Universidad Nacional Autónoma de Nicaragua

UNAN – León

Facultad de Ciencias y Tecnología

Departamento de Computación

"Propuesta de mecanismos de Seguridad Inalámbrica utilizando tecnología de Software Libre para apoyo en la administración de la Red en la Universidad BICU, 2015."

Tesis para optar al título de:

Maestría en Tecnologías de la Informática Empresarial

Presentado por:

Ing. Skinner Abelardo Guills.

Tutor:

Ing. Raúl Hermogenes Ruiz Cabrera, MSc.

León, Septiembre del 2015

Agradecimientos

Agradezco a mi Dios por darme la vida y la oportunidad de enriquecerme de sus conocimientos y sabiduría.

Por permitir levantarme y concluir con esta etapa y sueño de mi vida.
A mi madre que ha sido como padre durante esta etapa de mi vida, me ha enseñado a no darme por vencido

Agradezco a los docentes y amigos que tuvieron la paciencia de poder compartir sus conocimientos y poder terminar este proyecto de investigación.

Especialmente al MSc. Javier de Pedro Carracedo, MSc. Raúl Hermogenes Ruiz Cabrera y MSc. Jackeline Kerr. Agradezco con todo mi corazón por sus apoyos a lo largo de todo el proceso.

.

Resumen Ejecutivo

Con los avances de la tecnología, los equipos y las redes informáticas toman el centro de la escena. Esta a su vez son los lugares de trabajo, en la escuela, o en casa. El Internet ha hecho la seguridad de la red una prioridad, muchas personas todavía no saben lo suficiente. La seguridad de la red es algo más que un antivirus o actualizar los programas. Es tener en constante vigilancia su red para evitar intrusos, malware y otras amenazas comunes. [1]

Las herramientas de seguridad de software libre basado en sistemas Linux han evolucionado al uso de grandes, medianas y pequeñas empresas en su infraestructura de Red. Estas acciones ayudan a mejorar la seguridad y el rendimiento de los servicios en Monitoreo de la Administración de la Red y evitar posible ataques.

Con este proyecto se pretende proponer mecanismos de seguridad Inalámbrica para la red BICU utilizando tecnología de software libre, con el propósito de poder establecer alternativas de solución a sus necesidades como institución a servicio internet.

La elaboración de este proyecto tecnológico se utilizó PFSense Firewall, un sistema de seguridad completo de propiedad de licencia libre con grandes tendencias de uso en su funcionalidad y fácil manejo en la administración de todos sus servicios multifuncionales.

Contenido

Índice de Ilustraciones

Capítulo 1: Introducción

1.1 Antecedentes

En los últimos años se ha verificado la proliferación de redes inalámbricas. Esto se debe a varias razones, como el estilo de vida actual, la necesidad de mantener conectividad a redes locales o Internet de forma constante, el soporte a la movilidad y la mayor flexibilidad

En el año 1971 cuando un grupo de investigadores bajo la dirección de Norman Abramson, en la Universidad de Hawaii, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Ésta es la primera red de área local inalámbrica (WLAN), estaba formada por 7 computadoras situadas en distintas islas que se podían comunicar con un ordenador central al cual pedían que realizara cálculos. Uno de los primeros problemas que tuvieron y que tiene todo nuevo tipo de red inventada fue el control de acceso al medio (MAC), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí. En un principio se solucionó haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras mientras estuviera libre, de tal forma que cuando una de las otras estaciones se disponía a transmitir, antes "escuchaba" y se cercioraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, esto se conoce como CSMA (Carrier Sense Multiple Access). [2]

La irrupción de la nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas de futuros para el desarrollo de sistemas de comunicación, así como nuevos riesgos. La flexibilidad y la movilidad que nos proporciona las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya disparado en el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

En los últimos 10 años se ha visto un incremento apreciable en la demanda de instalación de sistemas basados en Linux en Latinoamérica. En el caso específico de Nicaragua, una gran cantidad de empresas ya tienen o necesitan tener Linux en sus servidores debido a su renombrada estabilidad, aunque muchas también se interesan porque su licencia de uso no tiene costo usualmente. [3]

Dada la importancia del tema de estudio existen Universidades nacionales e instituciones privadas de Nicaragua disponen de servidores de seguridad de software libre para garantizar un mejor servicio al acceso de conexiones inalámbricas que están dirigidas a los usuarios pertinentes.

BICU una Universidad Autónoma, Comunitaria y de Derecho Público, patrimonio de los pueblos indígenas, afrodescendientes y mestizos de las Regiones Autónomas de la Costa Caribe Nicaragüense, apartidaría, multiétnica, intercultural, laica y sin fines de lucro. Fue declarada Universidad Oficial de la Región Autónoma Atlántico Sur en la VIII Sesión Ordinaria de la primera legislatura el 23 de febrero de 1994 del Consejo Regional Autónomo Atlántico Sur. Es el lugar de estudio para este proyecto con el fin de desarrollar mecanismos de seguridad inalámbrica para uso pertinente a sus necesidades como institución.

Existen trabajos realizados basados a los temas de seguridad Informática en la UNAN-LEON, Msc. Valeria Medina realizo en el año 2008 el trabajo sobre el plan docente de seguridad informática para el plan académico 2007 dicho plan está dirigido a la carrea de Ingeriría en Telemática

1.2. Planteamiento del Problema

BICU una universidad autónoma funcionando desde 6 de junio de 1991 en la ciudad de Bluefields perteneciente del gremio de universidades de la CNU consta con 8 sedes, la principal está en la ciudad de Bluefields RAAS. En el año 2014 BICU cuenta con una matrícula de más de 7,000 (Siete mil) estudiantes de pregrado y grado, en las más de 40 carreras que brinda la universidad en sus ocho sedes universitarias. Sus capacidades tecnológicas en Hardware consta de 1,200 computadoras estas son: 1) Oficinas, Laboratorios de cómputo, Auditores, Bibliotecas, Cyber, Facultades, escuelas y centro de dato. En software la institución cuenta con el servicio aplicación académica, sistema contable, sistema plataforma virtual, sistema de vigilancia, sistema de ponchado, sistema de inventario en Bodega, Sitio Web y Sistema Bibliotecario.

Los problemas que actualmente enfrenta la red de la universidad BICU por no poseer mecanismos de seguridad se enfoca en 4 etapas:

1) Problemas de Saturación en la Red.

Esta problemática se basa en la lentitud de los servicios de conectividad a la red tanto externa e interna que posee BICU. Debido a esto, las entidades más afectadas son los trabajadores administrativos, docentes y estudiantes al uso de conectividad del internet que brinda dicha institución,

2) Acceso a los servicios de aplicaciones del centro de Datos.

El riesgo de vulnerabilidad a sus servidores de aplicaciones es un problema porque han registrado intentos de ataques a la página web, plataforma web y sistema académico. Estos ataques son más originados por medio de conexión inalámbrica, debido a que la navegación posee una libertad sin mecanismos de seguridad.

3) Segmentación.

La segmentación, un problema que también enfrenta la institución, debido que no existe una asignación que divida los servicios de conectividad a internet. Este problema ya mencionado abarca de forma general y crítica a los recursos de balanceo de carga y asignación de ancho de banda. Las entidades que están conectados al servicio alámbrica e inalámbrica son trabajadores, docentes y estudiantes quienes consumen los servicios de conectividad internet.

4) Autentificación de usuario.

La Autentificación de usuario, debido a que no existe un mecanismo de identificación y registros que lleve el control de los usuarios que se conectan a la red inalámbrica. Por ende es un desafío que la institución quiere lograr solucionar.

Propuesta

Con el proyecto de propuesta de mecanismos de seguridad inalámbrica utilizando tecnología de Software Libre para apoyo en la administración de la Red en la Universidad BICU, 2015, será una solución viable para cada una de las problemáticas mencionadas con el fin de optimizar sus recursos que poseen. Dicha propuesta en desarrollo de estudio abarca de métodos de solución que garanticen una mejor solución en sus mecanismos de seguridad en la red de la institución proponiendo técnicas de tecnología que cumpla con los requisitos y necesidades de la empresa.

1.3. Justificación

Los sistemas de redes y telecomunicaciones actualmente están sujetos a una innovación tecnológica altamente cambiante, trayendo consigo, que los sistemas basados en las comunicaciones inalámbricas no sean la excepción, por lo que evolucionan rápidamente.

Las redes fueron creadas por la necesidad de proveer acceso a las redes por medio de dispositivos de computo portátiles, lo cual evidentemente atrajo problemas hacia el medio de transmisión, debido a los intrusos que pueden entrar a la red libremente dando una posibilidad virtual de no ser detectados.

Las redes inalámbricas en los últimos años, han tenido un auge muy importante por lo que los mecanismos de seguridad que se desarrollaron en un inicio, rápidamente pasaron a ser superados por aquellos usuarios mal intencionados, los cuales buscan por ende penetrar a los sistemas en las vulnerabilidades de seguridad que estos presentan.

El presente proyecto a desarrollar sobre mecanismos de seguridad inalámbrica utilizando tecnología de Software Libre para apoyo en la administración de la Red, en la Universidad BICU, 2015, está enfocado a resolver alternativas de solución a la red inalámbrica de la institución.

Estos mecanismos seguridad están basados a varios procesos de solución la cual es balanceo de carga, estabilidad en la red, monitoreo en tiempo real, rastreo de los servicios de protocolo de red, registro identificación de usuarios, políticas de acceso páginas permitidas, portal cautivo, reportes estadísticos, escaneo de virus en la red y servicio firewall.

El proyecto tiene como beneficio directo a la institución universitaria BICU sobre cada uno de los problemas que actualmente posee. Los beneficios indirectos están dirigidos a las entidades estudiantiles y docente quienes son los que hacen parte del consumo diario del servicio de internet inalámbrica.

1.4 Objetivos

1.4.1 Objetivo General

- Implementar mecanismos de seguridad Inalámbrica utilizando tecnología de Software Libre para para apoyo en la administración de la Red, en la Universidad BICU 2015.

1.4.2 Objetivos Específicos

- Elaborar un documento de información de teoría acerca de los mecanismos de seguridad Inalámbrica y los métodos que se utiliza con Herramientas de Software Libre.

- Comparar los distintos tipos de cortafuegos de código abierto basados en las características de Hardware, considerando las posibilidades de implementación y selección.

- Desarrollar los mecanismos de seguridad inalámbrica ocupando técnicas de virtualización como medio más seguro y rentable en la presentación del proyecto.

Capítulo 2: Marco Teórico

2.1 Red Inalámbrica.

2.1.1 Introducción

Las redes inalámbricas se han convertido en una alternativa francamente interesante a las redes cableadas. Su bajo costo, facilidad de instalación y la libertad que ofrecen para poder conectarse en cualquier lugar, son factores por los que cada día las vemos más en una sala de conferencias, en un almacén, en el auto, desde casa, en el aeropuerto, en el hotel y en la cafetería, oficinas o Host-spots.

Las tecnologías de interconexión inalámbrica van desde redes de voz y datos globales, que permiten a los usuarios establecer conexiones inalámbricas a través de largas distancias, hasta las tecnologías de luz infrarroja y radiofrecuencia que están optimizadas para conexiones inalámbricas a distancias cortas. Entre los dispositivos comúnmente utilizados para la interconexión inalámbrica se encuentran los equipos portátiles, equipos de escritorio, asistentes digitales personales (PDA), teléfonos celulares, equipos con lápiz y localizadores. Las tecnologías inalámbricas tienen muchos usos prácticos. Por ejemplo, los usuarios de móviles pueden usar su teléfono celular para tener acceso al correo electrónico. Las personas que viajan con equipos portátiles pueden conectarse a Internet a través de estaciones base instaladas en aeropuertos, estaciones de ferrocarril y otros lugares públicos. En casa, los usuarios pueden conectar dispositivos a su equipo de escritorio para sincronizar datos y transferir archivos. [4]

2.1.2 ¿Qué es una Red Inalámbrica?

Una red inalámbrica es una red en la que dos o más terminales se pueden comunicar sin la necesidad de una conexión por cable. Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema. [5]

2.1.3 Categorías Red Inalámbrica.

Existen dos categorías de las redes inalámbricas:

a) Larga distancia: estas son utilizadas para distancias grandes como puede ser otra ciudad u otro país.
b) Corta distancia: son utilizadas para un mismo edificio o en varios edificios cercanos no muy retirados.

Ilustración 1 Categoría Red Inalámbrica

2.1.4 Tipos Redes Inalámbrica.

2.1.4.1 WPAN (Wireless Personal Área Network)

Incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Se usan varios tipos de tecnología para las WPAN.

2.1.4.2 Home RF (Home Radio Frequency)

Lanzada en 1998 por HomeRF Working Group (que incluye a los fabricantes Compaq, HP, Intel, Siemens, Motorola y Microsoft, entre otros) ofrece una velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros sin amplificador. A pesar de estar respaldado por Intel, el estándar HomeRF se abandonó en enero de 2003, en gran medida porque los fabricantes de procesadores empezaron a usar la tecnología Wi-Fi en placa (por medio de la tecnología Centrino, que incluía un microprocesador y un adaptador Wi-Fi en un solo componente).

La tecnología Zigbee (también conocida como IEEE 802.15.4) también se puede utilizar para conectar dispositivos en forma inalámbrica a un coste muy bajo y con bajo consumo de energía. Resulta particularmente adecuada porque se integra directamente en pequeños aparatos electrónicos (como, por ejemplo, electrodomésticos, sistemas estéreos y juguetes).

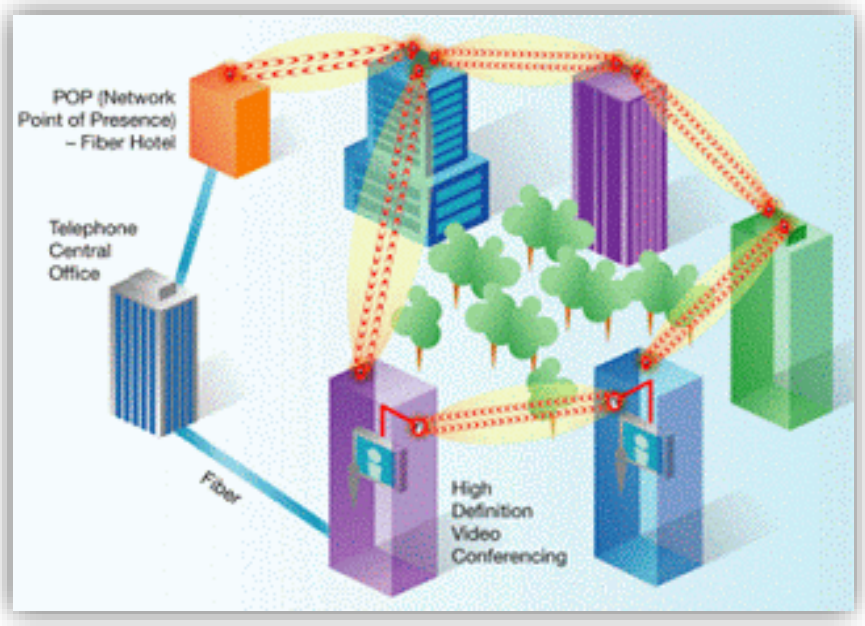


Ilustración 2 Home RF

2.1.4.3 WLAN (Wireless Local Área Network)

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías:

2.1.4.3.1 HiperLAN2 (High Performance Radio LAN 2.0)

Estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2, permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

2.1.4.3.2 2WMAN (Wireless Metripolitan Area Network).

Las redes inalámbricas de área metropolitana (WMAN) también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones. Las tecnologías WMAN permite a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, entre varios edificios de oficina de una ciudad o en un campus universitarios), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas. WMAN utiliza ondas de radios o luz infrarroja para transmitir los datos. La mejor red inalámbrica de área metropolitana es WiMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

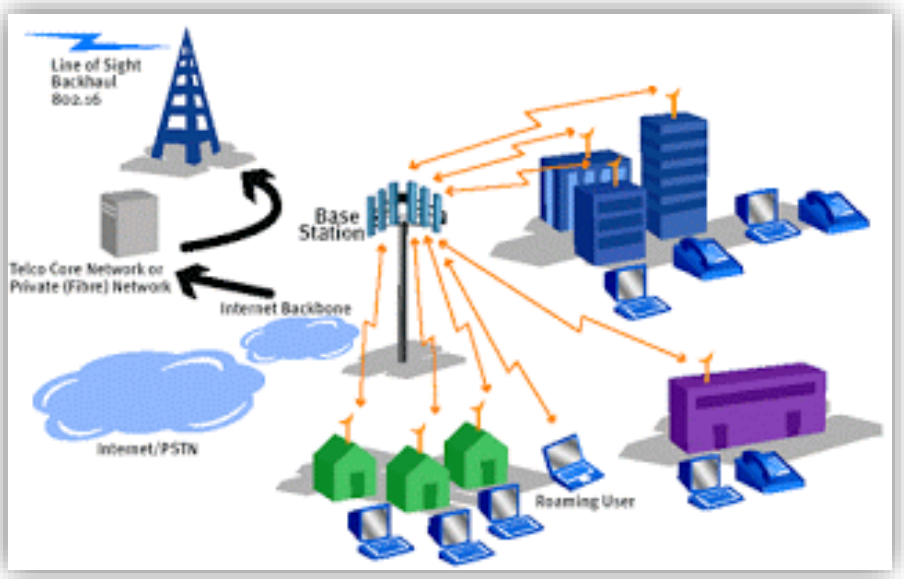


Ilustración 3 Wireless Metripolitan Área Network

2.1.4.3.3 WWAN (Wireless Wide Area Network)

Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélites que mantienen los proveedores de servicios inalámbricos. Las tecnologías principales son: GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunication System)

2.1.5 Ventajas y Desventajas de las Redes Inalámbrica.

2.1.5.1 Ventajas:

- Comodidad: Acceda a sus recursos de red desde cualquier ubicación dentro del área de cobertura de su red inalámbrica o desde cualquier punto WIFI.
- Movilidad: Ya no tiene que estar atado a su mesa, como ocurría con una conexión por cable. Usted y sus empleados pueden conectarse online, por ejemplo, desde una sala de conferencias.
- Instalación sencilla: No tiene que tirar cables, por tanto, la instalación puede ser rápida y económica.

2.1.5.2 Desventajas:

- Todavía no hay estudios certeros sobre la peligrosidad de las radiaciones utilizadas en las redes inalámbricas.
- Pueden llegar a ser más inseguras, ya que cualquiera cerca podría acceder a la red inalámbrica.

2.1.6 Importancia De Las Redes Inalámbricas En La Actualidad

El amplio uso de las redes inalámbricas ha ido creciendo vertiginosamente en la actualidad. Según datos estadísticos proporcionados por la compañía consultora InStat-MDR, los equipos hardware para redes inalámbricas de tipo 802.11 crecieron para el año 2006, sobrepasando los 40 millones de unidades, y su precio irá disminuyendo considerablemente en la medida de que se sigan utilizando como alternativa para implementación de redes. Las redes inalámbricas actualmente se encuentran instaladas en distintos lugares, incluso se prefiere en compañías grandes, como complemento a sus redes tipo Ethernet. Una de las más importantes razones del crecimiento de redes inalámbricas, es el mercado sorprendente de equipos inalámbricos como laptop, tarjetas inalámbricas para computadoras, celulares con conexión WIFI, entre muchos otros.

2.1.7 Seguridad de la Información.

Se llama seguridad de la Información a todas las medidas o precauciones que se adopta para evitar cualquier acción que comprometa la información. Sin importar la forma que tome la información o el medio de transmisión, siempre es necesaria la protección adecuada.

2.1.8 Seguridad de la Red

A medida que los sistemas de información crecen, la seguridad de los mismos debe hacerlo, así bien debido a la interconectividad que se genera entre estos y la generación de redes más amplias se tiene el siguiente concepto de seguridad de la red: Conjunto de herramientas y normas de seguridad para la protección de equipo activo dentro de una red.

