SOLUCIONES OPEN SOURCE PARA SEGURIDAD PERIMETRAL DE EMPRESAS PYMES

OPEN SOURCE SOLUTIONS FOR PERIMETER SAFETY FOR SMALL BUSINESSES

Aguilar Mallea Carlos Christian[1]

[1]Docente de la Facultad de Ciencias Integradas de Bermejo – Universidad Autónoma "Juan Misael Saracho"
Trabajo de investigación realizado para obtener el grado de Master en Informática

Dirección de correspondencia: Av. Petrolera S/N Bermejo-Tarija-Bolivia
Correo electrónico: christianaguilar89@gmail.com

RESUMEN

Las vulnerabilidades de seguridad a las que están expuestas las empresas pymes(Pequeña y medianas empresas), con una conexión directa a internet le permiten a personas inescrupulosas y con fines específicos robar información o dañarla, o no se centraliza la información vital de la empresa la cual es almacenada en cada una de las estaciones de trabajo; aunque se ve un acelerado crecimiento de las empresas pymes,la organización y planeación de estas se hace desordenada, descuidando sectores importantes en materia de seguridad de sus aplicaciones y sistemas de información, adicionalmente las pymes no cuentan con una infraestructura para soportar una solución de seguridad por considerarla costosa.

Tomando en consideración las dificultades mencionadas, se hace necesario que las empresas tomen conciencia de estos riesgos y mantengan una actitud preventiva, así como establecer un control de sus sistemas mediante evaluaciones periódicas, dando indicadores que permitan conocer el grado de exposición a sufrir ataques informáticos, y de esta manera, instaurar las medidas técnicas necesarias para proteger sus sistemas adecuadamente.

Esta solución propuesta está dirigida a las empresas pyme, dándole a conocer en primera instancia los potenciales riesgos a los que está expuesta y ofreciéndole las opciones de seguridad informática sin pagos de licencias, utilizados actualmente como base en la fabricación de sistemas de seguridad perimetral.

Palabras clave: Seguridad, Firewall, Redes, Sistema de Detección de Intrusos, Vulnerabilidades.

ABSTRACT

Security vulnerabilities to SMEs with a direct connection to the Internet allow unscrupulous and specific people to steal information or damage it, or it does not centralize the vital information of the company which is stored in each one of them. The workstations; Although it is seen an accelerated growth of SME companies, the organization and planning of these becomes disorderly, neglecting important sectors in the security of their applications and information systems, in addition SMEs do not have the infrastructure to support a security solution Considering it expensive.

Taking these advantages into account, a more detailed investigation makes it necessary for companies to be aware of these risks and to maintain a preventive attitude, as well as to establish a control of their systems through periodic evaluations, giving indicators that allow to know the degree of Exposure to computer attacks, and in this way, put in place the necessary technical measures to protect their systems properly.

This proposed solution is aimed at small and medium-sized enterprises, making them aware in the first instance of the potential risks to which they are exposed and offering them the computer security options without license payments, currently used as a basis in the manufacture of perimeter security systems.

Key words: Security, Firewall, Networking, Intrusion Detection System, Vulnerabilities.

INTRODUCCIÓN

Desde su invención hasta nuestros días, los ordenadores y las redes de datos se han consolidado en la vida cotidiana de las personas y las empresas en una gran variedad de actividades.

La red ARPANET, creada por el gobierno estadounidense como medio de comunicación para los diferentes organismos del país, sería la precursora de la que hoy conocemos como INTERNET. En aquel entorno, la seguridad era mínima. Se trataba de una red compuesta por una pequeña comunidad cuyos miembros eran de confianza.(Diego González Gómez, 2003).

Por el contrario, las redes globales sí requieren un mayor nivel de seguridad. Manejan notablesvolúmenes de información, atendiendo de forma independiente operaciones de distintos países que en muchas ocasiones intercambian datos privados. Es común hoy en día ver en las noticias que empresas de gran renombre reciben algún tipo de ataque con diversos fines, desde detener sus servicios hasta obtener algún tipo de información confidencial.

Con la posibilidad de interconectar múltiples ordenadores formando redes, surgieron nuevos y aplicaciones(HindTribak, 2012). Hoy en día los bancos hacen uso de redes para efectuar sus operaciones financieras, las empresas tienen almacenada información de sus clientes en bases de datos, y muchos comercios están presentes en Internet, de forma que cualquier usuario puede realizar una transacción desde cualquier lugar con acceso a la red de internet. Por tanto, la seguridad de la información de este tipo de empresas es de mucha importancia.

En la actualidad las violaciones de la Seguridad de la Información se han convertido en algo cotidiano. Ya no son solamente las grandes empresas objeto de ataque de hackers e intrusos con intensiones maliciosas, sino que dondequiera que exista una información vital o de determinado interés, existe la posibilidad latente de un ataque.

El término de detección de intrusiones es aplicable a distintas actividades. Existen alarmas de ladrones, o cámaras de vigilancia usadas por bancos o comercios. Todas tienen funciones de vigilancia, alarma y emiten alarmas cuando un determinado suceso tiene lugar. Pero en el área de informática para nosotros La detección de intrusiones es el proceso de monitorizar los eventos que ocurren en un sistema o red, para analizarlos en busca de problemas de seguridad.

MARCO TEÓRICO

Introducción seguridad informática. Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella, como bitnet o hepnet, por otra el auge de la informática de consumo unido a factores menos técnicos iba produciendo un aumento espectacular en el número de piratas informáticos. Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso worm o gusano de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días, y las pérdidas se estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses la agencia darpa (DefenseAdvancedResearchProjects Agency) creó el cert (ComputerEmergency Response Team), un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet.(Antonio Villalón Huerta, 2002).

Han pasado muchos años desde la creación del primer cert, y cada día se hace patente la preocupación por los temas relativos a la seguridad en la red y sus equipos, y también se hace patente la necesidad de esta seguridad. Si hace unos años cualquiera que quisiera adentrarse en el mundo underground casi no tenía más remedio que conectar a alguna BBS donde se tratara el tema, generalmente con una cantidad de información muy limitada, hoy en día tiene a su disposición gigabytes de información electrónica publicada en Internet. (Antonio Villalón Huerta, 2002).

