CCADET

CENTRO DE CIENCIAS APLICADAS Y DESARROLLO TECNOLÓGICO
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Informe Técnico

Análisis de Firewalls de Código Abierto vs Firewalls Comercial.

Autores

Miriam Valdés Rodríguez

María del Carmen Arelio Baranda

Alethia Patricia Estrella Ruiz

Fecha

Agosto de 2019

Tipo de Proyecto

PROYECTO INTERNO

Título: Análisis de Firewalls de código abierto vs Firewalls comercial

Autor: Miriam Valdés Rodríguez, María del Carmen Arelio Baranda, Alethia Patricia Estrella Ruiz

Resumen

Los *firewalls* protegen una red confiable de una red que no es de confianza al filtrar el tráfico de acuerdo con una política de seguridad específica. En la actualidad se están utilizando un conjunto diverso de firewalls en las organizaciones tanto de marca comercial como de código abierto (open source). Al respecto, este trabajo presenta un análisis que evalúa los firewalls actuales (comerciales y de código abierto) en términos de sus funciones y posteriormente los contrasta para determinar cuáles son las condiciones (criterios) que debe determinar el tomador de decisión antes de que considere utilizar una solución de código abierto o comercial en materia de seguridad informática. En este sentido, los administradores de red primero diseñan configuraciones de red, de un conjunto de requerimientos, luego implementan el nuevo diseño, y finalmente lo verifican monitoreando continuamente el comportamiento de la red. Una de nuestras observaciones es que la eficiencia de la red se puede mejorar observando los cambios en el comportamiento de la red supervisada, por lo que es necesario establecer un sistema de monitoreo en conjunto con una solución de firewall. Por otro lado, se observa la necesidad de establecer reglas y políticas, que deben ser diseñadas de manera eficiente. El diseño debe facilitar la representación de una política, así como su comprensión e implementación en el firewall. Finalmente se determina que es importante contar con técnicas y herramientas de administración de políticas que los administradores puedan usar para examinar, refinar y verificar la corrección de las reglas de filtrado de firewall con el fin de aumentar la efectividad de la seguridad del mismo.

Índice

Resumen 1

1.1 Modelo para la Interconexión de Sistemas Abiertos (OSI) 6
1.2 Clasificación de firewalls 8
1.2.1 Nivel de aplicación de pasarela 8
1.2.2 Circuito a nivel de pasarela 8
1.2.3 Capa de red o de filtrado de paquetes 8
1.2.4 Capa de aplicación 8
1 Firewalls Comerciales 8

1.1 Características de los firewalls UTM 9
1.1.1 Consideraciones para la elección de un firewall UTM 10
1.2 Palo Alto Networks 12
1.3 Fortinet 15
1.4 CheckPoint Software Technologies 19
2 Firewall de código abierto 24

2.1 Pfsense 25
2.2 Untangle 28
2.3 Opnsense 28
2.4 Packetfilter 30
2.5 IP Tables 31
3 Análisis 32

4 Resultados 37

Conclusiones 38

Agradecimientos 39

Tablas

Tabla 1 Resumen de las características de firewalls comerciales 23

Tabla 2 Resumen de las características de los firewalls de código abierto 31

Tabla 3 Cuadro comparativo de las características de firewalls comerciales vs de código abierto 32

Tabla 4 Cuadro comparativo del nivel de cobertura en el modelo OSI de firewalls comerciales vs de código abierto 34

Figuras

Figura 1 Malware más frecuente a nivel mundial 4

Figura 2 Esquema de la función de un Firewall 5

Figura 3 Nivel de filtrado de paquetes en un firewall en el Modelo OSI 7

Figura 4 Tecnologías y protocolos por capa del modelo OSI 7

Figura 5 Índice mundial de amenazas cibernéticas 2017 11

Figura 6 Cuadrante de Gartner para firewall 12

Figura 7 Top Firewalls Solutions 21

Figura 8 Next Generation Firewall 24

Figura 9 Resultados Firewall Comercial vs Firewall De código abierto 37

Introducción

Con la evolución de las redes informáticas la necesidad de proteger los archivos y otra información almacenada en las computadoras se ha vuelto imperativo. El Intercambio de archivos entre sistemas operativos y otro *software* en la red que son ampliamente distribuidos por los usuarios proporcionan condiciones favorables para ataques maliciosos, los cuales se han vuelto más prominentes en los últimos años (Wu *et al,* 2017). En consecuencia, la propagación de virus, gusanos, troyanos y otros *softwares* maliciosos han aumentado considerablemente (Misra *et al*, 2014).

De acuerdo a un estudio realizado por Check point Software Technologies LTD, en el periodo de enero a junio del 2017, la mayoría de los ataques a organizaciones a nivel mundial fueron perpetrados por los siguientes tipos de malware.

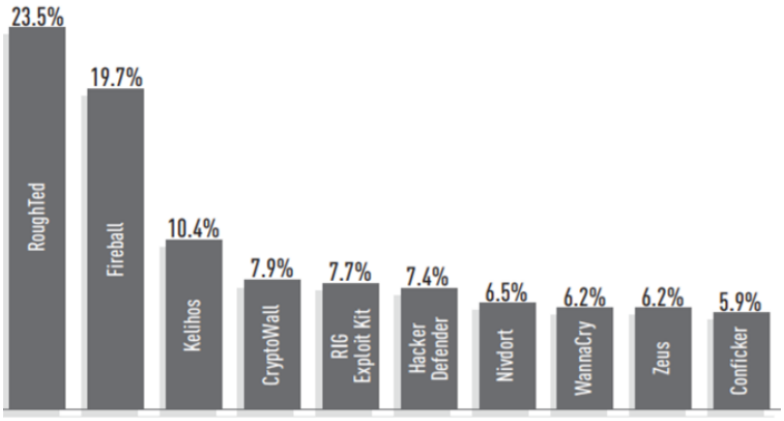

Figura 1. Malware más frecuente a nivel mundial.

Fuente: Check Point Reseach Mid-Year Report Cyber Attack Trends (2017).

Los *softwares* maliciosos o malwares son los programas escritos con la intención de causar algún tipo de daño a los sistemas y redes de una organización; mientras que los virus informáticos son la clase de malware más ampliamente reconocida. Una vez que un virus ingresa a una computadora o red, realiza dos funciones: infecta a otros programas copiándose y ejecuta códigos maliciosos que han sido incluidos por el autor.

Estos virus están especialmente diseñados para dañar el sistema y su efecto puede ser tan extenso que puede requerir la reconstrucción total del *software* y datos de la máquina o de la red comprometida. Debido a la naturaleza de propagación rápida de los virus informáticos, el daño puede multiplicarse en la topología misma la red en una fracción de tiempo (Misra *et al*, 2014).

Wu *et al* (2017) indica que uno de los objetivos de estos ataques es debido al alto valor de los datos relacionados con la organización, asimismo diversos reportes señalan que los ciberdelincuentes han perfeccionado sus infraestructuras de *backend* con el fin de aumentar la eficacia y los resultados de sus ataques. Es así que, en el Informe anual de seguridad de Cisco de 2016, la estimación en el ingreso anual promedio de estos ataques (*ransomware*) por campaña es de $34 millones de dólares (Divakaran *et al*, 2017).

Los atacantes (ciberdelincuentes) ya no se detendrán después de un solo ataque exitoso, sino que intentan llegar más lejos de las máquinas comprometidas por lo que el administrador de seguridad de la red tiene que combatir este tipo de intrusiones.

Al respecto, para mantener la seguridad y disponibilidad de una infraestructura productiva en los servicios de Tecnologías de Información y Comunicaciones en una organización, los *firewalls* son elementos cruciales de seguridad en la red como defensa contra estos ataques (Khoumsi *et al*, 2016).

Los *firewalls* protegen una red confiable de una red que no es de confianza al filtrar el tráfico de acuerdo con una política de seguridad específica (Kamara *et al*, 2003). Una política de seguridad de *firewall* consiste en reglas que se utilizan para filtrar el tráfico entrante y saliente (paquetes) de la red segura (Khoumsi *et al*, 2016). Una política de seguridad de *firewall* mal diseñada puede llevar a la aceptación de paquetes maliciosos o al rechazo de paquetes aceptables; por lo tanto, es necesario realizar un correcto diseño y análisis de las políticas de seguridad de *firewall* (Madhuri & Rajesh, 2013).

Figura 2. Esquema de la función de un Firewall.

De acuerdo con Hils et al (2017) actualmente todos los proveedores de *firewalls* comerciales ofrecen funciones para aplicar mejor las políticas (aplicaciones y control del usuario) o detectar nuevas amenazas (sistemas de prevención de intrusos [IPS], *sandboxing* y retroalimentación de inteligencia de amenazas, entre otras funciones) en una sola solución de seguridad informática.

El modelo que utilizan las soluciones de *firewalls* comerciales es la gestión unificada de amenazas (*Unified Threat Management*, UTM; por sus siglas en inglés), es un término de seguridad de la información que se refiere a una sola solución de seguridad y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red de la organización.

Un producto UTM generalmente incluye funciones como antivirus, *antispyware, antispam*, *firewall* de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, *network address translation*) y compatibilidad para redes privadas virtuales (VPN, *virtual private network*).

En este sentido y sin contar las crecientes amenazas de los atacantes, una red también puede volverse vulnerable cada vez que una organización experimenta crecimiento y cambio. A medida que las redes se vuelven más complejas, se espera cada vez más que respalden e impulsen los objetivos de una organización, por lo que las soluciones de seguridad simples ya no son adecuadas (Stevens, 2006). En la actualidad, los sistemas UTM se están convirtiendo rápidamente en la solución preferida para la seguridad de la red.

Por otro lado, la comunidad de código abierto ha desarrollado una variedad de herramientas de seguridad de la red. El uso habitual de herramientas de seguridad de código abierto en la industria se puede categorizar de la siguiente manera:

1. *Firewalls*, como *iptables*.
2. Sistemas de detección de intrusos, como *Snort*.
3. Herramientas de monitoreo de red, como *Multi Router Traffic Grapher* (MRTG).
4. Herramientas de evaluación de seguridad, como *Nikto* para escáneres de servidor web.

El *firewall* es un dispositivo de red que se utiliza para aislar la red interna de una organización desde redes externas, permitiendo que algunos paquetes pasen y bloqueen a otros. Permiten que dos entidades se conecten a sus redes a través de la infraestructura y los protocolos existentes, asegurando al mismo tiempo las redes privadas (Clark & Agah, 2015).

Las características convencionales de un *firewall* están estrictamente centradas en filtrar el tráfico y aplicar las políticas de seguridad local de una organización. Algunos *firewalls* son más sofisticados que otros, pero en general el filtrado se centra en paquetes individuales (filtros de paquetes), flujo de paquetes con estado (filtros con estado) o tráfico relacionado con la aplicación (aplicación de pasarelas). Todas estas características se construyen sobre las capas del modelo para la interconexión de sistemas abiertos y el único objetivo es permitir la comunicación únicamente en los canales definidos en la política.

Cuando un *firewall* recibe un paquete, primero se somete a un filtrado de capa de enlace, posteriormente se compara con un conjunto de reglas dinámicas y luego, el paquete se somete a comprobaciones de legalidad del paquete e *IP* y filtrado de puertos. Finalmente, se realiza la traducción de la dirección de red/puerto. Los *firewalls* sofisticados también reensamblan paquetes y realizan análisis a nivel de aplicación. Después de tomar una decisión de enrutamiento en el paquete, también se puede realizar el filtrado de salida. Véase figura 3. Cada una de estas operaciones es opcional, y el orden en que el paquete las atraviesa también puede diferir en diferentes *firewalls* (Kamara, 2003).

1.1 Modelo para la Interconexión de Sistemas Abiertos (OSI)

El modelo OSI (en inglés, *Open System Interconnection*) se compone de siete niveles de proceso, mediante el cual los datos se empaquetan y se transmiten desde una aplicación emisora, viajando a través de medios físicos hasta llegar a una aplicación receptora.

La capa de aplicación: proporciona los servicios utilizados por las aplicaciones para que los usuarios se comuniquen a través de la red. Es el nivel más cercano al usuario.

La capa de presentación: define el formato de los datos que se van a intercambiar entre las aplicaciones, ofreciendo un conjunto de servicios para la transformación de datos.

La capa de sesión: proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales: abre, mantiene y cierra la sesión entre dos sistemas.

La capa de transporte: permite intercambiar datos entre sistemas finales, dividiendo el mensaje en varios fragmentos. El servicio de transporte puede ser orientado o no orientado a conexión, tomando en cuenta la unidad de transferencia máxima MTU (en inglés, *Maximum Transmission Unit*).

