Configuración ACL Extendida

Nombre del Alumno:
Jireh Hernández Castillo
Matricula:
1717110620
Nombre del Docente:
MTI. Oscar Lira Uribe
Materia:
Aplicación de las Telecomunicaciones
Universidad:
Universidad Tecnológica de Tulancingo
Carrera:
ING. En Tecnologías de la Información y Comunicación
Grupo:
ITI91
Fecha:
19 de julio de 2020

Packet Tracer: Configuración ACL Extendida

Topología

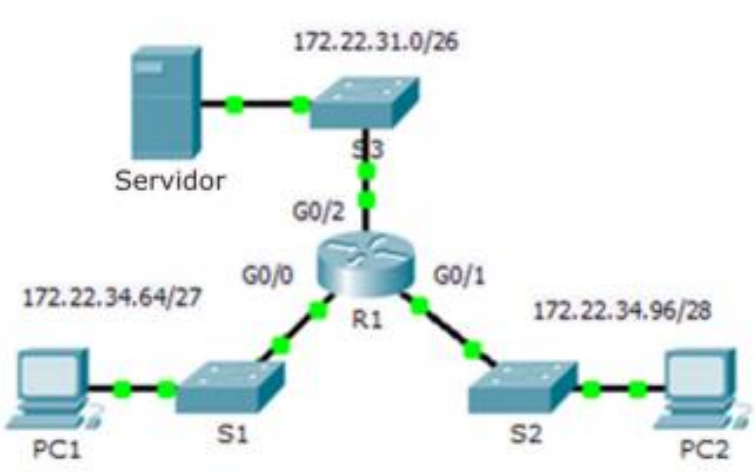


Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	172.22.34.65	255.255.255.224	N/D
	G0/1	172.22.34.97	255.255.255.240	N/D
	G0/2	172.22.34.1	255.255.255.192	N/D
Servidor	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Objetivos

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Situación

Dos empleados necesitan acceder a los servicios que proporciona el servidor. La PC1 solo necesita acceso FTP, mientras que la PC2 solo necesita acceso web. Ambas computadoras pueden hacer ping al servidor, pero no entre sí.

Parte 1: configurar, aplicar y verificar una ACL extendida numerada

Paso 1: configurar una ACL para que permita tráfico FTP e ICMP.

a) Desde el modo de configuración global en el R1, introduzca el siguiente comando para determinar el primer número válido para una lista de acceso extendida.
b) Agregue 100 al comando, seguido de un signo de interrogación.
c) Para permitir el tráfico FTP, introduzca permit, seguido de un signo de interrogación.

d) Esta ACL permite tráfico FTP e ICMP. ICMP se indica más arriba, pero FTP no, porque FTP utiliza TCP. Entonces, se introduce TCP. Introduzca tcp para refinar aún más la ayuda de la ACL.
e) Observe que se podría filtrar por PC1 por medio de la palabra clave host o bien se podría permitir cualquier (any) host. En este caso, se permite cualquier dispositivo que tenga una dirección que pertenezca a la red 172.22.34.64/27. Introduzca la dirección de red, seguida de un signo de interrogación.
f) Para calcular la máscara wildcard, determine el número binario opuesto a una máscara de subred.
g) Introduzca la máscara wildcard, seguida de un signo de interrogación.
h) Configure la dirección de destino. En esta situación, se filtra el tráfico hacia un único destino: el servidor. Introduzca la palabra clave host seguida de la dirección IP del servidor.
i) Observe que una de las opciones es <cr> (retorno de carro). Es decir, puede presionar la tecla Enter, y la instrucción permitiría todo el tráfico TCP. Sin embargo, solo se permite el tráfico FTP. Por lo tanto, introduzca la palabra clave eq, seguida de un signo de interrogación para mostrar las opciones disponibles. Luego, introduzca ftp y presione la tecla Enter.
j) Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la PC1 al Servidor. Observe que el número de la lista de acceso es el mismo y que no es necesario detallar un tipo específico de tráfico ICMP.
k) El resto del tráfico se deniega de manera predeterminada.

```
R1(config)#access-list 100 permit tcp 172.22.34.64?
A.B.C.D
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31?
A.B.C.D
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62?
A.B.C.D
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq?
eq
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
```

```
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del R1, el tráfico al cual se aplica la ACL 100 ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/0. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config-if)#int g0/0
R1(config-if)#ip access-group 100 in
```

Paso 3: verificar la implementación de la ACL.

a) Haga ping de la PC1 al Servidor. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
b) Desde la PC1, acceda mediante FTP al Servidor. Tanto el nombre de usuario como la contraseña son cisco.

