FIREWALLS DE NUEVA GENERACIÓN: LA SEGURIDAD INFORMÁTICA VANGUARDISTA

David Geovanny Cortes A.
ing_daavid@hotmail.com
Universidad Piloto de Colombia

Abstract— Firewalls are devices that seek to protect information, making them one of the main tools of information security. The organizations maintain a constant flow of information with their environments and through this flow, enterprises can be put at risk by various threats, both internal (leakage of information) and external (phishing, scams, malware). These threats are constantly evolving, so the firewall (the main defense mechanism and protection in the flow of information) must also adapt to changing environmental conditions. The traditional firewall evolves because of challenges such as decryption and inspection of SSL, IPS with anti-avoidance technology, application control based on context, and protection against network-based malware. These challenges have created a new market, where suppliers compete to diversify and meet the needs of their customers. The Magic Quadrant methodology allows us to observe the classification of these providers. These providers specialize in detailed customer requirements, making some more suitable for certain market sectors (organizational).

Key words— New generation firewall, provider, security, solution, filtering rules, identification and control applications, evading security, SSL, SSH, unknown traffic, threats, ports, users, devices, hardware, software, magic quadrant.

Resumen— Los firewall son dispositivos que buscan proteger la información, por lo que son una de las herramientas principales de seguridad informática. Las organizaciones mantienen un flujo constante de información con su entorno y a través de este flujo puede entrar en riesgo el propio negocio por diversas amenazas, tanto internas (fuga de información) como externas (suplantación, estafas, malware). Estas amenazas están en constante evolución, por lo que el firewall (principal mecanismo de defensa y protección en el flujo de información) también debe adaptarse a las cambiantes condiciones del entorno. Esto hace que el firewall tradicional evolucione a través de retos como el descifrado e inspección de SSL, IPS con tecnología antievasión, el control de aplicaciones basado en contexto y la protección contra malware basada en red. Estos retos han creado un nuevo mercado, donde los proveedores se diversifican y compiten para satisfacer las necesidades de sus clientes. La metodología del Cuadrante Mágico permite observar la clasificación de estos proveedores. Dichos proveedores se especializan en requerimientos detallados del cliente, lo que hace que algunos sean más aptos para ciertos sectores organizacionales.

Palabras clave— Firewall nueva generación, proveedor, seguridad informática, solución, reglas de filtrado, identificación y control de aplicaciones, evasión de seguridad, SSL, SSH, tráfico desconocido, amenazas, puertos, usuarios, dispositivos, hardware, software, cuadrante mágico.

I. INTRODUCCIÓN

La información ha cobrado un rol importante para el logro de los objetivos en las organizaciones. Esto le ha significado ser considerada en muchos casos como su activo más importante o su ventaja competitiva. Al ser un elemento tan relevante y diferenciador para la organización, en un ambiente competitivo, es objeto de diversas amenazas como el robo, la falsificación, el fraude, la divulgación y hasta la destrucción, entre muchas otras amenazas. Por lo anterior, la seguridad de la red es un problema corporativo cada vez más prioritario, enfatizado en los pilares de la seguridad como lo

son la confidencialidad, la disponibilidad y la integridad [1].

A partir de estos riesgos surge la necesidad de desarrollar ambientes confiables, de blindaje y protección; lo que se traduce en complejidad por las diversas interacciones que involucra. Por esta razón, se han desarrollado enfoques de seguridad como la defensa en profundidad (*defense in depth*), que tiene como propósito proteger la información a través de la aplicación de controles en distintas capas [1].

Una de estas capas es el perímetro, el límite lógico que separa la red corporativa de otras redes (la frontera con el entorno, con ambientes externos), incluyendo el Internet. En las metodologías de seguridad de esta capa, el firewall continúa teniendo vigencia y protagonismo como mecanismo de protección de las redes y ha sido un elemento imprescindible desde su aparición, hace más de 25 años [2].

El objetivo de este artículo es presentar una breve reseña sobre el estado del arte de los firewall de nueva generación, como herramienta principal de la seguridad informática en los últimos años. Adicionalmente, busca presentar las características de mercado que estos dispositivos están afrontando, desde los retos que tiene que enfrentar (traducidos en necesidades de los clientes y en las amenazas del entorno) hasta las posibles soluciones dadas por proveedores y expertos.