2.1.9 Seguridad Perimetral.

Definimos perímetro como la frontera de la red de área local. Sin embargo debido a que las redes se han convertido en extremadamente dinámicas y existen dispositivos que rompen con el concepto tradicional de seguridad perimetral como dispositivos móviles y accesos directos a Internet de algunos de estos dispositivos. Tenemos entonces que el perímetro comienza en donde la transferencia de datos. Para fines de esta tesis contemplaremos el perímetro como se explica en la definición inicial. Así entonces la seguridad relativa al perímetro son las precauciones que se tienen para la protección de ´este y su interior.

2.1.10 Seguridad Informática.

Se define como el conjunto de herramientas automatizadas cuya función es proteger los tres objetivos de la seguridad informática. Un sistema confiable es definido como aquel que posee la combinación apropiada de Confidencialidad, Integridad y Disponibilidad a efectos de soportar los objetivos particulares fijados por la institución.

2.1.10.1 Objetivos de la Seguridad Informática.

- **Confidencialidad.**

Su prioridad es que la información sea accedida solo por personal autorizado y de manera autorizada. Bajo los controles de Identificación, Autenticación y Autorización, se previene la divulgación no autorizada de información sensible. Los cuales se explican a continuación:

- ✓ Identificación: Es la forma en que los usuarios comunican su identidad a un sistema.
- ✓ Autenticación: Es el proceso por el cual se prueba que la información de identificación corresponde con el sujeto que la presenta.
- ✓ Autorización: Son los derechos y permisos otorgados a un individuo (o proceso) que le permite acceder a un recurso del sistema.

De este último objetivo se obtiene uno más Privacidad, cuyo objetivo de seguridad busca proteger la información del individuo, empleando controles para garantizar que la misma no sea diseminada o accedida en forma no autorizada.

- **Integridad.**

Se trata que toda la modificación a datos o información, es realizada por personas autorizadas de manera autorizada. Se protege la integridad de los datos, los procesos de manipulación de datos, la consistencia de los mismos de manera interna y externa. Se previene la modificación no autorizada de los sistemas e información.

- **Disponibilidad.**

La información y datos se encuentran disponibles para personal autorizado cuando sean necesarios. Así como la prevención de la interrupción del servicio y la pérdida de productividad.

2.1.11 Esquema de seguridad basado en Criterios Comunes.

Los criterios comunes surgen como resultado de la armonización de los criterios sobre seguridad software, mediante un proceso de evaluación en múltiples países. Se proporciona un conjunto común de requisitos funcionales para los productos de Tecnologías de la Información, ya sean hardware, software o firmware. De esta manera se establece un nivel de confianza en el grado en el que el producto TI satisface la funcionalidad de seguridad y ha superado las medidas de evaluación aplicadas. Así se garantizan las funciones de seguridad.

2.1.12 Niveles de seguridad.

Los niveles de seguridad describen diferentes tipos de seguridad y se enumeran desde el mínimo grado de seguridad al máximo. El estándar utilizado internacionalmente es el TCSEC Orange Book, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los E.U. Estos niveles han sido la base de desarrollo de estándares europeos y luego internacionales. Cada nivel requiere todos los niveles definidos anteriores.

- **Nivel D**

Este nivel contiene solo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y derechos en el acceso a la información.

- **Nivel C1: Protección Discrecional.**

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso. Con la actual descentralización de los sistemas de cómputo, el rol de súper usuario es segregado en múltiples actividades y es difícil distinguir entre los cambios que se ejecutaron por el usuario. El acceso de control discrecional es la distinción entre los usuarios y recursos. Se podrán definir grupos de usuarios con los mismos privilegios y grupos de objetivos sobre los cuales podrán actuar los usuarios o grupos de ellos a través de un control de identificación y autentificación.

- **Nivel C2: Protección de Acceso Controlado.**

Este subnivel fue diseñado para solucionar las debilidades del C1. Se tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitiendo o denegando datos a usuarios en concreto, con base no solo en los permisos, sino también en los niveles de autorización. Los usuarios de este nivel tienen autorización para realizar algunas tareas de administración del sistema, sin necesidad de ser administradores. De esta manera se permite llevar una mejor cuenta de las tareas relacionadas con la administración del sistema, ya que cada usuario es quien ejecuta el trabajo y no el administrador del sistema.

- **Nivel B1: Seguridad Etiquetada.**

Este subnivel, es el primero de los tres con que cuenta el nivel B. Se establece que el dueño del archivo, no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema se le asigna una etiqueta, con un nivel se seguridad jerárquico y con categoría.

- **Nivel B2: Protección Estructurada.**

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.

- **Nivel B3: Dominios de Seguridad.**

Refuerza a los dominios de instalación de hardware, existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además cada usuario tiene asignados lugares y objetos de acceso.

- **Nivel A: Protección Verificada.**

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales para asegurar todos los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El software y hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

2.2 Mecanismos de Seguridad Inalámbrica.

Introducción

La seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

Las redes Wifi basadas en los estándares IEEE 802.11 b/g se han popularizado en los últimos tiempos tanto en entornos domésticos, empresariales o urbanos. Los puntos de acceso Wifi se han multiplicado en los hogares de los usuarios de las redes de banda ancha, en las organizaciones como extensión de sus redes cableadas con el fin de facilitar un acceso más sencillo y flexible a datos y servicios corporativos sus empleados y qué no decir de los "hot-spots" que salpican nuestra arquitectura urbana (hoteles, aeropuertos, Palacios de Congresos, etc.) Son innegables las oportunidades que las redes inalámbricas proporcionan a sus usuarios pero, a su vez, ofrecen a los hackers nuevas oportunidades para conseguir acceso no autorizado a sistemas corporativos y sus datos. Estas limitaciones en la seguridad han conducido la investigación y desarrollo de nuevas soluciones de seguridad, alternativas a la inicialmente existente (WEP), para proteger las redes Wifi y proporcionar a las organizaciones que las utilizan la garantía que necesitan para sus sistemas y datos.

2.2.1 Mecanismos de Seguridad.

2.2.1.1 WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denominada ‘seed’ obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida. A continuación, WEP utiliza el ‘seed’ en un generador de números pseudo-aleatorio que produce una llave de longitud igual al payload (cuerpo más CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma. WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama. La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar

la parte del payload del cuerpo de la trama. Cuando se transmiten mensajes con el mismo encabezado, por ejemplo el FROM de un correo, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación.

Esto se soluciona utilizando un IV diferente para cada trama. La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continúa.

Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida. En cambio, 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas. A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

2.2.1.2 OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aun activando WEP, por lo tanto es un mecanismo poco fiable.

2.2.1.3 ACL (Access Control List)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

2.2.1.3 CNAC (Closed Network Access Control)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

2.2.2 Métodos De Detección De Redes Inalámbricas

El método de detección de una red inalámbrica se denomina Wardriving y es bastante sencillo. Bastaría con la simple utilización de una tarjeta de red inalámbrica WNIC (Wireless Network Interface Card), un dispositivo portátil (ordenador portátil o incluso un PDA) con un software para verificar puntos de acceso y pasearse por un centro de negocios o algún sitio donde nos conste la utilización de una red inalámbrica. El ordenador portátil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Una vez detectada la existencia de una red abierta, se suele dibujar en el suelo una marca con la anotación de sus características. Es lo que se denomina Warchalking, y cuya simbología se muestra a continuación:

SSID	
)(**Ancho de Banda**	Nodo Abierto
SSID **()**	Nodo Cerrado
SSID Contacto	
(W) Ancho de banda	Nodo WEP

Ilustración 4 Método Detención Redes Inalámbricas

Por ejemplo, el símbolo
Retina
) (
1.5

Identifica a un nodo abierto, que utiliza el SSID "Retina" y dispone de un ancho de banda de 1.5 Mbps. Esta simbología permite disponer de un mapa donde constan los puntos de acceso con sus datos (SSID, WEP, direcciones MAC,..).Si la red tiene DHCP, el ordenador portátil se configura para preguntar continuamente por una IP de un cierto rango, si la red no tiene DHCP activado podemos analizar la IP que figure en algún paquete analizado. En la figura 13 se muestra Warchalking y su simbología.

2.2.3 Vulnerabilidades Redes Inalámbricas.

Vulnerabilidad se define como la condición que podría permitir que una amenaza se materialice con mayor frecuencia, impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos o físicos. Lo cual genera un riesgo el cual se define como la probabilidad de que un agente de amenaza explote una vulnerabilidad.

Este tipo de redes es precisamente es la vulnerabilidad ya que cualquier persona con una terminal inalámbrica podría comunicarse con un punto de acceso privado si no se disponen de las medidas de seguridad adecuadas. Dichas medidas van encaminadas en dos sentidos: por una parte está el cifrado de los datos que se transmiten y en otro plano, pero igualmente importante, se considera la autenticación entre los diversos usuarios de la red. En el caso del cifrado se están realizando diversas investigaciones ya que los sistemas considerados inicialmente se han conseguido descifrar. Para la autenticación se ha tomado como base el protocolo de verificación EAP (Extensible Authentication Protocol), que es bastante flexible y permite el uso de diferentes algoritmos.

2.2.3.1 Ataques a las Redes WLAN.

2.2.3.1.1 Ataques pasivos.

Este tipo de ataque ocurre cuando un usuario no autorizado accede a la red para espiar información y, aunque no la modifica, la guarda para analizarla y poder realizar un ataque activo más tarde, o también por simple curiosidad sobre aspectos confidenciales. Este tipo de ataque es muy difícil de detectar por la no alteración de datos, pero, como administradores de la red, podemos darnos cuenta de alguna intrusión analizando el consumo de recursos; por ejemplo una reducción del ancho de banda, un incremento del tiempo de respuesta de los equipos, tiempos de carga y descarga, etc. [6] Los ataques pasivos más comunes son los siguientes:

- **Warchalking.**

El detectar redes inalámbricas se ha convertido en un pasatiempo muy popular, el warchalking consiste en recorrer lugares con una computadora portátil o un PDA compatible con WI-FI con el fin de buscar puntos de acceso inseguros o con fácil ruptura de seguridad; al encontrar estos puntos se dibuja (normalmente con yesos) uno de los tres símbolos siguientes:

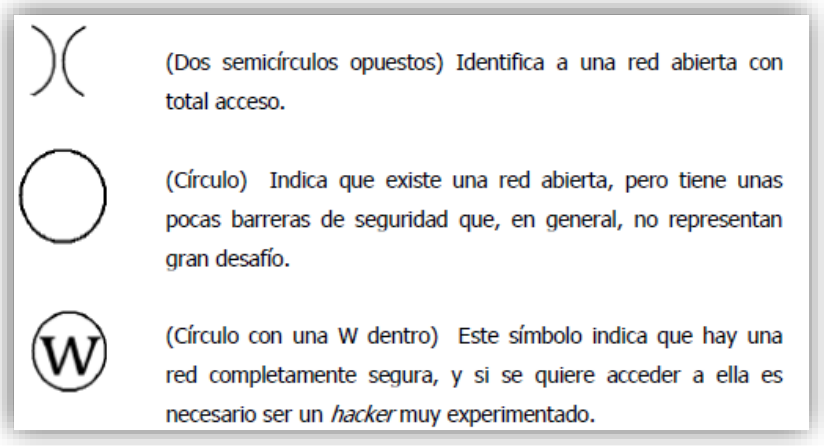


Ilustración 5 Warchalking Ataques Pasivos

- **Wardriving.**

El wardriving es básicamente lo mismo, pero se realiza desde un automóvil y se utiliza un GPS para obtener las coordenadas de los puntos de acceso de la red.

2.2.3.1.2 Ataques Activos

Romper ACL's basados en MAC: Una de las medidas más comunes que se utilizan para seguridad en una red Wireless es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar. Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacernos pasar por uno de los equipos que si tienen acceso a la red. Para llevar a cabo el ataque basta con esnifar durante un momento el tráfico y fijarnos en la MAC de cualquiera de los clientes, sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción. Esto es sencillo de implementar, por ejemplo en el sistema operativo Linux se puede realizar con el comando ifconfig dependiendo del tipo de tarjeta que tengamos. También existen otras utilidades para cambiar la

MAC como por ejemplo setmac. Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC podemos tener problemas, aunque generalmente en las redes "Wireless" esto no suele ser un problema muy grave ya que el punto de acceso no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, si queremos podemos "anular" a la máquina que le hemos "robado" la dirección MAC.

2.2.3.1.3 Ataques activos

Se dan cuando alguien no autorizado modifica o altera el contenido de la información y/o impide la utilización de la misma. Los más comunes son:

2.2.3.1.3.1 Enmascaramiento o suplantación

Se le llama también robo de identidad, imitación o falsificación. En este caso el Hacker se hace pasar como un usuario autorizado o suplanta a un cliente que se encuentra desconectado en ese momento.

Este ataque también se puede dar reemplazando un Punto de Acceso y haciendo creer que este punto de acceso pirata es legítimo. Los ataques tipo suplantación más usados son los siguientes:

- **Secuestro de sesión.**

En este ataque el hacker monitorea la red para recopilar usuarios, claves, direcciones MAC, SSID y elige un usuario X para enviarle un ataque de denegación de servicio y así desconectarlo; luego, el hacker se conecta a la red utilizando la información detectada del usuario eliminado. Comúnmente el secuestro de sesión no dura mucho tiempo, pero sí puede ser hecho a varios usuarios en la misma red. Los switches WLAN nos ayudan a descubrir este tipo de ataque.

- **Suplantación de dirección MAC.**

Este ataque se da más que todo cuando la red está protegida únicamente por la técnica de filtrado de direcciones MAC7 ya que es más fácil para el usuario detectar las direcciones MAC autorizadas y así utilizarlas en su equipo para suplantar una verdadera. Esta suplantación puede hacerse a través de software adecuado tal como Ethereal, NetStumbler o con un programa llamado Air Jack.

2.2.3.1.3.2 Denegación de servicio (DoS)

Estos ataques se hacen con el objetivo de volver inútil la red o para sacar clientes autorizados y así suplantarlos; es difícil detectarlos y erradicarlos, ya que duran poco tiempo y solamente es posible identificarlos en tiempo real, a diferencia del ataque de enmascaramiento, ya que éste se puede detectar analizando el comportamiento del punto de acceso. Las formas más comunes de denegar servicio son las siguientes:

- **Saturar el ambiente con ruido de RF**

La relación señal/ruido en todos los puntos de una red inalámbrica debe ser mayor o igual a 0.3 (30%) pues de lo contrario el ruido prácticamente anulará la señal y la red será inutilizable. Este ataque básicamente se da inyectando ruido RF en nuestro aire por medio de un generador de ruido RF o por medio de microondas.

- **Torrente de autenticaciones**

Este ataque se da cuando el hacker le envía al servidor Radius muchas peticiones de autenticación falsas de manera repetitiva y simultánea; entonces la red se mantiene ocupada tratando de autenticar estas peticiones a este usuario falso, por lo tanto los usuarios reales no tienen la oportunidad de autenticarse y no podrán acceder a la red.

- **Modificación de paquetes WPA**

El chequeo de integridad de paquetes del WPA permite sin querer los ataques de Denegación de Servicio, ya que si el hacker altera un par de paquetes, el TKIP-WPA detecta que 2 o más paquetes han sido modificados, entonces asume que lo están atacando y desconecta automáticamente a todos sus usuarios por un momento; al volver a conectarlos la red, el hacker puede alterar otra vez un nuevo par de paquetes y así lograr otra desconexión. El Air-Jack es el programa más usado para este tipo de ataque.

- **Signaling DOS**

Este ataque finaliza sesiones móviles activas en la red. Comprende el envío de pequeñas cantidades de datos para reiniciar una sesión después de que ésta haya sido liberada. El ataque de bajo volumen puede crear congestión en el controlador de radio de la red (RNC). Sobrecargar el RNC resulta en una denegación de servicio para el usuario.

- **Drenado de batería**

Este ataque envía paquetes a un cliente para evitar que éste entre en modo suspensión y así consume recursos de radio y agota las baterías de los dispositivos.

2.2.3.1.3.3 Retransmisión

A este ataque también se le conoce como Hombre-en-el-medio o MITM por sus siglas en inglés (Man-In-The-Middle). Se da cuando el hacker se ubica en el medio de la comunicación entre el punto de acceso y el usuario. Para esto el hacker debe haber analizado el tráfico previamente para conocer todos los datos del punto de acceso que quiere simular ser (el SSID, la dirección MAC, DHCP, etc.) y también los de los clientes de la red. Al emular el punto de acceso, el hacker puede bloquear la información que el cliente transmite o modificarla para engañar al receptor.

2.3 Servidores para Redes de Datos.

Introducción

Es un término que proviene del latín servitor cuyo uso ha cambiado en los últimos años. Un servidor es una computadora que forma parte de una red y que provee servicios a otras computadoras, que reciben el nombre de clientes. No es más que un sistema informático con un hardware y unas características especiales que son las que lo diferencian de los sistemas domésticos, este hardware es más preciso y soporta configuraciones más complejas que permiten un rendimiento mayor pudiendo albergar configuraciones de 128 Microprocesadores de última tecnología y varios terabytes de memoria RAM sin ser estas capacidades exageradas en absoluto.
Los servidores suelen utilizarse para almacenar archivos digitales. El cliente, por lo tanto, se conecta a través de la red con el servidor y accede a los archivos en cuestión. En ocasiones, la computadora puede cumplir con las funciones de servidor y de cliente de manera simultánea.

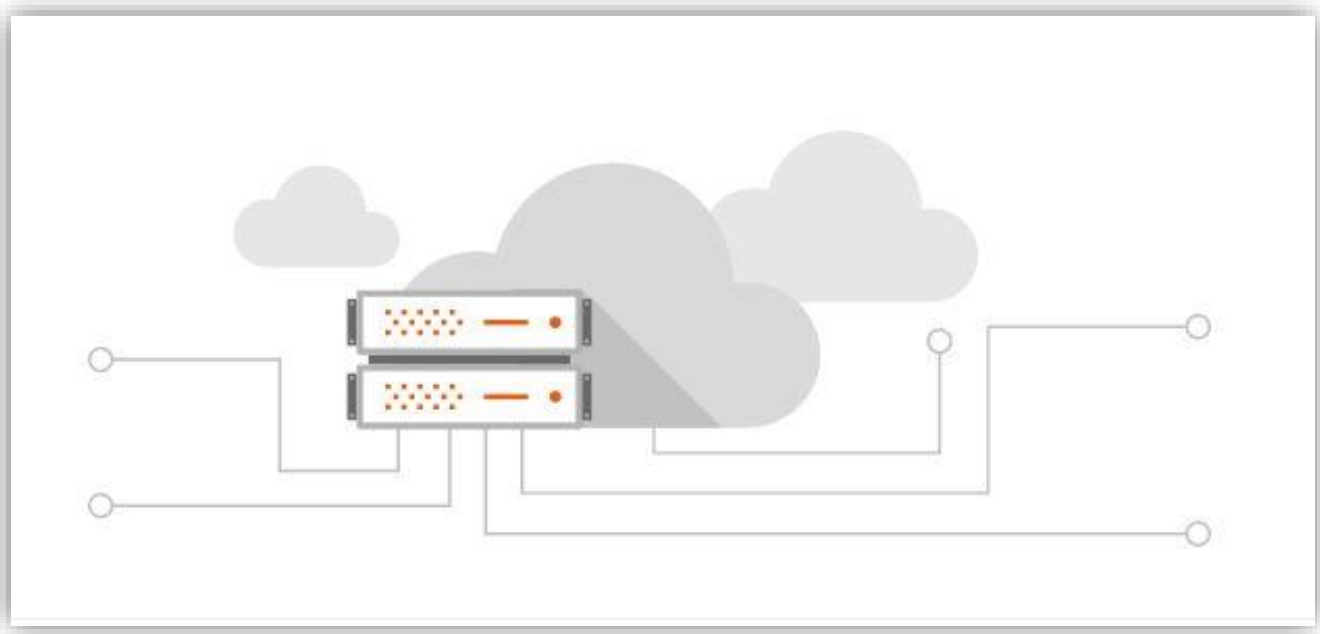


Ilustración 6 Servidores de Red de Datos

2.3.1 Tipos de servidores Datos de Redes

2.3.1.1 Plataformas de Servidor (Server Platforms).

Un término usado a menudo como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.

2.3.1.2 Servidores de Aplicaciones (Application Servers).

Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los conectan.

