4.1.3.5 CONFIGURACIÓN DE ACL ESTÁNDAR Y EXTENDIDA

Yanet Islas Yañez
ITI 91
Aplicación de Telecomunicaciones
MTI. Oscar Lira Uribe

Packet Tracer: Configuración de listas ACL IPv4 estándar

Topología

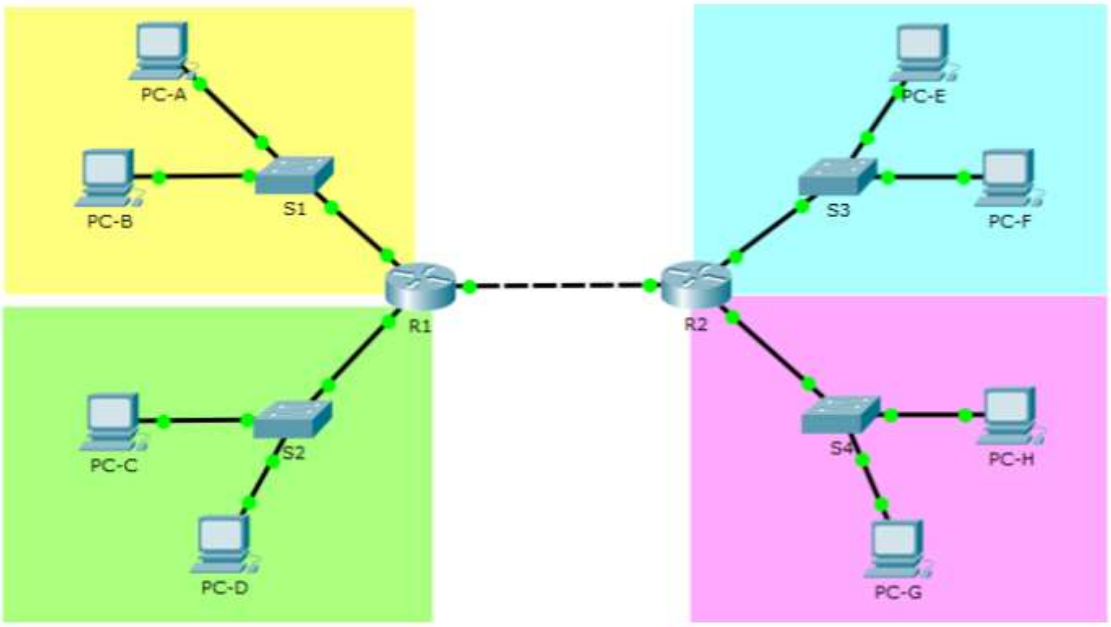

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.1.1	255.255.255.0	N/D
	G0/1	192.168.2.1	255.255.255.0	
	G0/2	192.168.250.1	255.255.255.0	
R2	G0/0	172.16.1.1	255.255.255.0	N/D
	G0/1	172.16.2.1	255.255.255.0	
	G0/2	192.168.250.2	255.255.255.0	
PC-A	NIC	192.168.1.100	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.150	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.50	255.255.255.0	192.168.2.1
PC-D	NIC	192.168.2.112	255.255.255.0	192.168.2.1
PC-E	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC-F	NIC	172.16.1.20	255.255.255.0	172.16.1.1
PC-G	NIC	172.16.2.100	255.255.255.0	172.16.2.1
PC-H	NIC	172.16.2.200	255.255.255.0	172.16.2.1

Objetivos

Restrinja el tráfico en la red configurando ACL estándar IPv4.

Aspectos básicos/situación

Una organización ha decidido recientemente a restringir el tráfico mediante ACL estándar IPv4. Como administrador de red, su trabajo es configurar dos ACL estándar IPv4 para restringir el tráfico a la LAN rosada y la LAN azul (consulte PT el diagrama de topología). También debe configurar un IPv4 estándar y nombrarlo ACL para limitar el acceso remoto al router R1. Las interfaces de router y el valor predeterminado/rutas estáticas han sido configuradas. El acceso SSH remoto también se ha habilitado en los routers. Necesitará la información de acceso siguiente para la consola, de vty, y el modo EXEC privilegiado:

Nombre de usuario: **admin01**

Contraseña: **ciscoPA55**

Contraseña secreta de habilitación: **secretPA55**

Parte 1: Configure la ACL IPv4 para restringir el acceso a la LAN rosada

En la parte 1, configurará y aplicará la lista de acceso 10 para restringir el acceso a LAN rosada.

Paso 1: Describir lo que desea alcanzar con la lista de acceso 10.

La lista de acceso 10 debe tener 4 entradas de control de acceso para hacer lo siguiente:

1) La lista de acceso 10 debe comenzar con el resultado siguiente: ACL_TO_PINK_LAN
2) PC-C del permiso para alcanzar la LAN rosada
3) El permit sólo la primera mitad de host en la LAN amarilla, de modo que puedan alcanzar la LAN rosada
4) Permitir que todos los hosts de la LAN azul para alcanzar la LAN rosada

La lista de acceso 10 se debe configurar en el router correcto, y aplicar a la interfaz correcta y la dirección correcta.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10  remark ACL_TO_PINK_LAN
R2(config)#access-list 10 permit host 192.168.2.50
```

