ACLs: Listas de Control de Acceso

Intro

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo al mismo tiempo el acceso de los usuarios internos a los servicios requeridos. Aunque las herramientas de seguridad, como por ejemplo: las contraseñas y dispositivos de seguridad física, son de ayuda, a menudo carecen de la flexibilidad del filtrado básico de tráfico y de los controles específicos que la mayoría de los administradores prefieren. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero impedir a los usuarios externos el acceso telnet a la LAN.

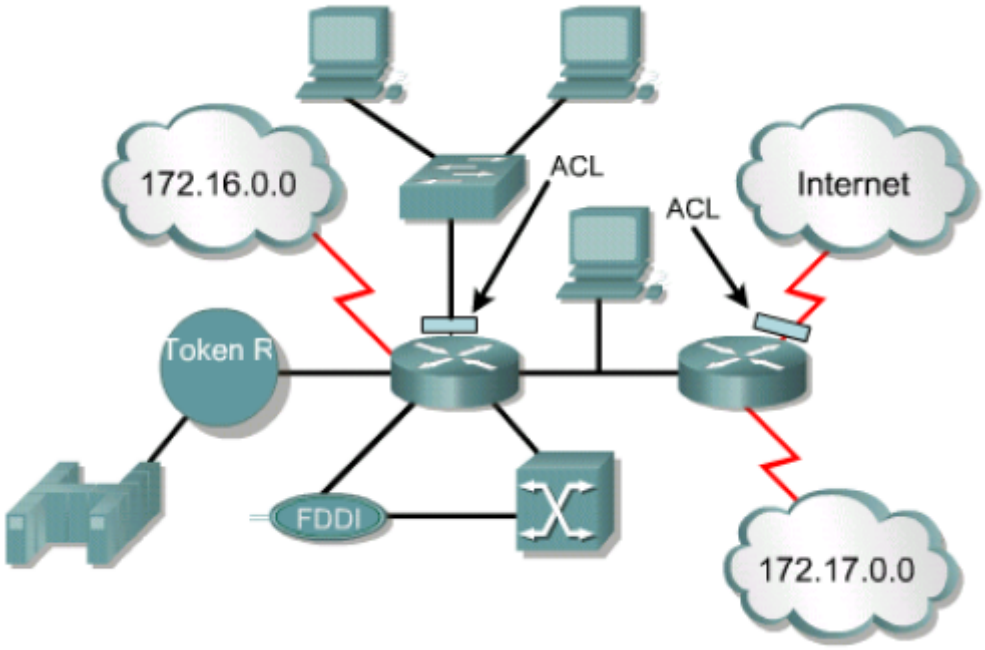
Los routers ofrecen funciones del filtrado básico de tráfico, como el bloqueo del tráfico de Internet, mediante el uso de las listas de control de acceso (ACLs). Una ACL es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior Este módulo introduce las ACL estándar y extendidas como medio de control del tráfico de red y explica de qué manera se utilizan las ACL como parte de una solución de seguridad.

Además, incluimos consejos, consideraciones, recomendaciones y pautas generales acerca del uso de las ACL e incluye los comandos y configuraciones necesarias para crear las ACL. Finalmente, brindamos ejemplos de ACL estándar y extendidas y su aplicación en las interfaces del router.

