Packet Tracer: demostración de listas de control de acceso Objetivos

Parte 1: verificar la conectividad local y probar la lista de control de acceso

Parte 2: eliminar la lista de control de acceso y repetir la prueba

Aspectos básicos

En esta actividad, observará cómo se puede utilizar una lista de control de acceso (ACL) para evitar que un ping llegue a hosts en redes remotas. Después de eliminar la ACL de la configuración, los pings se realizarán correctamente.

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP / Prefijo
R1	G0/0	192.168.10.1/24
	G0/1	192.168.11.1/24
	S0/0/0	10.1.1.1/30
R2	S0/0/0	10.10.1.2/30
	S0/0/1	10.10.1.5/30
R3	G0/0	192.168.30.1/24
	G0/1	192.168.31.1/24
	S0/0/1	10.10.1.6/24
PC1	NIC	192.168.10.10/24
PC2	NIC	192.168.10.11/24
PC3	NIC	192.168.11.10/24
PC4	NIC	192.168.30.12/24
Servidor DNS	NIC	192.168.31.12/24

Instrucciones

Parte 1: verificar la conectividad local y probar la lista de control de acceso

Paso 1: hacer ping a los dispositivos de la red local para verificar la conectividad.

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC2**.

b. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC3**.

¿Por qué se realizaron de forma correcta los pings?

Paso 2: hacer ping a los dispositivos en las redes remotas para probar la funcionalidad de la ACL.

a. Desde el símbolo del sistema de la **PC1**, haga ping a la **PC4**.

b. Desde el símbolo del sistema de la **PC1**, haga ping al **servidor DNS**.

¿Por qué fallaron los pings? (**pista**: utilice el modo de simulación o vea las configuraciones del router para investigar).

Parte 2: eliminar la ACL y repetir la prueba

Paso 1: utilizar el comando show para investigar la configuración de la ACL.

a. Desplácese hasta R1 CLI. Utilice los comandos **show run** y **show access-lists** para ver las ACL configuradas actualmente. Para obtener una vista rápida de las ACL vigentes, utilice **show access-lists**. Introduzca el comando **show access-lists** seguido de un espacio y un signo de interrogación (?) para ver las opciones disponibles:

```
R1# show access-lists ?
  <1-199> ACL number
  WORD ACL name
  <cr>
```

Si conoce el número o el nombre de la ACL, puede filtrar aún más el resultado del comando **show**. Sin embargo, el **R1** tiene solo una ACL, por lo que basta con el comando **show access-lists**.

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

La primera línea de la ACL impide cualquier paquete que se origine en la red **192.168.10.0/24** lo que incluye los ecos del protocolo de mensajería de control de Internet (ICMP) (solicitudes de ping). La segunda línea de la ACL permite que todo el resto del tráfico **ip** de **cualquier** origen atraviese el router.

b. Para que una ACL tenga efecto en el funcionamiento del router, debe aplicarse a una interfaz en una dirección específica. En esta situación, la ACL se utiliza para filtrar el tráfico que sale de una interfaz. Por lo tanto, todo el tráfico que sale de la interfaz especificada de R1 se examinará contra la ACL 11.

Aunque pueda ver la información de IP con el comando **show ip interface**, en algunos casos puede ser más eficaz utilizar solo el comando **show run**. Para obtener una lista completa de interfaces a las que se puede aplicar la ACL y la lista de todas las ACL configuradas, utilice el siguiente comando:

```
R1# show run | include interface|access
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface Serial0/0/0
 ip access-group 11 out
interface Serial0/0/1
interface Vlan1
access-list 11 deny 192.168.10.0 0.0.0.255
access-list 11 permit any
```

El segundo símbolo de tubería '|» crea una condición OR que coincide con 'interfaz' O 'acceso'. Es importante que no se incluyan espacios en la condición OR. Utilice uno o ambos comandos para buscar información sobre la ACL.

¿A qué interfaz y en qué dirección se aplica la ACL?

Paso 2: eliminar la lista de acceso 11 de la configuración.

Es posible eliminar las ACL de la configuración por medio de la emisión del comando **no access list** *[número de ACL]*. el **comando** no access-list cuando se usa sin argumentos elimina todas las ACL configuradas en el router. El comando **no access-list** [*número de ACL*] solo elimina una ACL específica. La eliminación de una ACL de un enrutador no elimina la ACL de la interfaz. El comando que aplica la ACL a la interfaz debe eliminarse por separado.

a. En la interfaz Serial0/0/0, quiten la lista de acceso 11 aplicada antes a la interfaz como filtro **saliente**:

```
R1(config)# interface s0/0/0
R1(config-if)# no ip access-group 11 out
```

b. En el modo de configuración global, elimine la ACL por medio del siguiente comando:

```
R1(config)# no access-list 11
```

c. Verifique que la **PC1** ahora pueda hacer ping al **servidor DNS** y a la **PC4**.