5 consejos para elegir un firewall de última generación

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

1 Seguridad avanzada y prevención de brechas de seguridad

Evite los ataques y detecte rápidamente las intrusiones de malware

La misión principal de un firewall deberá ser evitar las brechas de seguridad y mantener la seguridad de su organización. Sin embargo, dado que las medidas preventivas nunca serán 100 % eficaces, su firewall también deberá incluir funciones avanzadas para detectar rápidamente el malware avanzado si elude su primera línea de defensa. Invierta en un firewall que cuente con las siguientes funciones:

- Prevención para detener los ataques antes de que se adentren en el sistema
- El mejor IPS de última generación de su categoría integrado para detectar las amenazas sigilosas y detenerlas rápidamente
- Filtrado de URL para aplicar las políticas en cientos de millones de URL
- Sandboxing y protección frente a malware avanzado integrados para analizar continuamente el comportamiento de los archivos y detectar y eliminar las amenazas con rapidez
- Una organización de inteligencia de amenazas de primera clase que ofrece la inteligencia más reciente al firewall para detener las amenazas emergentes

2 Visibilidad integral de la red

Obtenga una mayor visibilidad para detener más amenazas

No se puede proteger de lo que no puede ver. Debe supervisar lo que sucede en su red en todo momento, de modo que pueda detectar el comportamiento incorrecto y detenerlo rápidamente. Su firewall deberá ofrecer una visión global de la actividad e información contextual completa para detectar:

- La actividad de las amenazas en usuarios, hosts, redes y dispositivos
- Dónde y cuándo se ha originado una amenaza, por qué otros lugares de su red extendida ha pasado y qué está haciendo ahora
- Los sitios web y las aplicaciones activas
- Las comunicaciones entre máquinas virtuales, las transferencias de archivos, etc.

Recursos adicionales

Exija más de su firewall. Descubra el NGFW Cisco Firepower.

Descripción general del NGFW de Cisco

Demostración del NGFW de Cisco

Testimonio de cliente: Downer Group

Visite cisco.com/go/ngfw

3 Opciones de implementación y gestión flexibles

Personalización para satisfacer las necesidades exclusivas de cada organización

Tanto si su empresa es pequeña, mediana o grande, su firewall deberá satisfacer sus requisitos exclusivos.

- Gestión de cada caso práctico: seleccione entre una gestión integrada o centralizada en todos los dispositivos
- Implementación en las instalaciones o en la nube mediante un firewall virtual
- Personalización con características que satisfacen sus necesidades: solo tiene que activar las suscripciones para obtener las funciones avanzadas
- Selección entre una amplia gama de velocidades de rendimiento

4 Mayor rapidez en la detección

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. Un firewall de última generación deberá ser capaz de:

- Detectar las amenazas en cuestión de segundos
- Detectar la presencia de una brecha de seguridad exitosa en cuestión de horas o minutos
- Priorizar las alertas para que pueda actuar con rapidez y precisar las acciones para eliminar las amenazas
- Facilitarle la vida al implementar una política uniforme de mantenimiento sencillo, con una aplicación automática en las diferentes facetas de su organización

5 No se trata de un lobo solitario, sino de un miembro de la manada.

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

Su firewall de última generación no deberá ser una herramienta aislada. Deberá comunicarse y funcionar junto con el resto de su arquitectura de seguridad. Elija un firewall que:

- Se integre sin problemas con el resto de herramientas del mismo proveedor
- Comparta automáticamente la información de las amenazas, los datos de evento, la política y la información contextual con herramientas de seguridad de red, correo electrónico, web y terminales
- Automatice las tareas de seguridad, como la evaluación del impacto, el ajuste de las políticas y la identificación de los usuarios