Para presentar estas generalidades de los firewall de nueva generación, se hablará en primera instancia de su definición; en segundo lugar, de su evolución a lo largo del tiempo, en tercer lugar, de la concepción de los firewall de nueva generación, en cuarto lugar, de las propuestas y servicios de este nuevo firewall; y finalmente, se discutirá acerca del mercado de estas herramientas de seguridad informática, sus proveedores y sus portafolios.

II. ¿QUÉ ES UN FIREWALL?

Un firewall es una herramienta de software o hardware que filtra todas las conexiones que ingresan a la red interna de la organización o que se dirige hacia el exterior de la misma. Básicamente, se implementa como un mecanismo de control de acceso lógico [2]. Específicamente, lo que se quiere evitar es que usuarios de Internet, que no han sido autorizados para ingresar a la red corporativa, puedan tener acceso o que miembros de la misma organización accedan a servicios externos para los cuales no han sido autorizados [3].

La importancia de estas herramientas de seguridad informática se basa en que operan como un filtro que examina todos los paquetes que se dirigen hacia la red corporativa y comparan la información del encabezado con reglas previamente establecidas (reglas de filtrado); como por ejemplo, la validez de la dirección IP y del puerto. Si estos criterios son adecuados, de acuerdo con las reglas de filtrado, el paquete que está en el flujo será entregado; en caso contrario, se descartará, desechándolo fuera del flujo de la red. En cambio, cuando los paquetes son enviados desde el interior de la red corporativa hacia internet, se realiza la misma operación [2].

De esta forma, al desechar paquetes que no están permitidos por no cumplir con las reglas de filtrado definidas, sus conexiones no son válidas. De acuerdo con esto, el firewall puede evitar la propagación de códigos maliciosos a través de la red, accesos no autorizados o posibles intrusiones de terceros a la red corporativa [2].

El alcance de estos dispositivos es limitado. Por ejemplo, no pueden proteger la información de la red ante la suplantación de identidades (también conocida como "*phising"*) o la estafa informática (también conocida como "*scam*"). Esto debido a que la mayoría de las organizaciones consideran que el correo electrónico es fundamental en sus operaciones y la funcionalidad del firewall puede ser engañado por este medio, al no poder aplicar las reglas de filtrado. Los actuales firewalls tampoco pueden proteger de una infección de malware, cuando estos atraviesan la red como un archivo adjunto o a través de medios removibles, básicamente por la inaplicabilidad de las reglas de filtrado definidas [2].

A. Reglas de filtrado

Generalmente, el acceso o el flujo de conexiones se permite o se niega en función de los criterios y

reglas que se definen con las partes interesadas, de acuerdo a sus necesidades, sus intereses y a las tendencias del mercado. Específicamente, existen dos enfoques: el restrictivo y el permisivo.

El enfoque restrictivo hace que todas las conexiones sean bloqueadas, excepto aquellas que están explícitamente permitidas dentro de los acuerdos de servicio estipulados y las reglas de filtrado definidas. Por el contario, el enfoque permisivo acepta todas las conexiones según los acuerdos de servicio y las reglas, exceptuando aquellas que están explícitamente restringidas [2].

De acuerdo con esto, la configuración del firewall depende del enfoque que se aplique, así como de los servicios que ofrece el proveedor, las necesidades de las partes interesadas o los miembros de la organización, teniendo en cuenta las labores que se desempeñan y los activos que se pretende proteger.

B. Importancia del firewall

Este mecanismo de seguridad continua siendo altamente utilizado en el entorno corporativo. Según un estudio de seguridad informática en Latinoamérica, el 76% de los ejecutivos de 14 países de esta región cuentan con una solución de este tipo; lo que ubica al firewall en el segundo lugar de los controles de seguridad más utilizados, después de los antivirus [4].

Esta utilidad del firewall se relaciona con los beneficios que proporciona dicho dispositivo en cuanto a la protección, debido al proceso de filtración de conexiones exteriores que suelen realizar algunos tipos de software maliciosos como gusanos, virus o botnets. De igual manera, los firewalls bloquean las conexiones de posibles intrusos en la red como medida de seguridad para el control de conexiones al exterior [2].

