5 Tips para elegir un *firewall* de próxima generación

Las crecientes amenazas de Internet exigen un *Firewall* de Próxima Generación (NGFW). Aquí le decimos cómo reconocerlo.

1 Prevención de Brechas y Seguridad Avanzada

Identifica ataques de manera anticipada y detecta al instante el *malware* infiltrado

El objetivo principal de un *firewall* es prevenir brechas de seguridad y mantener protegida su organización. Sin embargo, ya que las medidas preventivas no son 100% efectivas, su *firewall* también debería contar con capacidades avanzadas, como la detección instantánea del *malware* que haya superado su primera línea de defensa.

Invierta en un *firewall* con las siguientes capacidades:

- Detección de ataques antes de la infiltración
- El mejor IPS integrado de próxima generación, capaz de detectar amenazas silenciosas y detenerlas con rapidez
- Filtrado de URL, aplicando políticas en cientos de millones de ellas
- *Sandboxing* integrado y protección avanzada contra *malware,* detectando y eliminando amenazas con rapidez por medio de un análisis continuo del comportamiento de los archivos
- Una organización de inteligencia de amenazas de clase mundial, que permita ofrecer un *firewall* con las técnicas más actualizadas en la detección de las nuevas amenazas que emergen continuamente.

2 Visibilidad Integral de la Red

Detectar más es proteger mejor

Es imposible cuidarse de lo que no puede ver. Para detectar algún comportamiento inapropiado y detenerlo al instante, usted necesita vigilar continuamente todo lo que sucede en su red.

Su *firewall* debería ofrecerle una visión holística de la actividad y una percepción contextual total para detectar lo siguiente:

- La actividad de las amenazas a través de usuarios, servidores, redes y dispositivos
- El lugar y momento en que se origina una amenaza, las partes de la red extendida donde ha sido detectada y las acciones que está realizando en este momento
- Aplicaciones y sitios web activos
- La comunicación entre máquinas virtuales, transferencias de archivos y más

Recursos Adicionales

Exiga más de su *firewall.* Conozca más de Cisco Firepower NGFW.

Cisco NGFW Overview
Cisco NGFW Demo Customer Testimonial: Downer Group

Visite cisco.com/go/ngfw

3 Flexibilidad de Gestión y Opciones de Implementación

Configuración adaptable a las necesidades únicas de cada organización

No importa si el negocio que usted dirige es pequeño, mediano o una gran empresa, en cualquier caso usted necesita un *firewall* que sea capaz de solucionar sus necesidades específicas.

- Administración para cada caso de uso: Elija entre un gestor dentro del mismo *firewall*, o una administración centralizada de todos los *firewalls* en su red.
- Implemente de manera local, o en la nube a través de un *firewall* virtual
- Personalice su *firewall* con características que solucionen sus necesidades; sólo active las suscripciones para obtener capacidades avanzadas
- Elija entre un amplio rango de velocidades de rendimiento

4 El Tiempo de Detección Más Veloz

Detecte *malware* con mayor rapidez y reduzca el riesgo

El tiempo estándar para la detección de amenazas en la industria actual es de 100 a 200 días, ¡eso es demasiado! Un f*irewall* de próxima generación debería ofrecer soluciones con mayor rapidez:

- Detección de amenazas en segundos
- Localización de brechas de seguridad en horas o minutos
- Priorización de alertas para que usted tome acciones rápidas y precisas en la eliminación de amenazas
- Implementación de una política consistente que sea fácil de mantener, con aplicación automática a través de las diferentes facetas de su organización

5 Integración con Otras Herramientas

Una arquitectura de seguridad integrada habilita la automatización y reduce la complejidad

Su *firewall* de próxima generación no puede ser una herramienta aislada, debe comunicarse y trabajar en conjunto con el resto de su arquitectura de seguridad.

Elija un *firewall* con las siguientes características:

- Integración impecable con otras herramientas del mismo proveedor
- Envío automático de la información de amenazas, datos de los eventos, políticas e información contextual, a las herramientas de correo electrónico, el entorno web, los terminales y dispositivos y las herramientas de seguridad de la red
- Automatización de las operaciones de seguridad, como la evaluación del impacto, el ajuste de las políticas y la identificación del usuario