UNIVERSIDAD TECNOLÓGICA DE SAN LUIS RIO COLORADO

INVESTIGACIÓN 2, PARCIAL 3

MTRA. YOHANI PAOLA VALDEZ AYON

ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS

San Luis Rio Colorado, Sonora

Agosto, 2020

Una Lista de Control de Accesos (ACL: *Access Control List*) es una serie de instrucciones que controlan que en un *router* se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

Las ACL configuradas realizan las siguientes tareas:

- Limitan el tráfico de la red para aumentar su rendimiento.
- Proporcionan un nivel básico de seguridad para el acceso a la red.
- Filtran el tráfico según su tipo.
- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red.

Funcionamiento: Filtrado de Paquetes

Una Lista de Control de Accesos (ACL) es una enumeración secuencial de instrucciones permitir o denegar. Cuando el tráfico de la red atraviesa una interfaz de red configurada con una ACL, el router compara la información dentro del paquete IP con cada entrada de la lista en orden secuencial, para determinar si coincide con alguna. Este proceso se denomina filtrado de los paquetes.

El filtrado de los paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes, y la transferencia o el bloqueo de estos según criterios determinados. Las ACL estándares filtran sólo en la Capa 3, mientras que las ACL extendidas filtran en las capas 3 y 4 del modelo OSI.

El criterio de filtrado establecido en cada entrada de una ACL es la dirección IP de origen. Un router configurado con una ACL estándar toma la dirección IP de origen del encabezado del paquete y comienza a compararla con cada entrada de la ACL de manera secuencial. Cuando encuentra una coincidencia, el router realiza la instrucción correspondiente, que puede ser: permitir o bloquear el paquete, y finaliza la comparación. Si la dirección IP del paquete no coincide con ninguna entrada en la ACL, se bloquea el paquete por definición.

La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esto, una ACL que no tiene al menos una instrucción permitir bloqueará todo el tráfico.

Las ACL de entrada: procesan los paquetes entrantes al router antes de dirigirse a la interfaz de salida. Constituyen un elemento de eficacia, porque ahorran la sobrecarga de encaminar búsquedas si el paquete se descarta. Son ideales para filtrar paquetes de datos cuando la red conectada a una interfaz de entrada es el único origen de estos que se deben examinar.

Las ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida del router, y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica un mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

Ejemplos:

- En una entidad, por ejemplo, si su política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que lo bloqueen, lo que reduce considerablemente la carga de la red y aumenta su rendimiento.
- Una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de redes sociales.
- Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos.