PFSENSE y RASPBERRY al rescate de la seguridad en hogares y Pymes Colombianas

Martínez Pérez, Javier Eduardo.
Javiermp21@gmail.com
Universidad Piloto

Resumen—El presente artículo deja una puerta entre abierta a hogares y Pymes colombianas de utilizar y poner en marcha un sistema de seguridad perimetral, utilizando un software Open Source que inicialmente teniendo funcionalidades básicas se pondrá apunto con la ayuda de otros paquetes, fortaleciendo su core de aplicaciones. Partiendo de mencionar funcionalidades de gateway y firewall, se irán integrando funciones de VPN, antivirus, IDS/IPS, proxy server, radius server y portales cautivos.

Entrando en mención de hardware idóneo con recursos suficientes para suplir esta necesidad de seguridad en hogares y Pymes colombianas donde contamos con una cantidad de usuarios y sesiones controladas.

Abstract—This article leaves a door semi-opened to homes and colombian pymes to utilize and to put into motion a perimetral security system, it utilizes an open source software which initially having basic functionalities will be optimized with the help of other packages, strengthening its applications core. Starting to mention gateway functionalities and firewall, VPN functions are going to be integrated, antivirus, IDS/IPS, proxy servers, radius server and captive portals.

Beginning to mention the suitable hardware with enough resources to supply this necessity of security at home and colombian Pymes where we count with an use quantity and controlled sesions.

Índice de Términos—Gateway, ids, ips, pfsense, proxy, radius, raspberry pi, vpn.

I. INTRODUCCIÓN

Los hogares y las Pymes de Colombia son fuentes de información muy desprotegidas [1], actualmente el comportamiento de las mismas frente a eventos de seguridad informática es actuar reactivamente frente a estas adversidades. El comportamiento del mercado de las conexiones a internet para el 2014 se ha multiplicado por cuatro y más del 60% de Pymes se han conectado a la red [2]. Lo cual significa que cada día se enfrentan a eventos de seguridad que puede perjudicar en gran medida los hogares y las Pymes colombianas.

¿Cuál podría ser la mejor manera de prever situaciones que pongan en riesgo las comunicaciones e información de los hogares y Pymes Colombianas? Brindándoles una solución confiable, económica que esté al alcance de sus presupuestos y servicios de avanzada que les permita proteger la información familiar o empresarial que se exponga frente a internet.

PfSense es una distribución de código abierto sobre FreeBSD , que a partir del 2004 se proyecta como distribución de firewall y router [3]; se propone como una solución de fácil acceso e instalación en ambientes productivos de bajos costos y requisitos de hardware mínimos; Raspberry Pi es una hardware catalogado como un pc embebido [4] con recursos suficientes para llevar a cabo la instalación y puesta en marcha de un sistema de seguridad con software que cubra las expectativas de recursos necesarios para su coexistencia, los cuales pueden proponerse como una solución fácil y de gran alcance que puede mitigar los eventos de seguridad a los cuales se exponen día a día los hogares y Pymes colombianos.

II. SEGURIDAD INFORMÁTICA EN EL HOGAR Y LA PYME COLOMBIANA

En la actualidad la seguridad de la información es un elemento que no se sitúa en el nivel de importancia que tal vez requiera, el sin número de vectores de ataque que se puede presentar a los

cuales se exponen los hogares y las Pymes Colombianas en el mundo físico y digital es enorme, el sólo hecho de pensar: "la información que manejo o dispongo no me representa riesgo alguno", o que de alguna forma puedan adquirir información de las cuentas bancarias, espíen fotos personales, familiares o datos sensibles, que los niños y adolescentes se encuentren expuestos a redes inescrupulosas donde puedan comprometer su integridad, que los equipos de cómputo que dispongamos sean dispuestos a redes enormes para realizar tareas de las cuales no tengamos conocimiento alguno.

Actualmente existe la incertidumbre si en los hogares colombianos están preparados frente a este tipo de hecho. Se habla de un 48% de las Pymes no disponen de ningún tipo de tecnología para proteger su información [1].

