¿Cuales son los tipos de firewalls o cortafuegos que existen?

¿Cuales son los tipos de firewalls o cortafuegos que existen? Hemos visto en un post anterior qué es un firewall en computación o redes; ya tenemos un punto de partida; ahora hablemos de las clases que existen; hagamos una clasificación de resumen para nuestros clientes.

Software y Hardware

Hay firewalls de software y hardware. Pe

rs
on
al
me
nt
e
re
co
mi
en
do
te
ne
r
am
bo
s,
un
o
fí
si
co
y
un
o
ló
gi
co
.
Es
ta
si
ne
rg
ia
es
ga

na
do
ra
,
po
te
nc
ia
y
re
fu
er
za
nu
es
tr
o
es
qu
em
a
de
se
gu
ri
da
d
de
un
a
fo
rm
a
im
po
rt
an

te
.
Ca
da
fo
rm
at
o
ti
en
e
un
pr
op
ós
it
o
di
fe
re
nt
e
pe
ro
im
po
rt
an
te
.

Firewall físico

Un firewall de hardware es físico, como un enrutador de banda ancha, almacenado entre su red y puerta de enlace.Estos cortafuegos se lanzan como productos independientes para uso corporativo o, más a menudo, como un componente integrado de

un enrutador u otro dispositivo de red. Se consideran una parte esencial de cualquier sistema de seguridad tradicional y configuración de red. Los firewalls de hardware casi siempre vienen con un mínimo de cuatro puertos de red que permiten conexiones a múltiples sistemas. Para redes más grandes, hay disponible una solución de firewall de red más expansiva.

Cortafuegos lógico

Un firewall de software es interno: un programa en su computadora o servidor web que funciona a través de números de puerto y aplicaciones.

Se pueden personalizar y proporcionan un menor nivel de control sobre las funciones y características de protección. Un cortafuegos de software puede proteger un sistema de control estándar e intentos de acceso, pero tiene problemas con infracciones de red más sofisticadas.

Cortafuegos como servicio

También hay firewalls basados □□en la nube, conocidos como Firewall as a Service (FaaS). Un beneficio de los firewalls basados □□en la nube es que pueden crecer con su organización y, de manera similar a los firewalls de hardware, funcionan bien con la seguridad perimetral.

Existen varios tipos diferentes de firewalls según su estructura y funcionalidad. Estos son los diferentes firewalls que puede implementar, según el tamaño de su red y el nivel de seguridad que necesita.

Filtrado de paquetes

Los firewalls de filtrado de paquetes, el tipo más común de firewall, examinan los paquetes y prohíben su paso si no coinciden con un conjunto de reglas de seguridad establecido.

Este tipo de firewall verifica las direcciones IP de origen y destino del paquete. Si los paquetes coinciden con los de una regla «permitida» en el firewall, entonces es de confianza ingresar a la red.

Los firewalls de filtrado de paquetes se dividen en dos categorías: con estado y sin estado. Los firewalls sin estado examinan los paquetes independientemente uno del otro y carecen de contexto, lo que los convierte en objetivos fáciles para los piratas informáticos. En contraste, los firewalls con estado recuerdan información sobre paquetes pasados previamente y se consideran mucho más seguros.

Si bien los firewalls de filtrado de paquetes pueden ser efectivos, en última instancia proporcionan una protección muy básica y pueden ser muy limitados; por ejemplo, no pueden determinar si el contenido de la solicitud que se envía afectará negativamente a la aplicación a la que llega. Si una solicitud maliciosa que se permitiera desde una dirección de origen confiable resultara, por ejemplo, en la eliminación de una base de datos, el firewall no tendría forma de saberlo. Los firewalls de próxima generación y los firewalls proxy están más equipados para detectar tales amenazas.

A nivel de circuito

Como otro tipo de firewall simplista que está destinado a aprobar o denegar rápida y fácilmente el tráfico sin consumir recursos informáticos significativos, las puertas de enlace a nivel de circuito funcionan verificando el protocolo de enlace de protocolo de control de transmisión (TCP). Esta comprobación de protocolo de enlace TCP está diseñada para garantizar que la sesión de la que proviene el paquete sea legítima.