La capa de red: se encarga de definir el camino que seguirán los datos desde el origen hasta su destino a través de una o más redes conectadas mediante dispositivos de enrutamiento (router).

La capa de enlace de datos: se ocupa del direccionamiento físico dentro de cualquier topología de red, esta capa nos permite activar, mantener y deshabilitar la conexión, así como la notificación de errores.

La capa física: controla las señales por donde viajaran los datos (cable de par trenzado, fibra óptica, radio frecuencia).

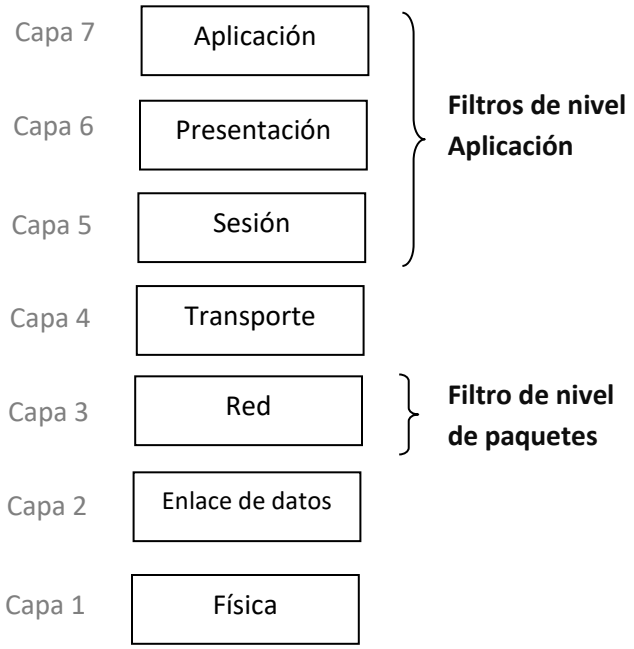

Figura 3. Nivel de filtrado de paquetes en un firewall en el Modelo OSI.

Las tecnologías y protocolos que soportan cada capa de aplicación del modelo OSI, se presentan en la siguiente figura:

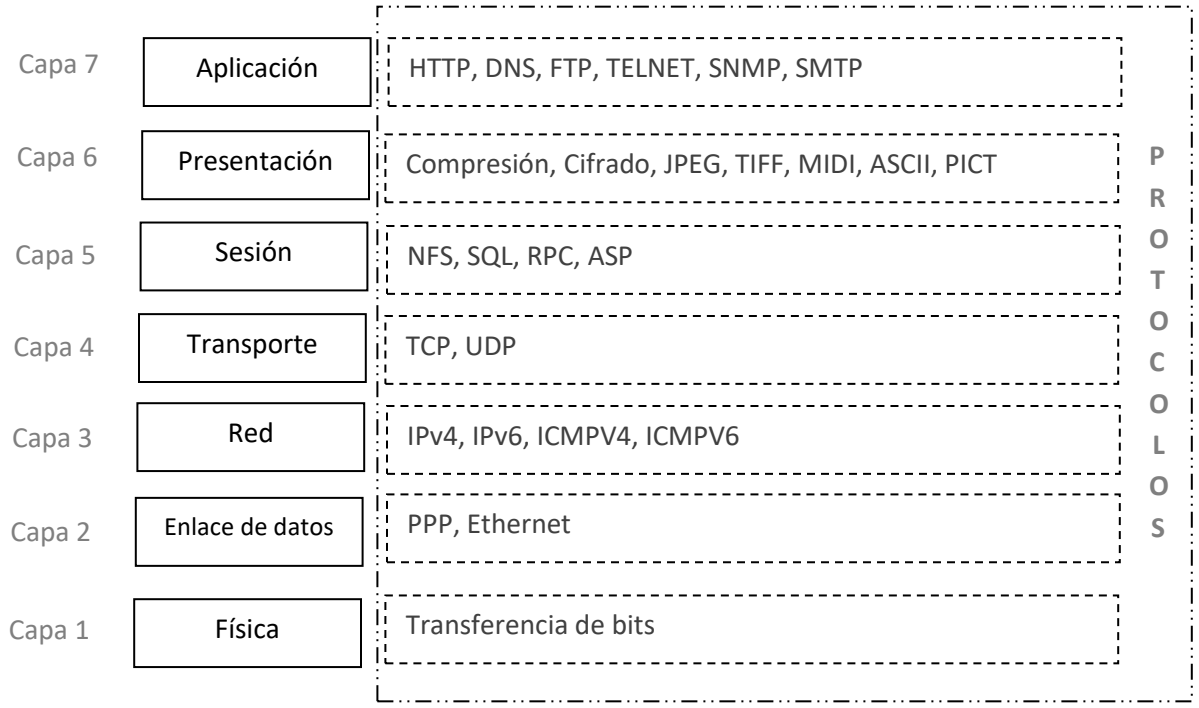

Figura 4. Tecnologías y protocolos por capa del modelo OSI.

En este sentido, se observa que algunos *firewalls* abarcan solamente el filtrado de paquetes para las capas de nivel 1, 2 y 3 del modelo OSI, mientras que otros incluso comprenden las capas 5, 6 y 7 de dicho modelo. Para el caso de los *firewalls* que brindan un nivel de protección hasta capa 3, se identifica la necesidad de contar con otra herramienta adicional para la protección de las capas restantes.

1.2 Clasificación de firewalls

1.2.1 Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores *FTP* y *Telnet*. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

1.2.2 Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

1.2.3 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 *firewalls* 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.

1.2.4 Capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder, e incluso puede aplicar reglas en función de los propios valores de los parámetros que aparezcan en un formulario web.

1 Firewalls Comerciales

De acuerdo con un estudio realizado por Gartner (2017) en dónde muestra un análisis comparativo de las fortalezas y debilidades de las diferentes marcas de *firewalls*; señala que las organizaciones seleccionan aquellas que permiten integrarse con otras tecnologías de seguridad, tal como pruebas de seguridad de aplicaciones, monitoreo de bases de datos, manejo de eventos e información de seguridad.

Algunas de las características de dichas soluciones tecnológicas incluyen un amplio rango de modelos y soportes para la virtualización y la creación de redes LAN virtuales, así como una gran capacidad de gestión y reporteo: diseñada para entornos complejos con un alto volumen de información, incluyendo prestaciones de administración multi-capa y gestión avanzada de reglas y políticas.

Stevens M. (2006) señala que estas soluciones comerciales se han integrado en dispositivos UTM (Gestión unificada de amenazas, *Unified Threat Management*). Han evolucionado desde *firewall* tradicional y dispositivos VPN y ofrecen capacidades mucho más integrales, como filtrado de URL,

bloqueo de spam, protección contra spyware, prevención de intrusiones y antivirus de puerta de enlace, así como capacidades de gestión, supervisión y registro centralizados.

Anteriormente, estas funciones eran manejadas por múltiples sistemas. Los UTM proporcionan una gama de soluciones de seguridad en un solo dispositivo, reduciendo los costos y simplificando todo el proceso de administración e instalación de sistemas de seguridad (Kilpatrick, 2003).

1.1 Características de los firewalls UTM

Filtrado de URL

Actualmente es necesario proporcionar protección en tiempo real contra amenazas web emergentes, incluidos *malware, phishing* y zombies / *bots*, y evitar la exploración en sitios web que contienen contenido no deseado, para garantizar el desempeño de una red. Asimismo, existe una creciente necesidad de proporcionar la capacidad de monitorear y bloquear otros sitios que, si se usan, pueden afectar la productividad y la capacidad de regular el ancho de banda.

Spam

El correo no deseado sigue siendo un problema importante, por lo que es importante contar con tasas de detección altas y precisas además de capacidades de limitación de velocidad. Esto exige herramientas que permitan que el filtrado identifique lo que es y lo que no es correo no deseado de forma más precisa, además de tener la capacidad de mitigar las áreas grises.

Prevención de intrusiones (IDS)

IDS están desarrollados para detectar ataques en la red y alertar al administrador de seguridad. Los dispositivos UTM agregan la capacidad de detener el ataque de forma automática o manual. La detección de dichos ataques originalmente se basa por completo en firmas, actualmente evolucionó para incluir algoritmos basados en heurística y comportamiento inteligente para detectar amenazas.

Antivirus

Los virus no han dejado de desarrollarse y mutar, por lo que los *firewalls* comerciales se mantienen al día con los cambios. Buscan proporcionar defensas multidireccionales que protejan a las redes no solo de virus y troyanos, sino también de malware polimórfico del lado del servidor, *rootkits, bootkits* y otras amenazas complejas, así como del creciente número de *keyloggers* y *malware* para captura de pantalla. También se está realizando un trabajo adicional para evitar la explotación por parte de redes de bots y otras herramientas de control malicioso, así como por infecciones de paso.

VPN

Es importante brindar conectividad segura para usuarios móviles, remotos y domésticos. Los dispositivos UTM incluyen capacidades VPN y proporcionar el protocolo Secure Sockets Layer (SSL) para el acceso seguro a las aplicaciones de una red.

1.1.1 Consideraciones para la elección de un firewall UTM

De acuerdo con Kurpjuhn T. (2013) las consideraciones para la adquisición de un dispositivo UTM que una organización debe tomar son:

Demanda de mayor rendimiento.

La disponibilidad de redes de alta velocidad y conexiones a Internet significa que las expectativas de lo que se puede hacer con un dispositivo UTM en tiempo real están aumentando de manera muy significativa. Ahora se espera que los dispositivos UTM puedan igualar la demanda de rendimiento de conexiones de 100Mbps y esta expectativa solo aumentará a medida que las redes se migren a velocidades de gigabits.

Amenazas crecientes de ataques dirigidos.

A pesar de que la mayoría de las organizaciones no esperan ser víctimas de una amenaza específica, incidencias de ciertos virus están creando conciencia y niveles de preocupación sobre el espionaje industrial, el sabotaje y el robo de datos. Esto está obligando a los desarrolladores a integrar capacidades cada vez más sofisticadas del Sistema de Prevención de Intrusos (IPS), además de *firewalls* simples, en sus dispositivos UTM.

Adopción más rápida de la conectividad de alta velocidad.

Se ha observado una aceleración gradual de las velocidades de las redes y tráfico de las mismas, por lo que los dispositivos UTM han sido capaces de mantener el ritmo y se han desarrolló a medida que evolucionó la migración a una mayor red y velocidad de ancho de banda. Sin embargo, se están adoptando velocidades más altas a un ritmo mucho más rápido, lo que hace que sea más crítico para los desarrolladores proporcionar dispositivos que puedan hacer frente a mayores niveles de rendimiento desde el principio.

Al respecto, el objetivo central de cualquier dispositivo UTM es asegurar la red; sin embargo, los eventos recientes, como los ataques ransomware de la variedad *WannaCry* han aumentado la importancia de garantizar que dichos dispositivos se mantengan actualizados y sean capaces de repeler amenazas nuevas y más avanzadas.

Los tipos de amenazas que están emergiendo son muy diferentes de los que hemos visto en el pasado, y las vulnerabilidades en las redes (virus y otro tipo de malware que captas simplemente navegando en la web o usando una aplicación web) han llegado un nivel de más del 50% de todas las amenazas.

En este sentido, Check Point Software Technologies muestra un mapa del índice de riesgo a nivel mundial de amenazas de malware y destaca las principales áreas de riesgo en todo el mundo. Véase figura 5. El índice de amenazas de Check Point se basa en la probabilidad de que una máquina en un determinado país sea atacada por malware, se deriva del *Threat Cloud World Cyber Threat*, que rastrea cómo y dónde ocurren los ciberataques en todo el mundo en tiempo real.

