**¿Qué es Next Generation FireWall (NGFW)?**

Un firewall de próxima generación (NGFW) es una plataforma de red integrada que forma parte de la tercera generación de tecnología de cortafuegos, combinando unos cortafuegos tradicionales con otras funcionalidades de filtrado de dispositivos de red, como unos cortafuegos de aplicaciones mediante la inspección profunda de paquetes en línea), Un sistema de prevención de intrusiones (IPS). También se pueden emplear otras técnicas, como la inspección de tráfico encriptada TLS / SSL, el filtrado de sitios web, la gestión de la calidad de servicio / banda ancha, la inspección antivirus y la integración de gestión de identidad de terceros (es decir, LDAP, RADIUS y Active Directory).

**¿NGFW vs. Firewall Tradicional?**

Los NGFW incluyen las funciones típicas de cortafuegos tradicionales, como el filtrado de paquetes, la traducción de direcciones de red y puertos (NAT), la inspección con estado y el soporte de redes privadas virtuales (VPN). El objetivo de los firewalls de próxima generación es incluir más capas del modelo OSI, mejorando el filtrado del tráfico de red que depende del contenido de los paquetes.

Los NGFW realizan una inspección más profunda en comparación con la inspección con estado realizada por los firewalls de primera y segunda generación. Los NGFW utilizan un estilo de inspección más completo, revisan las cargas útiles de paquetes y firmas coincidentes para actividades dañinas como ataques explotables y malware.

**Fortinet**

Fortinet es una empresa multinacional de Estados Unidos con sede en Sunnyvale, California. Se dedica al desarrollo y la comercialización de software, dispositivos y servicios de ciberseguridad, como firewalls, antivirus, prevención de intrusiones y seguridad en dispositivos de usuario, entre otros. Es la cuarta compañía de seguridad de redes más (grandes) por volumen de ingresos.

Fortinet desarrolla y comercializa hardware y software de seguridad y redes informáticas.46 Es conocida sobre todo por su gama de dispositivos de seguridad FortiGate, que combinan numerosas funciones de ciberseguridad.47 Según un informe de 2015 de la firma de analistas informáticos The Dell'Oro Group, Fortinet tenía un 8% de la cuota del mercado de dispositivos de seguridad informática por ingresos en 2014, frente al 2,9% de 2012.48 Esto la convierte en el cuarto proveedor del sector.49 Según Fortinet, el 35% de sus usuarios son pequeñas empresas, el 28% medianas empresas y 37% grandes corporaciones.

**Palo Alto Networks**

Palo Alto Networks, Inc. es una empresa de seguridad de redes y empresas con sede en Santa Clara, California. Los principales productos de la compañía son una plataforma que incluye firewalls avanzados diseñados para proporcionar seguridad de red, visibilidad y control granular de la actividad de red basada en la aplicación, el usuario y la identificación de contenido y ofertas basadas en la nube que amplían esos cortafuegos para cubrir otros aspectos de seguridad.

En 2009, la compañía lanzó una publicación que define el "firewall de próxima generación". Palo Alto Networks definió esta nueva generación de cortafuegos como conteniendo conocimiento de aplicación, visibilidad de pila completa, inteligencia extra-firewall y rutas de actualización además de las capacidades completas de firewalls tradicionales y sistemas de prevención de intrusiones. Además, la compañía define su tecnología de cortafuegos por las siguientes habilidades:

* Identificar aplicaciones sin importar el puerto, protocolo, táctica evasiva o Secure Sockets Layer
* Identificar y controlar a los usuarios independientemente de la dirección IP, la ubicación o el dispositivo
* Proteger contra amenazas conocidas y desconocidas
* Visibilidad y control de políticas de gran fin sobre el acceso a aplicaciones / funcionalidad
* Multi- gigabit, baja latencia, implementación en línea

En 2013 se agregó MSM - Mobile Security Manager para extender la seguridad del firewall a dispositivos móviles. En 2014 TRAPS se agregó a la lista de productos. Traps sirve como una versión de la protección de punto final, la protección del cliente sin el archivo de virus estándar más bien toma una vista diferente e intenta supervisar, detectar y frustrar la entrada del virus en el cliente mediante la supervisión de puntos de entrada comunes

**Forcepoint NGFW**

Forcepoint NGFW actúa como el centro de la seguridad de sus redes, centralizando el monitoreo, la administración y la elaboración de informes en diversos dispositivos virtuales, físicos y en la nube, así como dispositivos de terceros. Los flujos de trabajo optimizados simplifican las tareas administrativas diarias y la gestión de la seguridad para lograr una mayor eficiencia y un bajo costo total de propiedad (TCO).

Forcepoint NGFW utiliza un enfoque único e incorporado para optimizar la disponibilidad, la escalabilidad y el costo de las redes. El agrupamiento para la alta disponibilidad y un alto rendimiento, pueden utilizarse para centros de datos y otros casos de uso intenso de computadoras, lo que permite la escalabilidad de la administración de la red.

Características:

* Soporte para Amazon Web Services
* Gestión centralizada de hasta 2000 firewalls
* Opciones de software, implementación física, virtual y en la nube, que incluyen Amazon Web Services (AWS)
* Agrupamiento activo incorporado que escala a 16 nodos para alta disponibilidad
* Instalación plug-and-play de firewalls de redes remotas

**CUADRANTE MAGICO DE GARTNER (NGFW Gartner Magic Quadrant - Gartnet MQ)**

Los dispositivos unificados de gestión de amenazas ofrecen a las pequeñas y medianas Distribuidas con múltiples funciones de seguridad de red en un solo dispositivo. UTM Los compradores deben evaluar el rendimiento, la seguridad, la facilidad de uso, el apoyo local y la Manejar nuevas prácticas de SMB.

Para 2020, el 50% de las PYMES utilizarán capacidades de gestión de movilidad o inalámbricas de su UTM Plataformas para reforzar las políticas distintivas, a partir de 10% hoy en día.A través de al menos 2020, los mercados de firewall para SMB y firewalls empresariales permanecerán distinto.

Gartner define el mercado unificado de gestión de amenazas (UTM) como una red multifunción Productos de seguridad utilizados por pequeñas y medianas empresas (PYMES). Normalmente, las medianas empresas Tienen de 100 a 1.000 empleados (ver Nota 1). Los proveedores de UTM añaden continuamente nuevas UTM, y por lo tanto, abarcan el conjunto de características de muchas otras redes de seguridad

Soluciones, incluyendo:

* Firewall empresarial
* Los sistemas de prevención de intrusiones (IPS)
* Acceso remoto
* Puerta de enlace web segura
* Gateway de correo electrónico seguro