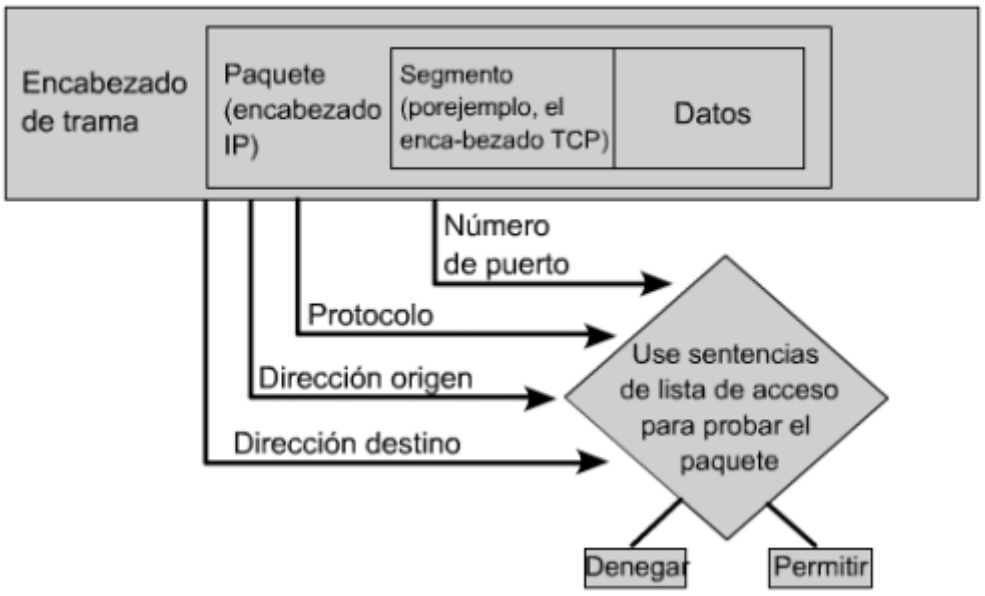
Las ACL pueden ser tan simples como una sola línea destinada a permitir paquetes desde un host específico o pueden ser un conjunto de reglas y condiciones extremadamente complejas que definan el tráfico de forma precisa y modelen el funcionamiento de los procesos de los routers. Aunque muchos de los usos avanzados de las ACL exceden el alcance de este apunte, ofrecemos detalles sobre las ACL estándar y extendida, su ubicación adecuada y algunas de las aplicaciones especiales de las mismas.

¿Qué son las ACL?

Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. Estas listas le informan al router qué tipo de paquetes aceptar o rechazar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas. Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red



Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX: protocolo utilizado por las redes Novell Netware). Las ACL se pueden configurar en el router para controlar el acceso a una red o subred.



Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

Las ACL se definen según el protocolo, la dirección o el puerto. Para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz. Las ACL controlan el tráfico en una dirección por vez, en una interfaz. Se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente. Finalmente, cada interfaz puede contar con varios protocolos y direcciones definidas. Si el router tiene dos interfaces configuradas para IP, AppleTalk e IPX, se necesitan 12 ACLs separadas. Una ACL por cada protocolo, multiplicada por dos

por dirección entrante y saliente, multiplicada por dos por el número de puertos.

Una lista, por puerto, por dirección, por protocolo

Con dos interfaces y tres protocolos ejecutándose, este router puede tener una cantidad total de 12 ACL distintas aplicadas.

Estas son las razones principales para crear las ACL:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red. Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

Si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

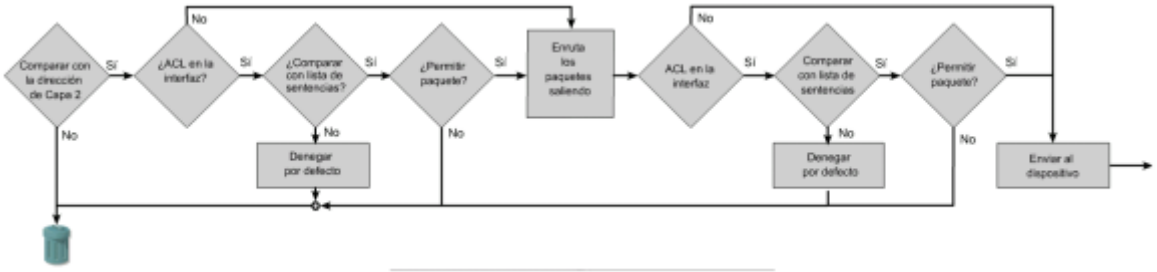
Funcionamiento de las ACL

Una lista ACL es un grupo de sentencias que definen si se aceptan o rechazan los paquetes en interfaces entrantes o salientes. Estas decisiones se toman haciendo coincidir una sentencia de condición en una lista de acceso y luego realizando la acción de aceptación o rechazo definida en la sentencia.

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición. Para que el proceso de revisión de una ACL sea más simple, es una buena idea utilizar un editor de textos como el Bloc de notas y pegar la ACL a la configuración del router.

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. A medida que una trama ingresa a una interfaz, el router verifica si la dirección de Capa 2 concuerda o si es una trama de broadcast.



Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz entrante. Si existe una ACL, entonces se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete cumple las condiciones, se lleva a cabo la acción de aceptar o rechazar el paquete. Si se acepta el paquete en la interfaz, se lo compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. A continuación, el router verifica si la interfaz destino tiene una ACL. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se lleva a cabo la aceptación o el rechazo del paquete. Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de Capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice deny any (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea deny any no sea visible como última

línea de una ACL, está ahí y no permitirá que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el deny any al final de las ACL para reforzar la presencia dinámica de la prohibición implícita deny.

ACL Continuación