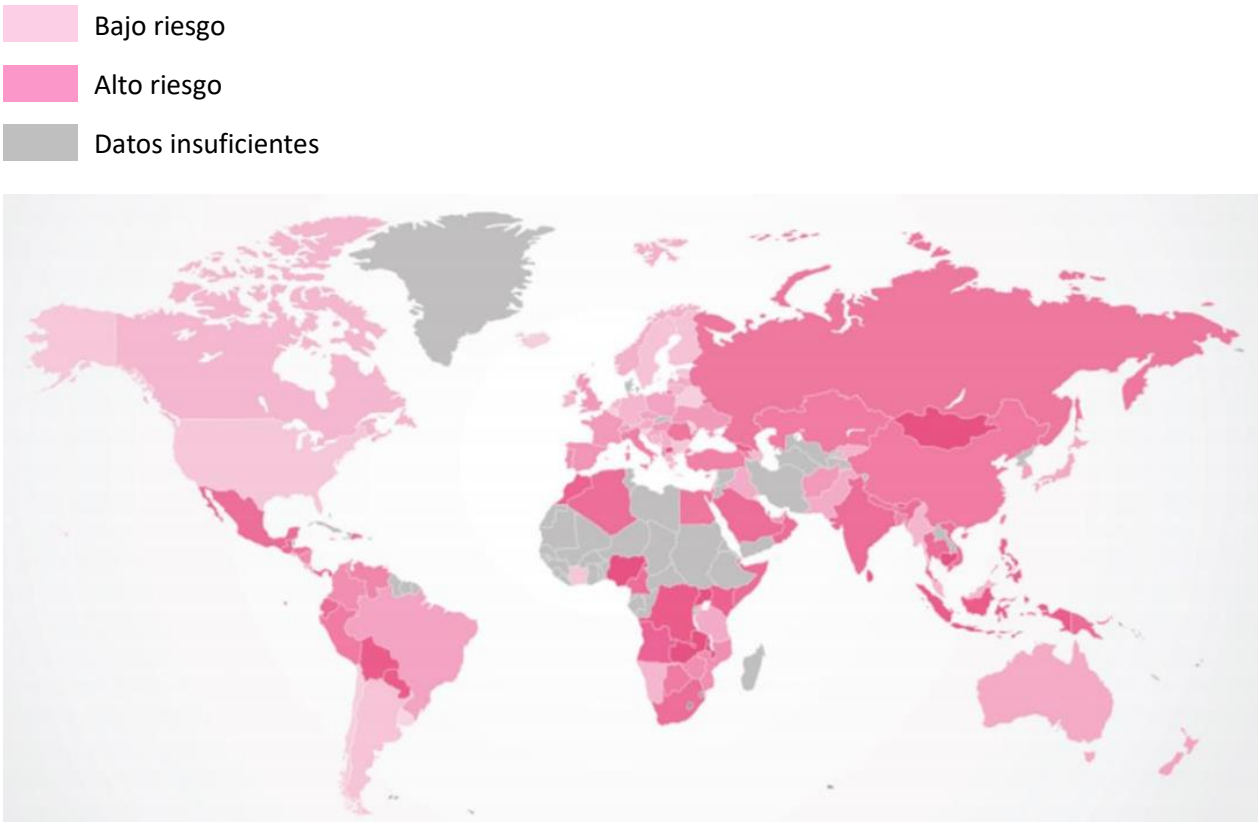

Figura 5. Índice mundial de amenazas cibernéticas 2017.

Fuente: Check Point Reseach Mid-Year Report Cyber Attack Trends (2017).

Gartnert (2017) indica que las marcas comerciales presentadas en su estudio lideran el mercado en cuanto a oferta de nuevas capacidades de seguridad, permitiendo a los clientes desplegarlos a un precio reducido, sin afectar la experiencia del usuario final y sin incrementar la carga de los empleados. Estos fabricantes además poseen un alto historial en la detección de vulnerabilidades en sus productos de seguridad. Entre las características comunes se incluyen fiabilidad, rendimiento consistente, y ser un producto fácil de gestionar, así como de administrar.

En la siguiente figura se presentan las marcas evaluadas por Gartner, ubicando de ellas dentro de sus cuatro cuadrantes, de izquierda a derecha es ponderado su visión de negocio y de abajo a arriba se califica su facilidad de implementación.

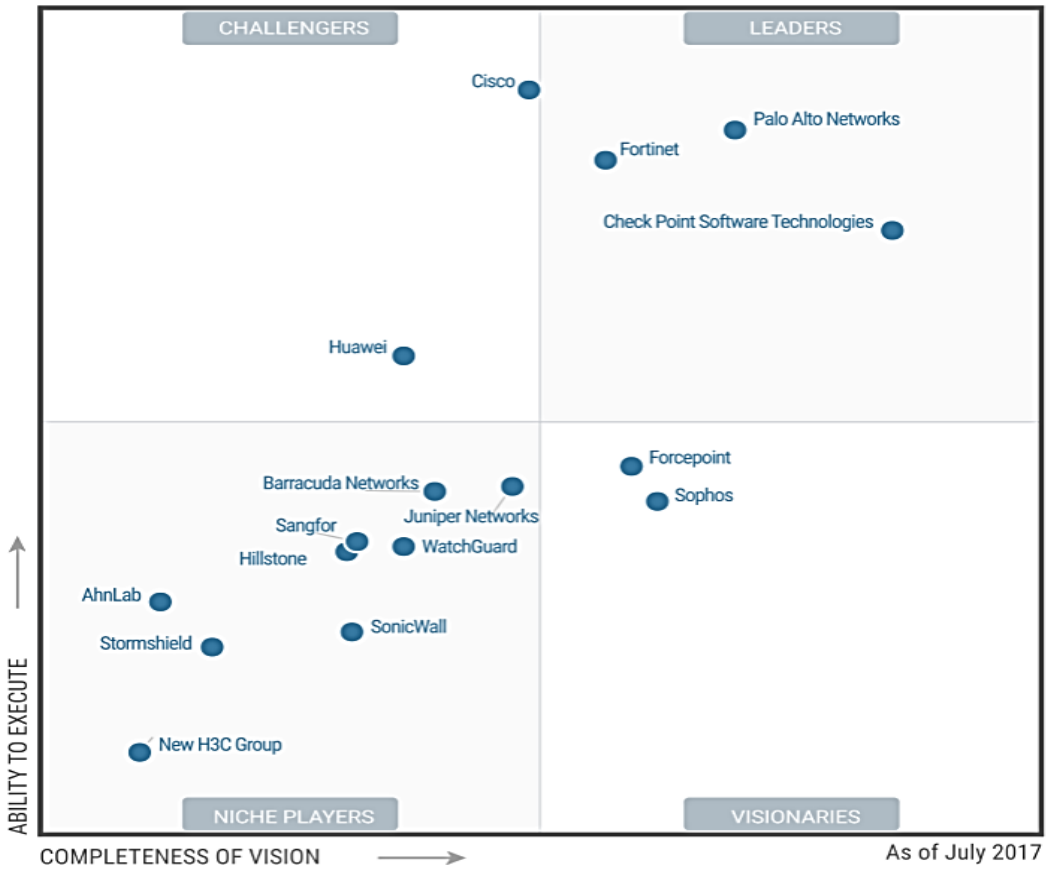

Figura 6. Cuadrante de Gartner para firewall.

Fuente: Gartnecrt (2017).

De la gráfica se observa que las marcas líderes en *firewall* comercial son Palo Alto Networks, Fortinet y CheckPoint Software Technologies.

1.2 Palo Alto Networks

La plataforma de seguridad de Palo Alto Networks proporciona una manera segura de habilitar las aplicaciones que los usuarios determinan, permitiendo el acceso a la vez que se evitan las amenazas de ciberseguridad. Inspecciona todo el tráfico de la red, incluidas las aplicaciones, las amenazas y contenidos, los cuales son vinculados al usuario independientemente de la ubicación o el tipo de dispositivo.

Entre los elementos de análisis de contenido y protección contra amenazas disponibles en dicho *firewall* se encuentran los siguientes:

Prevención de amenazas conocidas mediante IPS y antivirus o antispyware de red.

La protección contra una serie de amenazas conocidas se consigue con una inspección de un único paso mediante un formato de firma uniforme y un motor de análisis basado en flujos. Las funciones del sistema de prevención de intrusiones (IPS) bloquean exploits de vulnerabilidades en la capa de aplicación y de red (capas 3 y 7), desbordamientos de búfer, ataques de *DoS* y análisis de puertos.

La protección mediante antivirus o *antispyware* bloquea millones de tipos de malware, incluidos los que están ocultos en archivos comprimidos o el tráfico web (HTTP/HTTPS comprimido), así como virus en PDF conocidos. En cuanto al tráfico cifrado con SSL, puede aplicar de forma selectiva un descifrado basado en políticas y, a continuación, inspeccionar el tráfico en busca de amenazas, independientemente del puerto.

Bloqueo de malware desconocido o selectivo.

Este *firewall* tiene la herramienta *Wildfire*, la cual puede identificar y analizar el malware desconocido o selectivo (como las amenazas avanzadas persistentes) oculto en los archivos de varios sistemas operativos y versiones de aplicaciones. Esta herramienta observa y ejecuta directamente los archivos desconocidos en un espacio aislado virtualizado en la nube o en el dispositivo WF-500. Supervisa más de 420 comportamientos maliciosos y, si encuentra *malware*, desarrolla una firma y se la entrega automáticamente en escasos minutos. *WildFire* es compatible con todos los principales tipos de archivos, como PE, .doc, .xls y .ppt de Microsoft Office, el formato de documento portátil (PDF), Java Applet (jar y class) y los paquetes de aplicaciones de Android (APK). Además, tiene la capacidad de analizar los enlaces de los mensajes de correo electrónico a fin de detener los ataques de *phishing*.

Identificación de los hosts infectados por bots y las interrupciones de la actividad en la red a causa del *malware*.

La clasificación completa y contextual de todas las aplicaciones, en todos los puertos, incluido cualquier tráfico desconocido, a menudo puede revelar anomalías o amenazas en la red. Al respecto, Palo Alto tiene la aplicación App-ID de comando y control, los informes de comportamiento de *botnets*, el *sinkholing* de DNS y el DNS pasivo para vincular rápidamente el tráfico desconocido; los DNS sospechosos y las consultas de URL con *hosts* infectados. Asimismo, contiene funciones de inteligencia global para interceptar consultas de DNS de dominios maliciosos y aplicarles la técnica de *sinkhole*.

Limitación de trasferencias de archivos y datos no autorizadas.

Las funciones de filtrado de datos permiten a los administradores implementar políticas que reduzcan los riesgos asociados a las transferencias de archivos y datos no autorizadas. Las transferencias de archivos se pueden controlar explorando el interior del archivo (en lugar de comprobar simplemente la extensión) para determinar si se debe permitir la transferencia o no. Los archivos ejecutables, que por lo general se encuentran en descargas ocultas, se pueden bloquear para proteger la red de la propagación de *malware* oculto. Las funciones de filtrado de datos pueden detectar y controlar el flujo de patrones de datos confidenciales (números de tarjetas de crédito o de la Seguridad Social y patrones personalizados).

Control de la navegación web.

Palo Alto tiene un motor de filtrado de URL que es personalizable y totalmente integrado, lo que permite aplicar políticas exhaustivas de navegación por Internet, con lo que se complementa la visibilidad de las aplicaciones y las políticas de control que protegen la red de todo un abanico de riesgos asociados a las normativas legales y a la productividad.

Políticas basadas en dispositivos para el acceso a aplicaciones.

Este *firewall* tiene la herramienta GlobalProtect, que permite establecer políticas específicas para controlar qué dispositivos pueden acceder a recursos de red y aplicaciones concretos. Permite comprobar si el dispositivo móvil está actualizado e incluso verificar si tiene todos los parches aplicados antes de acceder a datos confidenciales.

Confirmación de hosts que se encuentran en riesgo.

El motor de correlación automatizada busca indicadores de peligro predefinidos en toda la red, correlaciona las coincidencias y pone de relieve automáticamente los hosts que se encuentran en riesgo, por lo que se reduce la necesidad de realizar una minería de datos manual.

Gestión de seguridad

Por otro lado, el *firewall* PaloAlto tiene integrada una plataforma de Gestión de seguridad de la red que puede gestionarse individualmente mediante una interfaz de línea de comandos (CLI) o una interfaz basada en navegador completamente equipada.

Incluso está proyectada para implementaciones a gran escala, a fin de aportar a nivel global funciones de visibilidad, edición de políticas, elaboración de informes y creación de *logs*. La flexibilidad y la forma práctica de su uso pueden ser utilizadas para realizar cambios en cualquier momento sin necesidad de preocuparse por los problemas de sincronización. La compatibilidad adicional con herramientas basadas en estándares, le permite integrar herramientas de gestión de terceros.

Elaboración de informes.

El *firewall* genera informes predefinidos, mismos que se pueden utilizar tal y como están, o bien pueden personalizarse o agruparse en un solo informe con el fin de adaptarse a los requisitos específicos.

Creación de logs.

El filtrado de logs en tiempo real facilita la rápida investigación forense de cada sesión que viaja por la red. El contexto completo sobre la aplicación, el contenido (incluido el malware detectado por *WildFire*) y el usuario puede utilizarse como criterio de filtrado. Los resultados se pueden exportar a un archivo para archivarlos sin conexión o realizar análisis adicionales.