c) Salga del servicio FTP del Servidor.
d) Haga ping de la PC1 a la PC2. El host de destino debe ser inalcanzable, debido a que el tráfico no está permitido de manera explícita.

```
Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
Connected to 172.22.34.62
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
```

```
C:\>ping 172.22.64.98

Pinging 172.22.64.98 with 32 bytes of data:

Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.
Reply from 172.22.34.65: Destination host unreachable.

Ping statistics for 172.22.64.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Parte 2: configurar, aplicar y verificar una ACL extendida con nombre

Paso 1: configurar una ACL para que permita acceso HTTP y tráfico ICMP.

a) Las ACL con nombre comienzan con la palabra clave ip. Desde el modo de configuración global del R1, introduzca el siguiente comando, seguido por un signo de interrogación.
b) Puede configurar ACL estándar y extendidas con nombre. Esta lista de acceso filtra tanto las direcciones IP de origen como de destino, por lo tanto, debe ser extendida. Introduzca HTTP_ONLY como nombre.
c) El indicador de comandos cambia. Ahora está en el modo de configuración de ACL extendida con nombre. Todos los dispositivos en la LAN de la PC2 necesitan acceso TCP. Introduzca la dirección de red, seguida de un signo de interrogación.
d) Otra manera de calcular el valor de una wildcard es restar la máscara de subred a 255.255.255.255.
e) Para finalizar la instrucción, especifique la dirección del servidor como hizo en la parte 1 y filtre el tráfico www.
f) Cree una segunda instrucción de lista de acceso para permitir el tráfico ICMP (ping, etcétera) desde la PC2 al Servidor. Nota: la petición de entrada se mantiene igual, y no es necesario detallar un tipo específico de tráfico ICMP.
g) El resto del tráfico se deniega de manera predeterminada. Salga del modo de configuración de ACL extendida con nombre.

```
R1(config)#ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host
172.22.34.62 eq www
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host
172.22.34.62
```

Paso 2: aplicar la ACL a la interfaz correcta para filtrar el tráfico.

Desde la perspectiva del R1, el tráfico al cual se aplica la lista de acceso HTTP_ONLY ingresa desde la red conectada a la interfaz Gigabit Ethernet 0/1. Ingrese al modo de configuración de interfaz y aplique la ACL.

```
R1(config)#int g0/1
R1(config-if)#ip access-group HTTP_ONLY in
```

Paso 3: verificar la implementación de la ACL.

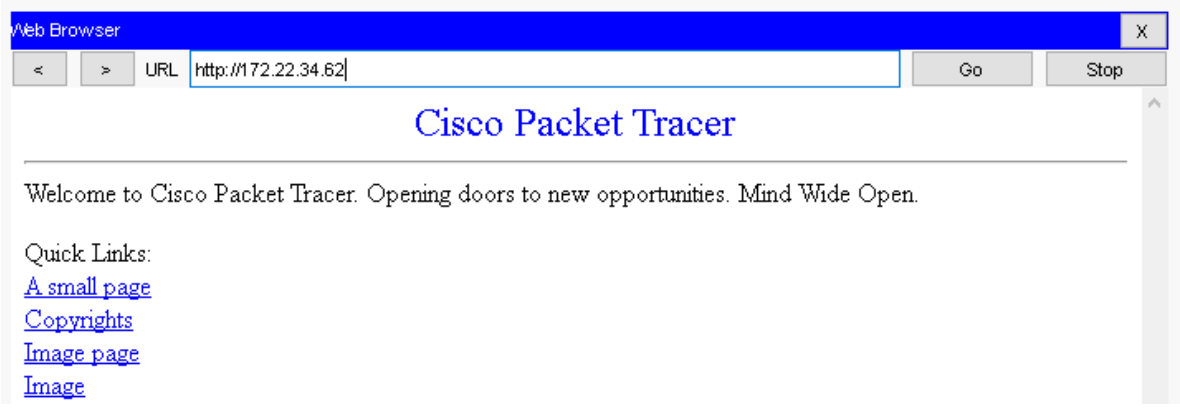
a) Haga ping de la PC2 al Servidor. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
b) Desde la PC2, acceda mediante FTP al Servidor. La conexión debería fallar.
c) Abra el navegador web en PC2 e introduzca la dirección IP de Server como URL. La conexión debería establecerse correctamente.

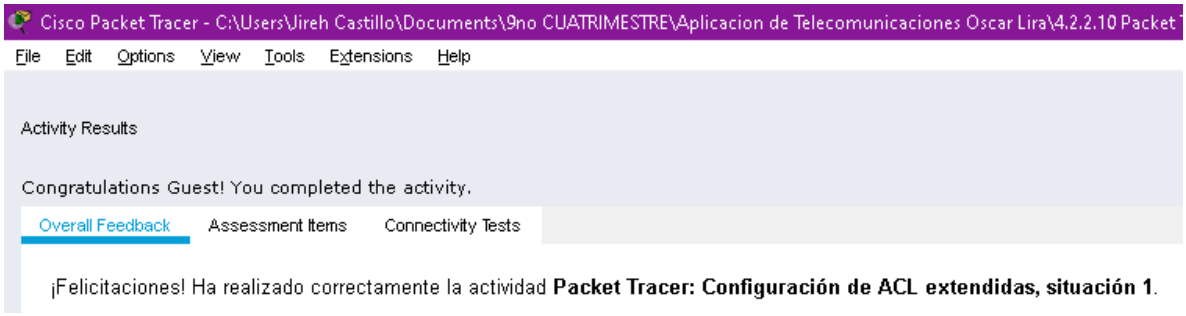
```
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Reply from 172.22.34.62: bytes=32 time=1ms TTL=127
Reply from 172.22.34.62: bytes=32 time=1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time=11ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```





Conclusión

La ACL extendida permite o deniega el acceso según la dirección IP de origen, la dirección IP de destino, el tipo de protocolo y los números de puertos. Dado que las ACL extendidas pueden ser muy específicas, tienden a aumentar su tamaño rápidamente. Cuantas más sentencias contenga una ACL, más difícil será administrarla.