5 Sugerencias para elegir un firewall de última generación

Invierta en un firewall de última generación (NGFW) centrado en las amenazas. Descubra si ofrece lo siguiente:

1 Defensa integrada contra amenazas

Consiga información sobre la que se puede actuar y de varios niveles.

Las amenazas persistentes y multivector de la actualidad se cuelan por los agujeros de la protección y eluden la detección. Un NGFW centrado en las amenazas ofrece las mejores tecnologías de seguridad de su clase que colaboran en la red y en los terminales y que, además, se gestionan por medio de una consola central. Las tecnologías de NGFW centradas en las amenazas, que se basan en firewalls stateful integrales, deben incluir estos componentes:

- IPS de última generación
- Protección frente a malware avanzado
- Control y visibilidad de aplicaciones
- Filtrado de URL por reputación
- VPN de nivel de las aplicaciones

▸ Con una protección frente a malware avanzado y amenazas integrada que relacione continuamente la inteligencia de amenazas de los distintos niveles de seguridad, podrá identificar los ataques sofisticados y protegerse ante ellos.

Recursos

Firewall de última generación: lista de requisitos que debe reunir

Informe técnico. Consiga la lista completa de los requisitos que debe cumplir su firewall para proteger a su empresa de los ataques.
Leálo ahora

Mejor visibilidad. Mejor protección

Vea un enfoque innovador de defensa frente a las amenazas y cómo lograr una protección continua contra las amenazas.
Vea el vídeo

Web de Cisco NGFW

Manténgase informado sobre las últimas tendencias y descubra las novedades en materia de seguridad de Cisco.
Obtenga más información

2 Indicadores de compromiso con capacidad de actuación

Acelere la detección de malware para mitigar los riesgos.

Actualmente, el plazo estándar en el sector para detectar una amenaza se sitúa entre 100 y 200 días: demasiado tiempo. Los NGFW deben aportar indicadores de compromiso (IoC) con capacidad de actuación que reúnan estos requisitos:

- Relacionen la inteligencia de seguridad de la red y de los terminales.
- Proporcionen una visibilidad muy precisa de los comportamientos de los hosts y los archivos sospechosos y maliciosos.
- Den prioridad a los hosts infectados para realizar una remediación rápida.

▸ Los IoC con capacidad de actuación permiten ver la actividad del malware en los hosts y en los terminales, comprender su repercusión, así como contener la amenaza y remediarla rápidamente.

3 Visibilidad integral de la red

Aumente la eficacia en materia de seguridad con una visión holística.

No se puede proteger lo que no se puede ver. Debe supervisar lo que sucede en su red en todo momento.

Un NGFW debe aportar una información contextual completa sobre los siguientes aspectos:

- Usuarios, sistemas operativos y dispositivos
- Comunicaciones entre máquinas virtuales
- Amenazas y vulnerabilidades
- Acceso a la Web y aplicaciones
- Transferencias de archivos y mucho más

▸ Este nivel de información permite identificar y suplir las lagunas de seguridad, así como ajustar las políticas con la finalidad de reducir el número de eventos significativos que requieren acciones adicionales.

4 Menos complejidad y menores costes

Unifique los niveles de seguridad e implemente sistemas de automatización para mejorar la eficacia.

La combinación de amenazas avanzadas y escasez de profesionales en materia de seguridad de TI suficientemente capacitados está llevando al límite a los departamentos de TI.

Busque un NGFW que tenga estas características:

- Consolida varios niveles de defensas en una única plataforma.
- Ofrece una seguridad uniforme y sólida a medida.
- Automatiza tareas de seguridad habituales, como la evaluación del impacto, el ajuste de las políticas y la identificación de los usuarios.

▸ Al reducir la complejidad y los costes, su equipo dispondrá de más tiempo para centrarse en los eventos más importantes.

5 Integración con soluciones de terceros

Saque el máximo partido de las inversiones en seguridad existentes.

Necesita ser capaz de compartir información y aprovechar mejor las tecnologías de seguridad de las que ya disponga para consolidar y agilizar las respuestas a los ataques.

Busque una plataforma de NGFW abierta y que se integre sin problemas con un ecosistema de soluciones de seguridad de terceros, como las siguientes:

- Sistemas de gestión de vulnerabilidades
- Sistemas SIEM y de visualización de redes
- Sistemas de incidencias y remediación del flujo de trabajo
- Control de acceso a la red (NAC) y mucho más

▸ La integración con soluciones de terceros reduce el número de tareas que debe asumir el departamento de TI y el coste total de propiedad (TCO). Además, fortalece las protecciones de varios niveles.

Tanto los ataques como el entorno de TI que tendrá que proteger seguirán evolucionando. Asegúrese de que el NGFW por el que se decante le ofrece **una protección frente a amenazas estrechamente integrada y de varios niveles**. Al compartir información y datos contextuales entre las funciones de seguridad, podrá acelerar la detección de amenazas y las respuestas en toda su organización, así como sacar el máximo partido de sus inversiones.

cisco

No es lo que hacemos; es lo que hacemos posible.

Conseguimos hacer realidad que la seguridad esté omnipresente.

Visite www.cisco.com/go/ngfw

Síganos en Twitter: @CiscoSecurity