Firewall

Un firewall es un sistema de defensa basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar, y tomar nota de todo aquello que ocurre, de acuerdo con una política de control de acceso entre redes.

Actúa a base de normas que establece el administrador de seguridad o de red. Dichas reglas definen las acciones correspondientes a llevar a cabo cuando se recibe un paquete que cumpla unas determinadas características.

El orden en el que se ponen las reglas de firewall es determinante. Normalmente cuando hay que decidir que se hace con un paquete se va comparando con cada regla del firewall hasta que se encuentra una que le afecta (match), y se hace lo que dicte esta regla (aceptar o denegar); después de eso no se mirarán más reglas para ese paquete. ¿Cuál es el peligro? Si ponemos reglas muy permisivas entre las primeras del firewall, puede que las siguientes no se apliquen y no sirvan de nada.

Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. En ella, se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall.

Un firewall puede funcionar mediante un filtrado simple de paquetes (stateless) o un filtrado dinámico de paquetes (stateful):

Filtrado stateless: mira el tráfico de la red, restringe o bloquea paquetes basándose en la dirección origen y otros valores estáticos. No son conscientes de los flujos de datos.

Se efectúan dos reglas: permitir paquetes entrantes desde internet puerto 80 a mi red y permitir paquetes saliente a direcciones de internet puerto 80 desde mi red. Con estas dos reglas, alguien malicioso desde internet podría mandar paquetes “truchos” y entrarían sin problema.

Los stateless firewalls son más rápidos y tienen un mejor desempeño bajo cargas de tráfico pesado.

Filtrado stateful: éstos sí pueden ver los flujos de tráfico de extremo a extremo. Son conscientes de las vías de comunicación y pueden implementar medidas de seguridad como el cifrado y túneles. En otras palabras, estos tipos de firewalls pueden decidir en que etapa de una conexión TCP nos encontramos y hacer reglas que permitan que los paquetes que sean respuesta de una conexión segura (o que efectúe yo) pasen y otros no.

Son mejores en lo que respecta a la identificación de conexiones no autorizadas.

Mediante tres reglas, establecemos el filtrado stateful, permitir conexiones ya establecidas y prohíbo las inválidas, además de permitir conexiones salientes de mi red a internet puerto 80. Entonces si me mandan un paquete “trucho” no pasaría nada porque firewall sabrá que yo no establecí esa conexión con anterioridad

Para los paquetes que van a la propia máquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas FORWARD.

Las reglas de NAT se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino. Estas son PREROUTING (utilizada para hacer DNAT, altera los paquetes antes de ser ruteados) y POSTROUTING (utilizada para hacer SNAT, altera los paquetes luego de ser ruteados)

Reglas:

Se toma por defecto la tabla filter.

Para utilizar otra tabla usar -t nat

Generalmente se define la variable I I=/sbin/iptables. Luego se utiliza al principio de todos los comandos con $I

-A append

-P Todos los paquetes que no coincidan con ninguna regla emplearán esa política de la cadena

ej. $I -P INPUT DROP

-d destino

-i interfaz

ej. -i eth0

-o interfaz de salida

ej. -o eth1

-s source

ej. -s $LAN (Se definio la variable LAN de la sgte manera LAN=10.0.1.0/24)

-j para aceptar, rechazar, dropear, SNAT, DNAT

ej. $I -A FORWARD -m state --state INVALID -j DROP

SNAT utilizado para postrouting, DNAT utilizado para prerouting

-p puerto (udp, tcp)

ej. -p udp --dport 53

-m módulo

Para no permitir nada más $I -A FORWARD/INPUT/OUTPUT -j DROP generalmente se coloca al principio.

Regla para natear $I -t nat -A POSTROUTING -s $LAN -o eth3 -j SNAT –to 200.3.1.2

INPUT está pensada sólamente para nuestro host local.

OUTPUT es donde filtramos los paquetes salientes de nuestro host local.

Puerto 53 consultas DNS. Puerto 22 acceso a ssh. Puerto HTTPS 443. Puerto 80 HTTP.

DNS

El DNS se usa principalmente para relacionar los nombres de host y destinos de correo electrónico con las direcciones IP.

Muy brevemente, la forma en que se utiliza el DNS es la siguiente. Para relacionar un nombre con una dirección IP, un programa de aplicación llama a un procedimiento de biblioteca llamado resolvedor, y le pasa el nombre como parámetro. El resolvedor envía un paquete UDP a un servidor DNS local, que después busca el nombre y devuelve la dirección IP al resolvedor, que entonces lo devuelve al solicitante. Una vez que tiene la dirección IP, el programa puede establecer una conexión TCP con el destino, o enviar paquetes UDP.

La esencia del DNS es la invención de un esquema de nombres jerárquico basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres.

La administración de un grupo grande y continuamente cambiante de nombres es un problema nada sencillo. En el sistema postal, la administración de nombres se hace requiriendo letras para especificar (implícita o explícitamente) el país, estado o provincia, ciudad y calle, y dirección del destinatario.

El DNS funciona de la misma manera. Conceptualmente, Internet se divide en 200 dominios de nivel superior, cada uno de los cuales abarca muchos hosts. Cada dominio se divide en subdominios, los cuales, a su vez, también se

dividen, y así sucesivamente. Todos estos dominios pueden representarse mediante un árbol, como se muestra en la figura. Las hojas del árbol representan los dominios que no tienen subdominios (pero que, por supuesto, contienen máquinas). Un dominio de hoja puede contener un solo

host, o puede representar a una compañía y contener miles de hosts.

Los dominios de nivel superior se dividen en dos categorías: genéricos y de país. Los dominios genéricos originales son com, edu, gov, int, net, org, etc.