2.3.1.3 Servidores de Audio/Video (Audio/Video Servers).

Los servidores de Audio/Video añaden capacidades multimedia a los sitios web permitiéndoles mostrar contenido multimedia en forma de flujo continuo (streaming) desde el servidor.

2.3.1.4 Servidores de Chat (Chat Servers):

Los servidores de chat permiten intercambiar información a una gran cantidad de usuarios ofreciendo la posibilidad de llevar a cabo discusiones en tiempo real.

2.3.1.5 Servidores de Fax (Fax Servers).

Un servidor de fax es una solución ideal para organizaciones que tratan de reducir el uso del teléfono pero necesitan enviar documentos por fax.

2.3.1.6 Servidores FTP (FTP Servers).

Uno de los servicios más antiguos de Internet, File Transfer Protocol permite mover uno o más archivos.

2.3.1.7 Servidores Groupware (Groupware Servers).

Un servidor groupware es un software diseñado para permitir colaborar a los usuarios, sin importar la localización, vía Internet o vía Intranet corporativo y trabajar juntos en una atmósfera virtual.

2.3.1.8 Servidores IRC (IRC Servers).

Otra opción para usuarios que buscan la discusión en tiempo real, Internet Relay Chat consiste en varias redes de servidores separadas que permiten que los usuarios conecten el uno al otro vía una red IRC.

2.3.1.9 Servidores de Listas (List Servers).

Los servidores de listas ofrecen una manera mejor de manejar listas de correo electrónico, bien sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, boletines de noticias o publicidad.

2.3.1.10 Servidores de Correo (Mail Servers).

Casi tan ubicuos y cruciales como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas (vía LAN y WAN) y a través de Internet.

2.3.1.11 Servidores de Noticias (News Servers).

Los servidores de noticias actúan como fuente de distribución y entrega para los millares de grupos de noticias públicos actualmente accesibles a través de la red de noticias USENET.

2.3.1.12 Servidores Proxy (Proxy Servers).

Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones. El servidor Proxy es el corazón del funcionamiento de la Red LAN como tal, ya que es el elemento activo del sistema que controla los tipos de paquetes de datos que entran a la Red LAN, así como también cumple con la función de ser un punto de entrada a Internet, desde las Estaciones de Trabajo o computadores de la red. Por su naturaleza de Servidor este equipo cumple con las siguientes tareas:

A. Filtro de contenido: se pueden restringir en sus archivos de configuración, a qué tipo de contenidos pueden acceder las estaciones de trabajo.

B. Cache de páginas: El Proxy almacena todas las páginas que se navegan desde las estaciones de trabajo, de manera que si en algún momento no hay navegación, el Proxy proveerá las páginas que se requieran desde las estaciones de trabajo, como si se estuviese navegando en Internet.

C. Asignar las direcciones de Red a cada Estación de Trabajo, mediante el uso del DHCP, (Dinamic Host Configuration Protocol o Configuración de Protocolo dinámico de hospedaje): Esto significa que las estaciones de trabajo de la Red LAN configuradas bajo esta característica, “buscaran” en la Red quien esta asignando las direcciones IP para poder navegar. Las estaciones encontrarán el servidor DHCP, el Servidor les asignara una dirección IP y luego se podrá navegar tranquilamente.

D. Administración del Firewall Algunos servidores Proxy también pueden contar con lo que se denomina un Firewall o pared de fuego, que cumple la tarea de “detener” posibles intromisiones externas a la Red Interna. Este software puede filtrar algunos agentes de virus y programas dañinos que pueden hacer que la navegación no funcione en las estaciones de trabajo.

En resumen su función es recibir la petición de servicio de Internet de un usuario (por ejemplo una página Web). Si pasa los filtros establecidos, el Proxy Server, asumiendo que también es un servidor caché, realiza un escaneo en su caché local de páginas Web recientemente descargadas. Si encuentra la página solicitada, se la envía al usuario sin tener que enviar la petición a Internet acelerando la repuesta del servicio. Si no está en caché, el servidor Proxy actuara en nombre del usuario con sus propias direcciones IP para pedir la página del servidor de Internet donde está alojada. Cuando la página es encontrada y se envía al Proxy, le es enviada al usuario que la había requerido al principio.

2.3.1.12.1 Ventajas del Proxy Server

A. Ahorro de Tráfico: las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
B. Velocidad en Tiempo de respuesta: el servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
C. Demanda a Usuarios: puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
D. Filtrado de contenidos: el servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.

2.3.1.12.1 Tipos de Servidores Proxy

2.3.1.12.1.1 Proxy de Web

Este Proxy proporciona un caché de memoria para los contenidos a los que el usuario accede, de tal forma que los devuelve actualizados sólo si han sido modificados desde el último acceso. De esta manera se optimiza el tráfico y el tiempo de consulta.

2.3.1.12.1.2 Proxy inverso

Se utiliza por seguridad y para disminuir la carga de trabajo del servidor web. Este tipo de servidores permite al usuario de Internet el acceso a servidores internos protegiéndolos de ataques y distribuyendo la carga entre varios servidores.

2.3.1.12.1.3 Proxy NAT

Se trata básicamente de un mecanismo para enmascarar diferentes direcciones IP que accederán a la red a través de una única dirección IP pública compartida. El servidor se encarga de distribuir las peticiones de los usuarios internos y de esta manera proporciona una mayor seguridad a cada equipo.

2.3.1.12.1.4 Proxy Transparente

Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP) Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxy para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración. Una ventaja de tal es que se puede usar para redes de empresa.

2.3.1.12.1.5 Proxy Abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red. En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido. Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

2.3.1.12.1.6 Cross-Domain Proxy

Típicamente usado por Tecnologías web asíncronas (flash, ajax, comet, etc.) que tienen restricciones para establecer una comunicación entre elementos localizados en distintos dominios. En el caso de Ajax, por seguridad sólo se permite acceder al mismo dominio origen de la página web que realiza la petición. Si se necesita acceder a otros servicios localizados en otros dominios, se instala un Cross-Domain proxy2 en el dominio origen que recibe las peticiones ajax y las reenvía a los dominios externos. En el caso de flash, también han solucionado creando la revisión de archivos XML de Cross-Domain, que permiten o no el acceso a ese dominio o subdominio. Modificación de contenidos: basándose en la misma función del filtrado, y llamado Privoxy (es un programa que funciona como proxy web), tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

2.3.1.13 Servidores Firewall

El concepto que define Wikipedia sobre Firewall, "Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios". [7] Los firewalls pueden ser implementados tanto en el hardware como en el software, o bien combinando los dos. Los firewalls generalmente se usan para evitar el acceso no autorizado a usuarios del internet hacia redes privadas que están conectadas a Internet, sobre todo aquellas que son Intranets. Todos los mensajes que entran o salen de la intranet pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplen las políticas de seguridad especificados. Las políticas de seguridad son el conjunto de reglas de seguridad, convenciones y procedimientos que gobiernan las comunicaciones dentro y fuera de una red.

2.3.1.13.1 Funciones Básicas.

A. Filtrar los accesos no autorizados (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de Transporte, Sesión, Presentación, y aplicación).
B. Llevar la contabilidad de las transacciones que se llevan a cabo en la red.

C. Alertar en caso de ataques o de comportamiento extraño de los sistemas de comunicación.

2.3.1.13.2 Existen varios tipos de técnicas para implementar un firewall.

A) Filtros a nivel paquete (Packet Filters)

Esta tecnología pertenece a la primera generación de firewalls la cual analiza el tráfico de la red. Cada paquete que entra o sale de la red es inspeccionado y lo acepta o rechaza basándose en las reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente para los usuarios de la red, pero es difícil de configurar. Además de que es susceptible a IP Spoofing.

Las reglas para rechazar o aceptar un paquete son las siguientes:

- Si no se encuentra una regla que aplicar al paquete, el paquete es rechazado.
- Si se encuentra una regla que aplicar al paquete, y la regla permite el paso, se establece la comunicación.
- Si se encuentra una regla que aplicar al paquete, y la regla rechaza el paso, el paquete es rechazado.

B) Firewall a nivel circuito (Circuit Level Firewalls)

Esta tecnología pertenece a la segunda generación de firewalls y valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez. El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.

C) Firewall a nivel aplicación (Application Layer Firewalls)

Pertenece a la tercera generación de firewalls. Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.

La mayoría de estos tipos de firewalls requieren software especializado y servicios Proxy. Un Servicio Proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como FTP o HTTP. Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.

D) Filtros dinámicos a nivel paquete (Dynamic Packet Filters)

Pertenece a la cuarta generación de firewall y permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o más técnicas para configurar el firewall. Un firewall es considerado la primera línea de defensa para proteger la información privada.

2.3.1.14 Servidores Telnet (Telnet Servers).

Un servidor telnet permite a los usuarios entrar en un ordenador huésped y realizar tareas como si estuviera trabajando directamente en ese ordenador.

2.3.1.15 Servidores Web (Web Servers).

Básicamente, un servidor web sirve como contenido estático a un navegador, carga un archivo y lo sirve a través de la red

2.4 Virtualización de Open Source.

Introducción

En el mundo de la informática, virtualización se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución. Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico. Lo más importante en este tema de virtualización es la de ocultar detalles técnicos a través de la encapsulación.

La virtualización se encarga de crear una interfaz externa que esconde una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Un avanzado desarrollo de nuevas plataformas y tecnologías de virtualización han hecho que se vuelva a prestar atención a este importante concepto

La máquina virtual en general es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware autónoma. Típicamente muchas máquinas virtuales son simuladas en un computador central. Para que el sistema operativo "guest" funcione, la simulación debe ser lo suficientemente grande (siempre dependiendo del tipo de virtualización).

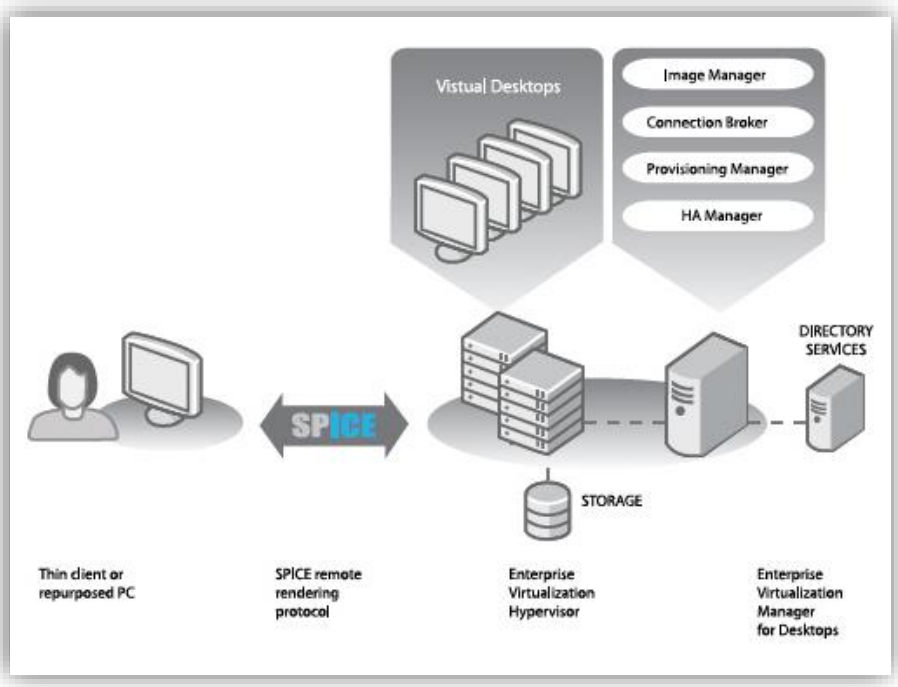


Ilustración 7 Virtualización de Open Source con Spice

2.4.1 Características de la Virtualización

2.4.1.1 Ventajas:

- Integrar varios servidores en una única computadora física. Esto nos permite optimizar el uso de recursos (CPU, memoria, almacenamiento, respaldos).
- Simplificar la realización de copias de respaldo (backup) y su restablecimiento. Todo un servidor virtual puede ser un único archivo.
- Migrar fácilmente servidores entre distintas computadoras.
- Incrementar la seguridad, utilizando servidores aislados para tareas diferentes.
- Reducción del hardware.
- Optimización y mejoramiento del uso de la capacidad de proceso de los servidores físicos.
- Reducción de los tiempos de parada.
- Administración global centralizada y simplificada.
- Mejora de los procesos de clonación y copia de sistemas.
- Migración en caliente de máquinas virtuales (sin pérdida de servicio).

2.4.1.2 Desventajas:

- Rendimiento inferior.
- Amplia dependencia del hardware de la maquina host (capacidad de procesamiento y almacenamiento del hardware).
- El sistema operativo anfitrión se vuelve un rol crítico.
- No se puede utilizar hardware que no esté soportado por el hipervisor.
- No se dispone de aceleración de vídeo por hardware (mayoría de los visores).

2.4.2 Técnicas de Virtualización

2.4.2.1 Virtualización de hardware.

Se implementan extensiones al procesador que facilitan la implementación de máquinas virtuales, las extensiones VMX en Intel y SMV en AMD, soportan la virtualización del hardware del procesador y no están ligadas a ningún entorno operativo concreto (VT-X).

2.4.2.2 Virtualización a nivel del Sistema Operativo.

En este esquema no se Virtualizar el hardware y se ejecuta una única instancia del sistema operativo (kernel). Los distintos procesos pertenecientes a cada servidor virtual se ejecutan aislados del resto sobre este mismo kernel, hay poca perdida de rendimiento y no se aprovechan todas las ventajas de la virtualización.

2.4.2.3 Para virtualización (paravirtualization).

La para virtualización consiste en ejecutar sistemas operativos guests sobre otro sistema operativo que actúa como hipervisor (host). Los guests tienen que comunicarse con el hypervisor para lograr la virtualización.

2.4.2.4 Virtualización completa (full virtualization):

La virtualización completa es similar a la para virtualización pero no requiere que los sistemas operativos guest colaboren con el hypervisor. En plataformas como la x86 existen algunos inconvenientes para lograr la virtualización completa, que son solucionados con las últimas tecnologías propuestas por AMD e Intel."

2.4.3 Virtualizadores más Importantes.

	FullVirt	Paravirt	Licencia	Arquitectura	Rendimiento	Cpu/Menoria/Hotplug	Notas
XEN	*	*	GPL	686,X86-64, Power PC ia64	Paravirtualizacion rapida, virtualizacion media	*	Full virtualizacion necesita VT/AMD-V
KVM	*	*	GPL	686,X86-64, Power PC, ia64, S390	Paravirtualizacion rapida, virtualizacion media	*	Full virtualizacion y paravirtualizacion necesita VT/AMD-V
VIRTUALBOX	*		GPL/PROPIETARIO	I686,X86-64	Rapido / Muy rapido		Modulo de kernel GPL, RPD soporte USB propietario
QEMU	*		GPL	686,X86-64, Power PC, ia64, SPARC, ARM	Lento / Medio (con Kqemu)		
VMWARE ESX	*		PROPIETARIO	I686, X86-64	Rapido / Muy rapido		
VMWARE SERVER/WOKSTATION/PLAYER		*		PROPIETARIO	I686, X86-64	Rapido / Muy rapido	Necesita modulos propietarios para el kernel

Ilustración 8 Virtualizadores más Importantes.

2.4.3.1 XEN

2.4.3.1.1 Ventajas

- Desempeño casi nativo.
- Permite virtualización completa y para virtualización.
- Puede funcionar aun en hardware que no soporta virtualización completa.
- Permite la migración en caliente de los sistemas clientes.
- Existe la convivencia entre servidores virtualizados y servidores para virtualizados.

2.4.3.1.2 Desventajas

- Los clientes deben ser modificados para su funcionamiento.
- No es compatible con la interfaz avanzada de configuración de energía (ACPI, APM) en tecnologías portátiles.
- No todo el hardware esta soportado.
- Problemas con algunos drivers propietarios.
- No admite varios chips de wlan y bridges Card bus.

2.4.3.2 KVM

2.4.3.2.1 Ventajas

- Está incluida en el kernel a partir de la versión 2.6.20.
- Permite virtualización completa.
- Puede ejecutar huéspedes Linux de 32 y 64 bits, así como Windows de 32 bits.
- Utiliza QEMU para el manejo de las máquinas virtuales, funciona como un driver de virtualización.
- Los procesadores virtuales de una máquina virtual son simples hilos del proceso anfitrión.
- Los sistemas clientes no necesitan modificaciones.

2.4.3.1.2 Desventajas

- Necesita un procesador con soporte para Virtualization Tecnology.
- Falta de opciones directas para la ejecución de sistemas operativos de otras arquitecturas (Las versiones en desarrollo están desarrollando estas características).

2.4.3.4 VMWARE

2.4.3.4.1 Ventajas

- Solidez, estabilidad, seguridad.
- Admite drivers en los entornos emulados.
- indicado para consolidación de servidores e investigaciones técnicas.

2.4.3.4.2 Desventajas

- Rendimiento mediocre del gestor de máquinas virtuales con hardware de bajo rendimiento.
- La versión gratuita es de uso personal y no empresarial.
- Al actualizar el kernel se debe ejecutar nuevamente el instalador.

2.4.4 Cómo funciona la virtualización y para qué sirve.

La virtualización está de moda. Si antes era una tecnología al alcance solamente de las grandes compañías. Ahora cualquier empresa pequeña o mediana tiene al alcance los beneficios de la virtualización, pero ¿qué es y para qué sirve?
La reducción de precios en el hardware y la presencia de productos software de virtualización cada vez más asequibles ha democratizado esta tecnología que, bien utilizada, puede poner a nuestra disposición más opciones de sistemas operativos, costes menores y un mayor control sobe nuestra estructura. Dentro de la estructura informática de una empresa ya hemos visto que los servidores pueden desempeñar un papel importante para centralizar recursos y utilizar herramientas específicas que incrementan la productividad a través de la mejora de los procesos de producción, planificación o comunicación.

La tecnología nos ofrece sin embargo la posibilidad de disponer de varios servidores con características muy distintas pero instalando físicamente una sola máquina. Este sistema se llama virtualización. A través de esta tecnología es posible hacer que los recursos de un ordenador, en este caso un servidor, puedan ser compartidos por una o más máquinas virtuales que se comportarán a su vez como servidores reales.

A cada una de estas máquinas virtuales se les pueden asignar recursos hardware diseñando distintas configuraciones con sus características independientes. Estos recursos pueden ser compartidos o se pueden bloquear de forma que cada máquina virtual tenga su propia memoria RAM, CPU, disco duro, recursos de red... En cada una de estas máquinas podemos instalar su propio sistema operativo y sus aplicaciones independientes.
La estructura es la siguiente: se instala en el ordenador huésped un Hypervisor o VMM, un gestor de máquinas virtuales que se ocupa de gestionar los recursos del servidor y de distribuirlos entre las máquinas virtuales. Este software o sistema operativo para máquinas virtuales se puede encontrar distribuido por empresas como Microsoft, VMWare, Parallels, Citrix y otras.

Una vez instalado el sistema operativo virtual, podemos ir creando nuestras máquinas virtuales independientes dentro del gestor de máquinas virtuales. Podemos, por ejemplo, instalar una máquina virtual con Windows Server para el servidor Exchange de correo, uno más con una aplicación CRM, otro con Linux en el que instalar un servidor Web.

