MONOGRÁFICO: Listas de control de acceso (ACL) - Utilización de ACLs en routers

SOFTWARE - Servidores

Escrito por Elvira Mifsud

Domingo, 30 de Septiembre de 2012 00:00

Indice del artículo

Utilización de ACLs en routers

Definición

En el ámbito de los dispositivos routers, las ACLs son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router.

Las ACL indican al router qué tipo de paquetes aceptar o rechazar en base a las condiciones establecidas en ellas y que permiten la administración del tráfico y aseguran el acceso, bajo esas condiciones, hacia y desde una red.

La aceptación y rechazo se pueden basar en la dirección origen, dirección destino, protocolo de capa superior y números de puerto.

Por lo tanto, una ACL es un grupo de sentencias que define cómo se procesan los paquetes que:

- Entran a las interfaces de entrada
- Se reenvían a través del router
- Salen de las interfaces de salida del router

En principio 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.

Es posible crear ACL en protocolos de red enrutados, como el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX), entre otros. Se debe definir una ACL para cada protocolo enrutado habilitado en la interfaz.

Además, se necesita crear una ACL por separado para cada dirección, una para el tráfico entrante y otra para el saliente.

Como hemos comentado, las ACL se definen según el protocolo, la dirección o el puerto. Por ejemplo, si el router tiene dos interfaces configuradas para IP, IPX y AppleTalk, 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 interfaces.

Se puede configurar una ACL por protocolo, por dirección y por interfaz.

- Una ACL por protocolo: para controlar el flujo de tráfico de una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- Una ACL por dirección: las ACL controlan el tráfico en una dirección a la vez de una interfaz. Deben crearse dos ACL por separado para controlar el tráfico entrante y saliente.
- Una ACL por interfaz: las ACL controlan el tráfico para una interfaz, por ejemplo, Fast Ethernet 0/0.

Las ACL no actúan sobre paquetes que se originan en el mismo router. Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.

- ACL de entrada: los paquetes entrantes se procesan antes de ser enrutados a la interfaz de salida.
- ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida y luego son procesados a través de la ACL de salida.

Objetivos de las ACL

En resumen, los objetivos que se persiguen con la creación de ACL son:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de vídeo, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Controlar el flujo del 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, el host-1 se le permite el acceso a la red de
- Producción, y al host-2 se le niega el acceso a esa red.
- Establecer qué tipo de tráfico se envía o se bloquea en las interfaces del router. Por ejemplo, permitir que se envíe el tráfico relativo al correo electrónico, y se bloquea el tráfico de ftp.
- Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

Funcionamiento de las ACL

Para explicar el funcionamiento utilizaremos el software Cisco IOS.

El orden de las sentencias ACL es importante .

- Cuando el router está decidiendo si se envía o bloquea un paquete, el IOS prueba el paquete, verifica si cumple o no cada sentencia de condición, en el orden en que se crearon las sentencias .
- Una vez que se verifica que existe una coincidencia, no se siguen verificando otras sentencias de condición .

Por lo tanto, Cisco IOS verifica si los paquetes cumplen cada sentencia de condición de arriba hacia abajo, en orden. Cuando se encuentra una coincidencia, se ejecuta la acción de aceptar o rechazar y ya no se continua comprobando otras ACL.

Por ejemplo, si una ACL permite todo el tráfico y está ubicada en la parte superior de la lista, ya no se verifica ninguna sentencia que esté por debajo.

Si no hay coincidencia con ninguna de las ACL existentes en el extremo de la lista se coloca por defecto una sentencia implícita **deny any** (denegar cualquiera). Y, aunque la línea deny any no sea visible sí que está ahí y no permitirá que ningún paquete que no coincida con alguna de las ACL anteriores sea aceptado. Se puede añadir de forma explícita por aquello de 'verla' escrita y tener esa tranquilidad.