Si bien son extremadamente eficientes en cuanto a recursos, estos firewalls no verifican el paquete en sí. Entonces, si un paquete contenía malware, pero tenía el protocolo de enlace

TCP correcto, pasaría de inmediato. Es por eso que las puertas de enlace a nivel de circuito no son suficientes para proteger su negocio por sí mismas.
Este tipo de cortafuegos aplica una variedad de mecanismos de seguridad una vez que se ha realizado una conexión UDP o TCP. Una vez que se establece la conexión, los paquetes se intercambian directamente entre los hosts sin mayor supervisión o filtrado.

Servidor Proxy

Un primer tipo de dispositivo de firewall, un firewall proxy sirve como puerta de enlace de una red a otra para una aplicación específica. Los servidores proxy pueden proporcionar funcionalidades adicionales, como el almacenamiento en caché de contenido y la seguridad al evitar conexiones directas desde fuera de la red. Sin embargo, esto también puede afectar las capacidades de rendimiento y las aplicaciones que pueden soportar.

Los firewalls proxy filtran el tráfico de red a nivel de aplicación. A diferencia de los firewalls básicos, el proxy actúa como intermediario entre dos sistemas finales. El cliente debe enviar una solicitud al firewall, donde luego se evalúa con respecto a un conjunto de reglas de seguridad y luego se permite o bloquea. En particular, los firewalls proxy monitorean el tráfico en busca de protocolos de capa 7 como HTTP y FTP, y utilizan la inspección de paquetes profunda y con estado para detectar tráfico malicioso.

Cortafuegos de inspección con estado

Estos cortafuegos combinan la tecnología de inspección de paquetes y la verificación de protocolo de enlace TCP para crear un nivel de protección mayor que cualquiera de las dos

arquitecturas anteriores podría proporcionar por sí solo.

Sin embargo, estos firewalls también ejercen una mayor presión sobre los recursos informáticos. Esto puede ralentizar la transferencia de paquetes legítimos en comparación con las otras soluciones.
A veces denominada tecnología de cortafuegos de tercera generación, el filtrado con estado logra dos cosas: clasificación de tráfico basada en el puerto de destino y seguimiento de paquetes de cada interacción entre conexiones internas. Estas nuevas tecnologías aumentan la usabilidad y ayudan a expandir la granularidad del control de acceso: las interacciones ya no se definen por puerto y protocolo. También se mide el historial de un paquete en la tabla de estado.

Los firewalls de traducción de direcciones de red (NAT)

Estos cortafuegos permiten que múltiples dispositivos con direcciones de red independientes se conecten a Internet utilizando una sola dirección IP, manteniendo ocultas las direcciones IP individuales. Como resultado, los atacantes que escanean una red en busca de direcciones IP no pueden capturar detalles específicos, lo que proporciona una mayor seguridad contra los ataques. Los firewalls NAT son similares a los firewalls proxy en el sentido de que actúan como intermediarios entre un grupo de computadoras y el tráfico externo.

Cortafuegos de inspección de múltiples capas con estado (SMLI)

El firewall de inspección multicapa con estado tiene capacidades de firewall estándar y realiza un seguimiento de las conexiones establecidas. Filtra el tráfico según el estado, el puerto y el protocolo, junto con las reglas y el

contexto definidos por el administrador. Esto implica el uso de datos de conexiones anteriores y paquetes de la misma conexión.

La mayoría de los firewalls dependen de la inspección de paquetes con estado para realizar un seguimiento de todo el tráfico interno. Este firewall está un paso por encima del filtrado de paquetes en su uso de monitoreo de múltiples capas.

Sin embargo, todavía no puede distinguir entre el tráfico web bueno y malo, por lo que puede necesitar software adicional.

Tipos de firewalls que existen

Cortafuegos de próxima generación (NGFW)

Funcionan filtrando el tráfico que se mueve a través de una red: el filtrado está determinado por las aplicaciones o los tipos de tráfico y los puertos a los que están asignados. Estas características comprenden una combinación de un firewall estándar con funcionalidad adicional, para ayudar con una inspección de red mayor y más autosuficiente.

Otros recursos valiosos del blog al respecto

- ¿Qué es la seguridad web? Definición, significado, concepto
- ¿Por qué es importante la seguridad del sitio web?
- ¿Cómo está mejorando la inteligencia artificial la industria del alojamiento web?

Conclusión

Habla ya con nuestros asesores respecto a la mejor solución de seguridad para tu sitio web, recomendamos usar el firewall físico como primera barrera y un software como cortafuegos perimetral de segunda instancia o en su defecto uno como servicio.

Ediciones 2019-22