2.4.5 Las ventajas de disponer de servidores virtualizados frente a servidores físicos son las siguientes.

- **Ahorro de costos**: Podremos adquirir un solo servidor, aunque más potente, y no tener que comprar más servidores sino solamente ir creándolos en el gestor de máquinas virtuales. También permite ahorro en el coste de mantenimiento y en el de personal, además de ahorrar espacio.
- **Crecimiento más flexible**: Instalar un nuevo servidor es mucho más sencillo y rápido frente a hacerlo con un servidor físico.
- **Administración simplificada:** Desde la consola del gestor de máquinas virtuales podemos aumentar o reducir los recursos para una determinada máquina, reiniciarla, instalar parches o simplemente borrarla en caso de problemas.
- **Aprovechamiento de aplicaciones antiguas:** Una de las ventajas de la virtualización es la posibilidad de conservar aplicaciones que funcionan en sistemas antiguos y aun así modernizar la infraestructura informática de la empresa. Esa aplicación puede "sobrevivir" en una máquina virtual independiente sin que haga falta conservar el ordenador antiguo.
- **Centralización de tareas de mantenimiento:** Podemos realizar copias de seguridad de un solo golpe de todas las máquinas, programar actualizaciones y otras actividades desde el gestor de máquinas virtuales. También podemos centralizar otras funciones.
- **Disminuye tiempos de parada:** Una ventaja importante, solucionar problemas o realizar copias de seguridad son tareas que se realizan en mucho menos tiempo. Por ejemplo, se puede clonar una máquina y seguir dando servicio mientras se realiza mantenimiento de la máquina virtual de producción como actualizaciones.
- **Mejor gestión de recursos:** Se puede aumentar la memoria o almacenamiento de la máquina huésped para aumentar los recursos de todas las máquinas virtuales a la vez, por lo que se aprovecha mucho mejor las inversiones en hardware.
- **Balanceo de recursos:** Es posible asignar un grupo de servidores físicos para que proporcionen recursos a las máquinas virtuales y asignar una aplicación que haga un balanceo de los mismos, otorgando más memoria, recursos de la CPU, almacenamiento o ancho de banda de la red a la máquina virtual que lo necesite.

Capítulo 3: Diseño Metodológico

3.1 Etapas

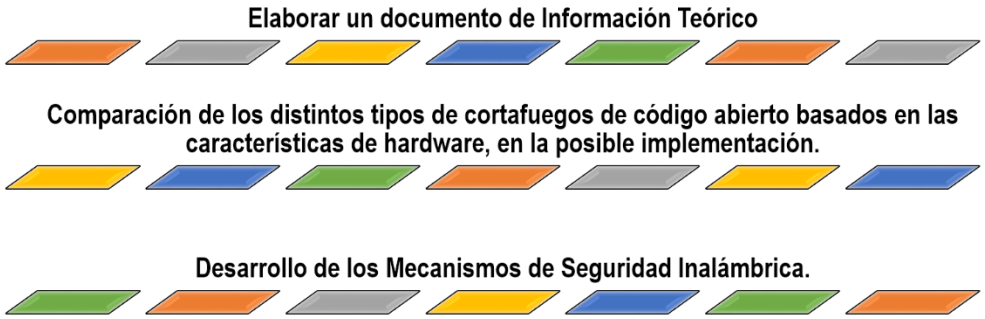


Ilustración 9 Etapas del Diseño Metodológico

3.1.1 Recolección de Información

En la primera fase de la investigación, se realizó un estudio sobre Mecanismos de Seguridad Inalámbrica, con el fin determinar los aspectos más importante a desarrollar en el tema de Tesis, organizando la información según a los temas a desarrollar. La secuencia de los contenidos teóricos es la siguiente:

- Introducción a las Redes Inalámbricas
- Mecanismos de Seguridad Inalámbrica
- Servidores para Redes de Datos.
- Sistemas de Virtualización de Open Source.

3.1.2 Selección de las herramientas con posible implementación.

En esta etapa se seleccionaron el conjunto de software a usar en el desarrollo de la posible implementación de los mecanismos de seguridad para la red inalámbrica de la Universidad BICU. Después de analizar cada herramienta y estas son las más adecuadas utilizando la plataforma PFSense 2.2.6. Tomando en cuenta su facilidad manejo por lo que se seleccionaron las siguientes aplicaciones:

- Sistema Operativo Free BSD UNIX.

- PFSENSE 2.2.5
  1. Squid Proxy
  2. DNS
  3. SquidGuard
  4. Light Squid Report
  5. BandWith
  6. Firewall
  7. Radius
  8. Portal Autentificación
  9. Aplicaciones de monitoreo en tiempo Real.

3.1.3 Elaboración y desarrollo de los laboratorios

Organización de los mecanismos de Seguridad Inalámbrica: Es el punto donde se sugiere el método de organización de la información según el nivel de complejidad que tienen cada uno de las herramientas de seguridad basadas a la necesidad de la empresa. El orden de los mecanismos a desarrollar es el siguiente:

- Instalación máquina Virtual.
- Instalación PFSense (Firewall).
- Instalación de Squid Proxy
- Squid Guard para reglas de acceso.
- Denegación de Servicio con Firewall.
- Sistema de Monitoreo
- Sistema de HAVP Firewall Antivirus.

Desarrollo para los mecanismos de seguridad: El formato a seguir para enunciar cada uno de los mecanismos de seguridad ocupando herramientas de software libre la propuestas es el siguiente:

Titulo

- Nombre de la Mecanismo de seguridad.

Objetivos

- Presenta una visión general de lo que se espera lograr y alcanzar en cada etapa desarrollo de los mecanismos de seguridad en la empresa BICU.

Introducción

Contiene informaciones generales de lo que posee cada mecanismo de seguridad en desarrollo de su contenido, y en algunos casos, aspectos específicos de funcionamiento.

Topología
Se expondrá una imagen donde se represente la topología de la red inalámbrica.

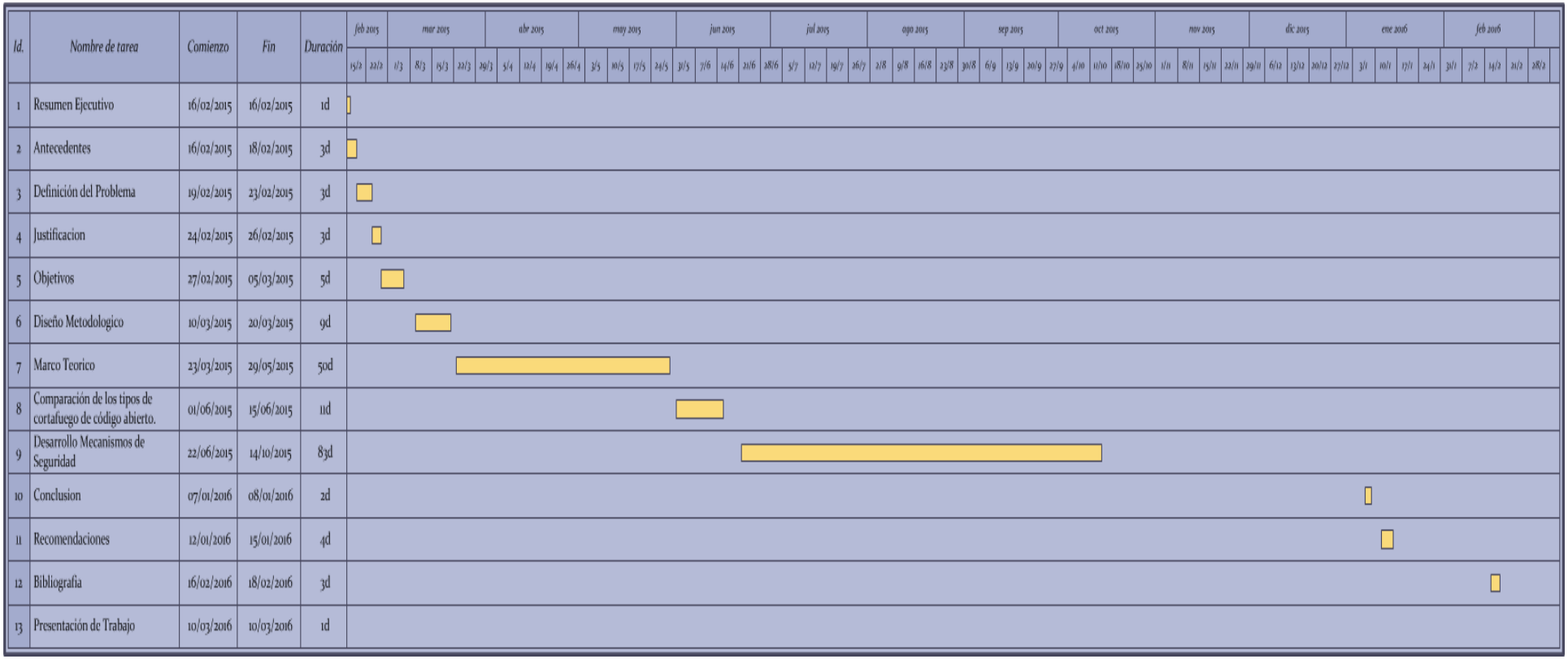
Requerimiento de Software y Hardware.

El software necesario para realizar los mecanismos de seguridad y la misma vez evaluar los requerimientos del hardware.

Desarrollo de los mecanismos de Seguridad utilizando herramientas de Software Libre.

Se explica de manera detallada los pasos a seguir.

3.2 Cronograma de Actividades



Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Resumen Ejecutivo	16/02/2015	16/02/2015	1d
2	Antecedentes	16/02/2015	18/02/2015	3d
3	Definición del Problema	19/02/2015	23/02/2015	3d
4	Justificacion	24/02/2015	26/02/2015	3d
5	Objetivos	27/02/2015	05/03/2015	5d
6	Diseño Metodologico	10/03/2015	20/03/2015	9d
7	Marco Teorico	23/03/2015	29/05/2015	50d
8	Comparación de los tipos de cortafuego de código abierto.	01/06/2015	15/06/2015	11d
9	Desarrollo Mecanismos de Seguridad	22/06/2015	14/10/2015	83d
10	Conclusion	07/01/2016	08/01/2016	2d
11	Recomendaciones	12/01/2016	15/01/2016	4d
12	Bibliografia	16/02/2016	18/02/2016	3d
13	Presentación de Trabajo	10/03/2016	10/03/2016	1d

Capítulo 4: Comparación de los distintos tipos de cortafuegos de código abierto basados en las características de Hardware en su posibilidad de Implementar.

4.1 Comparación de los tipos de corta fuegos de código abierto.

4.1.1 Firewall.

Es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna. También es frecuente conectar a los cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

4.1.2 Tipos de firewalls.

4.1.2.1 Firewall de Capa de Red o de Filtrado de Paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

4.1.2.2 Firewall de Capa de Aplicación

Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder. Un firewall a nivel 7 de tráfico HTTP suele denominarse Proxy, y permite que los computadores de una organización entren a Internet de una forma controlada.

4.1.2.3 Firewall Personal

Es un caso particular de cortafuegos que se instala como software en un Computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

4.1.3 Sistemas operativos Firewalls Open Source.

4.1.3.1 Endian

Es una distribución **GNU/Linux** de código abierto especializada en Routing/Firewalling, desarrollada por italian Endian Srl y la comunidad Endian. Está basada originalmente en IpCop otra distribución que a su vez fué un fork de SmoothWall.

4.1.3.1.1 Características

- Ipsec LAN a LAN VPN.
- NAT
- Soporte para DMZ.
- Gráficos detallados de las interfaces de red.
- Múltiples aliases en la interface WAN.
- Interfaz administrativa WEB bajo https.
- Detalle de todas las conexiones activas.
- Log detallado de todos los procesos del sistema.
- Envió de log a un syslog
- Servidor NTP.
- Servidor DHCP.
- Proxy, POP3 Antivirus.
- Proxy SMTP antispam
- Interfaz grafica de usuario (GUI) para configuración y administración de los servicios.
- IDS en interface WAN y LAN.
- Proxy SIP
- SMTP Proxy
- Squid Guardián.
- Filtro de contenidos.
- Advanced Proxy

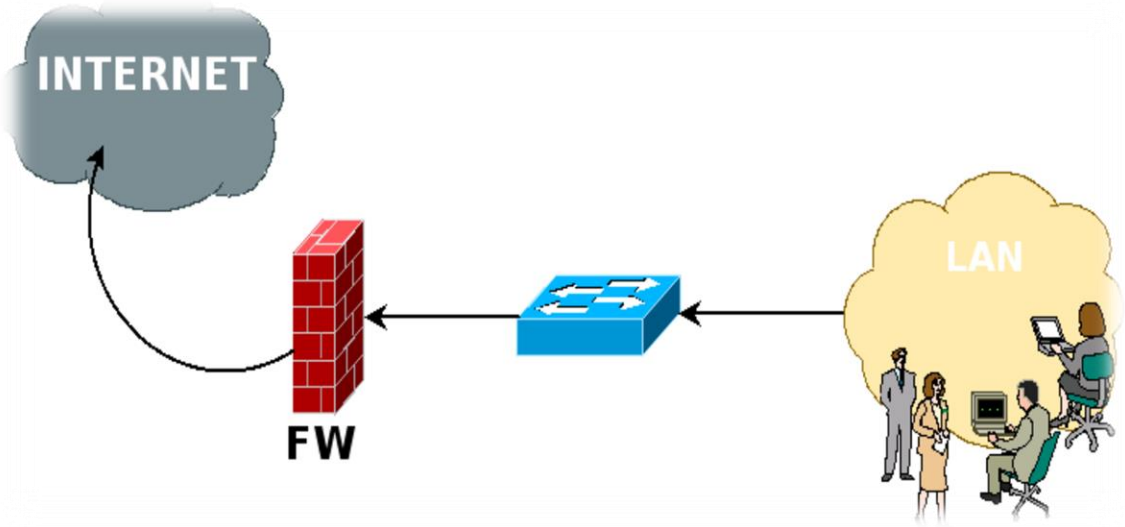


Ilustración 10 Endian Sistemas Operativos Firewall Open Source

4.1.3.1.2 RECURSOS:

- Equipo de cómputo, con distribución de endian Linux.
- Switch
- 4 Equipos de cómputo de la LAN.

4.1.3.1.3 REQUISITOS:

- Dar acceso a Internet a todos los usuarios de la pequeña LAN, haciendo NAT.
- Denegar el acceso del tráfico desde la red WAN hacia la red LAN.

4.1.3.2 Untangle

Es una plataforma para desplegar aplicaciones basadas en redes. La plataforma une estas aplicaciones alrededor de un GUI común, base de datos y señalamiento. Las aplicaciones sobre la plataforma de Untangle inspeccionan el tráfico de la red simultáneamente, lo cual reduce los requisitos de recurso de cada aplicación individual enormemente. La plataforma de Untangle soporta muchas aplicaciones de fuentes abiertas y software adicionales de comercial actualmente.

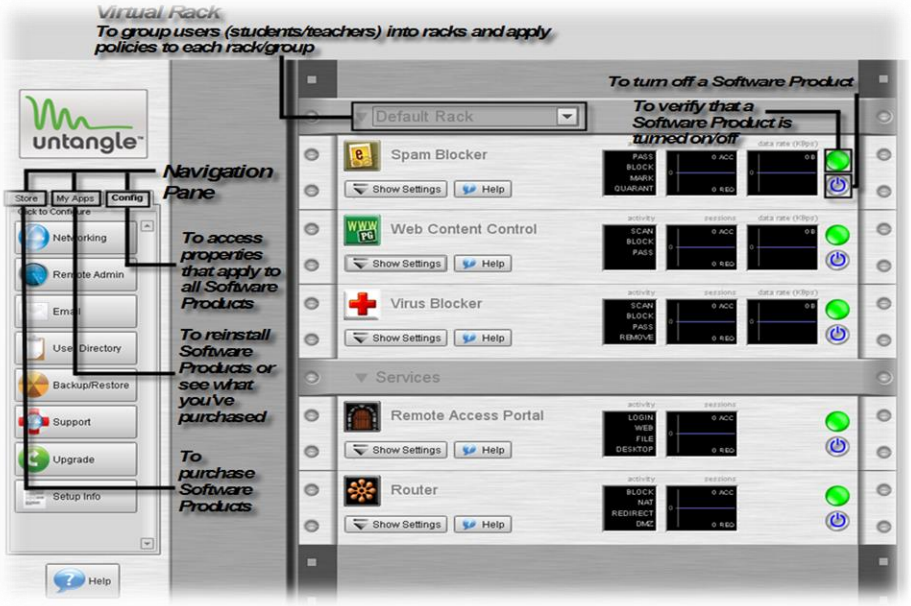


Ilustración 11 Untangle Sistemas Operativos Firewall Open Source

4.1.3.2.1 Requisitos de Hardware

RECURSOS	MÍNIMO	RECOMENDADO:	NOTA:
CPU:	1.0 GHZ	2.0+ GHZ	SE DEBE TENER UNA UNIDAD DE CD/DVD EN EL SERVIDOR O COMPUTADORA PARA INSTALAR UNTANGLE
MEMORY:	512 MB	1-2 GB	
HARD DRIVE:	20 GB	40+ GB	
NETWORK CARDS:	2	3+ (FOR DMZ)	

Ilustración 12 Untangle Requisitos Hardware

4.1.3.3 IpCop

IPCop es una Distribución Linux especializada; completa, configurada y lista para proteger su red. Además, está distribuida bajo licencia GNU General Public License, con todo el código fuente disponible para descargarlo, revisarlo o incluso ser modificado y/o recompilado por usted mismo para sus necesidades personales o por razones de seguridad. IPCop creció por múltiples necesidades. La primera de esas necesidades era la protección segura de nuestras redes personales y comerciales. Cuando IPCop empezó, en Octubre de 2001, había otros cortafuegos disponibles. De todas formas, el equipo que empezó IPCop sentía que las otras dos necesidades que IPCop cubre no estaban conseguidas; GPL y un sentido de comunidad.

4.1.3.3.1 Característica IpCop.

- Segura, Estable y altamente configurable distribución basada en Firewall.
- Web Server con páginas que permiten la sencilla administración del firewall.
- Cliente DHCP que permite obtener la dirección IP automáticamente desde el ISP.
- Servidor DHCP que permite una rápida y sencilla configuración de estaciones de
- trabajo en la red interna.
- Proxy DNS cache, que permite incrementar la velocidad de resolución de consultas
- de nombre de dominio.
- Web Proxy con cache que incrementa la velocidad de navegación por web.
- Detección de intrusos para advertir ataques desde la red externa.

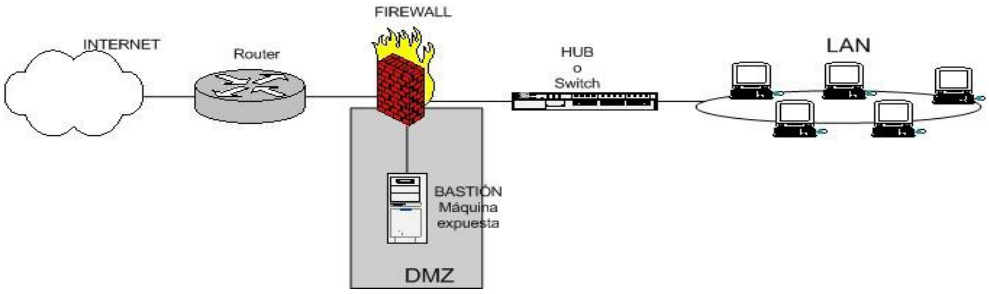


Ilustración 13 Sistemas Operativos Firewall Open Source IpCop

4.1.3.3.2 Funcionalidad IpCop.

- Acceso seguro por SSL a la interface de administración web.
- DHCP cliente / servidor.
- DNS dinámico.
- Lista de hosts sorteable desde la interface web.
- HTTP / FTP proxy (squid).
- IDS (snort) en todas las interfaces.
- Log local o remoto.
- NTP cliente / servidor.
- Servidor SSH (PSK o con password).
- Traffic shaping (en la interface RED).
- "Statefull" Firewall.
- Módulos "nat helper" para h323, irc, mms, pptp, proto-gre, quake3.
- Port forwarding (re direccionamiento de puertos).
- DMZ pin holes.
- Activar o desactivar ping en todas las interfaces.
- VPN (IPSEC).
- Gráficos de monitoreo de CPU, RAM, swap, HD, tráfico de RED, etc.

4.1.3.3.3 Requisitos de Hardware

- Arquitecturas: i386 y Alpha (PPC y Sparc están planeadas para versiones futuras).
- Memoria: de 12MB a 4GBDiscos: IDE, SCSI y SATA, soporta configuraciones con RAID.
- Placas de red: ISA/PCI (las soportadas por el kernel de Linux 2.4).
- CPU: Disponibilidad de kernel SMP para CPUs multicore.
- Dándole nuevas funciones a IPCop: Los Addons.

4.1.3.4 Vyatta.

Es un sistema basado en software opensource, que nos da la posibilidad de reducir los grandes gastos que demandaría la compra de equipamiento como por ejemplo Cisco. Se pueden implementar redes de mediana y gran escala, con el simple hecho de bootear el cd como live cd o también optar por usarlo desde una máquina virtual.