Resumen:

El *firewall* trabaja hasta la **capa 7 del modelo OSI**, abarcando un enfoque holístico de seguridad bajo las siguientes características:

Integración nativa de tecnologías que se sirven de una arquitectura de prevención de una sola pasada para ejercer un control positivo en función de las aplicaciones, usuarios y contenidos con el fin de reducir

la superficie de ataque de la organización; que favorecen la organización, visibilidad y comunicaciones abiertas; y que habilitan una estrategia de seguridad acorde desde la red hasta la nube, pasando por los *endpoints*.

Automatización de la creación y entrega de mecanismos de protección frente a nuevas amenazas para los entornos de red, de nube y de endpoint.

Capacidad de ampliación y flexibilidad que permiten proteger a los clientes a medida que crecen, abandonan su red física o adoptan nuevas tecnologías.

Uso compartido de inteligencia sobre amenazas que, gracias al efecto de red de una comunidad en la que se comparten datos globales y detallados acerca de amenazas, ofrece protección para minimizar la propagación de los ataques.

1.3 Fortinet

Proporciona una solución integrada de seguridad compuesta por las funcionalidades más eficaces que proporcionan una protección completa de las redes de comunicaciones, como son: *Firewall*, VPN (IPSEC y SSL), *Antimalware*, *Anti-Botnet*, *Anti-DOS*, Sistemas de Detección/Prevención de Intrusiones, Filtrado Web, Antispam, Control de Aplicaciones, Inspección de Contenido en SSL, *firewall* de aplicaciones WEB e inspección del acceso a aplicaciones cloud (CASI). Además, todas las funcionalidades de seguridad se integran de forma conjunta con funcionalidades añadidas como *Traffic Shaping*, Alta Disponibilidad, balanceo de carga, Aceleración y balanceo Wan, Soporte a VoIP, Controlador Wireless, enrutamiento dinámico RIP, OSPF y BGP, entre otros.

Los *firewalls* FortiGate suministran alto rendimiento, seguridad validada de múltiples niveles en las capas OSI y visibilidad granular para protección integral en toda la red de una organización. La tecnología de procesadores de seguridad (SPU) están diseñados específicamente para brindar un rendimiento escalable y una latencia ultra baja para capacidades de seguridad avanzadas. Fortinet tiene entre sus servicios de seguridad a FortiGuard Labs, quienes proporcionan actualizaciones continuas de inteligencia de amenazas y mitigación automática con el propósito de mantener sus dispositivos al día y de esta forma mitigar los ataques cibernéticos.

FortiGate reduce la complejidad y el costo total de propiedad junto con el respaldo de implementaciones escalables en el extremo de la red, el centro de datos, los segmentos internos y las sucursales distribuidas.

Entre los elementos de análisis de contenido y protección contra amenazas disponibles en dicho *Firewall* se encuentran los siguientes:

Firewall

Los equipos Fortinet poseen la funcionalidad de *firewall* basada en tecnología Stateful Inspection Packet. Esto le permite hacer un análisis exhaustivo de la cabecera de cada paquete, identificando la sesión a la que pertenece, checa el correcto orden de los paquetes y realizan un control sobre el tráfico de la red.

Las políticas del *firewall* controlan todo el tráfico que atraviesa el equipo FortiGate. Cada vez que el *firewall* recibe un nuevo paquete, analiza la cabecera de este para conocer las direcciones origen y destino, el servicio al que corresponde ese paquete, y determina si se trata de una nueva sesión o bien

pertenece a una sesión ya establecida y llega en el orden correcto. Este análisis de la cabecera es acelerado mediante el Circuito Integrado de Aplicación Específica FortiASIC, lo que permite a las plataformas FortiGate alcanzar un rendimiento mayor y un número de nuevas sesiones por segundo superior al de cualquier solución basada en la utilización de una CPU de propósito general.

Las políticas de seguridad son definidas en el *firewall* con base a las interfaces origen y destino. Este modo de definición de las políticas permite optimizar el rendimiento y el procesamiento de cada uno de los flujos, ya que para cada uno de los paquetes es identificado su origen y su destino y enviado entonces al módulo de routing. Esta organización permite que el paquete sea tan solo comparado contra las reglas definidas entre esos interfaces, comenzando por la superior de todas y descendiendo hasta encontrar aquella con que coincida en función de los diferentes parámetros configurables para cada política (par origen/destino, usuario, servicio, calendario, etc.). Si no se encuentra ninguna regla que coincidiera con el paquete analizado, éste sería descartado. Al tener que comparar contra un grupo menor que el total de las reglas definidas, el tiempo requerido disminuye, lo que agregado a la utilización de la tecnología FortiASIC confiere a los equipos FortiGate un alto rendimiento como *firewall*, llegando hasta 1 Terabps.

Inspección *Secure Sockets Layer* (SSL) y *Secure Shell* (SSH)

Dentro del perfil de protección se puede aplicar la configuración necesaria para efectuar inspección dentro de protocolos seguros basados en SSL, como HTTPS, SMTPS, POP3S, FTPS e IMAPS. De esta forma es posible aplicar dentro de los túneles SSL que atraviesen la plataforma inspección de contenidos, así como inspección *antimalware*, DLP o Control de aplicaciones. Además, existe la posibilidad de definir las excepciones del descifrado dentro del propio perfil, para evitar descifrar información

IP virtuales

Los dispositivos FortiGate permiten la configuración de IP's virtuales (VIP's) de manera que estas ofrecen balanceo de carga de servidores, teniendo la capacidad de que las peticiones realizadas a la IP virtual puedan ser atendidas por un grupo de servidores habilitados para ese efecto. La distribución del balanceo de carga puede ser configurada a nivel de puertos TCP o UDP, con la posibilidad de tener varios servicios desplegados en la misma IP y atendidos por grupos de servidores distintos. Cada uno de los servidores que componen grupo de balanceo, puede ser monitorizado a nivel ICMP, TCP o HTTP de manera que, ante el fallo de un servidor, el servicio continúa activo en el resto de equipos, dotando a la plataforma de alta disponibilidad.

De la misma forma, es posible configurar la IP virtual para que haga multiplexación del tráfico HTTP, de manera que varias conexiones externas se traducen en una única conexión entre el FortiGate y el servidor, haciendo que este consuma menos recursos al servir las peticiones entrantes.

Calidad de Servicio (QoS)

Mediante la aplicación de técnicas de Calidad de Servicio en la red, este *firewall* provee un servicio prioritario sobre el tráfico más sensible al retardo. Los equipos FortiGate permiten aplicar técnicas de priorización de tráfico y Calidad de Servicio (QoS), reservar ancho de banda para aquellas aplicaciones que sean más sensibles al retardo, o bien limitar el ancho de banda de aquellas aplicaciones que hagan un uso intensivo de los recursos de la red.

La Calidad de Servicio es una funcionalidad fundamental para poder gestionar el tráfico generado por la transmisión de voz y las aplicaciones multimedia. Estos tipos de tráfico son sensibles al retardo y a la

variación del mismo (jitter). Una adecuada gestión de la calidad de servicio permite la utilización de estas aplicaciones sin recurrir a una ampliación innecesaria del ancho de banda de la red, reservando el ancho de banda necesario y priorizando este tipo de tráfico ante otros menos sensibles al retardo como pueda ser el correo o el tráfico ftp.

La gestión de ancho de banda se realiza mediante la utilización de buffers que permiten regular los diferentes flujos de tráfico con base a la velocidad de transmisión de los paquetes. Lo que se consigue de este modo es evitar que los paquetes sean descartados, haciendo que se almacenen en el *buffer* hasta su transmisión, retrasando su envío hasta que sea posible. Los equipos FortiGate usan la técnica *Token Bucket* para garantizar y limitar el ancho de banda.

La bufferización se realiza en función de la prioridad asignada a cada flujo, pudiendo variar entre prioridad alta, media o baja. Si el ancho de banda no es suficiente para el envío de todos los paquetes almacenados, se transmiten en primer lugar los de prioridad alta.

Gestión del Ancho de Banda (*Traffic Shaping*)

Los parámetros de configuración del ancho de banda permiten definir un ancho de banda mínimo o un límite máximo para el tráfico identificado con esa política. El ancho de banda definido no puede superar el ancho de banda total disponible, pero puede ser empleado para mejorar la calidad del uso de esté por aquellas aplicaciones que hagan un uso intensivo del mismo, o bien aquellas aplicaciones sensibles al retardo. Así mismo, también es posible establecer traffic shaping por IP, de forma que sea aplicado por cada dirección IP, en lugar de por política.

Redes Privadas Virtuales (VPN)

Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL, además de PPTP, L2TP over IPSEC (Microsoft VPN) y GRE over IPSEC (Cisco VPN). De esta forma las organizaciones pueden establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet.

La funcionalidad VPN está integrada en la propia plataforma FortiGate sin necesidad de licencia, así como también se puede utilizar mediante la instalación de la suite de aplicaciones Forticlient Endpoint Security, que permite el establecimiento de VPNs desde un equipo cliente. También es posible integrarlo a través de software VPN de terceros (solo para IPSEC).

Escaneo de firmas

El escaneo de firmas analiza las cadenas de bytes de los ficheros que son conocidas para identificar virus. Si toda la cadena de bytes se identifica con un virus en particular, el archivo se considera infectado. Los sistemas antimalware basados en análisis de firmas constituyen el método más efectivo y más utilizado en la detección de virus.

El análisis incluye también el escaneo de las macros existentes en los archivos Microsoft Office en busca de cadenas conocidas de virus macro. Los macros son también analizados en búsqueda de comportamientos anómalos tales como importar y exportar código, escribir en el registro o intentos de deshabilitar características de seguridad

Para realizar este análisis de firmas existen dos elementos claves:

- Una base de datos que contiene las firmas de virus conocidos

- Un motor de escaneo que compara los archivos analizados con las firmas en la base de datos para detectar una concordancia indicando la presencia de un virus.

Por otra parte, el rendimiento es la clave para la detención eficiente de virus que cada vez son más y más complejos. La aceleración del reensamblado de los paquetes y la comparación con las firmas mediante FortiASIC es un componente clave que permite a FortiGate la realización de este análisis en tiempo real sin introducir retardo sobre el normal funcionamiento de la red y las aplicaciones.

A todo lo anterior hay que añadir la posibilidad de hacer offloading de la configuración del Antimalware enviando las peticiones de proceso a un servidor ICAP previamente configurado, el cual se encargaría de dirimir de manera externa la existencia de virus, enviando la respuesta al FortiGate para que este ejecute la acción que tenga configurada en cada caso.

Actualización de la Base de Firmas y Motor de Escaneo

Las actualizaciones del antimalware contienen la base del conocimiento de virus y el motor de escaneo, los cuales son continuamente actualizados por Fortinet y distribuidos mediante la red FortiGuard tan pronto como nuevos virus y gusanos son encontrados y difundidos.

Actualizaciones automáticas

Los equipos FortiGate son actualizados dinámicamente gracias a la red *FortiGuard Distribution Network* (FDN). Los servidores FDN se encuentran distribuidos a lo largo de todo el mundo con disponibilidad 24x7 para entregar nuevas firmas y motores para los dispositivos FortiGate. Todos los equipos FortiGate están programados con una lista de servidores FDN más cercanos de acuerdo a la zona horaria configurada en el equipo. Asimismo, las plataformas de gestión FortiManager pueden actuar como un nodo de la red FDN para los equipos que gestiona.

IDS (Sistema de Detección y Protección de Intrusión)

El Sistema de Detección y Protección de Intrusión de FortiGate constituye un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red.

El motor IDS provee seguridad hasta la capa de aplicación, sin mermar por ello el rendimiento de la red. La capacidad de IDS de los equipos FortiGate se basa en el módulo de routing, el módulo de *firewall* y la capa de aplicación. De esta forma el sistema de detección de intrusiones no se limita únicamente a la detección de ataques de nivel de red ni tampoco al análisis individual de cada paquete. FortiGate reensambla el contenido de los paquetes en línea y los procesa para identificar ataques hasta el nivel de aplicación (capa 7 del modelo OSI).

Cada sensor (Red, IP, Transporte, Aplicación) es un programa que genera un tráfico ínfimo. El sensor utiliza el hardware FortiASIC para acelerar la inspección del tráfico y chequear patrones de tráfico que concuerden con las firmas y anomalías especificadas. La arquitectura hardware asistida de detección de intrusión provee a los equipos FortiGate de rendimientos excepcionales únicos en el mercado.

