SECUINFOR

Centro de Operaciones
de Ciberseguridad

#SiempreAlerta

CÓMO ELEGIR Y EVALUAR UN NEXT GENERATION FIREWALL

Autor: Christian Mendoza Bonzo. MSIA

Objetivo: Describirles a los administradores de redes y tecnologías de la información en que consiste un Next GenerationFirewall así como los nuevos mecanismos de protección más innovadores y eficientes para la protección de su información.

Fecha: Octubre 3, 2017.

Introducción.-

En muchas ocasiones los administradores de red o analistas de seguridad se encuentran abrumados y usualmente, esto se debe a la necesidad de evaluar y discernir la mejor opción de seguridad perimetral que se ajuste a las necesidades de su entidad. En el mercado existen un sin número de marcas que dicen ser la mejor opción, ante esto, vamos a descubrir qué es un dispositivo de seguridad perimetral de próxima generación o Next Generation Firewall y los puntos claves que pueden hacer diferencia en nuestra elección.

Next Generation Firewall.-

Iniciemos por la definición básica, un firewall o equipo de seguridad perimetral es un dispositivo que puede ser físico o virtual (software) y trabaja a nivel de red, su función es permitir o bloquear el acceso hacia o desde un recurso. Estos dispositivos de seguridad perimetral han evolucionado con el tiempo añadiendo algunas características que las hemos clasificado acorde a sus características en funcionalidades operacionales, básicas y otras avanzadas que convierten a un sencillo dispositivo de seguridad perimetral en un firewall de próxima generación o Next Generation Firewall.

Como ya mencionamos, hemos clasificado las funcionalidades en tres categorías para su mejor comprensión, ahora veamos de qué se tratan.

Funcionalidades operacionales.-

Son aquellas funciones o características mínimas que deben de poseer todos los dispositivos de seguridad perimetral (firewalls), como son:

- Permitir o denegar el acceso hacia o desde una subred o host específico, mediante el uso de reglas de filtrado.
- Poseer la capacidad de hacer inspección de paquetes y seguimiento de cada sesión, es decir que sean stateful inspection.
- Capacidad de tener redundancia a nivel de la wan para permitir la distribución del tráfico sobre varios enlaces, esta característica es conocida en algunas ocasiones como multipath, link load balance, entre otros nombres.

- Capacidad de detección para suplantación de identidad de un equipo, esta característica es conocida usualmente como anti-Spoofing.
- Creación y re-envío del registro de evento por cada regla aplicada.
- Creación de reglas para limitar tipos de tráfico a nivel de direccionamiento ip, es decir en la capa de red.

Funcionalidades básicas.-

Estas características son necesarias para que un dispositivo de seguridad perimetral pueda ser considerado como un Next Generation Firewall y son descritas a continuación:

1. *Control de aplicaciones:* esta característica se refiere al reconocimiento aplicacional, es decir, el equipo (firewall) cuenta con la capacidad de reconocer, controlar y administrar el tráfico de cada aplicación que atraviesa por este dispositivo (firewall), por lo que poder identificar, manejar y gestionar la mayor cantidad de aplicaciones es primordial, este es uno de los puntos más importantes por no decir el principal, debido a que permite un control granular sobre el tráfico en la red y su acceso.
2. *Prevención & detección de intrusos:* es un módulo que se agrega al firewall y normalmente su motor utiliza firmas para ejecutar algoritmos de búsqueda que examinan cada uno de los paquetes que pasan por el dispositivo, a fin de encontrar coincidencias de ataques en el tráfico. Este módulo usualmente trabaja a nivel de la capa 7, es decir sobre las aplicaciones, sin embargo existen marcas que lo hacen solamente desde la capa 3. Dado que esta característica utiliza firmas, el contar con la mayor cantidad de estas para identificar y controlar, así como de un buen motor para su análisis, es importante.
3. *VPN:* Esta característica provee acceso remoto a los recursos internos (intranet, aplicaciones, sistemas, etc) de una organización, usando una comunicación segura (cifrada), y dicho acceso puede ser por usuario o para toda una organización o sitio remoto, las VPNs proporcionan siempre tres características: confidencialidad, integridad y autenticación.
4. *Anti Virus:* Esta característica es sumamente importante, puesto que permite analizar el tráfico a nivel de red, mas no de estación, es decir que dicho mecanismo está de forma centralizada embebido en el dispositivo de seguridad perimetral (firewall) y analiza todos los paquetes que pasan por él para determinar si dicho tráfico está libre de software malicioso conocido (malware).

5. *Calidad de Servicio:* es el mecanismo utilizado por este tipo de dispositivos (firewalls) para priorizar el tráfico, esto es muy importante para la disponibilidad de nuestros servicios, porque mediante este módulo podemos reservar un ancho de banda para cada aplicación o servicio en nuestra empresa, esto se traduce a un óptimo desempeño y experiencia de los servicios ofrecidos para nuestros clientes.