Seguridad. Se puede entender como seguridad una característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros. (Antonio Villalón Huerta, 2002).

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. Algunos estudios integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta última en sólo las dos facetas restantes, confidencialidad e integridad.(Antonio Villalón Huerta, 2002).

La confidencialidad explica que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

Generalmente tienen que existir los tres aspectos descritos para que haya seguridad: un sistema Unix puede conseguir confidencialidad para un determinado fichero haciendo que ningún usuario (ni siquiera el root) pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna. Dependiendo del entorno en que un sistema Unix trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de backup) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. (Juan David Gutiérrez, 2006).

Seguridad perimetral. La seguridad perimetral basa su filosofía en la protección de todo el sistema informático de una empresa desde "fuera", es decir, componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. (Nuria Rabadán, 2008).

Esto implica que cada paquete de tráfico transmitido debe de ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para las redes propias.

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. (Antonio Villalon Huerta, 2002).

Hardware. Es el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes, entre otros) o tarjetas de red. (Antonio Villalon Huerta, 2002).

Software. Es el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones. (Antonio Villalon Huerta, 2002).

Datos. Es el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. (Antonio Villalon Huerta, 2002). Los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar4.

Tipos de ataques. En los sistemas de información existen dos tipos básicos de ataques los internos y los externos.- Los tipos de ataque externos se producen por virus, ataques de hackers, explotación de vulnerabilidades del sistema. (Alvaro Gómez Vieites, 2014).

Los problemas relacionados con ataques externos no son demasiado conocidos por los administradores de sistemas, sobre todo en las Pyme, cuando se habla con el responsable de una Pyme o con el responsable de informática de una Pyme sobre los problemas relacionados con Hackers y otros problemas de seguridad, la respuesta es casi siempre la misma al suponer que no tienen nada en el sistema que pueda interesar a nadie. Este es el más común de los errores en la seguridad. (DubánMauricio Melo, 2015).

- Los internos se producen por empleados descontentos y consisten en robos o borrados de información del sistema, sabotaje, etc.

Uno de los problemas menos tratado en las empresas es la seguridad interna, normalmente los responsables de seguridad de las empresas se limitan a establecer una serie de criterios para prevenir estos problemas basados en la creación de carpetas o discos con acceso restringido y claves de usuario.(DubánMauricio Melo, 2015).

Virus. Un virus es una secuencia de código que se inserta en un fichero ejecutable denominado host, de forma que al ejecutar el programa también se ejecuta el virus; generalmente esta ejecución implica la copia del código viral – o una modificación del mismo – en otros programas. El virus necesita obligatoriamente un programa donde insertarse para poderse ejecutar, por lo que no se puede considerar un programa o proceso independiente. (Antonio Villalón Huerta, 2002).

Gusanos. El término gusano, acuñado en 1975 en la obra de ciencia ficción de John Brunner TheShockwaveRider hace referencia a programas capaces de viajar por sí mismos a través de redes de computadores para realizar cualquier actividad una vez alcanzada una máquina; aunque esta actividad no tiene por qué entrañar peligro, los gusanos pueden instalar en el sistema alcanzado un virus, atacar a este sistema como haría un intruso, o simplemente consumir excesivas cantidades de ancho de banda en la red afectada. Aunque se trata de malware muchísimo menos habitual que por ejemplo los virus o las puertas traseras, ya que escribir un gusano peligroso es una tarea muy difícil, los gusanos son una de las amenazas que potencialmente puede causar mayores daños(Antonio Villalón Huerta, 2002).

UTM. Gestión Unificada de Amenazas o (UnifiedThreat Management). Las soluciones UTM, son dispositivos de red que se encargan de proteger las redes de amenazas. Son considerados la evolución de un firewall tradicional, ya que incluye productos de seguridad que permiten el desempeño de múltiples funcionalidades de servicios de seguridad en un solo dispositivo. (Yamil Casas-Moreno, 2009).

Estos servicios de seguridad generalmente incluyen: Firewall, Detección y Prevención de Intrusos, Antivirus y Antispyware de red, VPN, Proxy, Control de Contenido, Balanceo de Cargas, QoS y Reportes.

Los dispositivos UTM permiten que las amenazas se gestionen desde consolas centralizadas, que permiten que todas las soluciones de seguridad puedan ser controladas y configuradas.(Hassan Berrio, 2011).

Las soluciones UTM integran funcionalidades de administración, monitoreo, y capacidades de hacer más eficiente la implementación y mantenimiento del equipo. (Hassan Berrio, 2011).

Las principales características de una solución UTM son:

- Reducción de costos: Solución de seguridad única.
- Simplicidad: Evita la instalación de múltiples plataformas de control.
- Fácil administración: GUI basada en interfaces web para fácil manejo.
- Desempeño: Protección sin degradar el desempeño de la red.

Las soluciones UTM incluyen las siguientes opciones:

- Firewall
- MultiWAN
- Proxy web
- Control de Contenido

Firewall o cortafuego. Un firewall o cortafuego es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes. Se puede definir un cortafuego como cualquier sistema (desde un simple router hasta varias redes en serie) utilizado para separar – en cuanto a seguridad se refiere – una máquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad. El espacio protegido, denominado perímetro de seguridad, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa, no confiable, llamada zona de riesgo. (Luis Villalta Márquez, 2013).

Máquina o host bastion. También se denominan gates. Se conoce a un sistema especialmente asegurado, pero en principio vulnerable a todo tipo de ataques por estar abierto a Internet, que tiene como función ser el punto de contacto de los usuarios de la red interna de una organización con otro tipo de redes. El host bastión filtra tráfico de entrada y salida, y también esconde la configuración de la red hacia afuera. (Raul Moreno, 2001).