III. EVOLUCIÓN DEL FIREWALL

Desde su aparición como solución para la seguridad informática, el firewall ha evolucionado buscando ofrecer distintas características de protección, según las necesidades de momento a las cuales se han enfrentado los usuarios y el mismo mercado.

Por ejemplo, el primer tipo de firewall que se desarrolló, se denominó firewall de filtrado de paquetes (*packet filter).* Este opera inspeccionando todos los paquetes que llegan a la red y en función de las reglas de filtrado. Funcionalmente, se puede decir que los paquetes son aceptados o descartados, de acuerdo a la verificación y cumplimiento de la información básica del paquete, como la dirección de origen y destino, el protocolo o el puerto [2].

El segundo tipo de firewall que se desarrolló, es el conocido por la inspección de estado (*stateful inspection*). Se diferencia del primer tipo porque adicionalmente lleva a cabo el seguimiento de los paquetes de datos y el estado de las conexiones que pasan a través de él [2]. En otras palabras, este sólo permite el paso de paquetes de datos que coinciden con una conexión activa y que según las reglas de filtrado se hayan reconocido como legítimas, los demás paquetes (que vienen de conexiones inactivas y que no cumplen con las reglas) son descartados y rechazados.

Otro tipo de firewall, históricamente aceptado como el tercer tipo, es reconocido como filtrado de aplicación (*application filtering*). La principal funcionalidad de este tipo es la capacidad de detectar si una conexión no deseada está tratando de evitarlo (cumpliendo con las reglas de filtrado establecidas) a través de una dirección IP y un puerto válido (esquivando el flujo de información donde está involucrado el mismo Firewall) [2]. Se puede decir que logra dirigir e inspeccionar aplicaciones específicas, ya que además de examinar el encabezado del paquete, también evalúa todo el contenido del mismo.

A pesar de todos los beneficios, el control de los firewall es muy superficial. De acuerdo con esto, actualmente su gestión debe ser complementada con otros controles relacionados con la seguridad perimetral, donde se deben incluir sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusos (IPS) [2].

De acuerdo con lo anterior, se deben incluir otros niveles considerados en la seguridad por capas. Esto se relaciona directamente con la aplicación de otros controles necesarios e imperantes para las

organizaciones, como antivirus, antispam, otras prácticas como el respaldo y el cifrado de información, soluciones de doble autenticación y hasta soluciones de seguridad para dispositivos móviles, cuando éstos son utilizados para acceder a la red corporativa [2]. Estos requerimientos abren paso a nuevas oportunidades en la seguridad informática que pueden ser saciadas por los firewall de nueva generación.

IV. ¿QUÉ ES UN FIREWALL DE NUEVA GENERACIÓN?

Como se ha venido describiendo, los firewalls surgieron para revolucionar la seguridad de la red satisfaciendo las necesidades y requerimientos actuales de los usuarios, garantizando la protección de la información. Los firewalls tradicionales se limitan únicamente a la revisión de paquetes por estado y a la implementación de reglas de control de acceso. La funcionalidad de estos antiguos mecanismos se ha vuelto obsoleta con la natural evolución de la tecnología y del mercado, por no mencionar la proactividad de los hackers; lo que hace que las amenazas sean más sofisticadas dejando atrás la eficacia de este sistema. Con el fin de proteger el negocio de estas amenazas dinámicas, en constante evolución, el firewall de nueva generación (NGFW por sus siglas en inglés), se ha desarrollado con el fin de ofrecer un nivel más profundo de seguridad de red, buscando la mejor protección para el flujo de información de las compañías actuales [1].

La clave de esta protección se basa en garantizar la inspección de todos los bytes de cada paquete. Adicionalmente, estas metodologías de revisión y protección de información han de mantener el rendimiento elevado y la baja latencia para que las redes con alto tráfico sigan funcionando óptimamente. De esta forma, su objetivo es buscar combatir amenazas eficazmente, abordando todos los problemas de productividad apremiantes, ya que todas las organizaciones requieren mayor control y profundidad en sus sistemas de seguridad informática [1].

