¿Qué es un firewall?

Filtra en función de:

- procedencia (equipo, rede, ou interface pola que entra).
- destino (equipo o rede de destino, interfaz pola que sae, porto de destino)
- protocolo de red
- contenido (tamaño de paauetes)

Tipos de firewall

Sobre el ámbito de aplicación

Firewall de red: controla el trafico de la red.

Firewall de sistema: instalado en el dispositivo en si.

Base de pila en la que trabaja.

Firewall de red: Filtran en función dos datagramas IP, segmentos TCP e datagramas UDP e sobre a base dunha serie der egras establecidas polo administrador Ademais do filtrado estes dispositivos adoitan facer NAT.

- Stateless: Analiza cada cabecera de paquete para comprobar si el paquete puede pasar.

- Stateful: Mejora el filtrado de paquetes porque guarda el estado de las conexiones establecidas na táboa de estado, trata os paquetes como forma de una conexión existente.

Application level firewalls (proxys) : Intermediarios entre a rede segura aceptando peticións de clientes e actuando como intermediarios.

- Permiten o rexeitan comunicacións en función de:

  Orixe e destino de comunicacións

  protocolo

  apliación empregada para comunicarse có exterior.

  Contido dos datos de aplicación.

- Autenticar ós usuarios contra bases de datos locales ou directorios (Active Directory, LDAP, Radius)

- Proporciona logs a nivel de aplicación (auditoría).

técnicas para filtrar paquetes

Xogos de regras (rulesets) : ACL

Filtrado de camiño inverso: Si las direcciones de las que viene las conoce la tabla de enrutamiento las deja pasar. Sino las rechaza.

Rutas de descarte: permite enviar o tráfico especificado a unha interface virtual de descarte. Impleméntase modificando a táboa de enrutamiento. É polo tanto un filtrado baseado na dirección IP de destino Filtrado en base a la direccion ip de destino.

En moitos firewalls perimetrais adoita aplicarse un filtrado coñecido como de entrada/saída (ingress/egress) de maneira que sexan o primeiro punto de control do tráfico. Para un rendemento óptimo, o habitual é filtrar no interface máis próximo; é dicir, o tráfico de saída cara a Internet filtralo no interface interno e o tráfico de entrada de Internet filtralo no interface externo.

Direcciones marcianas:

As direccións marcianas son todas aquelas que pola súa asignación non poden xerar tráfico Internet válido (e, polo tanto, seguramente enmascaran tráfico ilícito). As direccións a bloquear serían:

– Direccións reservadas pola IANA: 0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.0.2.0/24, 224.0.0.0/4, 240.0.0.0/4. 192.88.99.0/24, 198.18.0.0/15, 192.168.0.0/16

– Direccións recollidas no RFC 3232: este documento e establece unha base de datos online e en continuo cambio como referencia obrigada para a asignación dos rangos de direccións IP por IANA.

No caso de firewalls que están dentro de organizacións que usan direccionamento pri vado, habería que analizar cales destas redes están en uso para permitir o seu tráfico, blo queando o resto.

- Direccións non asignadas : denega a entrada e saída de tráfico orixinado en direccións válidas pero que non están en uso.

proceso de auditoría:

De los primeros pasos de uno de estos ataques es el network mapping.

- Equipos activos
- Puertos y aplicaciones ejecutándose en ellos.
- Sistemas operativos y versionaes.
- Topología de la red.

LOGS:

Hay que revisar periódicamente los logs para comprobar que no se ha violado la seguridad perimetral del sistema. Los mensajes indican que se ha cometido una violación de la política de seguridad perimetral.