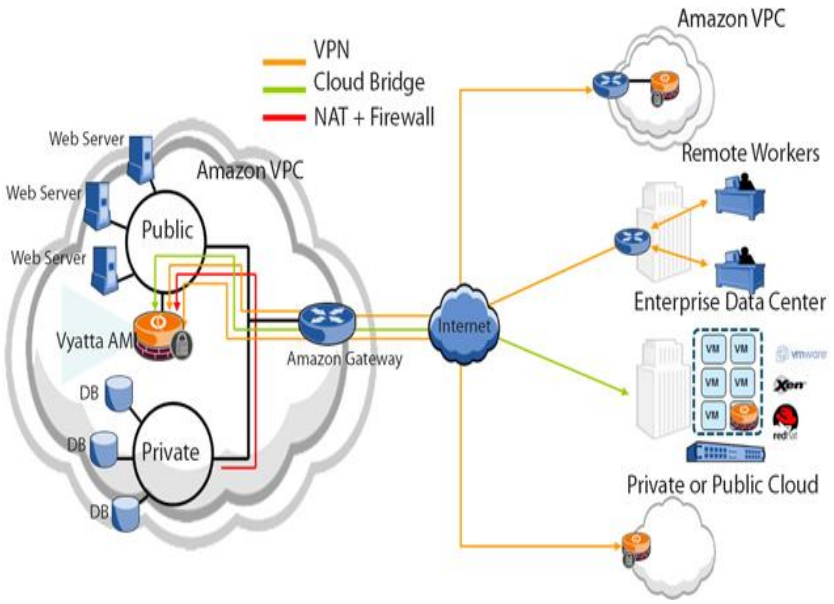


Ilustración 14 Sistemas Operativos Firewall Open Source VYatta

4.1.3.4.1 Característica Vyatta.

- Es GPL
- La configuración del mismo se guarda en un único archivo
- Posee una comunidad activa y tiene actualizaciones periódicas (2 por año).
- Protocolos de Ruteo y IP (Ipv4 y Ipv6, Rutas Estáticas, RIPV2, OsPFv2, BGPv4).
- Estático
- DHCP: Relay / Server / Client
- DNS: Forwarding / Dynamic DNS.
- Encapsulamiento (Ethernet, Frame Relay, 802.1Q Vlans, PPP, MLPPP, HDLC, PPPoE,, GRE, IP in IP).
- Performance y Optimización (Balanceo de Carga de Wan, QoS Priorizar y clasificar de Trafico, Ethernet Bonding, Control de Ancho de Banda, Web cache y filtrado de URL por categoría).
- Logging, Monitoreo y Seguridad.

4.1.3.4.2 Requisitos Hardware Vyatta.

- CPU
- Intel(R) Xeon(TM) CPU 2.80GHz 2 nucleos
- Memoria 2Gb DDR ECC
- Conectividad 2 Intel e100 - 1 Intel e1000.

4.1.3.5 PFSense

Es Una Distribución personalizada de FreeBSD Adaptado para su USO Como Firewall y Router. Se caracterizó Por Ser de código abierto, Puede Ser Instalado En Una Gran Variedad de Ordenadores, Y: Además Cuenta con Una Interfaz sencilla web para su configuración.

4.1.3.5.1 Características de PFSense 2.2.5

4.1.3.5.1.1 BandWith

Se utiliza para el seguimiento y el uso de ancho de banda de gráficos para cada LAN IP. BandWith es el ancho de banda de las conexiones a internet, o sea la cantidad de información que se puede transmitir por segundo, esta difiere del proveedor, hardware y el tipo de servicio que contrates.

4.1.3.5.1.2 Ifdepd.

Utilizado para la construcción de dependencias de la interfaz.

4.1.3.5.1.3 Ifstated.

Agrega el intervalo basado en conexión de comprobación.

4.1.3.5.1.4 Pfflowd.

Usado para convertir a mensajes de estado PF (un filtro de paquetes o cortafuegos basado en configuración dinámica de OpenBSD) a Cisco de flujo de red en Datagramas.

4.1.3.5.1.5 PFStat.

(Adds additional graphing functionality). Agregación adicional de funcionalidad de gráfico.

4.1.3.5.1.6 Ntop.

La habilidadad de agregar o registrar lo que sucedió en los datos históricos en la red.

4.1.3.5.1.7 Stunnel.

Añade la habilidad para envolver puertos estándar con capa de conexión segura.

4.1.3.5.1.8Pure-FTPd.

Añade la habilidad para hospedar archivos FTP.

4.1.3.5.1.9 Squid Transparent Proxy.

Un proxy cache para todo uso (En la Actualidad no se trabaja pero al ser es fijo.

4.1.3.5.1.10 Arpwatch.

Se utiliza para la observación de pares de direcciones IP y Ethernet.

4.1.3.5.1.11 Assp.

Es un antivirus incorporado en el server del Proxy de PFSense la cual trabaja en el escaneo de anti-spam.

4.1.3.5.1.12 Free RADIUS.

Un servidor de autenticación de Radios.

4.1.3.5.1.13 Mtr.

Una de las funciones de trazado de una mayor.

4.1.3.5.1.14 Nmap

Un escáner de puertos de la auditoría de seguridad.

4.1.3.5.1.16 Siproxd.

Un proxy con enmascaramiento para el protocolo SIP.

4.1.3.5.1.17 Spamd.
Un falso servidor SMTP utilizado como un bloqueador de spam.

4.1.3.5.1.18 Nut. (Adds support for UPS monitoring).
4.1.3.5.1.19 Snort.
Añade capacidades de detección de intrusiones.

4.1.3.5.2 Características de Tamaño del Hardware se clasifica en dos:
4.1.3.5.2.1 Requisitos mínimos de Hardware PFSense.
- CPU Intel Pentium/Amd Athlon 100Mhz
- 128mb RAM
- Lector CDROM
- 1gb Disco Duro
- 2 Tarjetas de Red
- Rendimiento requerido
- Características que podrían ser usadas

4.1.3.5.2.2 Rendimiento:
- 0 – 10Mbps: requerimientos mínimos.
- 10 – 20Mbps: No menos de 256mhz de Velocidad CPU.
- 21 – 50Mbps: No menos de 500mhz de Velocidad CPU.
- 51 – 200Mbps: No menos de 1.0Ghz de Velocidad CPU.
- 201 – 500Mbps: Hardware de clase servidor con tarjetas de red PCI-X o PCI-e, o hardware de nuevos PC de escritorio con tarjetas de red PCI-e. No menos de 2.0ghz de Velocidad CPU.
- 501+ Mbps: Hardware de clase servidor con tarjetas de red PCI-X o PCI-e. No menos de 3.0ghz de Velocidad CPU.

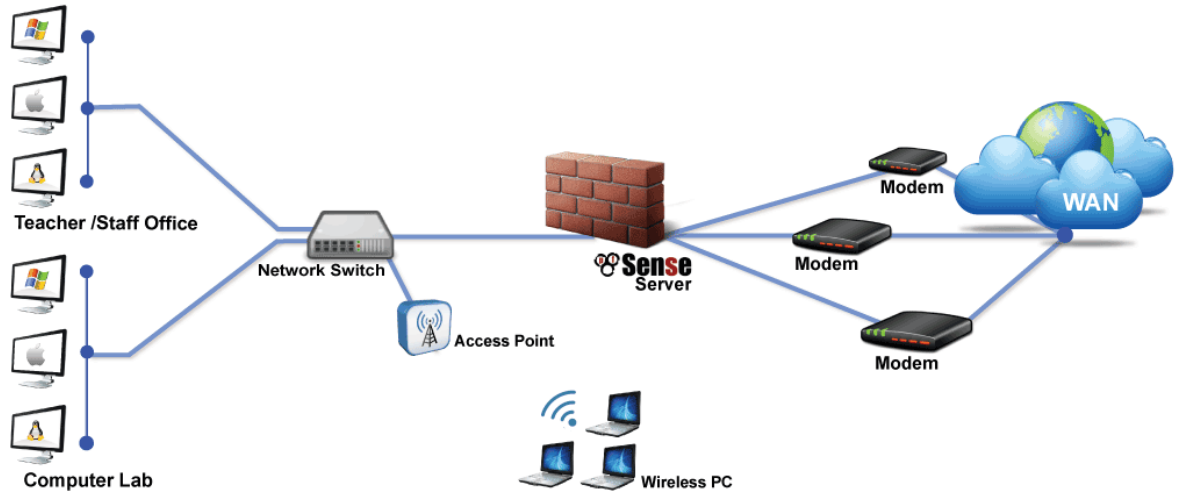


Ilustración 15 Sistemas Operativos Firewall Open Source PFSense

4.1.3.6 Monowall
Está basado en la versión 6.x de FreeBSD y se trata de uno de los mejores cortafuegos existentes. La versión completa de monowall pesa 12MB y se puede instalar en una tarjeta Compact Flash o arrancar desde un CD y solamente necesita un diskette o pendrive USB para ir guardando la configuración (que es un archivo XML). Toda la

administración del firewall se hace mediante una interfaz web basada en PHP y no se necesita conocer el funcionamiento de FreeBSD para hacerlo funcionar. Ofrece la opción de levantar un sin número de aspectos interesantes como Traffic Shaping y portal cautivo.

4.1.4 Conclusión de selección Firewall

Para crear los mecanismos de seguridad Inalámbrica se seleccionó el Corta fuego de código Libre PFSense, este sistema tiene muchas características y aspectos funcionales basados a su versatilidad de emplearlo vía live CD, USB, Virtualización VMware lo hace una herramienta portable y bastante útil. Y fácil de implementar en cualquier red. Su configuración vía web facilita en gran medida el trabajo de un administrador de red y por sobre todo, el respaldo de una gran comunidad que brinda soporte por medio de sus foros. A diferencias de los otros Firewall este es mucho más robusto, consume poco recurso, tiene una variedad de extensiones el cual son independientes en su configuración.

Capítulo 5: Desarrollo de los mecanismos de Seguridad Inalámbrica de acuerdo a la necesidad de la Empresa.


pfSense
Mecanismos
Seguridad
Inalambrica
FPSense 2.2.5

5.1 Organización de los Mecanismos de Seguridad Inalámbrica.

5.1.1 Programación de Actividades.

- ❖ Preparación del Equipo (Hardware), Instalación Sistema FreeBSD PFSense 2.2.5 Virtualizados.
- ❖ Menú de Configuración PFSense, WebConfigurator.

5.1.1.1 Preparación del equipo (Hardware).

Objetivo General

- Analizar el equipo de presentación del proyecto con los requerimientos (Hardware) más adecuados y mínimos para su funcionamiento de la virtualización de PFSense.

Objetivo Especifico

- Preparar los requerimientos de hardware funcionales para la Instalación de PFSense.
- Evaluar su capacidad de manejo mediante la virtualización en el equipo.

Introducción

PFSense es un sistema portable que carga en dispositivos USB y Disco duros y CD, el Firewall puede correr con máquinas con capacidades mínimas. Este punto mostrara la evaluación y preparación de cada requerimiento necesario de Hardware para la presentación del proyecto. Ocuparemos Virtual Box para evaluar la capacidad de funcionamiento en el equipo.

Requerimiento de Hardware Mínimos.

- ❖ Procesador Pentium(R) Dual-Core CPU E5400 2.71GHz.
- ❖ Disco Duro de 250GB.
- ❖ Memoria RAM de 2 GB.
- ❖ 2 Tarjetas de Red 1 Mbps.

Instalación de Software

En el desarrollo del proyecto se instaló un sistema operativo FreeBSD que es una distribución de Unix como servidor. Luego de tener bien en claro los objetivos del proyecto, se seleccionó el sistema operativo del servidor. Para elegir el mejor software para que ayude a cumplir con los objetivos del proyecto, se realizó una investigación comparativa de cuál de los sistemas operativos de servidor con aplicación incorporada es el más adecuado para el proyecto, los sistemas operativos con las aplicaciones integradas son: Untangle, Endian, PFSense, Monowall, SmoothWall, Squid. Después de verificar las especificaciones de cada sistema operativo, detalles técnicos y opiniones que se encontraron en la web, se determinó que el sistema operativo con la aplicación ideal para el proyecto es el sistema operativo de PFSense 2.2.5, un software libre que demuestra en la práctica ser un sistema muy estable y seguro con muchas funcionalidades de agregación de repositorios que se pueden añadir durante la Instalación la cual son Squid, Light Squidreports, Squidguard, HAVP antivirus y BandwidthD entre otros.

a) Instalación de Virtual Box para hacer la simulación del servidor Proxy.

Primer paso Instalar Virtual Box para hacer la simulación de la implementación del servidor proxy:

A) Escogemos la distribución del sistema operativo que es FreeBSD que es una versión de BSD Unix de la familia de Linux.

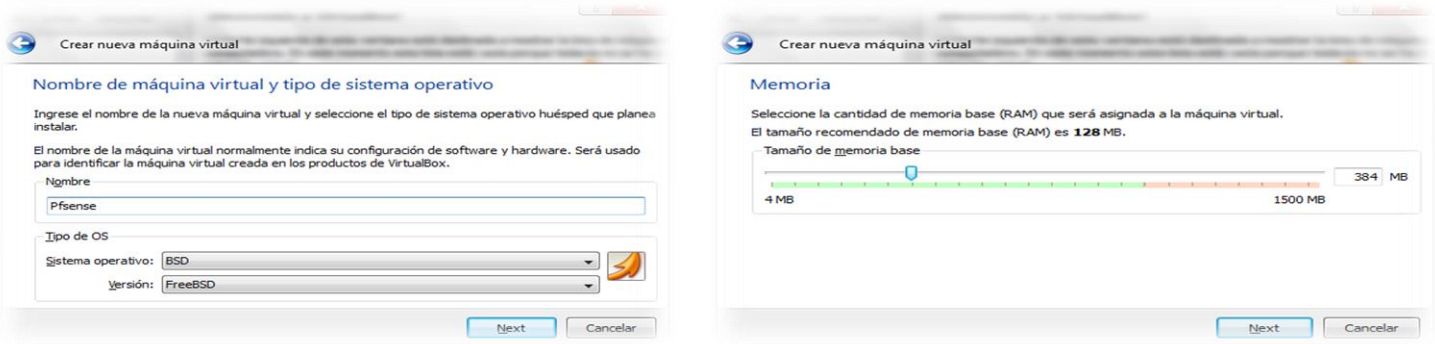


Ilustración 16 Preparación del equipo (Hardware).

B) Agregamos la capacidad de la memoria RAM esto dependerá del equipo que contenga su diversa capacidad pero si el equipo ofrece mayor RAM y mejor capacidad del procesador, mayor será el rendimiento esto aparecerá en los recomendaciones y requisitos de Hardware, pero en este ejemplo asignamos al servidor 384 de memoria.

C) Creación Disco duro Virtual nuevo

Escogemos el tipo de almacenamiento de disco duro seleccionamos la opción de Almacenamiento de expansión dinámica para poder arrastrar la capacidad de asignación de Disco duro le damos Next. Este es la ventana en que asignamos la capacidad de Disco duro en la máquina.

D) Terminando con la asignación del tamaño del disco duro y de memoria RAM nos saldrá la ventana lista para seguir con la Instalacion del servidor.

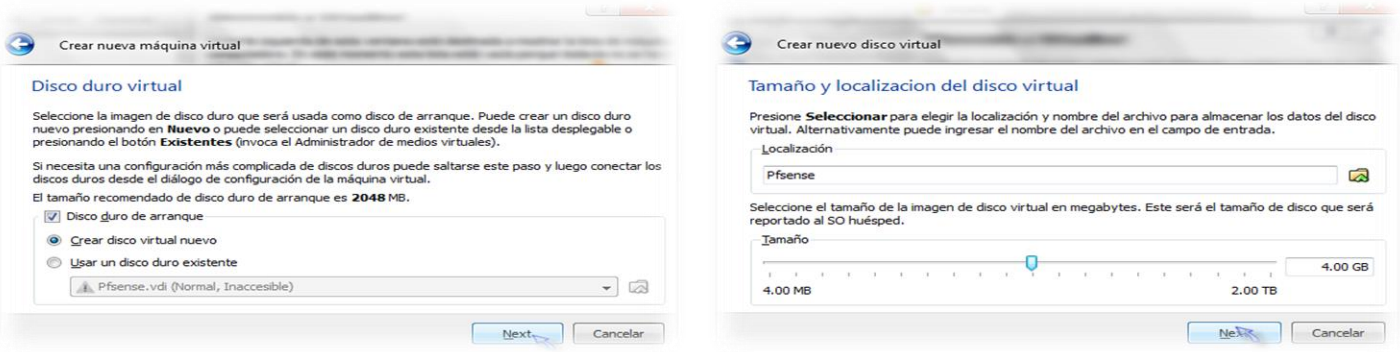


Ilustración 17 Disco Duro Preparación del equipo (Hardware).

Ahora configuramos las tarjetas de red Virtual para que cada tarjeta fisica tenga su respectiva interfaz este dependerá de cada interfaz o adaptador queramos utilizar en el server proxy, ocuparemos tres en este caso adaptador 1, adaptador 2 y adaptador 3

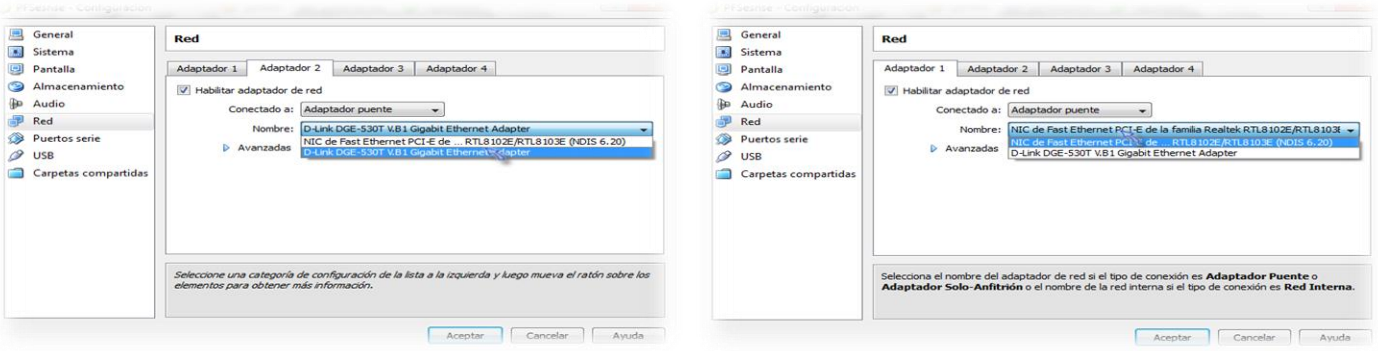


Ilustración 18 Memoria RAM Preparación del equipo (Hardware).

E) Arrancamos el sistema y nos saldrá la pantalla de bienvenida de la instalación del sistema PFSense. Nos aparece una serie de opciones:

1. Boot PFSense (Default) que es la opción que vamos a seleccionar para que pueda cargar el sistema. La cual significa booteo de arranque por defecto PFSense.

2. Boot PFSense with ACPI disabled.(Advanced Configuration and Power Interface) La función de ACPI es permitir al sistema operativo configurar y controlar cada componente de hardware por separado. De este modo, ACPI sustituye tanto a “Plug and Play” como a APM. Asimismo, ACPI proporciona diversos datos sobre la batería, interfaz de red, temperatura y ventilador e informa de acontecimientos en el sistema como “Cerrar la cubierta” o “Baterías poco cargadas”.