En este punto se puede afirmar que los firewalls de nueva generación son una herramienta fundamental para proteger a cualquier organización frente a las amenazas procedentes de Internet. Una de las ventajas competitivas de estos dispositivos vanguardistas es que proporcionan un punto centralizado (ver Figura 1) por el cual se puede controlar el tráfico desde distintas características como [5]:

- Dirección IP: de origen o de destino.
- Número de Puerto: de origen o de destino.
- Dominio: integración con el servicio de nombres de dominio (DNS), para simplificar el acceso a recursos que resultarían más difíciles de definir por otros medios.
- Tipo de aplicación: con técnicas de inspección profunda de paquetes, para controlar el funcionamiento de las aplicaciones web.
- Traducción de direcciones IPv4 por NAT en sentido de salida, y acceso IPv6 nativo a internet.
- Control del acceso remoto a redes corporativas.

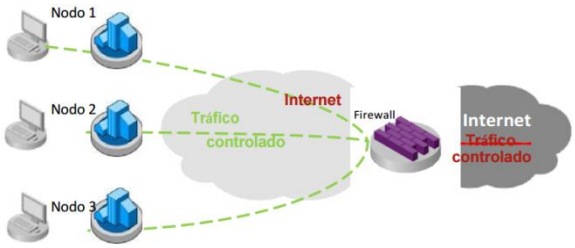

Figura 1. Posición y función del Firewall en el flujo de información.
Imagen tomada del sitio: http://www.interoute.es/sites/default/files/files/next_gen_fwall_service_description_v2_ES.pdf

V. PROPUESTAS Y SERVICIOS DE LOS NGFW

Los NGFW buscan satisfacer todas las actuales necesidades de las organizaciones en cuanto a seguridad informática. Básicamente estos deben inspeccionar todo el tráfico, incluidas las aplicaciones, las amenazas y el contenido, y lo vincula al usuario independientemente de la ubicación o el tipo de dispositivo (Ver Figura 2) [7].

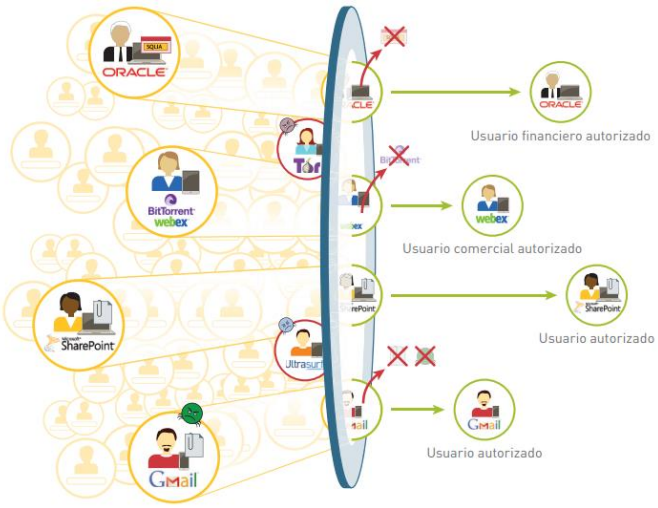

Figura 2. Gestión del NGFW
Imagen tomada del sitio:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-features-overview-es.pdf

Se puede decir que la aplicación, el contenido y el usuario, son los elementos que impulsan la gestión de la información en una organización, por ello se convierten en componentes integrales de la política de seguridad informática corporativa para toda la organización (Ver Figura 3) [7]. Algunos beneficios que ofrece la implementación de arquitecturas informáticas basadas en NGFW son [6]:

- Habilitación, de forma segura, a aplicaciones, usuarios y contenidos mediante la clasificación de todo el tráfico, la determinación del caso de uso empresarial y la asignación de políticas con el fin de permitir y proteger el acceso a las aplicaciones pertinentes.
- Mitigación de amenazas eliminando aplicaciones no deseadas para reducir la superficie de impacto y aplicación de políticas de seguridad selectivas para bloquear exploits de vulnerabilidades, virus, spyware, botnets y malware desconocido (APT).
- Protección para los centros de datos por medio de la validación de aplicaciones, el aislamiento de datos, el control sobre las aplicaciones no apropiadas y la prevención de amenazas de alta velocidad.
- Protección a los entornos de computación en la nube pública y privada con una mayor visibilidad y control; implementación, aplicación y manutención de políticas de seguridad al mismo ritmo que sus máquinas virtuales.
- Adopción de una informática móvil segura extendiendo la plataforma de seguridad empresarial a los usuarios y dispositivos independientemente de su ubicación.

