Configurar ACL (Acess-list) en Cisco packet tracer

En este laboratorio, configuraremos ACL en Cirsco Packet Tracer y veremos cómo la lista de acceso bloquea el tráfico basado en diferentes condiciones

La lista de acceso proporciona la capacidad de controlar el tráfico en la red. Podemos configurar una lista de acceso de acuerdo a nuestros requerimientos. La lista de acceso filtra el tráfico basado en la configuración.

El router IOS de Cisco tiene suficientes comandos a través de los cuales podemos controlar el tráfico de manera efectiva, sin embargo, el hardware especial como el firewall pix o los firewalls ASA tienen muchas características de seguridad adicionales.

Las reglas o condiciones de las listas de acceso se leen en serie, por lo que, si cualquier red que se niega antes no se permitirá incluso después de añadir la declaración de permiso, por ejemplo

1. Denegar 192.168.1.0 0.0.255

2. Permitir host 192.168.1.5

En las reglas de lista de acceso anteriores, hemos denegado toda la red 192.168.1.0 y en la segunda regla, estamos permitiendo el host de la misma red. Como las reglas de la lista de acceso se leen en serie, el router descartará todos los paquetes de esta red porque coinciden con la regla de denegación. El router leerá la segunda regla más tarde, pero hasta entonces el tráfico de esa red ya está denegado, así que tenemos que tener cuidado cuando configuremos las reglas de la lista de acceso.

Lista de acceso estándar vs. lista de acceso extendida

Lista de acceso estándar - La lista de acceso estándar sólo filtra el tráfico basado en la IP de origen. Esta lista de acceso no tiene ninguna otra forma de filtrar el tráfico por lo que proporciona una funcionalidad básica.

Características de la lista de acceso estándar

1. Una lista de acceso estándar es muy fácil de configurar.

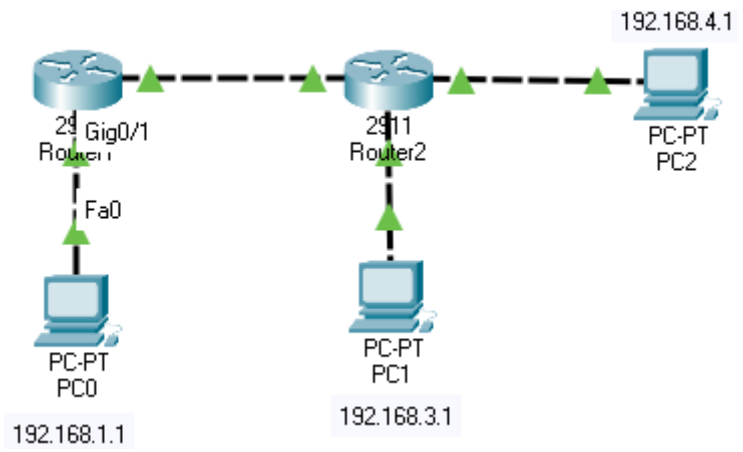
2. Es muy ligera para el procesador por lo que no sobrecarga el hardware.

Lista de acceso extendida - Las listas de acceso extendidas pueden filtrar el tráfico en función de la IP de origen, la IP de destino, los protocolos como TCP, UDP, ICMP, etc, y los números de puerto.

Características de la lista de acceso extendida

1. No es fácil de configurar en comparación con la lista de acceso estándar, sin embargo, proporciona muchos filtros que podemos utilizar para controlar el tráfico de manera eficiente.

2. Requiere más ciclos de procesador debido a la complejidad de las reglas definidas.



En esta configuración de lista de acceso estándar, bloquearemos el tráfico de PC0 para que no llegue al router 2.

Estamos usando los siguientes comandos para crear una lista de acceso.

A la lista de acceso estándar se le puede dar un número del 1 al 99, así que le daremos el número 1 a nuestra lista de acceso.

```
Router(config)#access-list 1 deny 192.168.1.1
Router(config)#access-list 1 permit any
```

Mientras creamos una lista de acceso, tenemos que asegurarnos de usar el comando permit any para permitir otro tráfico que no queramos bloquear porque hay un deny invencible al final de cada lista de acceso así que si este comando se omite entonces la lista de acceso bloqueará todo el tráfico.

Ahora, hemos creado la lista de acceso sin embargo no funcionará hasta que la apliquemos a la interfaz del router. Al activar la lista de acceso en la interfaz del router, debemos asegurarnos de que se está aplicando a la interfaz correcta y en la dirección correcta, de lo contrario la lista estándar no funcionará porque filtra el tráfico de acuerdo a la IP de origen.