III. ¿QUÉ ES PFSENSE?

PfSense es una distribución open source basada en FreeBSD, pensado como un software para suplir funciones de firewall o Routing, gestionado por medio de una interfaz web [3], que cumple las funciones de administración sin requerir conocimientos de BSD. Sin enfatizar en sus funcionalidades principales se encuentran muchas alternativas de configuración lo cual convierte a pfSense en un sistema versátil de amplia gama de opciones.

PfSense surge de un proyecto con funcionalidades de firewall llamado M0N0WAll, fundado por Chris Buechler y Scott Ullrich en el 2004 [5], los cuales querían incursionar más en dispositivos integrados y de recursos de hardware muy limitados. En sus comienzos duro un par de meses sin nombre. Sus dos primeras letras PF provienen de Packet Filter, se pensó en algún momento cambiarlo pero la fama se mantuvo con PfSense y se decidió mantener el nombre.

IV. ¿QUÉ ES RASPBERRY PI?

Raspberry Pi es un ordenador de placa reducida de bajo costo, desarrollado en el Reino Unido por la fundación Raspberry Pi [4], con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas. El nuevo modelo en el mercado Raspberry Pi B+ cuenta con un chip Broadcom BCM2835 que contiene una CPU a 700 MHz y poderlo escalar por overclok hasta 1 GHz sin perder garantía, un procesador gráfico GPU VideoCore IV, y 512 de memoria RAM. Actualmente el diseño no incluye disco duro o una unidad de estado sólido, el almacenamiento se basa en una memoria SD, tampoco incluye una fuente de alimentación, ni una carcasa. En la actualidad existen varias distribuciones de sistemas operativos enfocados para la instalación en dicha miniCPU como derivados de Debían y Fedora entre otros. Cabe resaltar que lo atractivo de dicha solución es de un coste muy económico y de fácil adquisición que actualmente cuenta con soporte internacional y diversidad de foros que promueven su utilización.

V. ¿QUÉ IMPLEMENTO Y COMO USO PFSENSE?

A. PfSense como gateway

Antes de comenzar a proponer este entorno, es necesario pensar ¿Dónde se ubica a pfSense? En entornos como hogares o Pymes se cuenta con una salida a internet, que es lo más común, por economía, porque es suficiente y cubre lo que se necesita; o se puede encontrar con lugares que existan varias conexiones hacia internet pero no se utilizan de la forma más óptima posible. PfSense como herramienta de red tiene componentes muy interesantes a explotar como su balanceo de cargas, lo cual puede servir para distribuir los canales de internet que se tengan. Por otra parte también cumple funciones de DHCP, DNS, VLAN, NAT, NTP, ROUTING, BRIDGE entre otras muchas más [3], [5]. Estas funciones bien administradas pueden ser opciones muy interesantes a explorar apoyando los intereses de incrementar el nivel de seguridad de la red. Esta y muchas más razones da a pensar que el mejor lugar para ubicar un sistema de seguridad

perimetral sea como Puerta de enlace, ya que por este filtro será la pasarela de custodia hacia y desde internet.

B. PfSense como firewall

Una de las tareas más importantes que pone a disposición pfSense es su labor como firewall y que en su nombre se levanta como Paquet Filter (PF), nativo de openBSD y que se considera por si sólo como uno de los sistemas operativos más seguros del mercado actualmente. Inicialmente como IP filter el cual era un sistema de filtrado limitada en sus órdenes de consola y que al no ser de fácil modificación fue descartado por el creador de PF, Daniel Hartmeier [3]. PF se dispuso como una solución de filtrado de paquetes, cortafuegos o muro de fuego (Firewall) basado en configuración dinámica (stateful rules) que se mantiene en la actualidad junto al proyecto de openBSD por el equipo de desarrollo del mismo y adoptado por la distribución de FreeBSD y desde el 2004 como parte del proyecto PfSense que con su interfaz gráfica lo convierte en algo más sencillo a manipular [5].