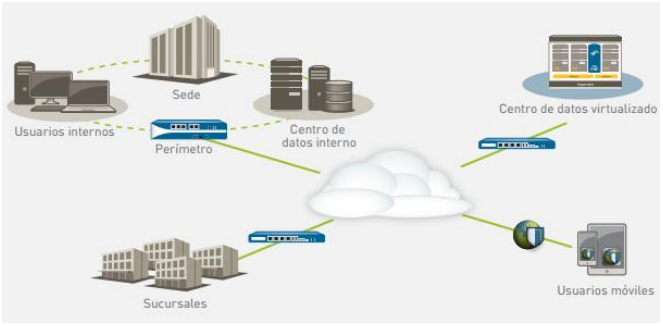

Figura 3. Alcance Políticas de Seguridad NGFW
Imagen tomada del sitio:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-features-overview-es.pdf

De acuerdo con esto, una herramienta de seguridad informática como estas debe ofrecer alternativas tales como [7]:

A. Identificación y control de aplicaciones en todos los puertos, en todo momento.

Los desarrolladores de aplicaciones ya no adoptan el estándar de mapeo puerto/protocolo/aplicación. Por lo que cada vez hay mas aplicaciones que son capaces de funcionar en puertos no estándar o pueden saltar de puerto (por ejemplo, las aplicaciones de mensajería instantánea, de intercambio de archivos P2P o de VoIP). Además, los usuarios ya tienen los conocimientos suficientes como para hacer que las aplicaciones se ejecuten a través de puertos no estándar (por ejemplo, RDP o SSH).

Los NGFW deben asumir que cualquier aplicación se puede ejecutar en cualquier puerto y que su próximo firewall debe clasificar el tráfico por aplicación en todos los puertos en todo momento. La clasificación del tráfico en todos los puertos será

un tema recurrente en todos los puntos que quedan; de lo contrario, los controles basados en puertos seguirán siendo burlados por las mismas técnicas que los han atormentado durante años [7].

B. Identificación y control para las herramientas de evasión de la seguridad.

Muy pocas aplicaciones pueden evadir intencionalmente las propias políticas de seguridad que protegen los activos digitales corporativos. Se puede decir que existen dos: las que sirven para evadir la seguridad (proxies externos, túneles cifrados no relacionados con VPN) y las que se pueden adaptar para lograr fácilmente el mismo objetivo (herramientas de administración de servidor/escritorio remoto).

Estas mismas herramientas son utilizadas cada vez con más frecuencia por los atacantes como parte de intrusiones contra la seguridad informática corporativa. Sin la capacidad de controlar estas herramientas de evasión de seguridad, las empresas no pueden aplicar sus políticas de seguridad y por tanto se exponen a los mismos riesgos que pensaban que sus controles estaban deteniendo [7]. Esta es la nueva alternativa que debe ofrecer el NGFW.

C. Configuración e inspección de SSL y control de SSH

La capacidad de descifrar el tráfico SSL es algo prioritario, no solo porque es cada vez más significativo dentro del tráfico empresarial, sino porque también habilita unas cuantas funciones claves más que resultarían incompletas o ineficaces sin la capacidad de descifrar SSL. Los elementos clave necesarios son el reconocimiento y descifrado del SSL en cualquier puerto, tanto de entrada como de salida; políticas de control sobre el descifrado y los elementos hardware y software necesarios para realizar el descifrado SSL y todas las conexiones simultáneas con rendimiento predecible.

Otro de los requisitos adicionales que deberá tener en cuenta es la capacidad para identificar y controlar el uso de SSH. En concreto, el control de SSH debe incluir la capacidad de determinar si se está utilizando como un redireccionador de puertos (local, remoto, X11) o para uso nativo (SCP, SFTP y acceso a la shell). Una vez que se conoce cómo se está utilizando el SSH se pueden crear políticas de seguridad apropiadas [7].