Funcionalidades Avanzadas.-

Antes de profundizar, es importante aclarar que hemos considerado como características avanzadas, aquellas funciones en los dispositivos de seguridad perimetral (firewalls) que extienden o proporcionan funciones para proveer nuevas capacidades de detección, control, manejo, tratamiento, análisis y/o gestión de las amenazas existentes o nuevas.

Después de investigar lo último en innovación de algunos fabricantes, sumando nuestra experiencia en la gestión y administración de otros dispositivos, les mencionamos las funcionalidades o características que nos llamaron la atención, dicho esto procedemos a hacer nuestra lista:

- *Control de aplicaciones:* dado que es la principal funcionalidad de todo NGFW, vamos a describir algunas cosas novedosas, sabemos que esta característica en la mayoría de los dispositivos de seguridad perimetral (firewalls) se basa sólo en firmas y por ende su cantidad es importante, sin embargo existen otros equipos que adicionalmente a las firmas tradicionales tienen la capacidad de monitorear, analizar y aprender sobre nuevas aplicaciones, esto es gracias a que utilizan inteligencia artificial, análisis estadístico y correlación. Vale destacar que muy pocos dispositivos tienen la función de filtrar el contenido de una aplicación, esto se traduce en la facultad de poder discernir si permiten o no una aplicación dentro de otra, para comprenderlo mejor citemos un ejemplo: con el filtrado de contenido de aplicaciones podríamos bloquear un juego como angrybirds, candycrush entre otros dentro de facebook y sin importar que la aplicación facebook esté cifrada, con lo cual se brindaría un control superior muy diferente a los tradicionales dispositivos en este punto.
- *Ataques o amenazas desconocidas (APT):* como es de dominio público, cada día surgen nuevos ataques, nuevo malware, exploits o una combinación de estos; sin embargo, algunos firewalls incorporan nuevas técnicas de detección utilizando análisis de comportamiento, inteligencia artificial o correlación de patrones de ataques para la detección de este

nuevo tipo de amenazas. Imaginen el escenario donde un atacante se descarga el código de exploit o malware, lo reescribe y/o combina con otro para formar un ataque nuevo y así explotar una vulnerabilidad existente en nuestra infraestructura, esta característica podría detectar estos cambios de patrones o utilizar el análisis de comportamiento para detectar, notificar y detener esta nueva amenaza.

- *Anti Virus:* este módulo es muy importante, pero la mayoría de los dispositivos de seguridad perimetral no lo *integran*, sólo lo ***incorporan***. Nos referimos a que algunos fabricantes recientemente están integrando esta funcionalidad para que trabaje con otros módulos como la de filtrado web (url filtering) o filtrado de correo (Anti spam), proporcionado un mayor control en diferentes frentes.

- *Inter-operatividad:* cuando elegimos un dispositivo de seguridad perimetral, muchos hemos deseado que se integre en ocasiones con otros equipos o soluciones de seguridad, sin embargo, muy pocos dispositivos brindan esta capacidad de comunicarse con un dispositivo de capa 2 (switch) o una solución de protección para puntos finales (endpoint), para ejecutar políticas de seguridad sobre estos. Por tanto, este es un punto a considerar en el momento de hacer un diseño de seguridad, porque permitirá escoger nuestra infraestructura y efectuar defensa en profundidad permitiendo una mayor visión y control de las amenazas.

- *Administración y control:* muchos fabricantes de dispositivos de seguridad perimetral, se han olvidado de un punto fundamental, el cual consiste en brindar la visibilidad y conocimiento de lo que está ocurriendo en un determinado momento de tiempo con: informes, correlación, seguimiento de auditorías y análisis estadísticos de la seguridad para que la toma de decisiones pueda ser asertiva por parte de la alta dirección. Para esto vamos a mencionar algunas características que definitivamente deben de ser consideradas al momento de elegir una herramienta de seguridad perimetral como: la identificación de los cambios efectuados en un momento de tiempo así como el detalle de cada campo, tener el monitoreo en tiempo real del tráfico, correlación de la información, generación de cubos de información, analizadores de eventos o registros, contar con gestión basada en roles, generación de alarmas y alertas.

Tenga en cuenta que en cualquier solución que estemos evaluando debemos de considerar la carga que se va a soportar, es decir, los módulos (features) que vamos a habilitar, teniendo en mente que al habilitar estas características se degrada el desempeño nominal del equipo, esto se debe a que se necesita

mayores recursos de procesamiento, memoria entre otros, por cada uno de los módulos que se active.

Si desea conocer cómo podemos ayudarlo a proteger su información confidencial, contáctenos a:

Email: info@secuinfor.com

PBX: +593 4-3726620

Website: www.secuinfor.com