Filtrado de paquetes. Por filtrado de paquetes se entiende la acción de denegar o permitir el flujo de tramas entre dos redes (por ejemplo, la interna, protegida con el firewall, y el resto de Internet) de acuerdo a unas normas predefinidas; aunque el filtro más elemental puede ser un simple router, trabajando en el nivel de red del protocolo OSI, esta actividad puede realizarse además en un puente o en una máquina individual. El filtrado también se conoce como screening, y a los dispositivos que lo implementan se les denomina chokes; el choke puede ser la máquina bastión o un elemento diferente. Antonio Villalon Huerta, 2002).

Proxy. Un proxy es un programa (trabajando en el nivel de aplicación de OSI) que permite o niega el acceso a una aplicación determinada entre dos redes. Los clientes proxy se comunican sólo con los servidores proxy, que autorizan las peticiones y las envían a los servidores reales, o las deniegan y las devuelven a quien las solicitó. Desde el punto de vista lógico, en el cortafuego, suelen existir servidores proxy para las aplicaciones que han de

atravesar el sistema, y que se sitúan habitualmente en el host bastión. (Allende, Sebastián, 2014).

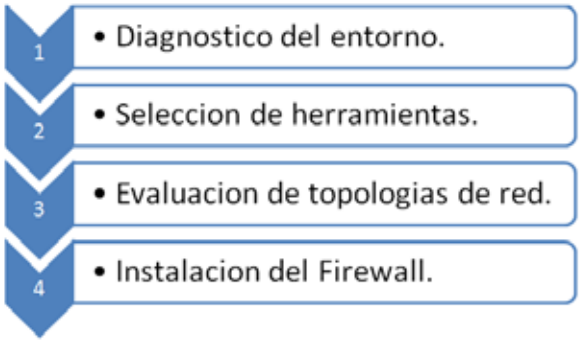
También se implementa en el choke un mecanismo de filtrado de paquetes, y en alguno de los dos elementos se suele situar otro mecanismo para poder monitorizar y detectar la actividad sospechosa.

Sistema de Detección de Intrusos. El diccionario Webster define una intrusión como "el acto de entrar en un lugar sin invitación." Cuando hablamos de la intrusión de detección, nos estamos refiriendo al acto de la detección de una intrusión no autorizada en una computadora de una red. Este acceso no autorizado, o la intrusión, es un intento de comprometer, o de otra manera hacer daño a los dispositivos de la red. (Allende, Sebastián, 2014).

La detección de intrusos es el proceso de monitorización de eventos que suceden en un sistema informático o red y el análisis de dichos eventos en busca de signos de intrusiones. Estos sistemas están continuamente supervisando los componentes de la red y las personas o intrusos que están intentando entrar ilegalmente en ella, describiendo las actividades o procesos que realizan individuos o sistemas no autorizados sobre elementos de la red. (Julio Gomez Lopez, 2009).

METODOLOGÍA

Para poder llegar a realizar una implementación de esta índole, se tienen que realizar una serie de pasos en los cuales se tuvieron que hacer hincapié en puntos relevantes, el mismo esta detallado de la siguiente manera:



Diagnostico del entorno, inicialmente se realizan estudios, del entorno en el cual se encuentran actualmente la empresas a la cual se quiere implantar este sistema de seguridad perimetral, para saber las falencias y bondades que el mismo presenta.

Selección de herramientas, luego de evaluar el estado actual de la empresa se deberá realizar una selección de las posibles distribuciones a implementar de acuerdo a las necesidades de la compañía y los alcances de cada una, posteriormente se realiza un análisis con herramientas forenses para detectar las vulnerabilidades de la red, con estos resultados se le da a conocer al personal del área de sistemas las ventajas de un dispositivo de seguridad perimetral; protegiendo tanto de las vulnerabilidades internas como externas.

Evaluación de topologías de red, se hará un análisis de las topologías de red, y el tipo de clase de la misma, lo cual nos dará un panorama más claro de que topología es la más adecuada para realizar la implantación de dicho sistema.

Instalacion del firewall, teniendo en claro el entorno actual y habiendo seleccionado tanto nuestras herramientas a utilizar como la topologías de red para el sistema de seguridad perimetral, se procede a realizar la instalación del firewall, haciendo notar sus características y módulos importantes que se podrían implementar a futuro.

Teniendo presente que para concretar la propuesta inicialmente se realizó una investigación la cual permitió obtener datos sobre la infraestructura de red que generalmente usan las pymes, con el propósito de abordar la implementación apropiada para la solución informática y reducir costos de implementación.

ANÁLISIS Y DISEÑO

Topología de red. Una vez están claros los objetivos que debe cumplir en este artículo, se debe real un análisis exhaustivo para diseñar la solución más adecuada.

Del análisis de objetivos se extrae, que, entre otras, dos conclusiones muy claras:

- El esquema de direccionamiento de red debe ser escalable.
- Se debe dividir la red en subredes, de manera que los servidores e impresoras estén en una red distinta a las estaciones de trabajo, para poder filtrar y monitorizar el acceso según convenga.

Es la única manera de implementar una solución que permita ampliar la capacidad de conexión en un gran número de equipos y poder tener una identificación de las comunicaciones.

Para lo mismo, se tiene que usar un sistema de direccionamiento privado, con direcciones de clase B (de una dirección de 4 octetos, 2 identifican la red y 2 identifican el host). Esto va reportar múltiples ventajas:

- Se pueden asignar 65534(2^{16}-2) direcciones de host por subred, con lo que se elimina totalmente el problema del número de direcciones (pasando de 254 a 65534).

- El hecho de disponer de más direcciones, hace que se pueda hacer una división lógica de los equipos, organizándolos por IP. Por ejemplo, si se usa la subred 172.20.0.0/16, se puede utilizar las direcciones que van de 172.20.10.1 a la 172.20.10.255 para identificar un grupo determinado (por ejemplo, el área de créditos de una entidad financiera), que es diferente a las direcciones que van desde 172.20.15.1 a la 172.20.15.255. A nivel de red, están en la misma subred (es decir, no se necesita ningún router para comunicarlas) ya nivel organizativo facilita mucho la creación de reglas y la identificación.

- Al tratarse de direcciones de red privadas, la topología de red queda escondida detrás del firewall, lo que aumenta la seguridad del sistema.

