Filtrado de paquetes en Linux

Este capítulo se ocupará de la máquina de estado y la explicará en detalle.

La máquina de estado es una parte especial dentro de iptables que en realidad no debería llamarse máquina de estado, ya que en realidad es un seguimiento de conexiones. Sin embargo, la mayoría de la gente lo reconoce por el primer nombre. El seguimiento de la conexión se realiza para que el marco de Netfilter conozca el estado de una conexión específica. Los cortafuegos que implementan esto generalmente se denominan cortafuegos con estado. Un firewall con estado generalmente es mucho más seguro que los firewalls sin estado, ya que nos permite escribir conjuntos de reglas mucho más estrictos.

Los paquetes se pueden relacionar con conexiones rastreadas en cuatro estados diferentes. Estos se conocen como **NEW**, **ESTABLISHED**, **RELATED** and **INVALID (**NUEVOS, ESTABLECIDOS, RELACIONADOS y NO VÁLIDOS). Discutiremos cada uno de estos en profundidad más adelante. Con la coincidencia --state podemos controlar fácilmente quién o qué puede iniciar nuevas sesiones.

El seguimiento de la conexión se realiza mediante un marco especial dentro del kernel llamado conntrack

Todo el seguimiento de conexiones se maneja en la cadena PREROUTING, excepto los paquetes generados localmente que se manejan en la cadena OUTPUT. Lo que esto significa es que iptables hará todo el recalculo de estados y demás dentro de la cadena PREROUTING. Si enviamos el paquete inicial en un flujo, el estado se establece en NEW dentro de la cadena de OUTPUT, y cuando recibimos un paquete de retorno, el estado cambia en la cadena de ENRUTAMIENTO PREVIO a ESTABLECIDO, y así sucesivamente. Si el primer paquete no lo originamos nosotros, el estado NUEVO se establece dentro de la cadena PREROUTING. Por lo tanto, todos los cambios de estado y los cálculos se realizan dentro de las cadenas PREROUTING y OUTPUT de la tabla nat.

Como ha visto, los paquetes pueden adoptar varios estados diferentes dentro del propio núcleo, según el protocolo del que estemos hablando. Sin embargo, fuera del núcleo, solo tenemos los 4 estados descritos anteriormente. Estos estados se pueden usar principalmente junto con la coincidencia de estado que luego podrá hacer coincidir los paquetes en función de su estado de seguimiento de conexión actual. Los estados válidos son NUEVO, ESTABLECIDO, RELACIONADO y NO VÁLIDO. La siguiente tabla explicará brevemente cada estado posible.

NEW	El estado NUEVO nos dice que el paquete es el primer paquete que vemos. Esto significa que se emparejará el primer paquete que vea el módulo conntrack, dentro de una conexión específica. Por ejemplo, si vemos un paquete SYN y es el primer paquete que vemos en una conexión, coincidirá. Sin embargo, el paquete también puede no ser un paquete SYN y aun así considerarse NEW. Esto puede generar ciertos problemas en algunos casos, pero también puede ser extremadamente útil cuando necesitamos recuperar conexiones perdidas de otros firewalls, o cuando una conexión está en timeout pero en realidad no está cerrada.
ESTABLISHED	El estado ESTABLISHED ha visto tráfico en ambas direcciones y luego coincidirá continuamente con esos paquetes. Las conexiones ESTABLISHED son bastante fáciles de entender. El único requisito para entrar en un estado ESTABLECIDO es que un host envíe un paquete y que luego reciba una respuesta del otro host. El estado NUEVO al recibir el paquete de respuesta a través del cortafuegos cambiará al estado ESTABLECIDO. Los mensajes de respuesta ICMP también pueden considerarse ESTABLECIDOS, si creamos un paquete que a su vez generó el mensaje ICMP de respuesta.
RELATED	El estado RELACIONADO es uno de los estados más complicados. Una conexión se considera RELACIONADA cuando está relacionada con otra conexión ya ESTABLECIDA. Lo que esto significa, es que para que una conexión se considere RELACIONADA, primero debemos tener una conexión que se considere ESTABLECIDA. La conexión ESTABLECIDA generará una conexión fuera de la conexión principal. La conexión recién generada se considerará RELACIONADA, si el módulo conntrack puede entender que está RELACIONADA. Algunos buenos ejemplos de conexiones que pueden considerarse RELACIONADAS son las conexiones de datos FTP que se consideran RELACIONADAS con el puerto de control FTP. Esto se usa para permitir que los mensajes de error ICMP, las transferencias FTP y los DCC funcionen correctamente a través del firewall. Ten en cuenta que la mayoría de los protocolos TCP y algunos protocolos UDP que se basan en este mecanismo son bastante complejos y envían información de conexión dentro de la carga útil de los segmentos de datos TCP o UDP y, por lo tanto, requieren módulos auxiliares especiales para entenderse correctamente.
INVALID	El estado NO VÁLIDO significa que el paquete no se puede identificar o que no tiene ningún estado. Esto puede deberse a varios motivos, como que el sistema se esté quedando sin memoria o que los mensajes de error de ICMP no respondan a ninguna conexión conocida. Generalmente, es una buena idea hacer DROP de todo en este estado.

Revision #1
Created 7 June 2022 06:45:15 by Admin
Updated 7 June 2022 06:56:37 by Admin