Packet Tracer: resolución de problemas de las ACL

Topología

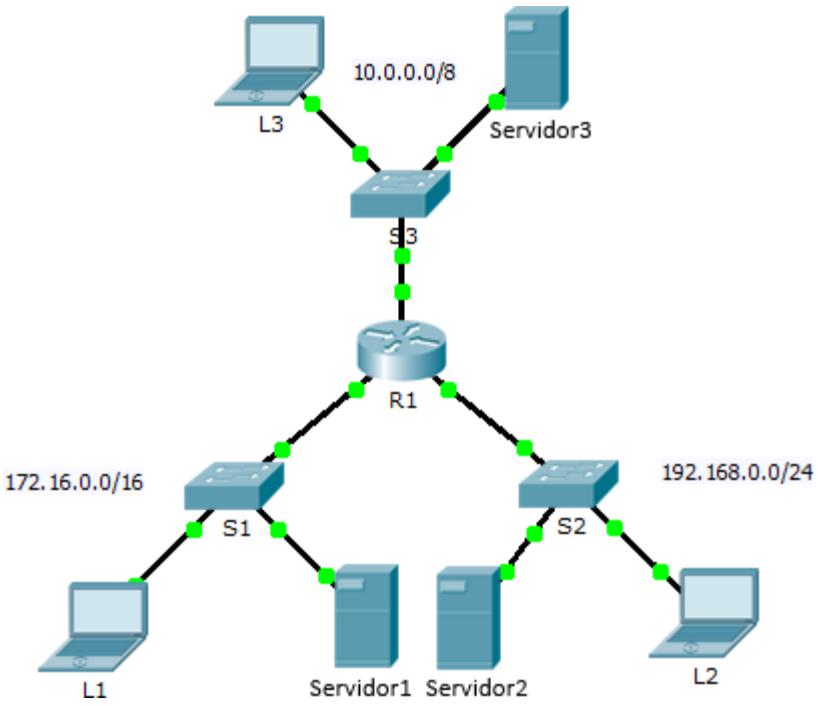

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
Server2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
Server3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

Objetivos

Parte 1: resolver el problema 1 de la ACL

Parte 2: resolver el problema 2 de la ACL

Parte 3: resolver el problema 3 de la ACL

Situación

En esta red, deberían estar implementadas las tres políticas siguientes:

- Los hosts de la red 192.168.0.0/24 no pueden acceder a ningún servicio TCP del **Servidor3**.
- Los hosts de la red 10.0.0.0/8 no pueden acceder al servicio HTTP del **Servidor1**.
- Los hosts de la red 172.16.0.0/16 no pueden acceder al servicio FTP del **Servidor2**.

Nota: todos los nombres de usuario y las contraseñas del FTP son "**cisco**".

No debe haber otras restricciones. Lamentablemente, las reglas implementadas no funcionan de manera correcta. Su tarea es buscar y corregir los errores relacionados con las listas de acceso en el **R1**.

Parte 1: resolver el problema 1 de la ACL

Los hosts de la red 192.168.0.0/24 no pueden acceder (intencionalmente) a ningún servicio TCP del **Servidor3**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L2**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L2**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Desde la **L2**, haga ping a **G0/2** del **R1**.

d. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **192_to_10** y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

e. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **192_to_10** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

El problema se resolvio con el comando "20 permit ip any any" ya que con el permitimos los demas servicios sin tomar en cuenta el servicio TCP

Parte 2: resolver el problema 2 de la ACL

Los hosts de la red 10.0.0.0/8 no pueden acceder (intencionalmente) al servicio HTTP del **Servidor1**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L3**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L3**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **10_to_172** y su ubicación en las interfaces. ¿La lista de acceso se colocó en la interfaz apropiada y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

d. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **10_to_172** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

La solución fue cambiar el sentido de la ACL inicialmente estaba en "out" pot lo que se cambio a "in"

Parte 3: resolver el problema 3 de la ACL

Los hosts de la red 172.16.0.0/16 no pueden acceder (intencionalmente) al servicio FTP del **Servidor2**, pero no deberían tener otro tipo de restricción.

Paso 1: determinar el problema de la ACL.

A medida que realiza las siguientes tareas, compare los resultados obtenidos con sus expectativas sobre la ACL.

a. Con la **L1**, intente acceder a los servicios FTP y HTTP de **Servidor1, Servidor2**, y **Servidor3**.

b. Desde la **L1**, haga ping a **Servidor1**, **Servidor2** y **Servidor3**.

c. Vea la configuración en ejecución en el **R1**. Examine la lista de acceso **172_to_192** y su ubicación en las interfaces. ¿La lista de acceso se colocó en el puerto apropiado y en el sentido correcto? ¿Existe alguna instrucción en la lista que permita o deniegue el tráfico a otras redes? ¿Las instrucciones están en el orden correcto?

d. Realice otras pruebas, según sea necesario.

Paso 2: implementar una solución.

Realice un ajuste a la lista de acceso **172_to_192** para solucionar el problema.

Paso 3: verificar que el problema se haya resuelto y registrar la solución.

Si el problema se resuelve, registre la solución. De lo contrario, vuelva al paso 1.

En este caso el problema fue el orden ya que primero permitia todo el servicio de "IP" para despues negar todo el servicio de "TCP" solo se debia intercambiar el orden entre ambos.

Tabla de calificación sugerida

Ubicación de la pregunta	Puntos posibles	Puntos obtenidos
Puntuación del registro	**10**	
Puntuación de Packet Tracer	**90**	
Puntuación total	**100**	

Conclusiones

Josue Macias Castillo:

En esta práctica se identificaron 3 tipos de errores comunes en las ACL extendidas nombradas el primer error tenía que ver con permitir todos los demás servicios sin tomar en cuenta el protocolo TCP con lo cual se agregó dentro de la configuración del ACL, el segundo tenía que ver con el sentido del ACL inicialmente estaba en “out” por lo que cambio a “in” para solucionarlo y el ultimo error fue el orden de las instrucciones la solución fue intercambiar el orden entre ambas instrucciones, al principio verifique todo como las direcciones y que las ACL estuvieran en los puertos correctos.

José Luis Ochoa Monroy:

Como sabemos, las ACL son una herramienta muy efectiva y económica para regular el tráfico que se permite o se deniega para cada integrante de una infraestructura de red. Los problemas presentes en esta actividad nos demuestran que es fundamental comprender el funcionamiento de estas configuraciones, ya que la falta de estos conocimientos puede llevarnos a que las políticas de nuestra infraestructura de red no se implementen correctamente. Una configuración de ACL se ejecuta línea por línea, desde la primera hasta la última, por eso primero deben ponerse las líneas que deniegan o permiten el tráfico de algún tipo para porciones específicas de la red, y finalmente utilizar comandos que permitan o denieguen el resto de tipos de tráfico para el resto de integrantes.