En cuanto a las redes, se utilizará el diseño clásico de firewall, de 4 subredes:

- Red WAN, o acceso al exterior, en este caso se trata del enlace del proveedor de Internet y para ejemplificar en la siguiente imagen vamos a poner la red 147.83.51.0/24.

- Red LAN, o red local, donde estarán todas las estaciones de trabajo de los usuarios, Se utilizará como se ha comentado, direccionamiento IP clase B, concretamente la red 172.16.0.0/16(hasta 65534 equipos).

- Red DMZ, la red desmilitarizada. Se trata de la red donde se instalan los servidores y servicios comunes (impresoras, faxes, fotocopiadoras, etc.). Se tiene un acceso muy restringido, así se garantiza que la zona está segura. En este caso se utilizará la red 172.18.0.0/16 (lo que permite la conexión hasta 65534 equipos).

- Red WLAN, la red inalámbrica. Red bajo autenticación donde se conectarán las estaciones de trabajo portátiles, PDA y teléfonos. Las redes inalámbricas se suelen considerar como redes no confiables y los permisos que se aplican suelen ser muy limitados. Como no es previsible dar acceso a demasiados equipos se escogerá para este ejemplo un direccionamiento clase C (hasta 254 equipos), concretamente 192.168.101.0/24.

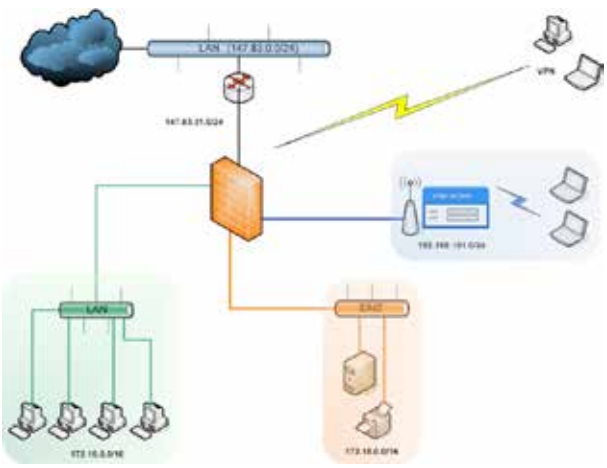


Figura 1. Diseño de infraestructura de red.

Además de división en redes se ha añadido un enlace remoto vía VPN para definir la estructura completa.

Esta topología permite, además, la utilización de más de un enlace WAN que daría redundancia a la conectividad y permitiría un balanceo de carga para aprovechar todos los enlaces.

Firewall. Software. La estructura central de todo diseño es el firewall, concretamente lo que se conoce como firewall de red. Un firewall de red es un dispositivo que actúa en la capa de red del modelo OSI. Estrictamente se trata de un dispositivo que enruta paquetes entre redes, como un router. A diferencia de un router, el firewall enruta paquetes en base a unas reglas definidas por el administrador.

Generalmente las reglas que definen el comportamiento de un firewall están basadas en características del paquete de red, como el protocolo de capa superior que contiene, direcciones IP de origen o destino, puertos TCP o UDP (lo que generalmente define que define ese tráfico), etc.

Además, los firewalls modernos son capaces de identificar trafico propiedades relativas o capas superiores, como por ejemplo el sistema operativo que lo ha generado (Windows, Linux, etc.), o el tipo de aplicación que lo está usando (aplicaciones de voz sobre IP, aplicaciones de trafico P2P, streaming de audio y video, etc.). Y también permiten la aplicación de reglas en función de un horario determinado.

Así pues, es sencillo definir una regla que, por ejemplo, solo permita el tráfico de streaming de video de ciertas emisoras de televisión definidas, fuera del horario laboral.

Uniendo todas las definiciones de todo el tipo de propiedades del tráfico, se pueden definir reglas muy complejas, que establezcan exactamente el tipo de comportamiento que se desea para la red.

En cuanto al conjunto de reglas definidas en un firewall, se definen y se aplican a nivel de interfaz de red (hay un conjunto de reglas para cada interfaz). El firewall enrutara todos los paquetes que entren en su interior, las reglas solo definirán que paquetes entran o no dentro del firewall.

Las reglas se ejecutan por orden ascendente, de manera que cuando un paquete cumple todas las condiciones de la regla, se establece la acción que la regla defina (permitir o no permitir) y no se revisan las siguientes reglas. Además de las acciones definidas, los firewalls también permiten registrar la acción realizada (lo que se conoce como escribir un LOG o LOGUEAR). Esto es muy útil para mantener registros de los sucesos y para identificar acciones no permitidas o estadísticas de tráfico.

Existen dos políticas aplicables al funcionamiento de un firewall, aceptar por defecto y denegar por defecto. Las reglas se ejecutan secuencialmente y cuando se llega al final de las reglas, el firewall decide qué hacer con el paquete en función de la política por defecto. Generalmente, los firewalls que se ponen en explotación por defecto en fases de desarrollo y optimización de las reglas, para después de estar bien definidas y verificadas (con lo que pocos paquetes usan la regla por defecto) se establece la denegación.

En cuanto a la arquitectura del equipo, existen dos tipos de firewalls de red:

- Firewalls hardware, que son aquellos equipos diseñados específicamente para realizar funciones de enrutado y filtrado de paquetes y para establecer comunicaciones VPN. Generalmente se usan para unir sedes de grandes infraestructuras, a través de redes públicas. Suelen tener un rendimiento y un coste elevados. Cisco Systems es una de las empresas más importantes que comercializan estos productos.

- Firewalls software, que son aquellos programas o sistemas operativos que se ejecutan en un equipo estándar, para realizar las funciones de un firewall. Su coste es muy inferior al de los firewalls hardware y a su vez permiten más flexibilidad. Pero generalmente requieren de una complejidad mayor, sobre todo en la fase de implementación. En cuanto a firewalls software, existe una multitud de productos, tanto implementados con software libre, como propietarios.

Para la solución propuesta se instalará un firewall por software, por motivos especialmente de coste y flexibilidad.