3. Boot PFSense in safe mode (Booteo PFSense en modo de prueba).

4. Boot PFSense in single user mode (Booteo PFSense en modo simple de usuario).

5. Boot PFSense with verbose logging.

6. Escape to loader prompt (salirse de la configuración de los comandos internos de la consola).

7. Reboot (Reiniciar el sistema).

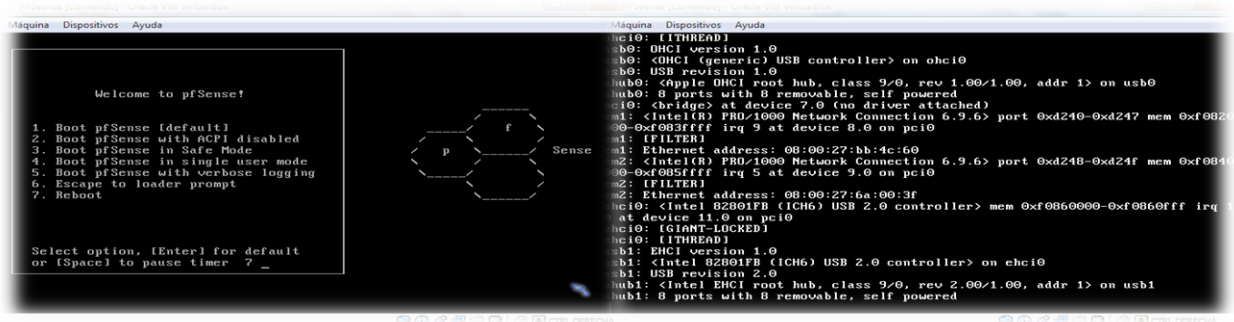


Ilustración 19 Instalación de Software PFSense

El sistema comienza a cargarse para entrar en modo de configuración. La siguiente ventana nos mostrara dos opciones: Presionar R para recuperar en modo anterior. Presionar "I" para Instalar el sistema pero en este caso no comenzaremos a instalar si no que creamos la interfaces primero en la siguiente pantalla, esperamos los 10 segundos que nos da para hacer la selección. Este es la pantalla de de las tarjetas de red virtual, tenemos tres interfaces en la que anteriormente habías declarado en virtual box ahora es asignar si es LAN o WAN, automáticamente nos detecta el sistema de PFSense tendremos que clasificarlo manualmente. Nos sale el mensaje que si queremos crear Vlan en este caso no lo haremos porque en la red de la BICU solo tenemos Swichts Plano (No configurables o no es de aplicación de administración). Em0 00:00:27:41: zb: 04, em1 00:00:27: bb: 4c:60, em2 00:00:27:6a:00:3f. Em0 le asignamos como WAN y em1 como LAN y la otra interfaz lo dejaremos como LAN. Ahora le damos que si "Y" para continuar con el proceso y el sistema comenzara en cargarse.

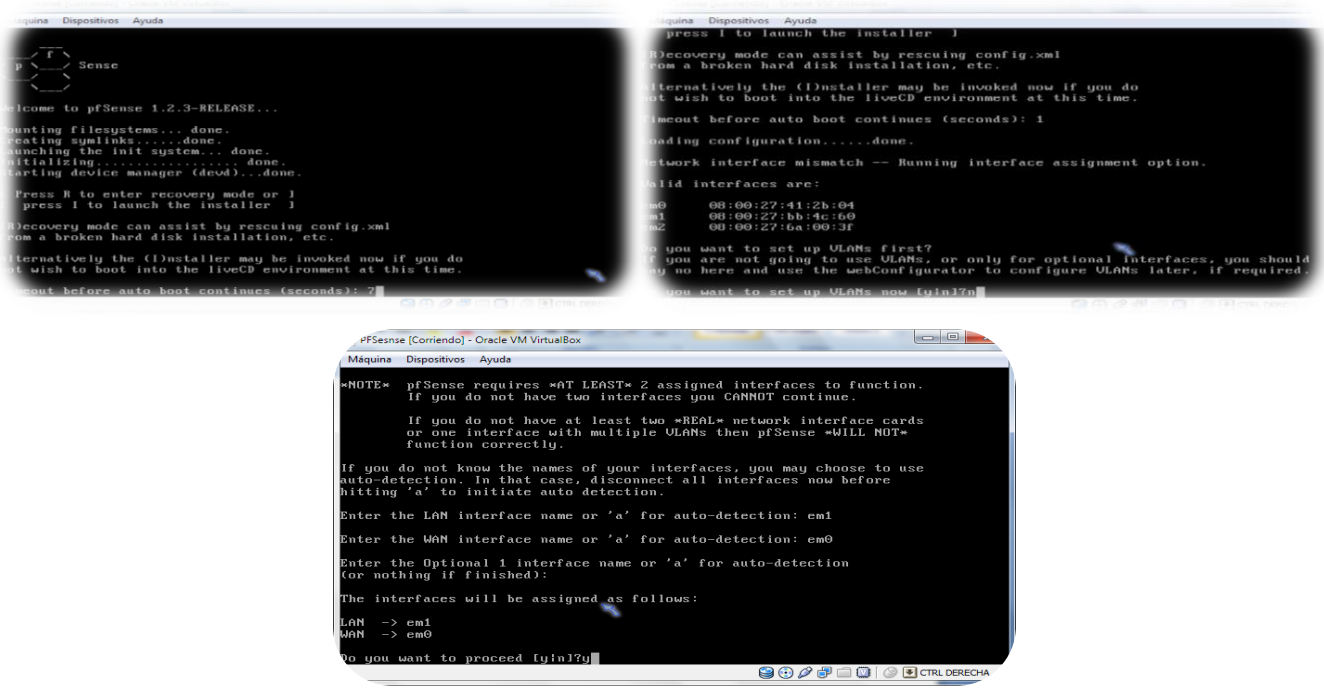


Ilustración 20 Instalación de Software Preparación Tarjeta de Red Virtual

b) Instalación y Configuración Menú PFSense

Estés es la pantalla de **consola** del servidor proxy de **PFsense** pero todavía no hemos instalado el sistema, pero como vemos en pantalla las interfaces que creamos anteriormente la tercera interfas lo levantaremos pero en la siguiente configuraciones o mas adelante, ahora vamos definir cada una de las opciones que hace cada una en la consola:

*** Bienvenidos a pfSense-1.2.3 de pfSense pfSense ***
LAN -> em1 -> 192.168.1.1
WAN -> em0 -> 0.0.0.0(DHCP)
pfSense configuración de la consola
****

0) **Cerrar sesión SSH** (solamente)
1) **Asignar interfaces**: Esto reiniciara la tarea de asignacion de interfaz, puede crear interfaces VLAN, reasignar las interfaces existentes, o asignar nuevos.
2) **Establecer la dirección IP LAN**: Esta opcion se puede utilizar de la manera obvia, para establecer la direccion IP de la LAN, pero tambien hay

algunas otras tareas utiles que suceden al restablecer la IP de la LAN. Para empezar, cuando esta se establece, tambien tienes la opcion de convertir DHCP encendido o apagado, y establecer el rango DHCP IP.
3) **Reiniciar contraseña webConfigurator**: Esta opcion se restablecera el nombre de usuario y contrasena WebGUI de nuevo a **admin** y **pfSense**,respectivamente.
4) **Restablecer los valores predeterminados de fábrica**: Esto restaurara la configuracion del sistema a los valores predeterminados de fabrica. Tenga en cuenta que esto no sera, sin embargo, realizar ningun cambio en el sistema de archivos o los paquetes instalados en el sistema operativo.
5) Reiniciar el sistema: Esto limpia el apagado del sistema de PFSense y reiniciar el sistema operativo
6) Sistema de Parada: Esto limpia apagar el sistema y, o bien fuera de detener o de energía, dependiendo en el hardware apoyo. No se recomienda para sacar siempre el enchufe de un sistema en funcionamiento, incluso incrustados sistemas.
7) Ping Host(Nombre de la direccion de la web o servidor): Solicita una dirección IP, incluyendo el numero de paquetes recibidos, los numeros de secuencia, los tiempos de respuesta, y el porcentaje de perdida de paquetes
8) Shell: Inicia un shell de linea de comandos. Muy útil, y muy potente, pero tambien tiene el potencial de ser muy peligroso.
9) PFtop: PFtop le da una visión en tiempo real de los estados de firewall, y la cantidad de datos que han enviado y recibidos. Puede ayudar a identificar las direcciones IP y las sesiones, de momento están usando el ancho de banda, y también puede ayudar a diagnosticar otros problemas de conexión de red.
10) Filtro de Registros: Utilizando la opción de filtro Registros, podrás ver ninguna de las entradas de registro de filtro aparece en tiempo real, en su forma cruda.
11) Reiniciar webConfigurator: Reiniciar el **WebConfigurator** se reiniciara el proceso del sistema que ejecuta el **WebGUI**.
12) pfSense desarrolladores Shell: La cascara de desarrolladores, que solía ser conocido como el pfSense shell PHP, es una herramienta muy poderosa que le permite ejecutar codigo PHP en el contexto del sistema en ejecucion. Al igual que con la consola normal, tambien puede ser muy peligroso utilizar, y facil para que las cosas van mal. Este es utilizado principalmente por los desarrolladores y los usuarios experimentados que estan intimamente familiarizado con PHP y pfSense la codigo base.
13) Actualización de la consola: Con esta opción, se puede actualizar mediante la introducción de una direccion URL completa a una imagen del firmware pfSense, o una ruta de acceso completa locales de una imagen cargada de alguna otra manera.
14) Desactivar Secure Shell (sshd): Esta opción le permitira cambiar el estado del dominio de Secure Shell, sshd.
99) Mover el archivo de configuración de dispositivo extraíble: Si desea mantener la configuración del sistema de almacenamiento extraible, como una memoria USB unidad, esta opcion se puede utilizar para trasladar el archivo de configuracion.

F)

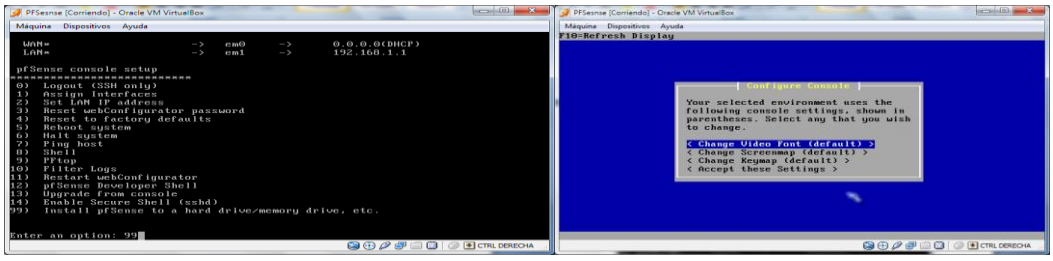


Ilustración 21 Instalación y Configuración Menú PFSense

Comenzamos a Instalar el sistema de PFsense pero para eso le damos la ultima selección de menu **99.** Nos saldra la pantalla de **Configure console** en esta pantalla escogemos la opcion **Accept these settings** para que acepte la configuracion anterior que le hicimos al server.En este paso la opción que seleccionaremos es Quick/Easy Install un modo facil de Instalacion. Esta ventana es la selección de los procesos que le vamos a dar al equipo en este caso la tarea que va realizar el servidor es multiproceso(Symetric multiproccesing kernnel) ya que hará varios procesos en la

red no solo conexión hacia internet si no como un sin número de procesos que actuara como Router. El sistema comienza a Reiniciar y dentro el proceso de Reinicio nos aparecerá la cuenta de usuario que crea por defecto el sistema la cual es “Admin” y como Password “PFSense” esto nos permitira seguir con la configuracion mediante WebConfigurator que es la web de configuracion.

Ilustración 22 Consola Instalación Multiproceso

c) Configuración PC Cliente WIFI y WebConfigurator

Estamos en el modo cliente del equipo en la que actuara si el servidor dará las respectivas configuraciones hacia el internet mediante la dirección IP privada que le asignamos como LAN al equipo.

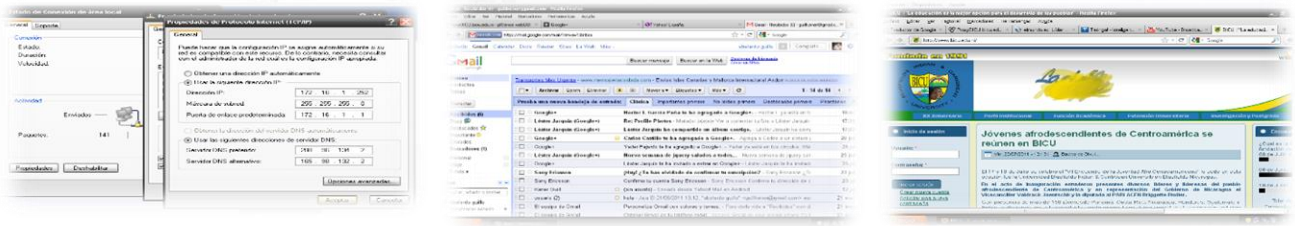


Ilustración 23 Configuración PC Cliente WIFI y WebConfigurator

Podemos visualizar que en la configuracion del Portal atravez WebConfigurator se hace sus respectivas configuraciones basicas (DNS, Nombre Host, Puerta de Enlace, Zona Horaria, las Interfaces etc…)

Ilustración 24 Configuración WIFI y WebConfigurator

5.1.2 Ordenamiento de los Mecanismos de Seguridad Inalámbrica Realizadas.

- Mecanismo 1: Squid Server
- Mecanismo 2: SquidGuard Sever
- Mecanismo 3: Clamv Server Antivirus
- Mecanismo 4: Firewall (ACL)
- Mecanismo 5: Portal cautivo (Radius)
- Mecanismo 6: BandwidthD (QoS)
- Mecanismo 7: LightSquid Reports.

Mecanismo 1: Squid Sever

Objetivo General

- Aplicar la configuración de Squid Server en PFSense.

Objetivo Especifico

- Instalar el repositorio Squid Server para cacheo de Páginas y filtrar direcciones web.

Introducción

Evaluaremos sus mecanismos atravez de su configuración fácil atravez de Web WebConfigurator. Squid Sever es un proxy caché para el soporte Web HTTP, HTTPS, FTP y mucho más. Se reduce el ancho de banda y mejora los tiempos de respuesta por el almacenamiento en caché y la reutilización de las páginas web solicitadas con frecuencia. Squid tiene extensos controles de acceso y hace un gran acelerador de servidor. Se ejecuta en la mayoría de los sistemas operativos disponibles, incluyendo Windows y está disponible bajo la GNU GPL.

Instalación Squid Sever

Squid 2.7.9_4.1 la versión estable como Proxy Cache pero para eso tenemos que ir primero en System-Packages-Squid en la parte de la derecha hay como un signo "+" le damos aceptar

Cuando le damos aceptar para que agregue el paquete en el sistema nos saldrá un mensaje que si queremos agregar el repositorio dentro del sistema le damos **Aceptar.**

Ilustración 25 Instalación Squid Sever Mecanismos de Seguridad

Configuración de Squid Sever.

Ya terminado el proceso de instalación nos vamos a la opción Services y nos debe aparecer el proxy instalado. En la Opción Proxy Server crear restricciones en el servidor. Elegimos la Interfaz con la que el Proxy server tendrá efecto para trabajar en este caso escogemos la Interfaz LAN y activamos la casilla TransparentProxy. Agregamos la dirección o la Ruta donde se guardara los registros del Proxy cache /var/Squid/logs mas con el puerto agregado 3128, dejamos por defecto el localhost en la parte de Visible Hostname.En la parte administrator email podemos agregar el correo del administrador del servidor "christeenlopez@hotmail.com,guillkener@yahoo.es". Seleccionamos el Idioma Spanish para que cuando hay error le muestre en pantalla en español el mensaje de error.

Ilustración 26 Configuración de Squid Sever

Activación Proxy Cache.

Ahora para activar el cache del Proxy nos vamos a la pestaña Cache Mgmt. En la parte Hard disk cache size por defecto 150 lo dejamos con esa cantidad. Hard disk cache System lo dejamos como UFS que es el formato viejo de Squid, en Hard disk cache location lo dejamos en la misma dirección /var/squid/cache, en Memory cache size lo dejamos con la cantidad de memoria cache que queramos ponerle en este caso son 256.

Ilustración 27 Activación Proxy Cache.

Mecanismos seguridad con Listas de Acceso o Restricciones en el server Proxy.

Configuración de Restricción(ACL) en esta parte haremos todos los pasos de restricciones a los sitios web mediante Squid y Squid Guard para bloqueo de dominios, bloqueos de autentificaciones, bloqueos por dirección IP, bloqueo por expresiones, bloqueo por tamaños de archivos durante este paso abordaremos todas las restricciones que se le puede hacer en el servidor.

- ***Denegación de Sitios Web***

La primera restricción será por denegar por sitios web para eso entramos a services-proxy server- en la pestaña Acces control o acceso de control, rellenamos la casilla Allowed subnets y agregamos la dirección de red que será afecta con el proxy en este caso es 172.16.1.0/24(mascara) y en la casilla Unrestricted IPs agregamos la dirección o el rango de dirección que será afecta el en la red 172.16.1.253

Ilustración 28 Denegación de Sitios Web

- ***Denegación de páginas con Blacklist***

Ahora nos movemos en la parte inferior buscamos la casilla Blacklist (Introduzca cada dominio de destino en una nueva línea que se bloqueará a los usuarios que tienen permiso para usar el proxy.

Pondremos un ejemplo de una página web que todavía hay acceso hacia ella luego lo bloquearemos en la casilla **Blacklist** http://www.playboy.com. Volvemos a cargar la página de pornografía y nos presentara un error en la que no se puede cargar el sitio web solicitada eso podemos hacer con diversos sitios web en la que el usuario de la institución no debe entrar a visitar.

Ilustración 29 Denegación de páginas WEB con Blacklist

- ***Denegación de páginas Web con TrafficMigmt***

Ahora vamos a hacer una restricción en la que va hacer primordial el peso de descargar de una página. Para realizar dicha restricción vamos a la pestaña TrafficMigmt y en el parámetro Máximum download size especificamos la cantidad máximo peso de descarga de la página en kilobytes, en este ejemplo colocamos 15 kilobytes y guardamos los cambios. Pero primero comprobaremos con una página que pase la cantidad de peso en este caso www.softonic.com es una web que tiene un peso de más 15 kilobytes pero si comprobamos antes que sea haya hecho la configuración tenemos conexión todavía. Ahora vemos que ya no está en línea por lo que ya aplicamos la configuración de peso en la configuración anterior Máximum download size con 15 kilobytes. Lo guardamos y en la siguiente pantalla ya nos cargara la página estará bloqueada.

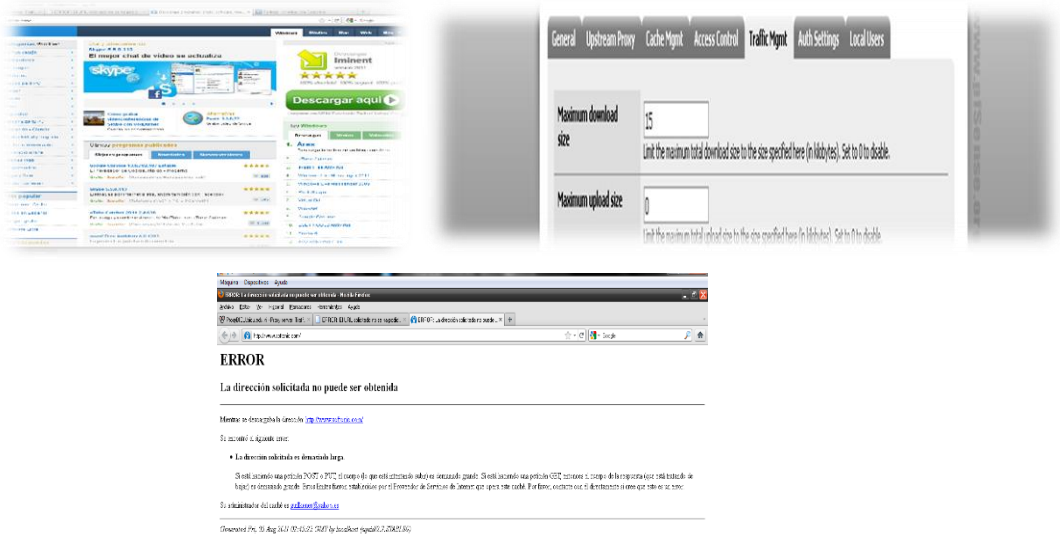


Ilustración 30 Denegación de páginas Web con TrafficMigmt

❖ ***Denegación de páginas web por autentificación Internet Laboratorios Informáticos WIFI.***

Vamos a crear una restricción que cuando un usuario de la red LAN quiera navegar en internet deba autenticarse contra el servidor proxy. La autenticación con el proxy no sirve si tenemos habilitado proxy transparente. Para poder crear la restricción de autenticación vamos a la pestaña General, le quitamos el check de la casilla del parámetro Transparent Proxy y guardamos los cambios. A crear la restricción para navegar a internet con autenticación en el proxy, para ello nos dirigimos a la pestaña Auth Settings y en el parámetro Authentication method vamos a seleccionar Local. Esto quiere decir que el método de autenticación va hacer local y guardamos los cambios. Luego vamos a crear los usuarios locales que se van a autenticar en el servidor proxy, para ello vamos a la pestaña Local Users y dentro de dicha pestaña vamos y damos clic en el cuadrito con el signo "+" para agregar un usuario local. Llenamos los parámetros correspondientes para crear el usuario y luego guardamos para que los cambios se apliquen. En este ejemplo el usuario es "lab2" y Password es "123".