Un Firewall es una herramienta de red que bloquea accesos no autorizados, permite conexiones autorizadas o monitorea el estado de las mismas. Muchas más funcionalidades se pueden encontrar o se puede configurar en los firewall como lo son limitar, permitir, cifrar o descifrar entre las diferentes conexiones que se estén causando. PfSense como se mencionó en PF trabaja con un estado Stateful rules, lo cual significa que trabaja a nivel de flujo de conexión, mantiene una tabla de estado que hace seguimiento de las sesiones que pasan el firewall y en función de ella hace inspección de cada paquete que atraviesa el dispositivo [5]. El mecanismo asume que si se permite el inicio de la conexión adicional que requiere esa aplicación será permitida.

C. PfSense como proxy

Un proxy como se puede observar es un examinador de paquetes y un intermediario en la red, el cual ayuda con funciones como controlar, manejo de la velocidad, filtrado, modificación de paquetes y ayuda a un ahorro de recursos. El proxy como una herramienta de la mano de un firewall, incrementan la seguridad de la red en gran medida, el proxy al estar examinando los paquetes de internet puede decidir si permitir o destruir según las políticas de permisividad de la red que se esté protegiendo.

Este software abre el paquete de red, examina su contenido y según su configuración destruye el paquete o permite su camino a su destino.

PfSense de la mano de squid [6], un proxy web con cache, el cual guarda conexiones recurrentes a servidores web y DNS el cual acelera sus procesos de decisión sobre si permitir o denegar conexiones ya almacenadas. Entre sus funcionalidades están servir como Proxy con cache de HTTP, HTTPS, FTP entre otros protocolos de internet, proxy para SSL, Jerarquías de cache, ICP, HTCP, CARP y cache digests, cache trasparente, WCCP, Control de acceso, gestión de tráfico, aceleración de servidores HTTP, SNMP y cache de resolución DNS [6]. Estas funciones acompañadas de pfSense con packet filter como firewall se comienza a dimensionar como un sistema de proporciones enormes, muy importante como un gestor de filtrado de contenido o examinadores de capa de aplicación para los hogares y las Pymes colombianas que como se mencionó son escenarios desprovistos de seguridad.

D. PfSense como antivirus

Los antivirus nunca están al 100% con respecto a las amenazas que se puede encontrar en la red, algunos más completos que otros protegen un gran número de amenazas comparadas con otros. Por cuestiones económicas o de recursos de las máquinas de computo que se poseen en hogares y Pymes, se deja de instalar un antivirus, pero el poder gozar de una protección que analice de primera mano los paquetes que están por descargar o recibir por medio de los correos electrónicos es una alternativa interesante a explotar o tener en mente para revisar.

PfSense de la mano de HAVP (HTTP antivirus Proxy) que es un proxy con filtro antivirus [7], este no hace el papel de cache o filtro de contenidos, el

sólo se encarga de analizar el tráfico completo en busca de script maliciosos o dañinos, examina cualquier tipo de archivo. Su forma de operar es iniciar la descarga e ir analizándolos y entregarlos al clientes después de ser revisados; la idea no es analizar archivos de gran tamaño puesto que las líneas de código que componen los virus no son demasiado grandes y pueden ser encontradas en archivos de pequeño tamaño. Los archivos de tamaños muy grandes pueden ocasionar la cancelación de la descarga, ya que la descarga y el análisis generan latencias de bajada del archivo lo cual puede significar una desventaja en este escenario.

Otra herramienta que complementa su acción de antivirus es ClamAV [8], distribuido bajo licencia GPL, un potente antivirus que se tiene a disposición como un repositorio de Squid proxy como herramienta de análisis, sumamente usado en servidores de correo electrónico en todo el mundo, aunque también puede analizar un sin número de archivos.

E. PfSense como portal cautivo

Una de las novedades muy utilizadas actualmente en ámbitos de uso público y que también se puede usar en el hogar y en las Pymes son los portales cautivos [3], [5], los cuales se pueden usar para autenticar las personas que accedan a la conectividad que se ofrece, de la mano con una buena gestión de red y usos de modos de autenticación como LDAP o radius. Se puede asegurar que las personas autorizadas en casa o en el trabajo tengan el acceso a dicho servicio de internet sin que terceros puedan tener acceso y perjudicar la conexión.