Una vez diseñada la topología de red y teniendo presentes los objetivos a cumplir, hay que escoger que opción de software se va a utilizar. Buscando por Internet, se encuentra muchas opciones que, a priori, cumplan los objetivos funcionales, pero cuando se investigan a fondo, muchas de eslla dejan de ser opciones claras, y bien sea por falta de funciones, o por coste.

Después de una elección inicial basada en hojas de especificaciones, webs de los productos, etc. se han probado 4 opciones para escoger el software final a utilizar, seguidamente mostraremos un resumen de las comparaciones realizadas:

Tabla 1. Comparación de firewalls parte 1.

NOMBRE	IDS	CONTROLADOR DE DOMINIO
Endian Firewall	SI, no posee opciones avanzadas de configuración.	No
pfSense	Opciones avanzadas de configuración, fácil manejo.	No
Sphirewall	SI, no posee opciones avanzadas de configuración.	Si
Zentyal (formerly eBox Plataforma)	SI, no posee opciones avanzadas de configuración.	Si, reemplazo 100% de Windows Server, puede ser administrado desde estación de trabajo Windows con las herramientas de Microsoft.

Tabla 2. Comparación de firewalls parte 2.

NOMBRE	DESCRIPCION	VPN IPSEC
Endian Firewall	Distribución Utm con firewall, anti-spam and anti-virus for web, FTP and e-mail, OpenVPN, IPsec, hotspot functionality, y portal cautivo. Endian Firewall Community (EFW) es una versión x86. El anti-virus para EFW es Sophos or ClamAV. Ids snort.	AES 256
pfSense	Distribución para firewall, router, DHCP server, Gateway, OpenVPN, IPsec, proxy and anti-virus (Snort).	AES 256
Sphirewall	Directa hook into Linux kernel packet stream, LDAP and user-based autenticación, user quotas, QOS, advanced analíticas, IDS, utilidades web, basado en distribución debian	3DES
Zentyal (formerly eBox Plataforma)	Zentyal es una distribución open-source router/firewall y small business server, hasta su versión 4.0 tenía soporte de firewall, vpn, IDS. En la última versión 4.1 solo soporte de correo, controlador de dominio, mensajería, firewall básico	3DES

Tabla 3. Comparación de firewalls parte 3.

NOMBRE	PROXY	INFORMES	DESEMPEÑO
Endian Firewall	limitaciones en filtro de contenido, por perfiles, las credenciales no pueden ser obtenidas de base externa	los Informes son muy básicos, es necesario instalar herramientas adicionales para interpretar la información	Al no instalarse entorno grafico se aprovechan los recursos, necesarios 8GB en RAM y procesador Intel core i5
pfSense	avanzado, las credenciales de los usuarios puedes ser obtenidas desde un controlador de dominio o servidor radius	Presenta gran variedad de informes y herramientas de análisis por tipos de servicio, los paquetes puedes ser instalados directamente desde la consola web	Al no instalarse entorno grafico se aprovechan los recursos, necesarios 8GB en RAM y procesador Intel core i5
Sphirewall	avanzado, las credenciales de los usuarios puedes ser obtenidas desde un controlador de dominio o servidor radius	los Informes son muy básicos, es necesario instalar herramientas adicionales para interpretar la información	se instala entorno gráfico, necesarios 8GB en RAM y procesador Intel core i7
Zentyal (formerly eBox Plataforma)	avanzado, las credenciales de los usuarios puedes ser obtenidas desde un controlador de dominio o servidor radius	los Informes son muy básicos, es necesario instalar herramientas adicionales para interpretar la información	se instala entorno gráfico, necesarios 16GB en RAM y procesador Intel core i7

Elección final. Luego de haber visto las características de 4 opciones implementar la solución propuesta, se hizo énfasis en dos de ellas por ser las que más se adecuan a nuestros objetivos, por lo tanto, pasamos hacer un detalle sus ventajas y desventajas de estos 2 firewalls:

ENDIAN FIREWALL

Ventajas:

- Bastante intuitivo para la configuración.
- No es muy pesado.
- Logs bastante claros.
- Interface cómoda a través de navegador.
- Las funciones de firewall, routing y nat las hace bien.

Desventajas:

- Soporte penoso si no se paga (desconozco cómo es si se paga).
- Foro sin aportes del equipo del proyecto.
- La configuración en consola tiene un largo periodo de aprendizaje dado que está basado en ficheros templates. que a través de cgi-bin desde el navegador se copian a los ficheros de configuración. NO hay documentación de cómo funciona.
- Solamente puede haber 4 interfaces (rojo, verde, azul y naranja) incluso instalando en una máquina física.
- Snort inline no funciona. Por mucho que te empeñes solamente alerta pero no corta.

PFSENSE

Ventajas:

- Interfaz intuitiva
- Configuración sencilla una vez que te has familiarizado con el interfaz, en un par de horas con el producto
- Foro con bastante información, aunque un poco antigua en algunos casos
- En el foro contestan técnicos del proyecto.
- Paquetes instalados del repositorio bajo demanda
- Sistema operativo FreeBSD.
- Funciona Snort inline y corta.

Desventajas:

- Documentación penosa.
- Hay 2 libros en el mercado. Uno de la versión 1.xx que está obsoleto en concordancia con el interfaz de la 2 y otro de la 2 que es un simple recorrido por las pantallas sin explicar nada. Ambos andan por los 40 euros en Amazon. No recomiendo ninguno de los 2.
- Configuración en consola respetando las configuraciones de los paquetes estándares.
- Muchas "cositas" ocultas que están desveladas en el foro en inglés.

Una vez se han evaluado los sistemas hay que tomar una decisión del sistema a implementar. Como las pruebas no se han realizado en un entorno real con una carga de trabajo ni una configuración real, se realizará una preselección del sistema en función de los criterios hasta ahora conocidos. Si después de hacer las pruebas en entorno real los resultados no son satisfactorios, se deberá volver al punto de elección.

Habiendo visto las especificaciones, reamente el sistema más adecuado es el pfSense.

Figura 2. Logo del firewall pfSense.