Veamos el proceso completo:

1. Cuando entra una trama a través de una interfaz, el router verifica si la dirección de capa 2 (MAC) concuerda o si es una trama de broadcast.
2. 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.
3. Si existe una ACL se comprueba si el paquete cumple las condiciones de la lista.
4. Si el paquete cumple las condiciones, se ejecuta la acción de aceptar o rechazar el paquete.
5. Si se acepta el paquete en la interfaz, se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz. Luego el router verifica si la interfaz destino tiene una ACL.
6. Si existe una ACL, se compara el paquete con las sentencias de la lista y si el paquete concuerda con una sentencia, se acepta o rechaza el paquete según se indique.
7. 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.

Creación de ACL

Utilizamos la herramienta de simulación Packet Tracer y una topología de red muy sencilla, formada por un router, dos switch y 2PCs, cada uno de ellos en una subred.

Trabajaremos desde el modo de configuración global: (config)#

Hay dos tipos de ACL y utilizan una numeración para identificarse:

- ACL estándar: del 1 al 99
- ACL extendida: del 100 al 199

ACLs estándar: sintaxis

Las ACL estándar en un router Cisco siempre se crean primero y luego se asignan a una interfaz.

Tienen la configuración siguiente:

```
Router(config)# access-list numACL permit|deny origen [wild-mask]
```

El comando de configuración global access-list define una ACL estándar con un número entre 1 y 99.

Se aplican a los interfaces con:

```
Router (config-if)# ip access-group numACL in|out
```

- **In**: tráfico a filtrar que ENTRA por la interfaz del router
- **out** : tráfico a filtrar que SALE por la interfaz del router.
- **wild-mask**: indica con 0 el bit a evaluar y con 1 indica que el bit correspondiente se ignora. Por ejemplo, si queremos indicar un único host 192.168.1.1 especifico: 192.168.1.1 con wild-mask 0.0.0.0 y si queremos especificar toda la red clase C correspondiente lo hacemos con 192.168.1.0 y wild-mask 0.0.0.255.

Para la creación de ACL estándar en importante:

- Seleccionar y ordenar lógicamente las ACL.
- Seleccionar los protocolos IP que se deben verificar.
- Aplicar ACL a interfaces para el tráfico entrante y saliente.
- Asignar un número exclusivo para cada ACL.

Ejemplo 1

Supongamos que queremos crear en un Router0 una ACL con el número 1 (numACL) que deniegue el host 192.168.1.2. Desde configuración global:

```
Router0(config)# access-list 1 deny 192.168.1.2 0.0.0.0
```

Si queremos eliminar una ACL:

```
Router0(config)# no access-list
```

Para mostrar las ACL:

```
Router0# show access-list
Standard IP access list 1
deny host 192.168.1.2
permit any
```

Recordar que para salir del modo de configuración global (config) hay que escribir 'exit'.

Ahora hay que utilizar el comando de configuración de interfaz para seleccionar una interfaz a la que aplicarle la ACL:

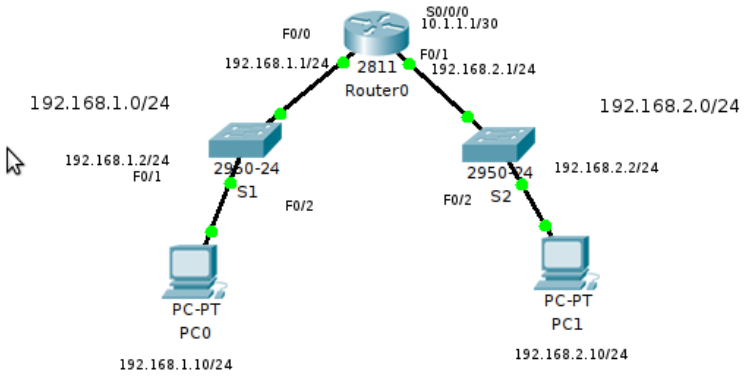
```
Router0(config)# interface FastEthernet 0/0
```

Por último utilizamos el comando de configuración de interfaz ip access-group para activar la ACL actual en la interfaz como filtro de salida:

```
Router0(config-if)# ip access-group 1 out
```

Ejemplo 2

Tenemos la siguiente topología de red.



Vamos a definir una ACL estándar que permita el trafico de salida de la red 192.168.1.0/24.