La funcionalidad IPS de FortiGate detecta y previene los siguientes tipos de ataques:

- Ataques de Denegación de Servicio (DoS)
- Ataques de Reconocimiento

- *Exploits*
- Ataques de Evasión de Sondas IDS
- *Botnets*

Resumen:

El *firewall* trabaja hasta la **capa 7 del modelo OSI**, es un dispositivo UTM con las siguientes características:

Rendimiento con baja latencia, gracias a la conjunción del procesador FortiASIC, diseñado para acelerar los procesos de nivel de red.

Dispone del sistema operativo de seguridad flexible, FortiOS, que cuenta con múltiples capas de protección contra amenazas y habilitar entornos más seguros.

Cuenta con servicios de suscripción FortiGuard, que se encargan de mantener todos los sistemas de FortiGate debidamente actualizados, en tiempo real y de forma automática; aspecto fundamental a la hora de enfrentarse a nuevas amenazas.

Permite aumentar la visibilidad de la red gracias a su capacidad de inspección profunda de todos los paquetes de datos que circulan por la red, evitando la propagación de infecciones y permitiendo priorizar el uso de ancho de banda para aplicaciones como la videoconferencia o la telefonía IP.

1.4 CheckPoint Software Technologies

Control de acceso

Firewall Software Blade de CheckPoint, permite controlar de forma segura el acceso a clientes, servidores y aplicaciones. Con una visibilidad detallada de los usuarios, grupos, aplicaciones, máquinas y tipos de conexión, *Check Point Firewall Software* Blade brinda una protección superior en toda la pasarela de seguridad.

Autenticación

La autenticación permite asignar permisos de acceso a individuos y grupos, según su nivel de responsabilidad y rol dentro de la organización. Al respecto, *Firewall Software Blade*, basado en un reconocimiento de identidad, proporciona sólidas capacidades de autenticación para confirmar la identidad de todos los usuarios y así poder establecer sus privilegios. Esto lo realiza a través de una funcionalidad integrada de reconocimiento de usuarios y máquinas a través de la puerta de enlace de seguridad y administración.

Modo Puente

Una puerta de enlace de seguridad en modo puente funciona como un *firewall* regular, inspecciona el tráfico y elimina o bloquea el tráfico no autorizado o inseguro, y es invisible para todo el tráfico de capa 3. Cuando el tráfico autorizado llega a la puerta de enlace, se pasa de una interfaz a otra a través de un procedimiento conocido como puente. *Firewall Software Blade* crea una relación en capa 2 entre dos o

más interfaces, por lo que cualquier tráfico que entre en una interfaz siempre sale de la otra. De esta forma, el *firewall* puede inspeccionar y reenviar el tráfico sin interferir con el enrutamiento IP original.

Políticas granulares.

El *firewall* posibilita la habilitación de definiciones de políticas granulares por usuario y grupo, lo que conlleva a una identificación completa del usuario, mediante una definición simple de la política basada en la aplicación por usuario o grupo directamente desde el dispositivo. La identificación de los usuarios se puede realizar en por medio de tres métodos: 1.- Consultando el directorio activo, 2.- A través de un portal cautivo y 3.- Instalar un agente del lado del cliente.

Traducción de direcciones de red (NAT)

Independientemente de que las computadoras tengan direcciones enrutables o no enrutables, ocultar sus direcciones reales es una medida de precaución para asegurarse de que dichas direcciones no se puedan ver desde fuera de la organización o desde otras partes de la misma. La dirección interna de una red contiene la topología de la red y, por lo tanto, ocultar esta información mejora en gran medida la seguridad.

Resumen:

El *firewall* CheckPoint Software Technologies trabaja hasta la **capa 7 del modelo OSI** con las siguientes características:

Proporciona una visibilidad detallada de los usuarios, grupos, aplicaciones, equipos y tipos de conexión en la red para que puedan asignar permisos a los usuarios y dispositivos adecuados.

Respecto a las políticas de seguridad ofrece un control granular de permisos sobre estas entidades; esto da como resultado un nivel de protección mayor.

Proporciona una identificación completa del usuario, lo que permite una definición de políticas sencilla basada en aplicaciones por usuario o grupo directamente desde el *firewall*.

Maneja una gestión integrada unificada, lo que permite simplificar la tarea de administrar su entorno de seguridad. Puede monitorear y controlar amenazas, dispositivos y usuarios con una interfaz gráfica altamente intuitiva que proporciona vistas, detalles e informes sobre su estado de seguridad. Así mismo permite administrar todas las puertas de enlace desde un completo y centralizado panel de control de seguridad.

Incluye el *software Check Point IPS Software Blade*, que protege la red mediante la inspección de paquetes que atraviesan la puerta de enlace. Se trata de un IPS con todas las funciones, que proporciona geoprotecciones y actualizaciones de definición de amenazas frecuentes y automatizadas. Debido a que el IPS forma parte de la arquitectura integrada de Blade de software, brinda las ventajas de despliegue y administración de una solución unificada y extensible.

Por otro lado, en un estudio realizado por *IT Central Station* (2017) reporta un ranking de los *firewalls* comerciales considerando las revisiones, ratings y comparaciones de diversos profesionales que han utilizado dichas herramientas. Véase figura 7.

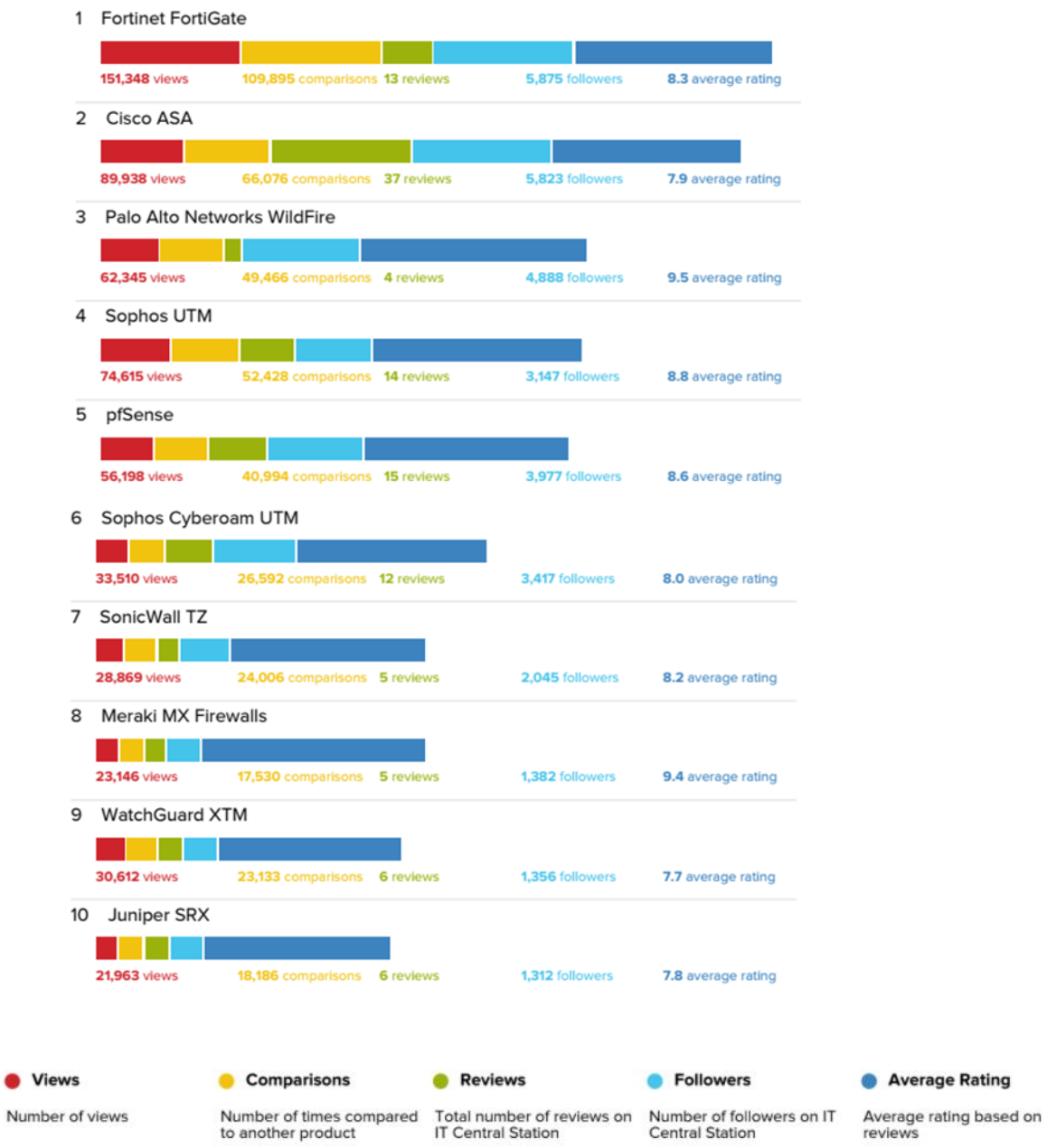

Figura 7. Top Firewalls Solutions.
Fuente: IT Central Station (2017).

Algunos de los estudios de caso analizados en dicho estudio se muestran a continuación:

Fortinet Fortigate

En el caso de una compañía farmacéutica / biotecnológica de 5,001 a 10,000 empleados, el encargado de la Automatización de procesos y seguridad enumera varias características para Fortinet FortiGate:

- Lo suficientemente flexible como para manejar todo lo que se requiera.
- El diseño de la configuración es fácilmente comprensible.
- Permite que las reglas de *firewall* sean programadas y nombradas de forma que sean "legibles".
- Soporte de VPN y protección antivirus.

Cisco ASA

De acuerdo a las observaciones de algunos casos de estudio, los administradores identificaron que este *firewall* tiene entre otras cualidades VPN de sitio a sitio y alta disponibilidad. Además, la integración de los servicios de FirePOWER (*Web Filtering* / IPS / *Malware Protection*) es un gran soporte para dicha plataforma.

La evidencia que arrojan estos casos de estudio indica que los servicios de FirePOWER permitieron un mejor control y visibilidad sobre el tráfico que atraviesa el perímetro de su organización. La alta disponibilidad ayudó a mejorar en gran medida la disponibilidad de los servicios al reducir el tiempo de inactividad causado tanto por los incidentes como por las operaciones de mantenimiento planeadas.

Palo Alto Networks WildFire

Para los administradores de red, el aspecto relevante de este *firewall* es la función de análisis dinámico de WildFire ya que tiene un papel decisivo en el bloqueo de una serie de nuevas amenazas antes de que las herramientas comunes de antivirus de escritorio pueden detectarlas. Por citar un ejemplo un ingeniero senior de seguridad de redes apunta que cuando *Wannacry* salió por primera vez, este *firewall* lo detectó en su red y eliminó las amenazas entrantes en segundos.

pFSense

Algunos casos de estudio señalan que las características más valiosas de pfSense que han encontrado son: Fácil de implementar y de usar, los gráficos de tráfico son excelentes y las herramientas que pueden incluirse como *squid, snort, squidguard, ntop, pfblogNG*, soportan dicha herramienta.

Sophos

De acuerdo a administradores de red, entre las características relevantes de dicho *firewall* están: El filtro web y el ATP (protección avanzada contra amenazas) son sobresalientes y fáciles de administrar, así como el WAF integrado (*firewall* de aplicaciones web) que permite al administrador proteger sin problemas los servicios HTTP/S sin tener que pagar miles de dólares. Además, con la inclusión del sistema Sandstorm para protección, el *firewall* se ve más fortalecido.

De lo anterior se observa que actualmente los *firewalls* comerciales manejan una gestión unificada de amenazas (UTM), que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad el cual ofrece varias funciones de seguridad en un solo punto en la red.

Un producto UTM generalmente incluye funciones como antivirus, *anti-spyware, anti-spam*, *firewall* de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, network address translation) y compatibilidad para redes privadas virtuales (VPN, virtual private network).

La ventaja de estos productos se basa en la integración de soluciones de seguridad, por lo que en una red de telecomunicaciones pudieran tener productos para cada tarea de seguridad por separado, ahora

los pueden tener todos en una sola con el apoyo de un único equipo y que se ejecuta en una sola consola.

Aplicaciones	Servicios									
	Firewall	Antispam	Antivirus	Antispyware	IPS	Filtrado web	VPN	QoS Calidad de servicio	Control de aplicaciones	Monitoreo
FORTINET	X	X	X	X	X	X	X	X	X	
Palo Alto Networks	X	X	X	X	X	X	X	X	X	X
CheckPoint Software Technologies	X	X	X	X	X	X	X		X	X

Tabla 1. Resumen de las características de firewalls comerciales.

En el tenor de estas ideas NSS Labs realizó un estudio de *firewalls* de siguiente generación (NGFW, por sus siglas en inglés) considerando los criterios de efectividad en la seguridad, como es su comportamiento, estabilidad y costo total.