Dispone de la posibilidad de implementar todos los objetivos, siendo un software totalmente libre y preparado para sistemas abiertos. Revisando sus requisitos de hardware, se puede comprobar que, al heredar la compatibilidad de FreeBSD, casi cualquier sistema será soportado.

Además, se ha investigado a través de otros usuarios del foro de pfSense la infraestructura montada y no es de prever que el sistema no tenga rendimiento esperado. Así pues, teniendo en cuenta esto, el siguiente paso es seleccionar el hardware para instalar dicho firewall.

Firewall hardware. Con la topología definida y el software seleccionado, se debe realizar la compra de una máquina que sea capaz de engranar en todas las variables del sistema.

La tecnología de red actual en casi todas las Pymes es de Gigabit Ethernet, eso quiere decir que el firewall debe ser capaz de enrutar paquetes a gigabit por segundo. Para ello y para garantizar la durabilidad del sistema, es importante que la maquina a adquirir sea bastante potente en temas de procesador y memoria. En cuanto al disco duro, es poco importante, ya que pfSense ocupa poco espacio. Cualquier disco de tecnología SATA (alto rendimiento para bajo número de accesos, es decir, discos para equipos de usuarios) será adecuado (frente a los discos SCSI, más caros que tiene un alto rendimiento para un numero de accesos moderadamente alto, para servidores multiusuario).

En cuanto al tema físico, es conveniente que sea una maquina robusta. Para protegerla de las incidencias eléctricas (muy frecuentes en las instalaciones de edificios en general), se priorizará el que tenga una fuente de alimentación redundante, para poder conectar a dos fuentes de corrientes distintas (una de ella será un sistema de alimentación ininterrumpida).

En cuanto a la cantidad de tarjetas de red tenemos que tener como mínimo 2 tarjetas una para la LAN y otra para la WAN.

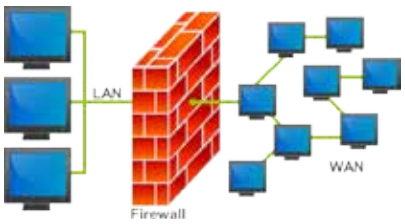


Figura 2. Arquitectura genérica.

Como se puede evidenciar los requisitos de hardware son accesibles en cuestión de costos puesto que el pfSense puede correr en un equipo con características limitadas, pero mucho dependerá del tamaño de la red, las subre-

des que se tenga internamente y el tráfico de datos de nuestra red.

IMPLEMENTACIÓN

Como ya sabemos y vimos en anteriores puntos vamos a implementar el firewall Pfsense en nuestra red propuesta, por lo tanto, vamos a seguir una serie de pasos para realizar dicha instalación. Para este articulo instalare la versión de 32bits en un equipo con 4GB RAM con un procesador Intel dual core y 2 interfaces de red (una para la WAN y otro para la LAN).

Descargamos el ISO desde el URL de pfSense 2.3.1, escogemos arquitectura (para este artículo 32 bits), plataforma (LiveCD con instalador) y damos click a uno de los mirrors para descargarlo.

Figura 3. Página oficial de descarga del Pfsense.

Al descargar el ISO (por lo general es comprimido en gz, por lo que hay que descomprimirlo) generamos un CD o una USB booteable y hacemos boot nos saldrá una opción en la cual dejamos la opción por defecto.

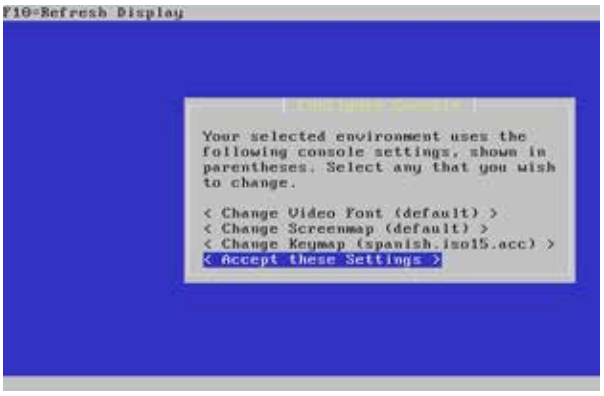


Figura 4. Opciones de instalación del Pfsense

Elegimos la opción de fácil instalación.

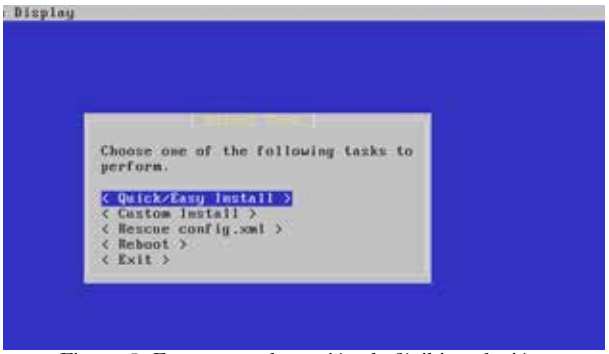


Figura 5. Entramos a la opción de fácil instalación.

Esperamos mientras se instala el Sistema Operativo.

Figura 6. Pfsense copiando paquetes de instalación.

Seleccionamos la configuración del kernel.

Figura 7. Selección tipo de kernel.

Una vez terminado la instalación le damos Reboot para que se reinicie el sistema y podamos entrar a la configuración del pfsense.

Figura 8. Reiniciando el sistema.

configurar el entorno, como se puede ver reconoció las 2 tarjetas de red una para la WAN y la otra para LAN.

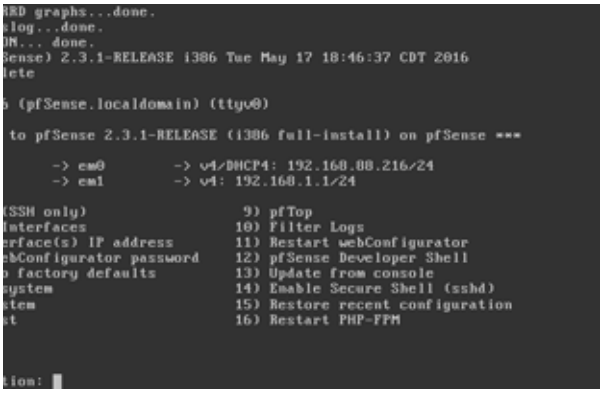


Figura 9. Entorno de configuración del pfsense.