```
R2(config)#access-list 10 permit 192.168.1.0 0.0.0.127
R2(config)#access-list 10 permit 172.16.1.0 0.0.0.255
R2(config)#int g0/1
R2(config-if)#ip access-group 10 out
```

Paso 2: Crear, aplicar y probar access-list 10.

Después de configurar y aplicar la lista de acceso 10, debería poder ejecutar las siguientes pruebas de la red:

1) Un ping de la PC-A a un host en la LAN rosada debe tener éxito, pero un ping de la PC-B debería denegarse.
2) Un ping de la PC-C a un host en la LAN rosada debe tener éxito, pero un ping de la PC-D se debe denegar.
3) Los ping desde los host en la LAN azul a los hosts de la LAN rosada deben tener éxito.

¿Qué mensaje se devuelve a las PC cuando un ping se deniega debido a una ACL?

Destination Host Unreachable

¿Permiten a qué direcciones IP en la LAN amarilla hacer ping a los host en la LAN rosada?

De 192.168.1.1 a 192.168.1.127

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 172.16.2.200: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 172.16.2.200 with 32 bytes of data:

Reply from 172.16.2.200: bytes=32 time=1ms TTL=126
Reply from 172.16.2.200: bytes=32 time<1ms TTL=126
Reply from 172.16.2.200: bytes=32 time<1ms TTL=126
Reply from 172.16.2.200: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Request timed out.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Request timed out.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Reply from 172.16.2.200: bytes=32 time=1ms TTL=127
Reply from 172.16.2.200: bytes=32 time<1ms TTL=127
Reply from 172.16.2.200: bytes=32 time<1ms TTL=127
Reply from 172.16.2.200: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 172.16.2.200

Pinging 172.16.2.200 with 32 bytes of data:

Reply from 172.16.2.200: bytes=32 time<1ms TTL=127
Reply from 172.16.2.200: bytes=32 time=3ms TTL=127
Reply from 172.16.2.200: bytes=32 time=1ms TTL=127
Reply from 172.16.2.200: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.2.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Parte 2: Configure la ACL IPv4 estándar para restringir el acceso a la LAN azul

En la parte 2, configurará y aplicará la lista de acceso 20 para restringir el acceso a LAN azul.

Paso 1: Describir lo que desea alcanzar con la lista de acceso 20.

La lista de acceso 20 debe tener 3 entradas de control de acceso para hacer lo siguiente:

1) La lista de acceso 20 debe comenzar con el siguiente comentario: ACL_TO_BLUE_LAN
2) Permita que PC-A se comunique con la LAN azul
3) Impida que la LAN amarilla se comunique con la LAN azul
4) Permita que todas las otras redes se comuniquen con la LAN azul

La lista de acceso 20 se debe configurar en el router correcto, y aplicar a la interfaz correcta y la dirección correcta.

```
R2(config)#access-list 20 remark ACL_TO_BLUE_LAN
R2(config)#access-list 20 permit host 192.168.1.100
R2(config)#access-list 20 deny 192.168.1.0 0.0.0.255
R2(config)#
R2(config)#access-list 20 permit any
```

```
R2(config)#int g0/0
R2(config-if)#ip access-group 20 out
```

Paso 2: Crear, aplicar y probar access-list 20.

Después de configurar y aplicar la lista de acceso 20 debe poder ejecutar las siguientes pruebas de la red:

1) Solo PC-A en la LAN amarilla puede emitir pings correctamente a la LAN azul.
2) La emisión de pings desde los hosts de la LAN amarilla hacia la LAN azul debería fallar.
3) Se debería aceptar la emisión de pings desde los hosts de las LAN verde y rosada hacia los hosts de la LAN azul.

```
Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:

Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.
Reply from 192.168.250.2: Destination host unreachable.

Ping statistics for 172.16.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Paso 3: Introduzca un ACE en la lista de acceso 20.

Necesita realizar un cambio en la lista de acceso 20. Inserte una entrada de control de acceso en la lista de acceso 20 para permitir que la PC-A alcance la LAN azul. Inserte el ACE antes de otro permiso de la lista de acceso 20 y deniegue las entradas de control de acceso.

¿Cómo se inserta o quita un ACE en una línea específica de una ACL?

se ingresa ACL usando las palabras clave y argumentos de lista de acceso ip como si el ACL numerado

¿Qué línea introdujo el ACE en él?

access-list standard 20

Parte 3: Configuración de una ACL IPv4 estándar con nombre

En la parte 3, configurará y aplicará una ACL IPv4 estándar con nombre para restringir el acceso remoto al router R1.

Paso 1: Describa lo que desea lograr con la ACL estándar con nombre.

La lista de acceso nombrada debe hacer lo siguiente:

1) En R1 cree una ACL estándar de nombre ADMIN_VTY
2) Permita un solo host: PC-C
3) Aplique la ACL a las líneas VTY

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard ADMIN_VTY
R1(config-std-nacl)#permit 192.168.2.50
R1(config-std-nacl)#exit
R1(config)#line vty 0 4
R1(config-line)#access-class ADMIN_VTY in
```

Paso 2: Pruebe access-list ADMIN_VTY.

Después de configurar y aplicar la lista de acceso ADMIN_VTY, debe poder ejecutar la prueba siguiente de la red:

1) Se debería poder establecer una conexión SSH del host PC-C a R1.
2) Las conexiones desde todos los otros hosts deberían fallar.

Activity Results

Congratulations Guest! You completed the activity.