La primera cuestión que se plantea es ¿dónde instalar la ACL? ¿en qué router? ¿en qué interfaz de ese router?.

En este caso no habría problema porque solo tenemos un router, el Router0. Pero la regla siempre es **instalar la ACL lo más cerca posible del destino**.

```
Router0#configure terminal
Router0(config)#access-list 1 permit  192.168.1.0    0.0.0.255
Router0(config)#interface S0/0/0
Router0(config-if)#ip access-group 1 out
```

Ahora borramos la ACL anterior y vamos a definir una ACL estándar que deniegue un host concreto.

```
Router0(config)#no access-list 1
Router0(config)#access-list 1 deny 192.168.1.10 0.0.0.0 Router0(config)
#access-list 1 permit 192.168.1.0 0.0.0.255
Router0(config)#interface S0/0/0
Router0(config-if)#ip access-group 1 out
```

ACLs extendidas

Las ACL extendidas filtran paquetes IP según:

- Direcciones IP de origen y destino
- Puertos TCP y UDP de origen y destino
- Tipo de protocolo (IP, ICMP, UDP, TCP o número de puerto de protocolo).

Las ACLs extendidas usan un número dentro del intervalo del 100 al 199.
Al final de la sentencia de la ACL extendida se puede especificar, opcionalmente, el número de puerto de protocolo TCP o UDP para el que se aplica la sentencia:

- 20 y 21: datos y programa FTP
- 23: Telnet
- 25: SMTP
- 53: DNS
- 69: TFTP

Definir ACL extendida, sintaxis:

```
Router(config)# access-list numACL {permit|deny} protocolo fuente
[mascara-fuente destino mascara-destino operador operando] [established]
```

- **numACL**: Identifica número de lista de acceso utilizando un número dentro del intervalo 100-199
- **protocolo**: IP, TCP, UDP, ICMP, GRE, IGRP
- **fuente | destino**: Identificadores de direcciones origen y destino
- **mascara-fuente | mascara-destino**: Máscaras de wildcard
- **operador**: lt, gt, eq, neq
- **operando**: número de puerto
- **established**: permite que pase el tráfico TCP si el paquete utiliza una conexión establecida.
    - Respecto a los protocolos:
    - Sólo se puede especificar una ACL por protocolo y por interfaz.
    - Si ACL es entrante, se comprueba al recibir el paquete.
    - Si ACL es saliente, se comprueba después de recibir y enrutar el paquete a la interfaz saliente.
    - Se puede nombrar o numerar un protocolo IP.

Asociar ACL a interfaz, sintaxis:

```
Router(config-if)# ip access-group num_ACL {in | out}
```

Ejemplo 1

En el esquema anterior, denegar FTP entre las subredes y permitir todo lo demás.

```
Router0(config)# access-list 101 deny tcp 192.168.2.0  0.0.0.255 192.168.1.0   0.0.0.255 eq 21
Router0(config)# access-list 101 deny tcp 192.168.2.0  0.0.0.255 192.168.1.0 0.0.0.255 eq 20
Router(config)# access-list 101 permit ip any any
Router(config)# interface F0/1
Router0(config-if)#ip access-group 101 in
```

Ejemplo 2

En el esquema anterior, denegar solo telnet a la subred 192.168.1.0.

```
Router0(config)# access-list 101 deny tcp 192.168.1.0  0.0.0.255  any eq 23
Router(config)# access-list 101 permit ip any any
Router(config)# interface F0/0
Router0(config-if)#ip access-group 101 out
```

Ubicación de las ACLs

Es muy importante el lugar donde se ubique una ACL ya que influye en la reducción del tráfico innecesario.

El tráfico que será denegado en un destino remoto no debe usar los recursos de la red en el camino hacia ese destino.

La regla es colocar las:

- ACL estándar lo más cerca posible del destino (no especifican direcciones destino).
- ACL extendidas lo más cerca posible del origen del tráfico denegado. Así el tráfico no deseado se filtra sin atravesar la infraestrucra de red

<< Anterior - Siguiente >>