Configuramos nuestra LAN.

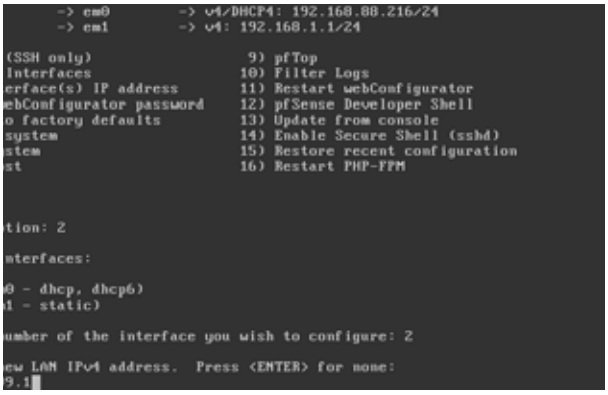


Figura 10. Configuración del a red LAN.

A la configuración DHCP le damos “n”, y al webConfigurator le damos “y”.

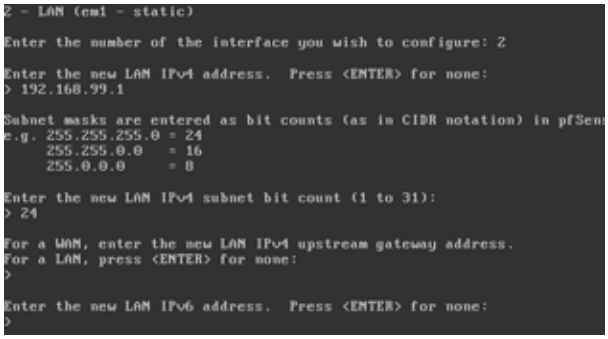


Figura 11. Configuración del a red LAN 2.

Ahora nos tocara configurar la red WAN en la cual tenemos que especificar el Gateway por donde saldremos a internet.

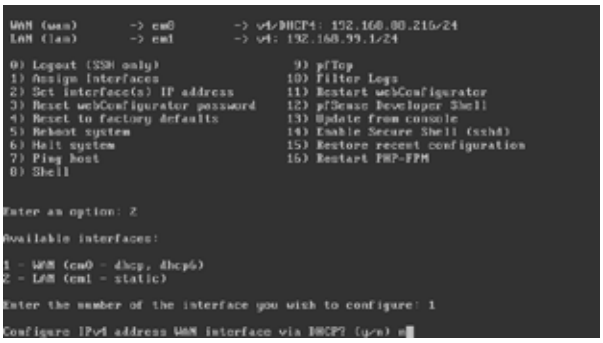


Figura 12. Configuración del a red WAN.

Figura 13. Configuración del a red WAN 2.

De esta manera quedaría toda la configuración del pfsense.

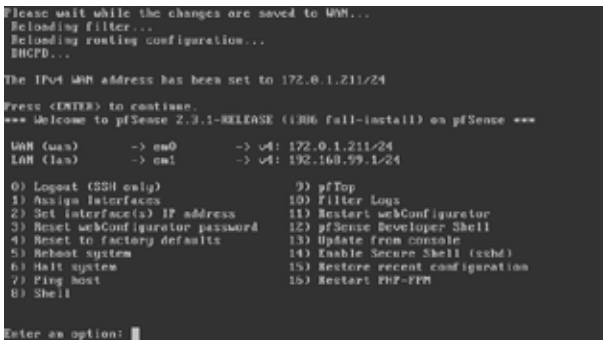


Figura 14. Configuración final del pfsense.

Entramos por el administrador WEB a pfSense.

Figura 15. Acceso al entorno de administración pfsense

Ahora estamos en el entorno de administración web del pfsense.

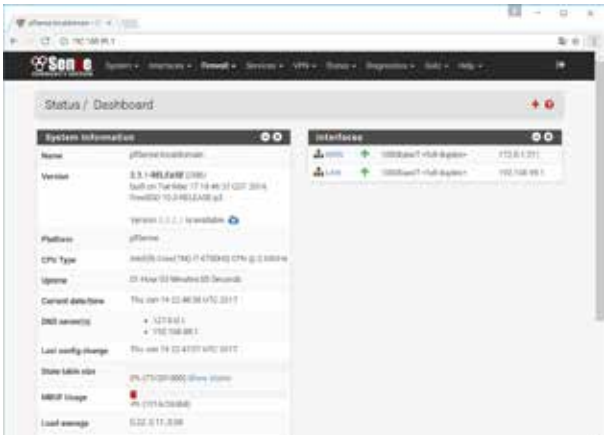


Figura 16. Entorno de administración pfsense.

Reglas de cortafuegos

Luego de tener una instalación básica del pfSense, podemos empezar a declarar las reglas, ubicándonos en la opción:

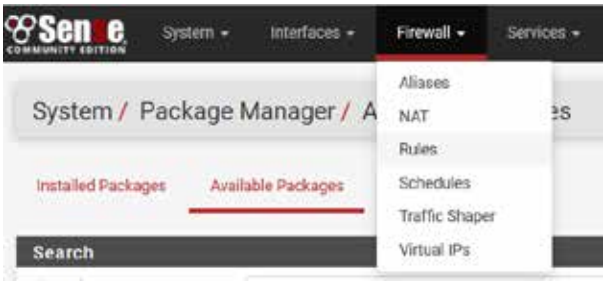


Figura 17. Opción de reglas.

Figura 18. Declaración de reglas pfSense.

Estamos ahora en el corazón del cortafuego. Aquí se decide qué conexiones se permiten y cuáles no.

Tenemos que entender el cortafuego como una caja con una serie de puertas de entrada. Se trata de dejar o no dejar entrar (paquetes de información) por cada una de las puertas que tenemos. Este concepto es muy importante, ya que si un paquete de información puede entrar por una puerta querrá decir que saldrá (en principio) por cualquier otra. Por tanto, en lo que se refiere a las salidas sólo nos ocuparemos de seleccionar cuál queremos. Nada más que esto.

