hardware y software utilizado en esta organización en particular, por lo que se está elaborando documentación del resto de

los servicios de red ofrecidos por el departamento de cómputo de la facultad.

Capítulo 10

Apéndice

10.1. Etiquetado IEEE 802.1Q

Los términos utilizados en el etiquetado 802.1Q son los siguientes:

- Identificador de VLAN (VLAN identifier) (VID): la porción de 12 bits de la etiqueta VLAN en el marco del encabezado es usado para especificar una VLAN explicita, cuando otros tipos de VLAN están habilitados, este valor puede ser usado por un switch para identificar a qué puerto va dirigido.
- Port VLAN identifier PVID: Es un mecanismo de clasificación que asocia un puerto de un switch con una VLAN específica. Por ejemplo, un puerto con un PVID de tres asigna todos los marcos no etiquetados recibidos en este puerto a la VLAN 3.
- Marco etiquetado. El campo de 32 bits llamado VLAN tag en el marco encabezado identifica un marco como perteneciente a una VLAN especifica, los marcos no etiquetados son marcados (tagged) con esta clasificación, cuando ellos salen de un switch a través de un puerto por una VLAN específica.
- Marco no etiquetado. Este es un marco que no posee una VLAN.
- Pertenencia de puertos a una VLAN. Es un conjunto de puertos que forman el domino de broadcast para una VLAN especifica.
- Permanencia no etiquetada. Un puerto de un switch que ha sido configurado como perteneciente no etiquetada de una VLAN especifica. Cuando un marco no etiquetado sale a través del switch y a través de un puerto miembro no etiquetado, el encabezado del marco permanece sin cambios. Cuando un marco etiquetado sale a través del switch y de un miembro no etiquetado la etiqueta es eliminada y el marco etiquetado es cambiado a un marco no etiquetado.
- Miembro etiquetado: un puerto que ha sido configurado como miembro de una VLAN específica. Cuando un marco no etiquetado sale del switch a través de un puerto miembro etiquetado, el encabezado del marco es modificado para incluir los 32 bits de la etiqueta de asociación con el PVID. Cuando un marco etiquetado sale a través de un puerto miembro etiquetado, el encabezado del marco permanece sin cambios.

Bibliografía

[1] CARP. Common address redundancy protocol. http://www.e-compugraf.com/sciret/index.php?

[2] Clustering. Clustering using pfsense. http://pfsense.nsa.co.il/tutorials/carp/carp-cluster-new.htm.

[3] Douglas E. Comer. *Redes de Computadoras, Internet e Interredes.* Editorial Pearson Education, 1995.

[4] Alta disponibilidad. Alta disponibilidad. http://www.gestiopolis.com/delta/term/TER170.html.

[5] FreeBSD. Balanceo de carga. http://en.wikipedia.org/wiki/Load_balancing.

[6] FreeBSD. Instalación de freebsd. http://www.stn.com/web/stn52.html.

[7] FreeBSD. Página web del proyecto freebsd. http://www.freebsd.org/releases/7.1R/hardware.html.

[8] FreeBSD. Página web del proyecto freebsd. http://www.countersiege.com/doc/pfsync-carp/.

[9] Ipcop. Página web del proyecto ipcop. http://www.ipcop.org.

[10] Robert W. Lucke. *Building Clustered Linux Systems.* Editorial Pearson Educación, 1995.

[11] Monowall. Página web del proyecto monowall. http://www.monowall.org.

[12] Pfsense. Página web del proyecto pfsense. http://www.pfsense.org.

[13] Pfsync. Redundant firewalls with openbsd and pfsync. http://www.kernel-panic.it/openbsd/carp.

[14] Tanembaum Ronald. *Redes de computadoras*. Prentice Hall, 2000.

[15] Smothwall. Página web del proyecto smoothwall. http://www.smoothwall.org.

Glosario

1

10GBASE-T3 Es el estandar Ethernet mas reciente y más rápido, contiene siete tipos de medios para LAN, MAN y WAN., pág. 5.

A

ACK Es un mensaje que se envia para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es ”ha llegado y además ha llegado correctamente”.

ADSL Asymetric Digital Suscripter Line. ADSL es un tipo de l’nea DSL. Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

B

BIOS El Sistema Básico de Entrada/Salida (Basic Input-Output System) es un conjunto de instrucciones que localiza y carga el sistema operativo en la RAM. Este software está instalado en la placa base.

Boot Blocks Bloques de Arranque. Estan localizados al inicio de la partición, para permitir al SO arrancar el sistema, comúnmente son conocidos como MBR ó Master Boot Record.