Este tipo de servicio aparte de limitar a terceros al uso innecesario de recursos, también permite informar sobre el uso aceptable del servicio, el tiempo permisible de uso de la red entre otras. PfSense nativamente implementa un portal cautivo con estas características para poder interactuar.

F. PfSense como radius server

Radius server se comporta como un AAA [9], el cual es un protocolo de autenticación, autorización y administración para aplicaciones de acceso a la red, dicho servicio de autenticación de la mano de un portal cautivo es un sistema poderoso de frente a una red WIFI hogareña o empresarial, para poder blindar la red ante accesos no autorizados.

PfSense utiliza a FreeRadius como un repositorio más o paquete descargable dentro de sus posibilidades a manipular y configurar, totalmente integrable con el portal cautivo y vinculado con políticas de red como VLAN o políticas de firewall, proxy, etc.

G. PfSense como virtual private network o VPN

En la actualidad como se menciona la red a la que se está vinculado para poder acceder a servicios de correo electrónico, mensajería instantánea, navegación, como medio para compartir archivos, accesos a portales bancarios, tanto desde dispositivos de computo fijos o móviles desde cualquier lugar del mundo, dejando una puerta abierta a la exposición de información de mucha relevancia para terceras personas que quieran vulnerar o acceder a dicha información para afines extorsivos o cometer ilícitos o solamente ser utilizados como robots para ampliar su capacidad de procesamiento. Para solventar dichas vulnerabilidades se ha dispuesto de mecanismos de acceso a la red LAN sobre redes públicas las cuales se conocen como redes privadas virtuales o VPN, las cuales establecen un túnel de comunicación segura entre la red pública y la red LAN [3], [5] logrando acceder a los recursos internos o que sean aplicadas las mismas reglas que se han producido por PF, Proxy, antivirus entre otras que ya se han mencionado, cuidando y protegiendo las comunicaciones. Es de gran importancia mencionar que esto ya no sólo aplica para grandes empresas o multinacionales, sino también para hogares y Pymes ya que los costos subyacentes para prestar dicho servicio no son altos, salvo que si se habla que se debe de tener algún nombre de dominio público o

IP para canalizar dicho servicio de VPN, los cuales en la actualidad no son muy altos.

OpenVPN se presta sobre PfSense para brindar este tipo de características, es una solución de conectividad sobre licencia GPL y ofrece combinaciones de nivel de seguridad y facilidad de uso. Una combinación de diferentes protocolos soportado por PfSense hace que esta integración genere buenos frutos para cifrar las comunicaciones y asegurar cualquier medio en el que se encuentre el usuario.

H. PfSense como IDS/IPS

Todos los temas que se han tratado hasta el momento cubren perfectamente un sistema de seguridad básico y que puesto el alcance para hogares y Pymes puede que no sea tan amplio. Existen aún muchas más opciones de blindar pfSense y convertirlo en una herramienta de avanzada en pro de la seguridad de los hogares y Pymes de Colombia.

Las funcionalidades de IDS e IPS, estos son software que monitorean y pueden llegar a tomar decisiones como en el caso del IPS. El IPS puede ejercer control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. El IDS sólo detecta los accesos no autorizados a un computador o a una red y realiza un análisis pormenorizado del tráfico el cual entra a analizar y comparar con una base de datos de firmas de ataques conocidos o comportamientos sospechosos.

Snort [10] al tener comportamientos de IPS o IDS, sin mencionar muchas más alcances del mismo, se integra como paquete complementario de PfSense para darle a esta herramienta un toque sutil como una poderosa herramienta de seguridad todo en uno frente a descubrir brechas de seguridad dispuestas en la red de hogares y Pymes que se quiera custodiar.

VI. ¿QUÉ MÁS SE PUEDE INCLUIR EN PFSENSE?

Para no extender demasiado en la posibilidad de paquetes o herramientas adaptables a PfSense, que con todo lo mencionado puede llegar a suplir UTMs comerciales o hasta las nuevas conceptualizaciones de firewall "*Next Generation Firewall NGFW*", existen muchas herramientas de las cuales se puede sacar provecho dentro de la distribución de PfSense, por ejemplo:

NMAP: Se cataloga como un software de escaneó de sistemas informáticos en busca de vulnerabilidades, estos sistemas pueden ser usados en redes tanto grandes como pequeños, es de resaltar que para el uso de estas herramientas se debe de tener un conocimiento amplio de los comandos a usar y poder entender y traducir sus resultados.