D. Control funcional de aplicaciones

La supervisión continua del estado para comprender las diferentes funciones que cada aplicación puede admitir, y los diferentes riesgos asociados, es un requisito fundamental que ofrecen los NGFW. De esta forma, deben clasificar continuamente cada aplicación y realizar un seguimiento de los cambios que puedan indicar que se está utilizando una función diferente en este momento.

E. Gestión sistemática el tráfico desconocido.

Los NGFW pueden proporcionar la capacidad de ver todo el tráfico desconocido, en todos los puertos, en una consola de gestión única y analizar rápidamente el tráfico para determinar:

1. Si es una aplicación interna o personalizada.
2. Si es una aplicación comercial sin una firma.
3. Si es una amenaza.

Además, ofrecen las herramientas necesarias, no solo para ver el tráfico desconocido sino también para gestionarlo sistemáticamente, controlándolo mediante políticas, creando firmas personalizadas, enviando un PCAP de las aplicaciones comerciales para su posterior análisis o realizando investigaciones forenses para determinar si se trata de una amenaza.

F. Búsqueda de amenazas en todas las aplicaciones, en todos los puertos.

Los NGFW deben promover la habilitación segura de aplicaciones, porque es lo que los negocios solicitan. Para esto hay que aceptar dicha aplicación y rastrearla en busca de amenazas. Todas las aplicaciones pueden comunicarse a través de una combinación de protocolos (por ejemplo, SharePoint utiliza CIFS, HTTP y HTTPS, y requieren de una política de NGFW más sofisticada que únicamente la de "bloquear la aplicación o permitirla ciegamente"). El primer paso es identificar la aplicación (independientemente del puerto o el cifrado), determinar las funciones que quiera permitir o denegar y, a continuación, analizar los componentes permitidos buscando cualquiera de las amenazas (exploits, virus/malware o spyware, etc.) o incluso información confidencial o sensible [7].

G. Implementación de controles constantes de todos los usuarios, independientemente de su ubicación o tipo de dispositivo.

Los NGFW tienen visibilidad y control de tráfico constantes, sin importar el lugar donde se encuentre el usuario. Los NGFW pueden ejercer cualquier control de condiciones o accesos esto sin obstruir la actividad del usuario final, o suponer una molestia operativa injustificada para el administrador, o un coste significativo para la organización [7].

H. Simplificación de la seguridad de la red incorporando control de aplicaciones.

Su negocio se basa en las aplicaciones, los usuarios y el contenido, el NGFW permite que se construyan políticas que apoyen directamente las iniciativas empresariales propias. El uso de un contexto compartido de aplicación, usuario y contenido en todos los aspectos (visibilidad, políticas de control, logging y reporting) le ayudará a simplificar su infraestructura de seguridad de manera significativa. Las políticas de firewall basadas en dirección IP y puerto, además de las políticas separadas para el control de aplicaciones, IPS y antimalware sólo complicarán el proceso de gestión de políticas y pueden incluso llegar a obstruir la actividad del negocio [7].

I. Capacidad y rendimiento con un control total de aplicaciones.

Los firewall basados en puertos junto con otras funciones de seguridad de diferentes orígenes tecnológicos, implica por lo general la existencia de capas de red, motores de análisis y políticas redundantes, lo que finalmente se traduce en un rendimiento deficiente. Desde el punto de vista del software, el NGFW se puede diseñar para hacer esto desde el principio. Además, dada la necesidad de realizar tareas de procesamiento intensivas (como por ejemplo, identificación de la aplicación, prevención de amenazas en todos los puertos, etc.) ejecutadas sobre altos volúmenes de tráfico y con baja tolerancia a la latencia asociada con la infraestructura crítica, los NGFW pueden tener también un hardware diseñado para dichas tareas, es decir, un sistema específico dedicado para networking, seguridad y análisis de contenidos [7].

J. Funciones propias de un firewall, tanto en forma de hardware como virtual.

La creación y eliminación dinámica de aplicaciones dentro de un centro de datos virtual potencializa los problemas de identificación y control de aplicaciones de un enfoque centrado en la dirección IP y el puerto. Los NGFW pueden proporcionar una integración profunda con el entorno de virtualización para simplificar la creación de políticas basadas en aplicaciones a medida que se abren y se cierran nuevas máquinas virtuales y aplicaciones. Esta es la única manera de asegurarse de que es capaz de dar soporte a la evolución de las arquitecturas de centros de datos con flexibilidad operativa mientras que hace frente a los riesgos y a los requisitos de cumplimiento de normativas [7].