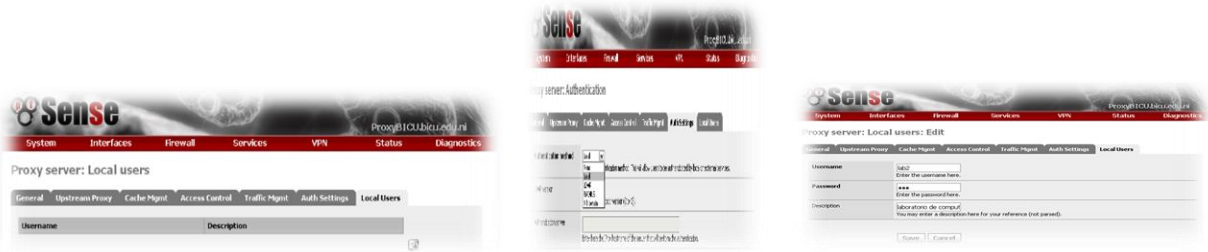
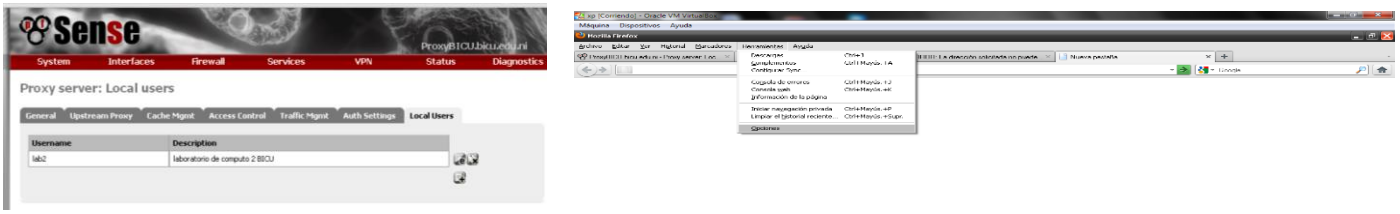


Ilustración 31 Denegación de páginas web por autentificación Internet Laboratorios Informáticos WIFI.

Aquí como lo muestra la imagen siguiente se ve el usuario creado correctamente. Si queremos añadir más usuarios repetimos los dos anteriores pasos y listo.



Ahora desde el equipo que está dentro de la red LAN, abrimos el navegador y vamos a configurar en el navegador el proxy, ya que recuerden que el proxy no está trabajando como trasparente. Para configurar el proxy en el navegador y realizar la prueba vamos a Herramienta-opciones-Avanzado-Red-configuración. No va a parecer una imagen como la que se muestra a continuación, seleccionamos la opción Configuración manual del proxy y en el parámetro Proxy HTTP ingresamos la dirección Ip y el puerto por donde escucha las peticiones del servidor proxy, seleccionamos la casilla opción Usar el mismo proxy para todo y le damos un check y aceptar. Cerramos el navegador y lo volvemos a abrir e ingresamos a una página en internet y nos debe aparecer un cuadro solicitando usuario y contraseña para navegar en internet en este caso es usuario "lab2" contraseña "123".

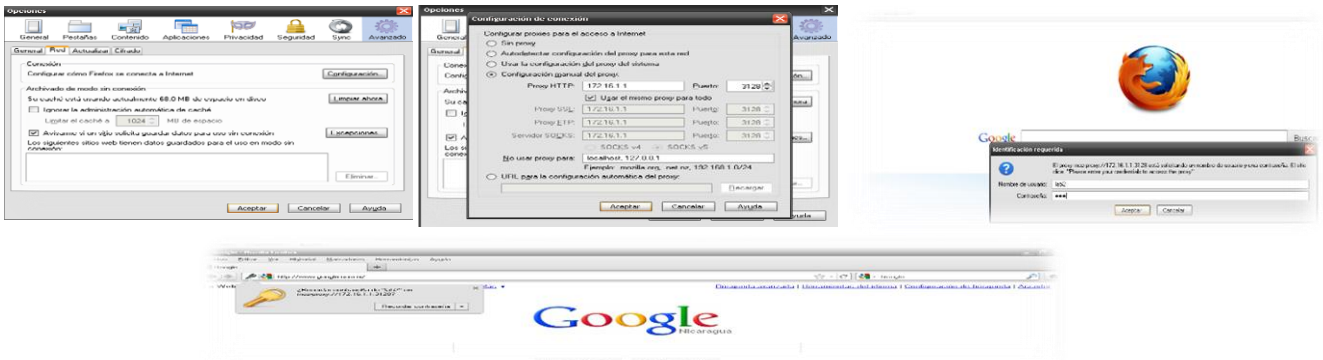


Ilustración 32 Denegación de páginas web por autentificación Internet Laboratorios Informáticos WIFI.

- ***Denegación de páginas web por Bloqueo de Dirección IP.***

Crear restricción por dirección IP. Para hacer dicha restricción en el PFSense nos dirigimos a la pestaña Access control y en el parámetro Banned host addresses colocamos la Ip del host a restringir la navegación y guardamos para que se aplique los cambios. Esto se hará cuando el usuario tiene conflicto de IP se podrá deshabilitar el acceso a internet por un tiempo establecido por el administrador para que dicha configuración Ip no le cause problema al usuario en la red. Listamos su configuración IP y verificamos que la IP si corresponda con la dirección IP que se le va a aplicar la restricción.Ahora abrimos el navegador e intentamos ingresar a una página cualquiera en internet y veremos que no tenemos conexión a internet por la Ip restringida al equipo.

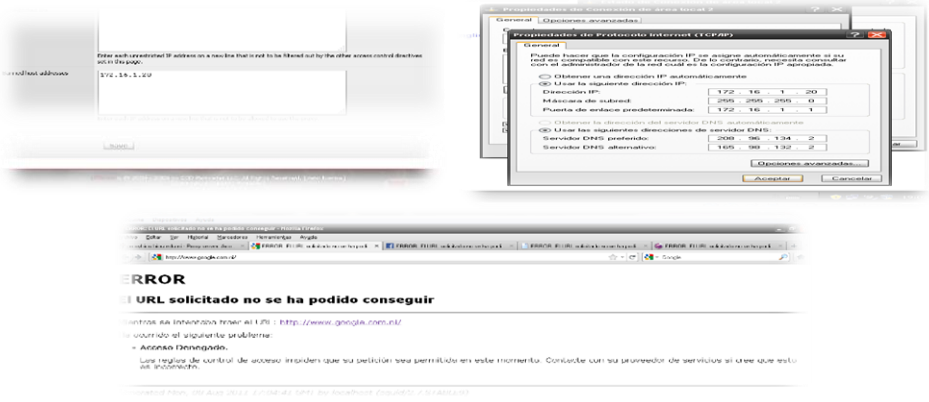


Ilustración 33 Denegación de páginas web por Bloqueo de Dirección IP.

Mecanismo 2: SquidGuard

Objetivo General

- Aplicar la configuración de Squid Guard en PFSense.

Objetivo Especifico

- Instalar el repositorio Squid Guard para Filtrado de Páginas.
- Crear políticas de acceso a páginas web.

Introducción

Desarrollaremos cada filtración de las páginas web de acceso través de las políticas de acceso que requiera la institución. Filtrado de URL es un método de bloquear el acceso a ciertos sitios web basados en la dirección web. Hay varios productos comerciales disponibles para URL o el filtrado de contenido, pero en realidad se puede establecer un sistema muy robusto por su cuenta utilizando SquidGuard y PFSense. SquidGuard es un plugin muy útil para el servidor proxy Squid popular que se puede utilizar para bloquear o redirigir las peticiones web en la red. SquidGuard tiene una larga lista de características que se pueden personalizar para satisfacer sus necesidades. También es muy rápido y no ralentizar el acceso a Internet para los usuarios.

Instalación SquidGuard

Instalación del complemento Squidguard para el servidor proxy Squidguard (Es un redirector de dirección URL utilizada para el uso de listas negras con los proxy software Squid, para ello nos vamos a la pestaña System del PFSense y seleccionamos Packages. Buscamos el complemento o paquete y al frente aparece un cuadrito con un signo "+", damos clic sobre él para instalar. Ya realizado el paso anterior nos va a aparecer el proceso de instalación y esperamos a que termine. Luego de que termine la instalación vamos a la pestaña Services y nos debe de aparecer el nombre proxy filter. Si aparece dicho nombre es porque el Squidguard instalo correctamente y damos doble clic sobre dicho nombre.

Dentro del Proxy Filter para que el Squidguard empiece a funcionar vamos al parámetro Enable y al frente nos va a aparecer un cuadrito para generar un check, generamos el check y damos clic en Apply. Nos saldrá el mensaje que Squidguard está iniciado.

Ilustración 34 Instalación SquidGuard

Mecanismos seguridad con por Dominios SquidGuard.

- ***Denegación de Sitios Web por Categorías para Bloqueo de Dominios.***

Para generar restricciones dentro del Squidguard primero vamos a la pestaña Target categorías para crear una nueva categoría. Para agregar la categoría debemos dar clic sobre el cuadrito con el signo "+". Le asignamos un nombre a la categoría y vamos al parámetro Domain List y añadimos los dominios que queremos restringir. En este caso como prueba son los dominios facebook.com y Wikipedia.org y damos clic en guardar. Luego vamos a crear una regla de grupo para aplicársela a la categoría creada en el paso anterior, para ello nos dirigimos a la pestaña Groups ACL y damos clic sobre el cuadrito que tiene un signo "+". Los parámetros a básicos a configurar son: ((Name: Asignamos un nombre para la ACL. Client (origen): dirección ip del equipo al cual le vamos a aplicar la ACL. Si queremos aplicársela a una red completa colocamos el ID de red con su respectiva mascara)). Target Rules: damos clic sobre el símbolo > que aparece en color verde y buscamos la categoría creada anteriormente con el nombre que le asignamos en las opciones que aparecen al frente de la categoría que son Access colocamos deny, esto va a denegarlos dominio que queremos restringir. Guardamos los cambios.

Ilustración 35 Denegación de Sitios Web por Categorías

Ya está creada la ACL que me va a denegar lo dominios especificados en la categoría Paginas. Ahora vamos hacia el equipo que está dentro de la red para realizar las pruebas de los dominios. Abrimos el navegador e ingresamos a los dominios denegados anteriormente. En este ejemplo denegamos facebook.com y wikipedia.org.

Ilustración 36 Denegación de Sitios Web por Categorías para Bloqueo de Dominios

En este paso podremos observar también que el dominio facebook.com también el proxy está denegando la conexión hacia la página web.

❖ ***Denegación de Sitios Web por Expresiones.***

Ahora vamos a restringir con el proxy por **expresiones**. Para realizar las restricciones por expresiones nos dirigimos a la pestaña **Target categories** que se encuentra dentro del paquete **Proxy Filter** y luego damos clic en el cuadrito que contiene la letra "**e**" para editar la categoría que aparece. Ya estando en la **categoría** nos dirigimos al parámetro **Expressions** e ingresamos las **expresiones a bloquear**, en este caso son "**sexo** y **porno**", en el parámetro **Redirect mode** seleccionamos la opción **"in error page enter message"** para poder agregar un mensaje personalizado y el mensaje personalizado se agrega en el parámetro **Redirect**. Las expresiones deben de ir separadas por una **tubería**. Ya cuando tengamos las expresiones añadidas **guardamos.**

Desde la máquina que está en la **red LAN** ingresamos a www.google.com y buscamos las expresiones que se añadieron en el paso anterior las cuales se van a denegar. En la imagen siguiente se muestra ingresando a www.google.com y buscando la expresión **"sexo"** y le damos Enter y veremos que no tiene acceso a buscar esa palabra.

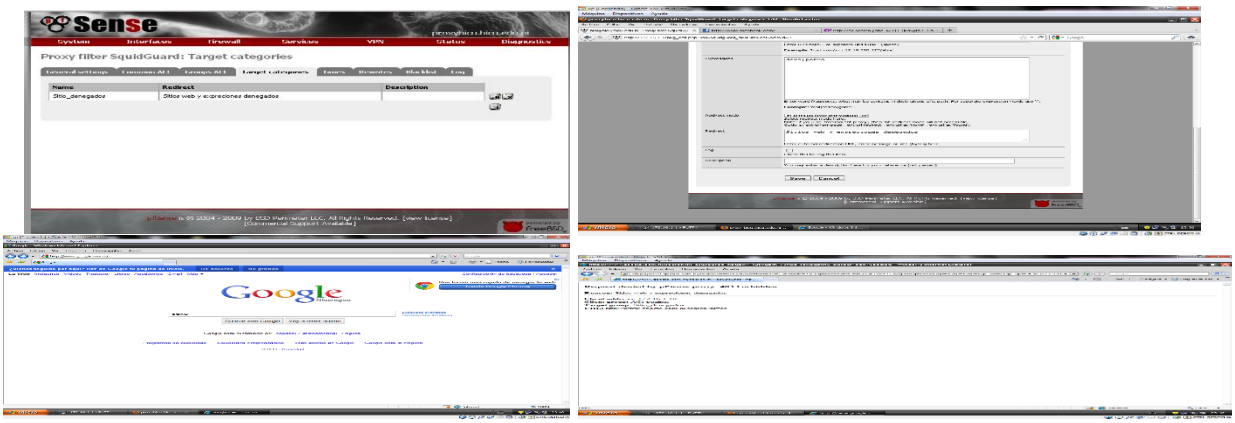


Ilustración 37 Denegación de Sitios Web por Expresiones.

❖ **Denegación Grupos Lista de Control de Acceso (ACL)**

En esta sección se instaló un paquete de lista de Restricciones llamado shallalist que incorpora un conjunto de Restricciones y filtros desde audio, Radio, RSS, Noticias, Videos, Compras, Deportes, Cines etc… en Otros… Para esto descargamos el paquete desde Squid Guard y lo añadimos

Ilustración 38 Denegación Grupos Lista de Control de Acceso (ACL)

Mecanismo 3: Antivirus HAVP Firewall

Objetivo General

- Aplicar la configuración de HAVP Antivirus Firewall en PFSense.

Objetivo Especifico

- Instalar el repositorio HAVP Antivirus Firewall para Escaneo de información malicioso y páginas web contenido de virus de troyano entre otros.

Introducción

Utilizar HAVP con Squid, SquidGuard en beneficio de las ACL de Squid (filtro sólo algunos archivos por ejemplo, exe, bat). Se puede utilizar como havp caché principal de pedido, por lo almacenado en caché Squid no tienen que ser escaneados de nuevo. Pero esto no da mejorar el rendimiento todo el tiempo. Sólo si el Squid tiene el archivo ya está en la memoria caché, será más rápido. De lo contrario, el rendimiento puede caer porque el archivo tiene que pasar havp y Squid. Debe utilizar una CPU rápida si utiliza both. Las desventaja es que en caché infectada ya no es explorado por HAVP.

Instalación HAVP Antivirus Firewall.

Instalar **Antivirus en PFSense** con **HAVP antivirus** para eso Nos vamos en **System**- **Packages-"+"** y buscamos para agregar un repositorio más en **PFSense** como **Proxy server**, para hacer una doble capa de protección a cada usuario en la que tiene uso al servidor proxy pueda ser protegido de amenazas de Virus por la Red. Comenzará la Instalación.

Ilustración 39 Instalación HAVP Antivirus Firewall.

Configuración de Antivirus HAVP.

Al menú **Services**-**Antivirus**-**Settings.** Le indico que **actualice** y que lo siga haciendo cada **24Hrs**. Tras esto, voy a **Http proxy** y configuro el **proxy mode** en **parent for Squid** para relacionarlo con **Squid Server** y no afectarlo que ambos conserve las misma configuración, indico la interface **LAN**, las otras opciones los habilitamos como que escaneo de las imágenes y los streams y que bloquee si hay error al descargar fichero y que logue, puedo definir algún dominio en lista blanca pero en este caso no lo hare solo necesito que me bloqueo de sitio que contenga Virus. Tras esto voy a **General Page** y lanzo el **servicio Http proxy antivirus** y **Antivirus server.** Tras la Finalización de la configuración **HAVP antivirus** quedara los procesos Habilitados

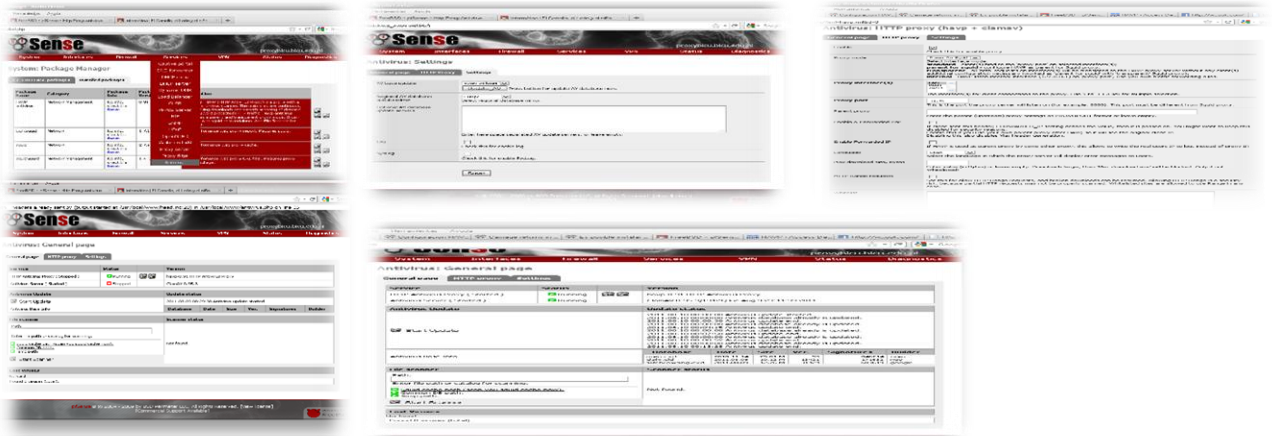


Ilustración 40 Configuración de Antivirus HAVP.

Actualizar la base de Datos del Antivirus atravez de la consola de PFSense.

Luego vamos en la **consola del server** nos conectamos con el **Putty** le damos en la Opción "**8**" que es la parte de configuración de Shell del sistema de PFSense.

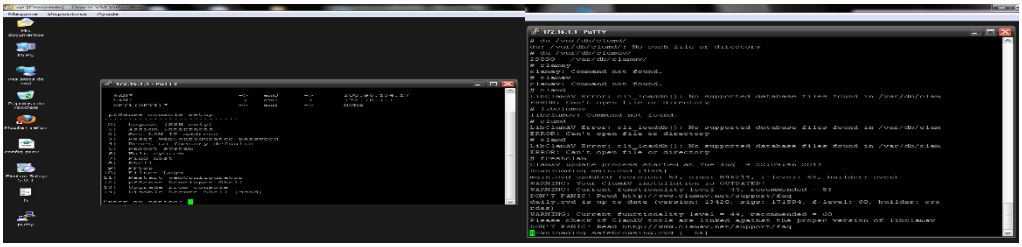


Ilustración 41 Actualizar la base de Datos del Antivirus atravez de la consola de PFSense

Mecanismos seguridad con Antivirus HAVP.