NSS Labs señala que, con la aparición de nuevas aplicaciones web y amenazas de seguridad, los f*irewalls* están evolucionando aún más. Los *firewalls* de próxima generación tradicionalmente se han implementado para defender la red en el límite, pero las empresas han ampliado las opciones de implementación para incluir la segmentación interna.

A medida que las tendencias de la Web 3.0 impulsan las aplicaciones comerciales críticas a través de puertos de *firewall* que anteriormente estaban reservados para una sola función, como HTTP, la tecnología de *firewall* tradicional está limitada. No puede diferenciar entre el tráfico HTTP real y los servicios que no son HTTP haciendo un túnel sobre el puerto 80, como VoIP o mensajería instantánea. Indica que se debe realizar una monitorización a nivel de aplicación además del análisis de puerto y destino, por lo que los cortafuegos están evolucionando para abordar esta mayor complejidad.

Ya no es posible confiar únicamente en las combinaciones de puertos y protocolos para definir aplicaciones de red. El *firewall* de próxima generación debe ser capaz de realizar una profunda inspección de paquetes en todos los paquetes, en todos los puertos y en todos los protocolos, a fin de determinar qué aplicaciones se ejecutan sobre qué puertos y así protegerlos de manera efectiva. Además, con el uso ampliado de SSL / TLS en gran parte del tráfico que atraviesa la red moderna, se requiere la inspección del contenido encriptado.

Al respecto, algunas empresas como Cisco, Fortinet, Check Point, Palo Alto, entre otras, están actualmente integrando este tipo de aplicaciones a sus *firewalls* comerciales. Véase figura 8.

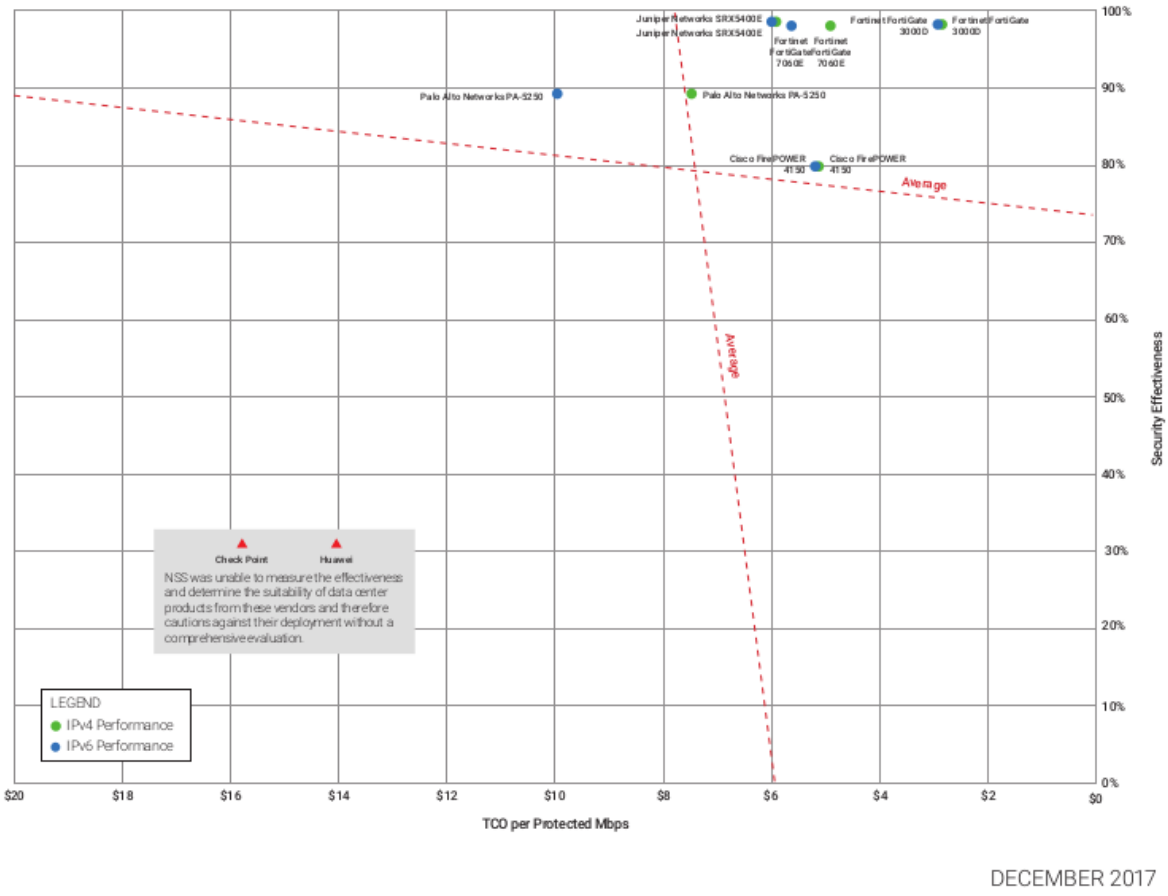

Figura 8. Next Generation Firewall.
Fuente: Next Generation Firewall Methodology v8.0, NSS LABS (2017).

2 Firewall de código abierto

El *software* de código abierto por lo general se refiere al *software* cuyo código fuente está disponible para que cualquiera pueda estudiar, usar y adaptar (Open Source Initiative, 2017). En el desarrollo de *software*, el término de código abierto se trata de un *software* cuyo código fuente está disponible, por lo que el desarrollador proporciona derechos y obligaciones para manipular o improvisar y redistribuir según la necesidad del proyecto, teniendo el control total del mismo. Eso no significa que sea gratuito, sino que solo está disponible. Dado que los programadores que modifican y venden *software*, brindan soporte técnico, lo que implica que pueden cobrar por ello.

Por lo tanto, un *firewall* de código abierto se refiere a *software* de seguridad disponible de desarrolladores con licencia GPL v1 o v2, integrada con utilidades de seguridad y herramientas diseñadas para filtrar e

inspeccionar paquetes con estado y protocolos de capa de aplicación como HTTP, FTP y SMTP (Thakur Amit, 2015).

Además, se extiende a la funcionalidad VPN, SSL e IPsec, por lo que existen distribuciones de *firewall* de código abierto que están en uso como resultado de esta emergente solución de seguridad. La mayoría incluye un *proxy* web conocido como "Squid"; ayuda de varias formas, como el filtrado de contenido y el de tráfico.

La idea de Squid se generó con el concepto de mejorar la experiencia del usuario al ahorrar ancho de banda de los ISP y escalar sitios web comerciales sin actualizar el hardware. El crecimiento exponencial aparece en el despliegue de Squid en sitios web empresariales y de pequeña escala.

La aplicación y características de un *firewall* van desde lo simple a lo sofisticado, en el caso de los *firewalls* de código abierto proporcionan seguridad contra diferentes intrusiones. Es de observar que hay escaso soporte oficial para estas herramientas de código abierto, el uso de dicho *software* lleva riesgos inherentes por lo que se debe tener especial cuidado. Sin embargo, si existen redes de soporte, aunque algo no tradicionales como la publicación de preguntas en listas de correos, lo cual puede resultar a menudo útil (Howlett, 2004).

Al respecto, se han considerado los siguientes *firewalls* para comparar sus características, limitaciones y ventajas.

2.1 Pfsense

Pfsense es una distribución libre del sistema operativo FreeBSD modificada para ofrecer el servicio de *firewall* y *router*. Posee una interfaz para su administración vía web, llamada WebGUI, es una plataforma poderosa y flexible de enrutamiento y filtrado. Tiene aplicaciones con propósitos específicos, tales como para servicios de VPN, DNS, Sniffers y DHCP a estos se les llama módulos, lo cuales están diseñados exclusivamente para PFsense. Posee varias funcionalidades, aparte de *firewall*, balancea cargas, puede ser servidor PPPoE para la autenticación de usuarios, puede implementar enlaces redundantes por medio del protocolo CARP, realiza reportes y monitoreo. El mecanismo de filtrado utilizado por PFsense se llama *packet filter* (PF), es un filtrado de paquetes a nivel de *kernel* y utilidades de entorno de usuario para el control de las funcionalidades del mismo.

La suite PFsense posee múltiples paquetes disponibles dentro de una lista del mismo sistema operativo, su instalación es simple y rápida, posee herramientas de monitorización, protocolos de ruteo, paquetes de filtrado, entre otros.

Filtrado de paquetes

Una de las principales funciones de pfSense, independientemente del rol en el que se implementa, es el filtrado tráfico. Solo permite el tráfico en la interfaz donde éste se inicia. Cuando hay una conexión que coincide con una regla de aprobación en su *firewall*, una entrada se crea en la tabla de estado del *firewall*, donde la información sobre las conexiones activas a través del *firewall* es retenida. La respuesta a este tráfico se da por medio de las conexiones iniciadas dentro de su red que permite automáticamente de volver a su red por la tabla de estado. Esto incluye cualquier tráfico relacionado que utilice un protocolo diferente, como los mensajes de control ICMP que pueden proporcionarse en respuesta a un TCP, UDP u otra conexión.

El *firewall* regula el tamaño de la tabla de estado, varía según la RAM instalada en el sistema, pero puede ser aumentado en tiempo real a la dimensión deseada. Cada estado ocupa aproximadamente 1 KB de RAM, este parámetro debe ser considerado para dimensionar la memoria requerida.

PfSense ofrece numerosas opciones para la gestión del estado:

Keep state – Trabaja con todos los protocolos.

Modulate state – Trabaja solo con TCP y genera ISNs (Initial Sequence Numbers) por cuenta del host

Synproxy state – Los Proxy inician las conexiones TCP para ayudar los servers de spoofed TCP SYN floods

None – No se mantiene ninguna información sobre el estado

PfSense utiliza p0f, una avanzada herramienta de red para huellas dactilares digitales que habilita la filtración a través el sistema operativo al inicio de la conexión. Así mismo posibilita la administración de políticas de enrutamiento con alta flexibilidad para la selección del gateway sobre las reglas de base para el equilibrio de ancho de banda, *failover, backup* sobre ADSL, entre otros.

Posibilidad de creación de Alias de grupos de IP y nombres de IP, networks y puertas. Estas características ayudan a mantener la configuracion limpia y facil de entender, especialmente con configuraciones con varios IP públicos y numerosos servidores.

Por otro lado, realiza un filtro en la capa dos, lo que posibilita puentear interfaces y filtrar el tráfico entre estas.

NAT

La traducción de direcciones de red (NAT) permite conectar múltiples computadoras a Internet usando una sola dirección IP pública; pfSense habilita estas implementaciones, pero también acomoda configuraciones NAT mucho más avanzadas y complejas requeridas en redes con múltiples direcciones IP públicas.

NAT está configurado en dos direcciones: entrante y saliente. El NAT saliente define cómo se traduce el tráfico que sale de su red destinada a Internet. La NAT entrante se refiere al tráfico que ingresa a su red desde Internet. El tipo más común de NAT es de entrada y el más familiarizado con el puerto es hacia adelante.

Routing

Una de las principales funciones de un *firewall* es el tráfico de enrutamiento, además del filtrado y la realización NAT, como lo son las rutas estáticas, los protocolos de enrutamiento, enrutamiento de direcciones IP públicas y visualización de información de enrutamiento.

Bridging

Normalmente, cada interfaz en pfSense representa su propio dominio de difusión con una subred IP única, actuando de la misma manera que los interruptores separados. En algunas circunstancias, es deseable o necesario combinar múltiples interfaces en un solo dominio de difusión, donde dos puertos en

el *firewall* actúan como si estuvieran en el mismo interruptor, excepto que el tráfico entre las interfaces se puede controlar con reglas de *firewall*. Esto se conoce comúnmente como un *firewall* transparente.

VLAN

Las VLAN proporcionan un medio para segmentar un solo interruptor en múltiples dominios de difusión, permitiendo que un solo interruptor funcione de la misma manera que múltiples interruptores. Esto se usa comúnmente para la segmentación de la red de la misma manera que se podrían usar múltiples conmutadores para colocar los hosts en un segmento específico como configurado en el interruptor. Cuando se emplea el enlace entre conmutadores, los dispositivos en el mismo segmento no necesitan residir en el mismo interruptor.

Múltiple conexiones WAN

Las diferentes capacidades WAN (multi-WAN) de pfSense le permiten utilizar múltiples conexiones de Internet para lograr un mayor tiempo de actividad y capacidad de rendimiento. Antes de continuar con una configuración de múltiples WAN, necesita una configuración de dos interfaces en funcionamiento (LAN y WAN), pfSense es capaz de manejar muchas interfaces WAN, con múltiples implementaciones usando 10-12 WANs en producción. Tiene la capacidad de escalar aún más que eso, y dicha interfaz WAN adicional se denomina interfaces OPT WAN.