VI. MERCADO Y PROVEEDORES DE LOS NGFW

De acuerdo a la amplia gama de necesidades y características de clientes para los NGFW y partiendo de sus requerimientos y las particularidades (relacionadas con sus negocios, herramientas y plataformas tecnológicas), el mercado de los NGFW es muy diverso. Se puede decir que existen muchas necesidades que se satisfacen a través de varios productos o servicios. Esto está directamente relacionado con las alternativas que se están buscando y que se mencionaron anteriormente. Este complejo espectro de posibilidades brinda un entorno comercial atractivo, donde se encuentran diversos proveedores, que según sus estrategias de mercado, se diferencian y buscan satisfacer a cada uno de sus clientes, buscando la competencia perfecta. Se puede decir que existen más de 15 compañías, internacionalmente, especializadas en ofrecer servicios de seguridad informática a través de herramientas como los NGFW.

Estas compañías diversifican su portafolio (a través de alternativas y servicios) teniendo en cuenta las necesidades y particularidades de sus clientes. Gartner, Inc propone una estrategia para clasificar todos los proveedores de NGFW y entender la dinámica del mercado. Esta metodología se llama el Cuadrante Mágico del firewall de redes empresariales. Esta metodología clasifica a los

proveedores de acuerdo a la evaluación de dos variables: la integridad visional (portafolio de alternativas y ofrecimientos) y la capacidad de ejecución (cumplimiento). El desempeño de los proveedores según estos dos aspectos permite clasificarlos en cuatro categorías: lideres (buena visión y buena ejecución), desafiantes (buena ejecución, poca visión); visionarios (buena visión, poca ejecución) y competidores (poca visión, poca ejecución). En la Figura 4 se puede observar la clasificación de los proveedores de NGFW, en abril del 2015, según la metodología mencionada anteriormente [8].

Figura 4. Cuadrante Mágico del Firewall de Redes Empresariales, Abril 2015
Imagen tomada del sitio:
http://www.bradreese.com/blog/5-28-2015.pdf

VII. OPINIONES DE LOS EXPERTOS: NECESIDADES Y PRODUCTOS.

Como se ha venido mencionando, muchas de las soluciones y alternativas a los requerimientos organizacionales en seguridad informática, están siendo solventadas por varios proveedores y sus portafolios diversificados.

Algunas marcas líderes se atreven a opinar sobre las necesidades más representativas que se encuentran dentro de los clientes y sugieren el portafolio (proveedor) que les ayudaría a mejorar sus políticas de seguridad informática [9]. Por ejemplo, PC COM Mayorista argumenta que las necesidades de los clientes dependen principalmente del tamaño de las organizaciones y los medios o canales de información utilizados. Por lo que sugiere que por ejemplo Barracuda Firewall tiene mayor desempeño con empresas de menor tamaño; en cambio, NGF se especializa en compañías de mayor flujo de información

Por otra parte, ProtektNet aconseja los servicios de Cyberoam por su amplia oferta en capacidad de reportes y eficacia informática. Mientas Sourcefire sugiere que para las necesidades de control de aplicaciones y seguridad, Cisco ofrece un mejor portafolio. Finalmente, Fortinet menciona innovadoras metodologías de seguridad informática que garantizan la total protección de la información a través de la inteligencia artificial.

VIII. CONCLUSIONES

A través de toda la revisión documental y de los hallazgos teóricos se puede concluir que los firewall son dispositivos protagónicos en la protección de información, por lo que son la herramienta predilecta en seguridad informática. También se puede decir que debido a que las organizaciones mantienen un flujo constante de información con su entorno, y que a causa de este flujo se genera el riesgo por diversas amenazas, tanto propias (internas) como ajenas (de origen externo).

Todas estas amenazas evolucionan constantemente, por lo que el firewall también debe buscar adaptarse a las cambiantes condiciones del entorno (nuevas amenazas o nuevos requerimientos de los clientes). Esta evolución hace que el firewall tradicional se desarrolle cumpliendo con nuevos desafíos como el descifrado e inspección de SSL, IPS con tecnología antievasión, el control de aplicaciones basado en contexto y la protección contra malware basada en red.