Cada puerta tiene pues sus reglas, que se ejecutan según el orden en que están puestas. De la primera hacia la última de la lista. Digo "hacia la última" porque cuando un paquete de información cumple una de las reglas se hace la acción que dice la regla y ya no se miran las siguientes.

¿Y qué pasa si se llega a la última regla y ninguna de ellas se ajusta a nuestro paquete de información? Pues que el paquete no pasa. Si no hay regla, el paquete es bloqueado.

¿Y qué acciones puede hacer una regla? Pues tres: dejar pasar (pass), bloquear (block) y rechazar (reject). La diferencia entre bloquear y rechazar es importante. Si se bloquea, simplemente se ignora el paquete de información que se está recibiendo. Si se rechaza, se comunica al emisor que no se quiere el paquete. Por tanto, normalmente se bloquea. ¿Por qué? Pues porqué bloquear es silencioso, es no hacer caso al emisor y nada más.

También podemos desactivar reglas. Las reglas desactivadas se ven «difuminadas» en la lista de reglas. Ello resulta especialmente interesante cuando se precisa de reglas ocasionales. Por ejemplo, para tareas de administración de la red.

No vamos a entrar en detalle de declaración de reglas puesto que esto es un apartado muy amplio, existe amplia información sobre las reglas de pfSense, pero la mejor documentación está en el idioma Ingles y se las encuentra generalmente en foros de discusion.

SISTEMA DE DETECCIÓN DE INTRUSOS

Otra de las opciones que deberíamos habilitar para nuestro entorno de red es la de IDS/IPS.

Un sistema de detección de intrusos (IDS) por red compara el tráfico con una serie de patrones para identificar comportamientos maliciosos. El sistema de detección de intrusos más conocido y completo es Snort.

Snort descarga periódicamente un conjunto de reglas y en función del trafico genera una serie de alertas. El problema de los IDS, es que generan demasiadas alertas, muchas de ellas, falsos positivos, con lo que ese debe ser cauto antes de sacar conclusiones precipitadas.

PfSense no dispone de ningún detector de intrusos, aunque permite instalar snort como un paquete adicional de manera automática desde la propia interfaz web, como se puede ver en la siguiente figura.

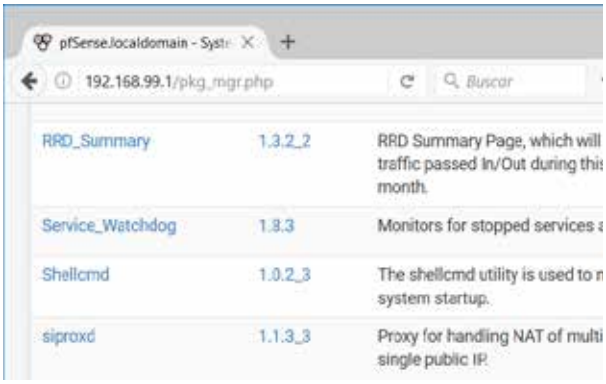


Figura 19. PfSense permite instalación Snort.

Una vez instalado Snort, en la configuración se debe incluir un código para descargar las reglas que se puede obtener de www.snort.org.

CONCLUSIONES

Finalmente, el sistema se ha instalado con éxito y podrá ser adecuado según requerimiento de cada uno, se ha cumplido con lo propuesto de realizar la instalación de una solución de protección perimetral con software libre. Cabe aclarar que para facilidad y demostración el sistema fue instalado en un entorno virtual con las características especificadas en el punto de implantación.

El uso de este sistema de sistemas de esta índole nos da la ventaja que es escalable y minimiza costos.

Este firewall Pfsense es una distribución de BSD el cual se deriva de Unix que funciona como Firewall, Portal Cautivo, servidor VPN, DDNS, DHCP, entre otras, que realizando la configuración correcta no tendría que envidar nada a sus competidores tanto de software libre y de sistemas de pago, puesto que existen más de 1 millón de implementaciones de Pfsense a nivel mundial que han mostrado resultados exitosos.

Pfsense está soportado comercialmente por BSD Perimeter INC. El cual ofrece soporte comercial especializado para esta solución de seguridad para redes LAN y WAN No se requiere conocimientos avanzados en línea de comandos de BSD para poder manejar el sistema operativo.

Se puede acceder a la GUI de Pfsense a través de un explorador de internet (IE, Mozilla, Chrome etc.) Pfsense se puede instalar sobre cualquier arquitectura de PC Pfsense es una solución de seguridad de código abierto es decir que cualquier desarrollador puede añadir mejoras al S.O bajo ciertas condiciones legales.

RECOMENDACIONES

Como recomendación para implementar estos tipos de redes, se debe tener una estructura redundante para permitir la flexibilidad de aplicar actualizaciones y parches del sistema en máquinas secundarias.

Así mismo cabe aclarar que el software que se usa en producción siempre debe ser actualizado a medida que vayan saliendo las actualizaciones.

REFERENCIAS BIBLIOGRÁFICAS

Martines Puentes, J. (2011). Sistema Inteligente de Deteccion de Intrusos. Madrid – España.

Berenson, L. M. (2014). Estadística para la administración (1 ed.). Estados Unidos: Pearson Education.

Yáñez Guevara, D. (2013). Sistema de Deteccion y Prevencion de Intrusos para el Control de la Vulnerabilidad en los Servidores de la Facultad de Ingenieria en Sistemas, Electronica e Industrial de la Universidad TŸecnica de Ambato. Ambato.

Contreras Rufino. (2013). La Universidad de Oviedo enseña con éxito su proyecto en seguridad perimetral.

Tutorial de instalación pfSense 2.0.1 nanoBS, consultado el 1 de mayo de 2017. http://pheriko.blogspot.mx/2012/03/pfsense2instalaciondesdecero.html, https://doc.pfsense.org

Snort externo unido a un pfSense http://www.bellera.cat/josep/snort2pfsense

Todo lo relativo a softwares cortafuegos en Wikipedia,

http://en.wikipedia.org/wiki/Category:Firewall_software