- ***Denegación de Datos Maliciosos con Antivirus HAVP.***

Tecleamos el comando "**freshclam"** para actualizar la base de datos del servidor antivirus. Comenzará descargar las actualizaciones. Después tecleamos el comando "**clamd**" para ver si la base de datos del antivirus se actualizo correctamente. Ahora comprobamos si el servidor antivirus me bloquea las páginas que contengan virus nos dirigimos a esta página que contiene virus http://www.eicar.org/download/eicar.com. Como vemos en pantalla si lo hizo.

Mecanismo 4: Sistema de Autentificación (Radius) de Acceso por Usuario.

Objetivo General

- Aplicar la configuración de Autentificación (Radius) en PFSense.

Objetivo Especifico

- Configurar el Portal Cautivo para acceso por usuario inalámbrico por la Red en PFSense.

Introducción

Sistema Portal cautivo es un método de mecanismo de seguridad de acceso que en muchas empresas de negocios y universidades emplean para aplicar técnicas de mejora a su red y tener el control y organización de sus usuarios en la red, privatizando recursos de datos de acceso al que se registre y pueda consumir el servicio de internet. Para emplear este mecanismo PFSense tiene el servicio incorporado de servidor Radius que garantizara el registro de los clientes en este caso los estudiantes de la universidad.

Configuración Portal Cautivo Radius acceso inalámbrico.

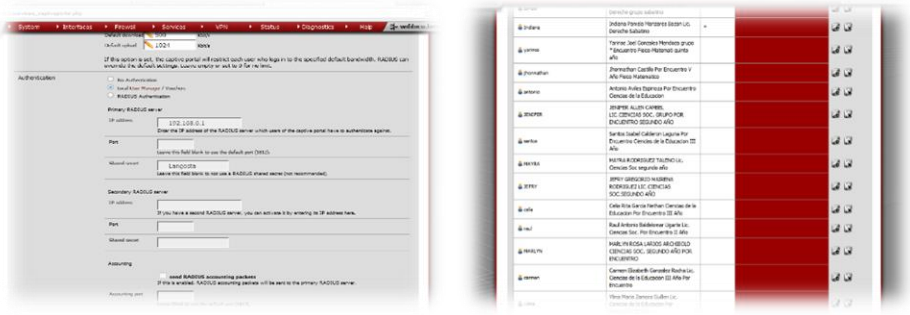


Ilustración 42 Configuración Portal Cautivo Radius acceso inalámbrico.

- ***Denegación de acceso por Portal cautivo (Radius) PFSense.***

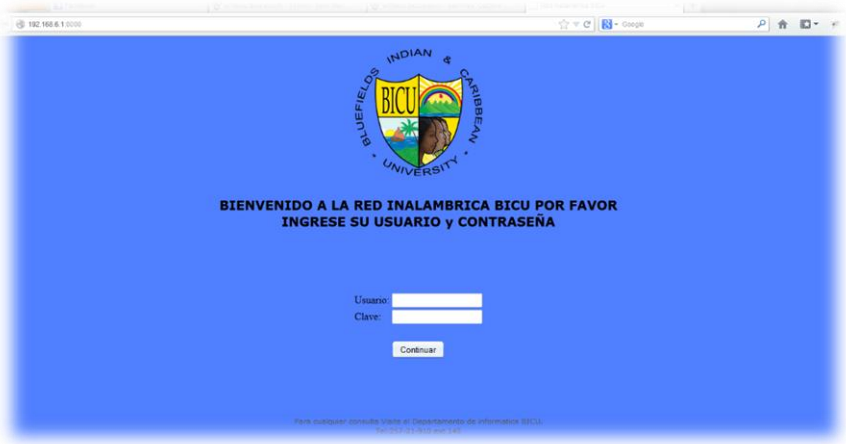


Ilustración 43 Configuración Portal Cautivo Radius acceso inalámbrico.

Mecanismo 5: Activación Firewall con PFSense.

Objetivo General

- Aplicar la configuración Firewall en PFSense.

Objetivo Especifico

- Establecer las reglas de acceso con Firewall PFSense a los protocolos de comunicación en la red.

Introducción

El Firewall permitirá redirigir al servidor que protocolos de acceso tiene el usuario a través de la red inalámbrica o los servicios que tiene acceso, para esto crearnos las reglas o Rules para poder bloquear todo tráfico que no esté contemplado en el servidor Firewall de PFSense.

❖ ***Denegación de protocolos de acceso a través de PFSense Firewall.***

Configuración Firewall para bloqueos de P2P y puertos de Inseguridad.

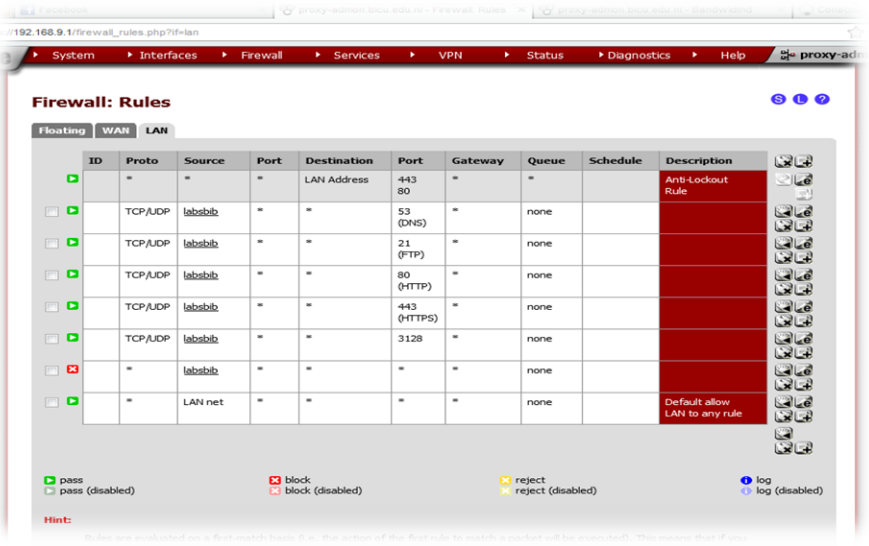


Ilustración 44 Denegación de protocolos de acceso a través de PFSense Firewall.

Mecanismo 6: Sistemas de Monitoreo en tiempo Real por Protocolos de comunicación y páginas web.

Objetivo General

- Aplicar la configuración de sistemas de monitoreo en PFSense.

Objetivo Especifico

- Instalar BandwidthD para monitorear el consumo de ancho de Banda por protocolos de comunicación.
- Instalar LightSquid Reports para ver la lista de páginas web que el usuario visita y así garantizar el administrador de la red un completo auditorio mediante gráficas.
- Configurar RRD sistema de estado Gráficos que determina y visualiza el tráfico por paquetes, sistema (procesador, memoria y rendimiento) y calidad.

Introducción

El sistema de monitoreo en un red es indispensable, porque el administrador de la red necesita visualizar los recursos o paquetes de datos esta a su vez pueden ser por protocolos que saturen la conectividad de red, el monitoreo garantizara al administrador tener un buen control de su recurso de ancho de banda dirigido a la red inalámbrica.

Instalación BandwidthD monitoreo de ancho de Banda.

En este paso vamos Instalar **BandwidthD** para monitorear el uso del ancho de banda de cada equipo en la red. Pero para eso nos vamos **System**-**Packages**- **BandwidthD**. Comenzará la descarga y la Instalación.

Ilustración 45 Instalación BandwidthD monitoreo de ancho de Banda.

Configuración BandwidthD.

Ahora nos vamos a la pestaña **Services**-**BandwidthD** en la ventana principal comenzamos configurar los parámetros de opciones. En la opción **Interfaces** seleccionamos cual es la interfaz que va ser monitoreado por defecto dejamos en la interfaz **LAN** como ejemplo. En la opción **Subnet** agregamos la dirección IP a la sub red que va ser monitoreada por la aplicación de **BandwidthD** "**172.16.1.0/24**", habilitamos la opción **promiscuous** y guardamos. Nos vamos en la pestaña **Access BandwidthD** y nos muestra la tabla de consumo de ancho de banda por secciones de protocolo de **HTTP, VPN**, **P2P**, **TCP**, **UDP**, **ICMP** cada una uno representa un color único para diferenciar y medir con exactitud el nivel de consumo en cualquier protocolo usado en la red por un equipo "**X**". Se muestra una tabla de barra dependiendo el consumo del equipo "**X**" se mostrara con su respectivo color, los informes gráficos de consumo son representados por día, semana, mes y año. Como se muestra en pantalla lo clasifica la sub-red o por el Subnet.

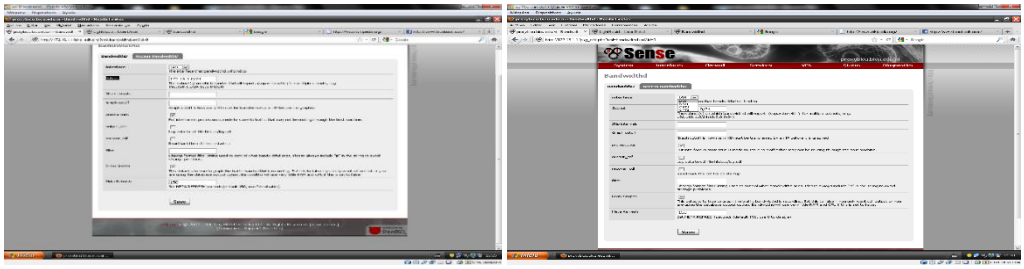


Ilustración 46 Configuración BandwidthD.

- ***Mecanismo Seguridad de Sistema de Monitoreo BandwidthD.***

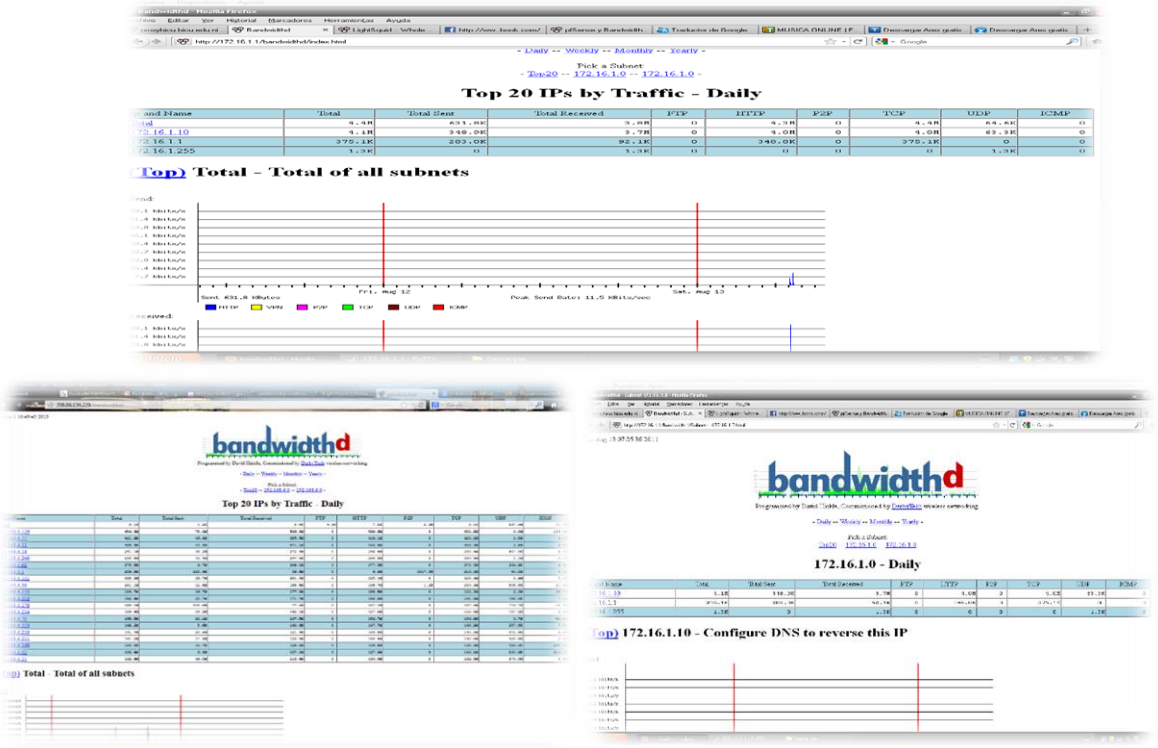


Ilustración 47 Mecanismo Seguridad de Sistema de Monitoreo BandwidthD.

❖ ***Mecanismo Seguridad con LightSquid Reports para monitoreo de páginas que visita el usuario.***

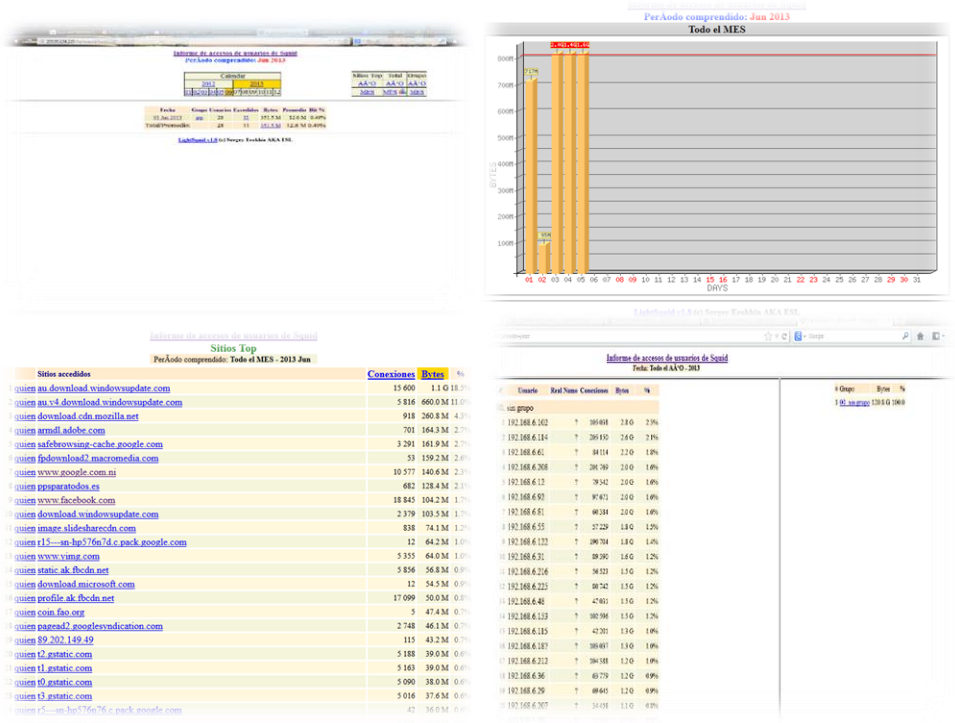


Ilustración 48 Mecanismo Seguridad con LightSquid Reports para monitoreo de páginas que visita el usuario

❖ ***Mecanismo Seguridad con RRD sistema de estado Gráficos para monitoreo en tiempo real, visualiza el tráfico por paquetes, sistema (procesador, memoria y rendimiento) y calidad.***

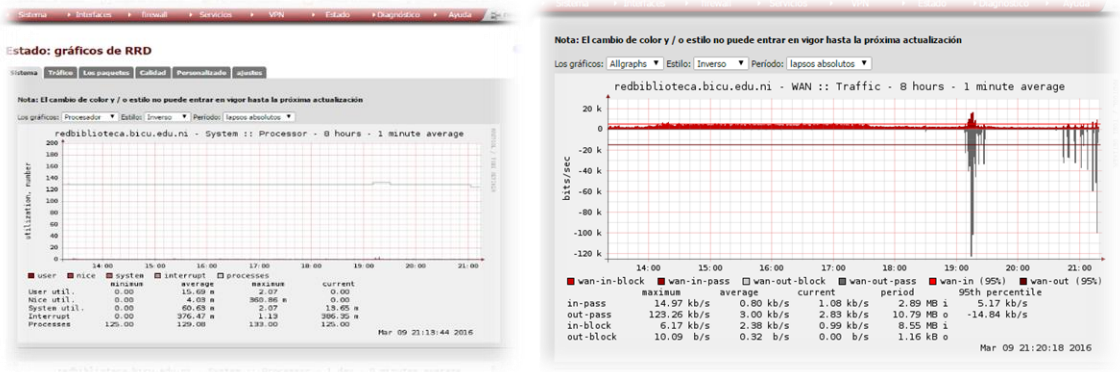


Ilustración 49 Mecanismo Seguridad con RRD sistema de estado Gráficos para monitoreo en tiempo real.

Capítulo 6: Conclusiones

6.1 Conclusiones

Con la finalización de este trabajo tesis se logró cumplir con los objetivos propuestos, llegando a las siguientes conclusiones:

1. La facilitación de información teórica acerca de los mecanismos de seguridad Inalámbrica y los métodos que se utiliza con Herramientas de Software Libre le proporciona a los investigadores y estudiantes un gran apoyo sus conocimientos.

2. Los diseños de presentación de los mecanismos de seguridad facilitara a los estudiantes e investigadores una correcta compresión de las técnicas a ocupar en la seguridad inalámbrica.

3. Cada secuencia de los mecanismos de seguridad Inalámbrica está organizado con sus procesos y objetivos de alcance para soluciones viables.

4. Se han abordado temas relacionados con Mecanismos de Seguridad Inalámbrica para contribuir conocimientos y emplear a redes pequeñas, medianas y grandes para su desarrollo.

6.2 Recomendaciones

Las recomendaciones que se describen a continuación son a base de abarcar más técnicas seguridad Inalámbrica ocupando herramientas de Software para una futura implementación para la universidad BICU.

1. Se ha intentado que los temas presentados en este proyecto de investigación estén basados a solucionar de manera evolutiva y actualizada los métodos de seguridad más óptimas y viables para las redes inalámbricas en las instituciones pequeñas, medianas y grandes.

2. Para mayor administración y explotación con la Herramienta PFSense es recomendable manejar tecnología QOS (Quality Of Service, Cualidad de Servicio), esto permitirá regular el flujo de ancho de banda para aplicaciones de internet como programas de descargas, Voz, Video, audio etc. Se podrá lograr un Balanceo de carga más adecuada en la asignación de ancho de banda por estación de trabajo o por grupos de dirección IP en la Red LAN.

3. Implementar técnicas de Virtualización de Datos en la nube con Proxmox (KVM y OpenVZ) a los servidores de la Red, mejorando sus servicios de centro de datos con buena administración de sus recursos.

4. Proponer servicio VPN ocupando PFSense como recurso viable a la unificación de una red virtual a sus sistemas contables y administrativos.

Bibliografía

[1] N. Arellano, «Seguridad en la Red,» 15 Mayo 2012. [En línea]. Available: http://seguridadenlasredescomputacionales.blogspot.com/. [Último acceso: 5 Agosto 2015].

[2] L. C. Escola, «Blog Historia de la Informatica,» 2 Diciembre 2010. [En línea]. Available: http://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/. [Último acceso: 7 Agosto 2015].

[3] S. Potoy, «tianguisvirtual,» 19 Noviembre 2012. [En línea]. Available: http://www.tianguisvirtual.net/index.php/27-instalacion-y-configuracion-de-servidores-linux. [Último acceso: 7 Agosto 2015].

[4] S. Microsoft, «Microsoft,» 3 1 2005. [En línea]. Available: https://msdn.microsoft.com/es-es/library/cc784756(v=ws.10).aspx. [Último acceso: 5 2 2016].

[5] «blogspot,» 17 Mayo 2012. [En línea]. Available: http://lasinformaticas2012.blogspot.com/2012/05/los-avances-tecnologicos-redes.html. [Último acceso: 15 Agosto 2015].

[6] T. V. V. D. Leon, *Vulnerabilidades y Niveles de seguridad de Redes WIFI,* Guatemala, 2010.

[7] Wikipedia, «Wikipedia,» 23 2 2010. [En línea]. Available: http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29. [Último acceso: 2016 1 4].

[8] W. Stalligs y L. Brown, Computer Security Principles and Practice, United States of America: Pearson Education, 2012.

[9] M. Goodrich y R. Tamassia, Introduction to Computer Security, United States of America: Pearson Education, 2014.

[10] C. M. B. y. P. Jim, «La guía definitiva para el Abierto de pfSense,» de *Pfsense*, Portugal, Copyright © 2009 Christopher M. Buechler, 2009, p. 690.