SURICATA: Es un software open source de alto rendimiento, con funcionalidades de IDS, IPS o motor de monitoreo de seguridad de red. Mantenido y desarrollado por Open Information Security Foundation (OISF), entre sus características se menciona, una alta escalabilidad, identificación de protocolos, identificación de archivos, comprobación de MD5 y extracción de archivos.

POSTFIX FORWARDER: Es una herramienta de gran utilidad en la lucha contra el spam, pero de gran demanda de CPU. Es capaz de identificar Zombie blocker, Header Checks, Body checks, Access list, entre otras.

PFBLOQUER: Es una herramienta que complementa a PfSense para crear bloques de URL generando un alias el cual puede bloquearse por el mismo vinculado a una política. Entre sus características encontramos contri_block, XMLRPC sincronización, frecuencia de actualización de listas y también da la posibilidad de crear listas de redes y asignarlas a un alias.

MAILSCANNER: Esta herramienta también se puede implementar como un filtro de seguridad para el correo luchando contra el anti-spam, al igual que postfix-forwarder genera un alto consumo de CPU, lo cual para llevar a cabo una instalación sobre

raspberry pi, no es recomendable puesto que solo se cuenta con un único proceder a una velocidad razonable de procesamiento.

Se pueden citar muchas más, pero las mencionadas en este documento son suficiente razón para no dejar de lado esta distribución tan interesante.

VII. Instalación y mantenimiento

El presente documento no está pensado como un alcance o un tutorial para instalar y llevar a puesta en marcha este sistema de seguridad, más sólo se busca generar la curiosidad e invitar a los usuarios interesados en aprovechar esta herramienta open source en beneficio propio logrando llevar a cabo dicha implementación por cuenta propia.

Antes que nada se debe comenzar por realizar la descarga de la versión de PfSense que se desea instalar, esto se realiza en la página de www.pfSense.org, en la sesión de descargas, allí se encuentra release para instalaciones nuevas, actualizaciones de sistemas o versiones ya compiladas para virtualización. Se recomienda experimentar la opción de instalación nueva con el fin de poder experimentar instalar un sistema freeBSD, el cual actualmente no representa un reto dada una versión tan intuitiva como lo es PfSense. En esta sección se encuentra imágenes compiladas para llevar a unidades de cd, o memorias o paquetes para poder ser instalados como sistemas embebidos en otros sistemas operativos. En la actualidad dado el fraude que se pueden presentar por realizar descargas se utilizan medios para verificar la integridad de dichas descargas comprobando su contenido con medios como MD5 o Sha1, PfSense.org da las autenticaciones que ellos tienen para sus imágenes y se puede comparar dicha firma digital del archivo.

El proceso de instalación es muy sencillo [3], cabe resaltar que en sólo 10 pasos se puede tener este sistema en marcha, como lo muestran en el canal de youtube “[PfSense] Instalación y configuración”. Es de mencionar que dicha instalación se puede hacer para sistemas reales como sistemas virtuales.

La idea inicial para no complicarse con el tema de configuración de todas las herramientas mencionadas es comenzar paulatinamente a interactuar con el sistema, por ejemplo: lograr iniciarlo como gateway, luego configurarlo como firewall y aplicar políticas adecuadas sobre las redes que se definan, y determinar un nivel de prioridades con respecto a la importancia de las herramientas que se determinaron en este documento y comenzar a probar sus alcances, para lo cual se recomienda utilizar sistemas virtuales para probarlos antes de llevarlos a la herramienta en producción.

VIII. Costos y necesidades del proyecto para poder llegar a su implementación.

En la actualidad las comunidades de open source son enormes y la documentación que se tiene hoy en día con las bases de datos asequibles por la red y con motores de búsqueda como Google, podemos encontrar foros de ayuda mutua y esfuerzos por lograr cometidos comunes que ayudan con información precisa. Incluso se puede encontrar video tutoriales en YouTube, los cuales generan una guía más amplia y detallada, que para los usuarios que no domine tecnicismos fuertes en áreas de redes o informática, les puede ayudar para poder implementar un sistema de gran envergadura como lo es PfSense.