Para aplicarla, debemos utilizar el siguiente comando.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip access-group 1 out
```

Una lista de acceso se aplica a la interfaz del router en las direcciones de entrada y salida. Sólo podemos habilitar 1 lista de acceso por interfaz y dirección.

En el ejemplo anterior, se habilita una lista de acceso en el puerto gigabit Ethernet del router 1 en la dirección de salida, ya que queremos bloquear el tráfico de PC0 para que no llegue al router 2.

Una vez habilitada la lista de acceso, podemos comprobar si funciona adecuadamente generando tráfico. Esto se puede comprobar haciendo ping al router desde el host.

A continuación, se muestra el resultado cuando el router 2 hace ping desde el host.

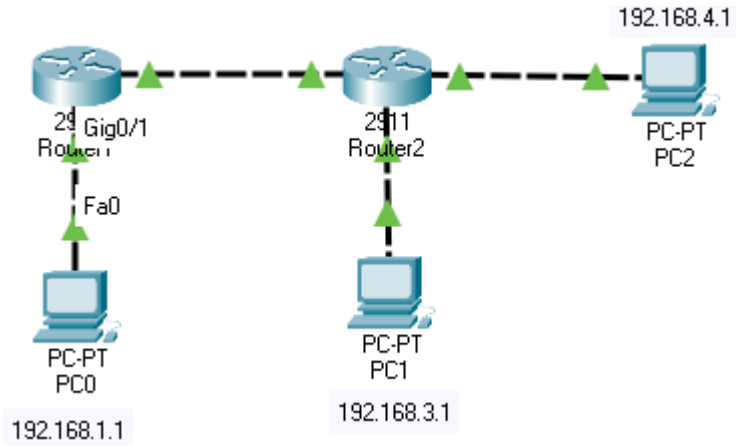
```
C:\>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:
```

```
Respuesta de 192.168.1.2: Host de destino inalcanzable.

Respuesta de 192.168.1.2: Host de destino inalcanzable.

Respuesta de 192.168.1.2: Host de destino inalcanzable.

Respuesta de 192.168.1.2: Host de destino inalcanzable.
```

Podemos utilizar el siguiente comando para verificar si la lista de acceso ha bloqueado paquetes.

```
Router#show access-lists
Standard IP access list 1
10 deny host 192.168.1.1 (4 match(es))
20 permit any
```

Como se ve en la salida del comando, la condición deny ha bloqueado el tráfico del host, 4 coincidencias son para los paquetes de ping que fueron enviados al router.



Como hemos comentado, una lista de acceso extendida puede filtrar el tráfico en función del protocolo, por lo que bloquearemos a PC2 para que no pueda hacer ping a todos los demás dispositivos de la red.

Hemos utilizado los siguientes comandos para crear la lista de acceso

```
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#deny icmp host 192.168.4.1 any
Router(config-ext-nacl)#permit ip any any
```

Los números 100 a 199 están reservados para la lista ampliada. Hemos elegido el número 100 y hemos añadido dos condiciones a la lista.

Hemos aplicado esta lista de acceso en la dirección de entrada en el router 2.

Sólo se bloquea el tráfico ICMP, este protocolo se utiliza para la funcionalidad de ping, por lo que ahora PC2 no debería ser capaz de hacer ping a ningún dispositivo de la red, sin embargo, el resto del tráfico está permitido.

Podemos probar la lista de acceso generando tráfico ICMP utilizando el comando ping desde el PC2.

Como se esperaba, el tráfico es bloqueado por el router. Por favor, compruebe el resultado del ping a continuación

```
C:>Ping 192.168.4.2

Haciendo ping a 192.168.4.2 con 32 bytes de datos:

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Estadísticas de ping para 192.168.4.2:

Paquetes: Enviados = 4, Recibidos = 0, Perdidos = 4 (100% de pérdida),
```

```
C:\>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Respuesta de 192.168.4.2: Host de destino inalcanzable.

Estadísticas de ping para 192.168.1.1:

Paquetes: Enviados = 4, Recibidos = 0, Perdidos = 4 (100% de pérdida),
```

La lista de acceso bloqueó 8 paquetes que se generaron desde el PC2

```
Router#sh access-lists
Extended IP access list 100
10 deny icmp host 192.168.4.1 any (8 match(es))
20 permit ip any any
```