Estos procesos evolutivos (de retos, amenazas, necesidades y soluciones) han creado un nuevo mercado, donde los proveedores también deben adaptarse a través de la diversificación y la competencia perfecta, para así lograr satisfacer a sus clientes. La metodología del Cuadrante Mágico

permite observar la clasificación de estos proveedores de acuerdo a su desempeño. Dichos proveedores se especializan en requerimientos detallados del cliente, lo que hace que algunos sean más aptos para ciertos sectores organizacionales de acuerdo a tendencias.

De acuerdo a todo lo anterior se puede hacer una reflexión basada en el ciclo evolutivo de las cosas. Las amenazas y riesgos mejoran sus intromisiones y cambian a través del tiempo. Esto provoca una secuencia reactiva, que conlleva también a la evolución de las tecnologías y procesos, con el ánimo de competir por la prevención y mitigación estas amenazas y riesgos. Un ejemplo claro de este ciclo es el proceso de adaptación de los firewalls.

También es válido resaltar la comunicación y el mercadeo que debe darse en este sistema. Sin estos procesos no habría evolución. Las compañías deben conocer las nuevas tendencias y alcances de las amenazas a la seguridad de la información, como también deben conocer las propuestas y alternativas que ofrecen las tecnologías y procesos en cuanto a la protección de la información. Sin estos procesos comerciales, no habría desarrollo informático.

Para finalizar, se puede decir que hoy en día se evidencia una gran gama de tecnologías y fabricantes que contribuyen con la mitigación y prevención sobre la inseguridad informática. De igual forma, las amenazas no paran de evolucionar para continuar con la competencia. Sin embargo, es de admirar los procesos de avance y conocimiento que se están dando continuamente. Con todo esto, se puede afirmar que es incierto pero esperanzador el futuro de la seguridad informática, tal cual el proceso histórico del firewall.

IX. REFERENCIAS

[1] J. López, «¿Que es un Firewall de Nueva Generación?,» GTI, 16 Mayo 2014. [En línea]. Available: http://noticias.gti.es/fabricantes/que-es-firewall-de-nueva-generacion/. [Último acceso: 29 Abril 2016].
[2] M. Mendoza, «¿Por qué es necesario el firewall en entornos corporativos?,» 29 Julio 2014. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/. [Último acceso: 30 Abril 2016].
[3] I. López, «25 años de Firewall: ¿sigue siendo efectivo?,» welivesecurity, 25 Julio 2014. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/07/25/25-anos-de-firewall-sigue-siendo-efectivo/. [Último acceso: 2016 Abril 30].
[4] Palo Alto Networks, «Guía para compradores de Firewalls,» PAN_BG_090513_ES, Santa Clara, 2013.
[5] ESET Latinoamérica, «ESET Security Report Latinoamérica,» ESET LLC, Buenos Aires, 2014.
[6] INTEROUTE, «Descripción del servicio de Firewall de Red de Nueva Generación,» Interoute Communications Limited, London, 2012.
[7] «Resumen del cortafuegos de nueva generación de Palo Alto Networks,» PAN_SS_NGFOV_102914, Santa Clara, 2015.
[8] Palo Alto Networks, «10 cosas que su próximo firewall debe hacer,» PAN_WP_10PT_ES_091013, Santa Clara, 2013.
[9] A. Hils, G. Young y J. D'Hoinne, «Magic Quadrant for Enterprise Network Firewall,» Gartner, Inc, 2015.
[10] G. Domínguez y C. Soto, «Firewalls de Nueva Generación,» securitic, México, 2014.
[11] «Guía para compradores de Firewalls». USA Patente PAN_BG_090513_ES.indd, 9 Mayo 2013.

Autor:
Ingeniero Electrónico graduado de la Universidad San Buenaventura en el año 2006 y Especialista en Gerencia Tecnología de la Universidad EAN. Cuenta con una amplia experiencia en redes, telecomunicaciones y seguridad informática, aplicada en entornos organizacionales. Específicamente, ha desplegado proyectos con productos como Juniper Networks, Radware, Infoblox y Hillstone Networks, en diversos sectores de la industria Colombiana.