Hablando de las necesidades que se requieren para cumplir con un sistema avanzado como lo es PfSense e incluyendo estas magnificas herramientas que fortalecen su funcionalidad primaria, se habla primero del tiempo necesario para instarla y configurarla, lo cual puede significar semanas de revisar y fortalecer los conocimientos sobre PfSense; en este documento sólo sembramos las conceptualizaciones necesarias como punto de partida para llevar a cabo una sólida investigación o generar la duda para una persona que quiera incursionar en el uso de estas herramientas. Se sabe que para que un software pueda operar requiere de un hardware que lo soporte, por esto se ha recomendado el uso de raspberry como hardware idóneo para incursionar y poner en marcha un sistema de estos, ya que tiene lo justo y necesario para poder mantener redes LAN de pocos usuarios

los apenas necesarios para coexistir en el hogar o en Pymes.

Actualmente se habla de un costo aproximado por adquirir dicho hardware alrededor de unos US$ 75, lo cual es un precio apenas justo para un sistema limitado y de gran variedad de posibilidades como lo es raspberry. Recapitulando en los párrafos de VPN se trató de la necesidad de un servicio de dominio público o IP dedicada, que puede verse como un sobre costo del plan de internet del cual se dispondrá para realizar las conexiones al mismo, donde esto puede equivaler a US$ 30 sobre el plan que se esté pagando en el momento.
Sin hablar del costo del software necesario para la implementación de un sistema tan fuerte como lo es PfSense, ¿Cuánto pagaría usted?, ¿Cuál sería el costo que le puede demandar anualmente mantenerlo? Estas preguntas y muchas más pueden realmente sorprenderlo si compara esta herramienta con otras comerciales que ofrecen servicios similares y que el costo es alrededor de 10 veces más que el valor de raspberry Pi, teniendo en cuenta que para un hogar o Pymes es alto mantener anualmente estos sistemas por el costo de licenciamiento anual.

¿Valdrá la pena incursionar en PfSense por tan poco? el hecho de sentir seguridad en el lugar que interactúan los hogares y las Pymes para poder implementarlo.

REFERENCIAS

[1] El tiempo, Redacción tecnológica. (2013, 12, 17). Para las Pymes en Colombia, la tecnología es costosa e innesesaria. [Online] Available: http://www.eltiempo.com/
[2] Evaluamos, Orlando Rojas Pérez. (2013, 12, 13). 60.6% de las MYPYMES colombianas están conectadas a internet. [Online] Available: http://www.evaluamos.com
[3] Christopher M. Buechler, Jim Pingle, "pfSense: The Definitive Guide", Based on pfSense Version 1.2.3, Copyright © 2009 Christopher M. Buechler.
[4] Matt Richardson, Shawn Wallace. "Getting Started with Raspberry Pi", impreso, 1ra ed. Brian Jepson. United States of America: O'Reilly, 2012, pp. 1–16.
[5] Matt Williamson. "pfSense 2 Cookbook". Ebook, 1ra ed. Akshara Aware, Birmingham: Packt Publishing ltd. 2011.
[6] Kulbir Saini. "Squid Proxy Server 3.1". Ebook. 1ra ed. Mithun Sehgal. Birmingham: Packt Publishing ltd. 2011.
[7] HVAP, Christian Hlgers.. HAVP Documentarion. [Online] Available: http://www.server-side.de/
[8] ClamAV, Tomasz Kojm, "ClamAV User Manual". Ebook, © 2007 – 2013 Sourcefire Inc.
[9] Dirk van der Walt. "FreeRadius, Beginner's Guide". 1ra ed. Srimoyee Ghoshal. Birmingham: Packt Publishing ltd. 2011.
[10] Martin Roesch, Chris Green "SNORT, Use manual 2.9.6". Ebook. Sourcefire Inc. 2013.