Virtual Private Network

Las VPN proporcionan un medio para canalizar el tráfico a través de una conexión encriptada, evitando que ser visto o modificado en tránsito. PfSense ofrece tres opciones de VPN con IPsec, OpenVPN y PPTP.

Traffic Shaper

La configuración del tráfico o también conocido como la calidad de servicio de la red (QoS), es un medio para priorizar la red tráfico que atraviesa el *firewall*. QoS ofrece un medio para priorizar diferentes tipos de tráfico, asegurando que los servicios de alta prioridad reciben el ancho de banda que necesitan antes de los servicios de menor prioridad. El asistente de modelador de tráfico en pfSense brinda la capacidad de configurar rápidamente el QoS. Así mismo se pueden crear escenarios y reglas personalizadas para tareas más complejas.

Wireless

PfSense incluye funciones de conexión inalámbricas integradas que le permiten convertir la instalación de pfSense en un punto de acceso inalámbrico, utilizando una conexión inalámbrica 802.11 como una conexión WAN, o ambas.

Portal Cautivo

La función Portal cautivo de pfSense permite dirigir a los usuarios a una página web antes de darle acceso a Internet. Desde esa página, puede permitir que los usuarios accedan a Internet después de hacer clic a través de ésta, o solicitar autenticación. También se puede usar con usuarios que utilizan una red conectada mediante cable.

2.2 Untangle

Untangle Unified threat management (UUTM) es un *firewall* de capa de aplicación OSI 7 que filtra el tráfico en función de la dirección IP, el número de puerto, el protocolo y los usuarios, así como grupos de Active Directory.

UUTM es una solución Linux completa de código abierto con OpenVPN incorporado. Se puede actualizar en hardware a bajo costo. Provisto de una interfaz gráfica para configuración y administración, UTM es una distribución de fuente abierta con menos tiempo de inactividad, funciones de respaldo en vivo junto con cero estreses de instalación y configuración. El tiempo de instalación es rápido y la mayoría de las extensiones se pueden activar usando el consumo normal de recursos. Como la configuración se realiza con interfaz gráfica, es bastante simple de instalar con una interfaz clic y sin conocimiento técnico de una línea de comandos.

- Web Filter, para evitar ingresar a sitios no deseados.
- Virus Blocker, que impide el ingreso de virus a nuestra red.
- Reports, para saber quién se encuentra en línea.
- Spam Blocker, para impedir el spam dentro de la red.
- OpenVPN, que permite accesos remotos seguros dentro de la red.
- AdBlocker, esta aplicación impide la publicidad invasiva.
- Protocol Control, para evitar el uso de la red para juegos en línea.
- Phish Blocker, que impide el robo de identidad.
- Intrusión Prevention, para detectar y proteger del ataque de hackers.
- QoS, prioriza el tráfico dentro de la red.
- *Firewall*, para proteger la red de intrusos.
- Spyware Blocker.

2.3 Opnsense

El conjunto de funciones del Firewall OPNsense incluyen el proxy de caché directo, la configuración del tráfico, la detección de intrusiones y una versión del cliente OpenVPN. Se basa en FreeBSD y utiliza un marco Modelo Vista Controlador (MVC) recientemente desarrollado basado en Phalcon.

El enfoque de OPNsense en la seguridad tiene características como la opción de usar LibreSSL en lugar de OpenSSL (seleccionable en la GUI) así como una versión personalizada basada en HardenedBSD.

El mecanismo de actualización robusto y confiable ofrece a OPNsense la capacidad de proporcionar importantes actualizaciones de seguridad en forma oportuna.

Traffic Shaper

La configuración del tráfico dentro de OPNsense es muy flexible y se organiza en torno a los pipes, colas y las reglas correspondientes. Las pipes definen el ancho de banda permitido, las colas se pueden usar para establecer un peso dentro de la pipe y, finalmente, las reglas se utilizan para aplicar la configuración a un determinado flujo de paquetes. Las reglas de configuración se manejan independientemente de las reglas del *firewall* y otras configuraciones.

Autenticación de dos factores

La autenticación de dos factores también conocida como verificación 2FA o 2 pasos es un método de autenticación que requiere dos componentes, como un pin / contraseña más un token. OPNsense ofrece soporte completo para autenticación de dos factores (2FA) en todo el sistema utilizando Google Authenticator.

Los servicios 2FA compatibles incluyen:

-Interfaz gráfica de usuario OPNsense
-Portal cautivo
-Red privada virtual - OpenVPN e IPsec
-Caching Proxy

Portal cautivo

El Portal cautivo permite forzar la autenticación o la redirección a una página para acceder a la red. Esto se usa comúnmente en las redes hot spot, pero también se utiliza ampliamente en las redes corporativas para una capa adicional de seguridad en el acceso inalámbrico o de Internet. OPNsense ofrece la mayoría de las funciones empresariales, incluida la asistencia de Radius.

Red privada virtual: IPsec y OpenVPN GUI

OPNsense ofrece una amplia gama de tecnologías VPN que van desde las modernas VPN SSL hasta las IPsec, así como también las opciones de L2TP y PPTP.

Detección y Prevención de Intrusos (IPS)

El sistema IPS en línea de OPNsense se basa en Suricata y utiliza Netmap para mejorar el rendimiento y minimizar la utilización de la CPU. Este sistema de inspección profunda de paquetes es robusto y puede usarse para mitigar amenazas de seguridad a velocidad de cable.

Soporte integrado para reglas abiertas de ET

ETOpen Ruleset es un conjunto de reglas *anti-malware* IDS / IPS que permite a los usuarios con limitaciones de costos mejorar significativamente su detección de malware basada en la red.

Lista negra SSL integrada (SSLBL)

Un proyecto mantenido por abuse.ch. El objetivo es proporcionar una lista de certificados SSL "incorrectos" identificados por abuse.ch para asociarlos con actividades de malware o botnet.

Rastreador de Feodo integrado

Feodo (también conocido como Cridex o Bugat) es un troyano utilizado para cometer fraude ebanking y robar información sensible de la computadora de las víctimas, como detalles de tarjetas de crédito o credenciales. Por el momento, Feodo Tracker está rastreando cuatro versiones de Feodo.

Informes y monitoreo

OPNsense ofrece opciones para informar y monitorear el sistema, incluye:

-Una versión de los gráficos RRD con la opción de acercar y exportar datos.

-Exportador de Netflow
A través de un analizador de flujo de red se puede monitorear los usuarios activos, interfaces, puertos y aplicaciones.

-Insight. Analizador de flujo de red integrado
OPNsense también ofrece un analizador Netflow integrado sin la necesidad de complementos o herramientas adicionales, similar a lo que puede encontrar en productos comerciales de alta gama.

Dashboard

OPNsense ofrece una función de panel para verificar rápidamente el estado del Firewall PFsense.

Las características generales de este *firewall* son:

-*Traffic Shaper*
Permite la autenticación con dos factores para iniciar sesión en la administración del sistema.
Portal cautivo para el inicio de sesión de los usuarios, ideal para redes Wi-Fi de invitados en nuestro hogar o empresa.
-*Proxy* caché transparente con soporte para lista negra.
-VPN incorpora tanto los modos site to site como road warrior, además, es compatible con IPsec y OpenVPN. Asimismo, también incorpora compatibilidad con PPTP, aunque no es recomendable su uso.
Tiene la opción de HA (*High Availability)* y hardware *failover,* para que en caso de caída de un *firewall* automáticamente entre el siguiente.
Incorpora un IDS (sistema de detección de intrusiones) y también IPS (sistema de detección de intrusiones).
-Servidor DNS, DNS Forwarder, DHCP server, DHCP relay, Dynamic DNS etc.
Permite ver gráficos del tráfico en tiempo real, exportar los datos a un servidor remoto, guardar la configuración cifrada, subirla a Google Drive e incluso se pueden instalar plugins para aumentar el número de opciones disponibles.

2.4 Packetfilter

Packetfilter es el sistema más popular de BSD para *firewalls*. Su objetivo es filtrar el tráfico de Ethernet. Packetfilter es capaz de normalizar y acondicionar tráfico, proporcionando calidad de servicio y activando la traducción de direcciones de red. Soporta TCP/IP y permite hacer NAT (*Network Address Translation*). PF además es capaz de normalizar, acondicionar tráfico y proveer un control de ancho de banda para las comunicaciones.

Está basado en permitir o denegar el tráfico de red basado en el encabezado de cada paquete acorde a las reglas de filtrado, este encabezado es revisado por el packet filter y una vez realizado el *firewall* puede: enviar el paquete a su destino; descartar el paquete sin notificar al remitente o rechazar el paquete. Derivado de que el filtrado tiene la capacidad de revisar cada uno de los paquetes de entrada y salida, este puede identificar si existe alguna insistencia de una dirección ip de origen hacia destino en particular. Packet filter no lleva un registro del estado de las conexiones que atraviesan el *firewall*.

2.5 IP Tables

IP Tables es una estructura de tabla genérica para la definición de conjuntos de reglas de filtrado de paquetes. Cada regla dentro de una tabla consiste en un número de clasificadores (coincidencias) y una acción conectada (objetivo). IP Tables está fuertemente conectado a Netfilter que crea una interfaz desde la definición del lenguaje de IP Tables a la pila de red del *kernel*. Netfilter es un conjunto de reglas dentro del *kernel* que permite que sus módulos registren funciones de devolución de llamada. Cada función registrada se llama para cada paquete que pasa la pila de red. Los diversos módulos pueden evaluar el paquete en diferentes características y llevar a cabo algunas acciones especiales dependiendo de los resultados de la evaluación. Así mismo realiza traducción de direcciones de red (NAT) o mantiene registros de *log*. Está disponible en prácticamente todas las distribuciones de Linux actuales. Tiene la capacidad de monitorizar el estado de una conexión y redirigir, modificar o detener los paquetes de datos basados en el estado de la conexión y no solamente por el origen, destino o contenido del paquete.

Iptables tiene tres tablas incorporadas a su núcleo, cada una de las cuales contiene algunas cadenas predefinidas con la opción de crear nuevas tablas mediante módulos de extensión. El administrador puede crear y eliminar cadenas definidas por usuarios dentro de cualquier tabla. En las tablas al principio todas las cadenas están vacías y solo tienen una política de destino que permite que todos los paquetes pasen sin ser bloqueados o alterados.

En este sentido se presenta en un cuadro a manera de resumen las características de los *firewalls* mencionados anteriormente, Tabla 2.

Aplicaciones	**Servicios**									
	Firewall	Antispam	Antivirus	Antispyware	IPS	Filtrado web	VPN	QoS Calidad de servicio	Control de aplicaciones	Monitoreo
Pfsense	**X**				**X**	**X**	**X**	**X**		**X**
Untagle	**X**				**X**	**X**	**X**	**X**		**X**
Opnsense	**X**				**X**		**X**	**X**		**X**
Packetfilter	**X**							**X**		
IP Tables	**X**									

Tabla 2. Resumen de las características de los firewalls de código abierto.

3 Análisis

Derivado de las características encontradas en los *firewalls* comerciales y de código abierto se realiza una comparación en términos de los servicios que ofrecen en función del soporte, hardware, operación y actualización de dichas herramientas.

Aplicaciones		Servicios									
		Firewall	Antispam	Antivirus	Antispyware	IPS	Filtrado web	VPN	QoS Calidad de servicio	Control de aplicaciones	Monitoreo
Comercial	**FORTINET**	X	X	X	X	X	X	X	X	X	
	Palo Alto Networks	X	X	X	X	X	X	X	X	X	X
	CheckPoint Software Technologies	X	X	X	X	X	X	X		X	X
De código abierto	**Pfsense**	X				X	X	X	X		X
	Untagle	X				X	X	X	X		X
	Opnsense	X				X		X	X		X
	Packetfilter	X							X		
	IP Tables	X									

Tabla 3. Cuadro comparativo de las características de firewalls comerciales vs de código abierto.

Se identifica de la tabla 3 que los *firewalls* comerciales analizados integran los servicios de filtrado para el tráfico de paquetes de una red externa a interna y viceversa; además de protección maliciosa referente a virus, *spam, spyware*. Se observa que es posible administrar el ancho de banda de la red (QoS), filtrar URL (web), administrar conexiones VPN y en algunos casos monitorear la red; por lo que en estos casos es necesario utilizar una herramienta adicional para el monitoreo de red.

Para el caso de los *firewall*s de código abierto, se observa que todos permiten filtrar el tráfico de una red.