BSD Son las iniciales de Berkeley Software Distribution (en español, Distribución de Software Berkeley) y se utiliza para identificar un sistema operativo derivado del sistema Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

C

CISCO Es una empresa multinacional, principalmente dedicada a la fabricación, venta, mantenimiento y consultoria de equipos de telecomunicaciones., pág. 96.

D

Deny of Service Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legitimos. Normalmente provoca la perdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Diffie-Hellman Algoritmo de encriptación que permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima.

DMA (Direct Access Memory) Permite a cierto tipo de componentes de ordenador acceder a la memoria del sistema para leer o escribir independientemente de la CPU principal.

F

FreeBSD (www.freebsd.org) Es un sistema operativo, derivado de BSD Unix, con licencia GNU. Es similar a las distribuciones Linux actuales, pero directamente de BSD.

H

HSRP Es un protocolo de propiedad de CISCO CISCO que permite el despliegue de ruteadores redundantes tolerantes a una falla en una red.

HTTP Protocolo de hipertexto, es el protocolo usado en cada transacción de la web.

I

ICMP Subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no esta disponible o que un ruteador o host no puede ser localizado., pág. 36.

IEEE Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización entre otras cosas.

IETF (Internet Engineering Task Force), o (Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivo contribuir a la ingeniería de Internet, actuando en diversas areas tales como transporte, seguridad, etc.

Iptables Formato de reglas definidas a nivel de kernel para permitir o bloquear paquetes IP. Estas reglas son utilizadas por las distribuciones Linux basadas en RedHat o en Fedora comunmente en su mayoria.

iSCSI Es un estandar oficial ratificado el 11 de Febrero de 2003 por la Internet Engineering Task Force que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3., pág. 5.

L

Lempel–Ziv–Oberhumer Es un algoritmo de compresión sin perdida de datos que se centra en la velocidad de descompresión.

M

Malware Es un software que tiene como objetivo infiltrarse en el sistema y da–ar la computadora sin el conocimiento de su due–o, con finalidades muy diversas, ya que en esta categoria encontramos desde un troyano a un spyware.

N

NAT Network Address Translation, es un mecanismo que permite realizar un cambio de ip utilizando encapsulamiento para poder comunicar dos redes con rangos de ips distintas.

NetBSD Es un sistema operativo de la familia Unix (en si no se le puede llamar ün Unix", ya que esta es una marca comercial de AT& T, pero se denomina como "sistema de tipo UNIX.º "derivado de UNIX"), open sourse y libre, y es disponible para mas de 56 plataformas hardware.

O

OpenVPN Es un proyecto Open Source y esta licenciado bajo la GPL. Su principal objetivo es la creación de Redes Privadas Virtuales en sistemas basados en Linux, en la actualidad se ofrecen para la mayoria de los sistemas operativos.

OPT Se llaman así las interfases opcionales cuando se cuenta con mas de 2 interfases de red, y se les puede cambiar el nombre para una mejor configuración.

P

P2P Se refiere a una red que no tiene clientes ni servidores fijos, sino que una serie de nodos que de comporta simultaneamente como clientes y servidores respecto a los demas nodos.

Portal-Captivo Es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. Permite autenticar los usuarios para evitar un uso excesivo de recursos.

R

RDP Es un protocolo desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la informacion procesada que recibe del servidor) y un servidor Windows (recibiendo la información ingresada por el usuario en el terminal mediante el raton el teclado).

Red de Area Amplia (Wide Area Network o WAN) Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

Red de Área Local (Local Area Network o LAN) Es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada fisicamente a un edificio o a un entorno de 200 metros o con repetidores podriamos llegar a la distancia de un campo de 1 kilometro.

Round-Robin Esquema de Selecci—n de equipos en una lista, en donde se seleccionan uno a uno hasta que nuevamente inicia.

S

Squid Es un popular programa de software libre que implementa un servidor proxy y un demonio para cache de páginas web, publicado bajo licencia GPL.

SSH Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

T

TCP Network Address Translation, es un mecanismo que permite realizar un cambio de ip utilizando encapsulamiento para poder comunicar dos redes con rangos de ips distintas.

U

UDP Network Address Translation, es un mecanismo que permite realizar un cambio de ip utilizando encapsulamiento para poder comunicar dos redes con rangos de ips distintas.

Unix Es un sistema operativo portable, multitarea y multiusuario.

V

VoIP Es un termino en general para una familia de tecnologías de transmisión para la entrega de comunicaciones de voz sobre redes., pág. 44.

VPN VPN red privada virtual (Virtual Private Network) Es una tecnología de red que permite extender la red local sobre una red pública como Internet, en donde la comunicación va cifrada.

VRRP Es un protocolo de redundancia diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. Sin embargo es de licencia propietaria implementado por CISCO CISCO.