Pfsense y Untagle tienen servicios de filtrado web, IPS, conexiones VPN y permiten administrar el ancho de banda de la red, así como herramientas de monitoreo.

Opnsense además de tener un servicio de administración de ancho de banda, funge como un IPS, administra VPN y tiene herramientas para el monitoreo de red.

Con el *firewall* Packet Filter se puede además de filtrar el tráfico de la red, administrar el ancho de banda de ésta. Por su parte, IPtables solo funge como un mecanismo de filtrado de paquetes.

Derivado de lo anterior, se observa que un *firewall* comercial está integrado por un conjunto de servicios que fortalece la seguridad de una red de telecomunicaciones en una misma aplicación; manejando un esquema con estas características bajo aplicaciones de código abierto implica contar con más de una herramienta para cubrir los servicios mostrados en la tabla 3.

Por otra parte, el soporte que ofrecen las soluciones propietarias está avalada por el fabricante de dichos productos o por los proveedores de servicios contratados, así mismo la actualización de las firmas de aplicaciones las realiza de forma automática apoyada por laboratorios especializados; es de suma importancia este último punto ya que diversos estudios revelan que hay incrementos de nuevos ataques lo que implica que se deben de programar soluciones que los mitiguen o rechacen.

En el caso de las aplicaciones de código abierto no cuentan con soporte de parte del desarrollador de dicha aplicación por lo que es necesario recurrir a los foros de ayuda en línea, que en mucho de los casos sus aportaciones no solucionan el problema específico y deriva en un mayor tiempo de respuesta a un incidente de seguridad. Para las actualizaciones de firmas de aplicaciones los administradores de estas aplicaciones deben realizar dicha tarea de forma manual, lo que implica contar con el personal dedicado exclusivamente a dichas tareas. Aunado a estas características es de considerar que no cuentan con hardware de propósito específico, limitando el rendimiento de la aplicación.

Así mismo, estas aplicaciones al ser un *software* de código abierto se tiene la disponibilidad pública del código fuente, incluidos posibles delincuentes y atacantes. Los atacantes pueden estudiar el código fuente y explotar vulnerabilidades que pueden deberse a errores de programación mucho más rápidamente. Además, las aplicaciones de código abierto generalmente se desarrollan conjuntamente mediante contribuciones voluntarias de grupos y comunidades a través de Internet. Los atacantes también pueden contribuir con partes del código al *software* de esta manera. La seguridad del nivel del código generalmente depende de las revisiones realizadas por los encargados de mantener el proyecto u otros contribuyentes.

Aplicaciones		Nivel de cobertura en el modelo OSI						
		Capas						
		1	2	3	4	5	6	7
Comercial	**FORTINET**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	Palo Alto Networks	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	CheckPoint Software Technologies	**X**	**X**	**X**	**X**	**X**	**X**	**X**
De código abierto	**Pfsense**	**X**	**X**	**X**	**X**	**X**	**X**	
	Untagle	**X**	**X**	**X**	**X**	**X**		
	Opnsense	**X**	**X**	**X**	**X**			
	Packetfilter	**X**	**X**	**X**	**X**			
	IP Tables	**X**	**X**	**X**	**X**			

Tabla 4. Cuadro comparativo del nivel de cobertura en el modelo OSI de firewalls comerciales vs de código abierto.

4 Resultados

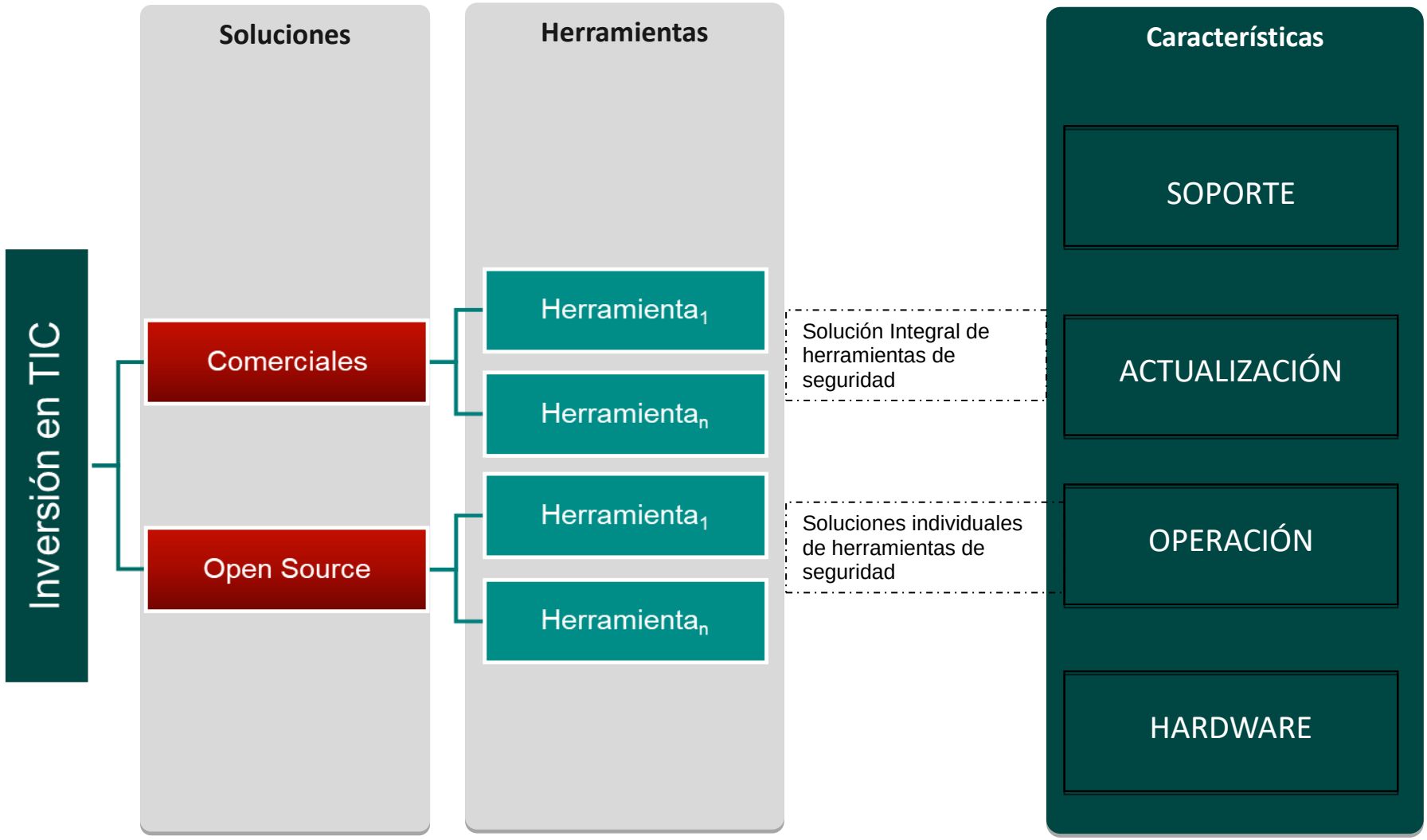

Figura 9. Resultados Firewall Comercial vs Firewall de Código Abierto

La adquisición de un *firewall* de código abierto o comercial implica una inversión en Tecnologías de la Información y Comunicaciones. Son herramientas que coadyuvan en la protección de la seguridad perimetral de una red de telecomunicaciones; actualmente hay una gran variedad de éstas disponibles en el mercado.
Al respecto, el *firewall* comercial es una solución integral de herramientas de seguridad mientras que un de código abierto se trata de soluciones individuales. Para la toma de decisiones en la adquisición de alguno en particular se debe ponderar los siguientes atributos: soporte, actualización, operación y hardware aunado al contexto en el que se pretende implementar.

Conclusiones

Los *firewalls* son una herramienta indispensable para la seguridad de las TIC. A la hora de elegir una de estas, sea libre o comercial es necesario tener una visión holística no solo de los recursos, financieros, de cómputo y telecomunicaciones y de las políticas para el uso de estos, sino que también se deben considerar las competencias laborales para que la asimilación de tecnología sea una ventaja competitiva contra las amenazas de la seguridad e integridad de los datos así mismo obtener el mejor rendimiento a la inversión tecnológica.

Mientras que, para la implementación de un *firewall* de código abierto, se requiere de mayor tiempo y de especialistas altamente capacitados en temas de seguridad. Los *firewalls* comerciales se caracterizan por los siguientes cuatro atributos:

a) Soporte. Un *firewall* de código abierto no cuenta con soporte por parte de un proveedor o fabricante, lo que impacta en la atención de algún incidente.
b) Actualización. La actualización de firmas de aplicaciones en los *firewalls* de código abierto es artesanal, esto implica que una persona debe realizar esta tarea de forma continua.
c) Operación. la operación de un *firewall* de código abierto requiere de gran expertiz y dedicación de un recurso humano de tiempo completo.
d) Hardware. La solución de código abierto no cuenta con hardware de propósito específico, lo que limita el rendimiento adecuado de la solución.

Agradecimientos

Ing. Dulce Campos del Razo, Coordinación de Universidad Abierta y Educación a Distancia (CUAED UNAM).
Ing. Rafael Sandoval Vázquez, Facultad de Ingeniería, UNAM.
M.A.T. Manuel Ignacio Quintero Martínez, Coordinación de Seguridad de la información / UNAM-CERT
Emmanuel Gómez Cantoya, Centro de Ciencias Aplicadas y Desarrollo Tecnológico. (CCADET- UNAM)

Referencias Bibliográficas

Aguirre, E.; Bautista, J.; Guerrero, A. E.; Hernández, A. A., Hernández, S., Hernández G. (2017) Comparación de los Modelos OSI y TCP/IP. **Ciencia Huasteca. Boletín Científico de la Escuela Superior de Huejutla**, Universidad Autónoma del Estado de Hidalgo. 5(10) https://www.uaeh.edu.mx/scige/boletin/huejutla/n10/r1.html

Check Point Research (2017) Cyber attack trends. **Mid-Year Report**, p. 1-19.

Check Point https://www.checkpoint.com/products-solutions/next-generation-firewalls/

Divakaran, D. M.; Fok, K. W.; Nevat, I.; Thing, V. (2017) Evidence gathering for network security and forensics. **Digital Investigation**, 20, p. S56eS65.

Einar-Lanfranco, M. (2010) Integración de herramientas de seguridad para redes informáticas, **UNIVERSIDAD NACIONAL DE LA PLATA Facultad de Informática**, p. 1-89

Fortinet, https://www.fortinet.com/products.html

Hils, A.; D'Hoinne, J.; Kaur, R. (2017) Magic Quadrant for Enterprise Network Firewalls, Gartner, ID: G00310171.

Howlett, T. (2004) Open Source Security Tools Practical Applications for Security, Prentice Hall, p. 17

Kamara, S.; Fahmy, S.; Schultz, E.; Kerschbaum, F.; Frantzen, M. (2003) Analysis of vulnerabilities in Internet firewalls. **Computers & Security**, 22(3), p. 214-232.

Khoumsi, A.; Erradi, M.; Krombi, W. (2016) A formal basis for the design and analysis of firewall security policies. **Journal of King Saud University – Computer and Information Sciences**, ARTICLE IN PRESS.

Kilpatrick, I. (2007) UTMS or point solutions? **Infosecurity**, 4(2), p. 42.

Kurpjuhn, T. (2013) The evolving role of the UTM appliance. **Network Security**, 2013(1) p. 8-11

Madhuri, M.; Rajesh, K. (2013) Systematic detection and resolution of firewall policy anomalies. **International Journal of Research in Computer and Communication Technology**, 2 (12), p. 1387–1392.

Misra, A. K.; Verma, M.; Sharma, A. (2014) Capturing the interplay between malware and anti-malware in a computer network. **Applied Mathematics and Computation** 229, p. 340–349

PaloaltoNetworks (2014) Descripción General Del Cortafuegos, DataSheet, https://www.paloaltonetworks.es/content/dam/pan/es_ES/assets/pdf/datasheets/firewall-features-overview-es.pdf, p. 1-6

Opne Source Initiative (2017) https://opensource.org/faq#osd

Paloalto, https://www.paloaltonetworks.com/

Stevens, M. (2006) UTM: one-stop protection. **Network Security**, 2006(2), p.12-14

Thakur, A, (2015) Open Source Firewall Implementation. Bachelor's Thesis, **Turku University of Applied Sciences**, p. 1-35.

Wu, S.; Zhang, Y.; Cao W. (2017) Network security assessment using a semantic reasoning and graph based approach. **Computers and Electrical Engineering**, 64, p. 96-109.