Packet Tracer - Configure ACL extendidas: Escenario 1

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Puerta de enlace predeterminada
R1	G0/0	172.22.34.65	255.255.255.224	N/D
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
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: Configure, aplique y verifique una ACL extendida numerada

Parte 2: Configure, Aplique y Verifique una ACL extendida con nombre

Antecedentes / Escenario

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. Configurar ACL extendidas: escenario 1

Instrucciones

Parte 1: Configure, Aplique y Verifique una ACL extendida numerada

Paso 1: Configure una ACL para permitir FTP e ICMP desde PC1 LAN.

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.

```
R1(config)# access-list ?
  <1-99> IP standard access list
  <100-199> IP extended access list
```

b. Agregue **100** al comando, seguido de un signo de interrogación.

```
R1(config)# access-list 100 ?
  deny Specify packets to reject
  permit Specify packets to forward
  remark Access list entry comment
```

c. Para permitir el tráfico FTP, introduzca **permit**, seguido de un signo de interrogación.

```
R1(config)# access-list 100 permit ?
  ahp Authentication Header Protocol
  eigrp Cisco's EIGRP routing protocol
```

```
  esp Encapsulation Security Payload
  gre Cisco's GRE tunneling
  icmp Internet Control Message Protocol
  ip Any Internet Protocol
  ospf OSPF routing protocol
  tcp Transmission Control Protocol
  udp User Datagram Protocol
```

d. Cuando se configura y aplica, esta ACL debe permitir FTP e ICMP. ICMP aparece en la lista anterior, pero FTP no. Esto se debe a que FTP es un protocolo de capa de aplicación que utiliza TCP en la capa de transporte. Ingrese TCP para refinar aún más la ayuda de ACL.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D Source address
  any Any source host
  host A single source host
```

e. La dirección de origen puede representar un único dispositivo, como PC1, mediante la palabra clave **host** y, a continuación, la dirección IP de PC1. El uso de la palabra clave **any** permite cualquier host en cualquier red. El filtrado también se puede realizar mediante una dirección de red. En este caso, es cualquier host que tiene una dirección que pertenece a la red 172.22.34.64/27. Ingrese esta dirección de red, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D Source wildcard bits
```

f. Calcule la máscara comodín determinando el opuesto binario de la máscara de subred / 27.

11111111111111111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000 **= 11111** 0.0.0.31

g. Introduzca la máscara wildcard, seguida de un signo de interrogación.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D Destination address
  any Any destination host
  eq Match only packets on a given port number
  gt Match only packets with a greater port number
  host A single destination host
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  range Match only packets in the range of port numbers
```

h. Configure la dirección de destino. En este escenario, estamos filtrando el tráfico para un único destino, que es el servidor. Introduzca la palabra clave host seguida de la dirección IP del servidor.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
  dscp Match packets with given dscp value
  eq Match only packets on a given port number
  established established
  gt Match only packets with a greater port number
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  precedence Match packets with given precedence value
  range Match only packets in the range of port numbers
  <cr>
```

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, ingrese **ftp** y presione la tecla **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535> Port number
  ftp File Transfer Protocol (21)
  pop3 Post Office Protocol v3 (110)
  smtp Simple Mail Transport Protocol (25)
  telnet Telnet (23)
  www World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

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.

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

k. El resto del tráfico se deniega de manera predeterminada.

l. **Ejecute el comando show access-list** y verifique que access list 100 contenga las instrucciones correctas. Observe que la declaración **deny any any** no aparece al final de la lista de acceso. La ejecución predeterminada de una lista de acceso es que si un paquete no coincide con una sentencia de la lista de acceso, no se permite a través de la interfaz.

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
    20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

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

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

Nota: En una red operativa real, no es una buena práctica aplicar una lista de acceso no probada a una interfaz activa.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Paso 3: Verifique 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**.

```
PC> ftp 172.22.34.62
```

c. Salga del servicio FTP.

```
ftp> quit
```

d. Ping de PC1 a PC2. El host de destino no debería ser accesible, porque la ACL no permitía explícitamente el tráfico.

Parte 2: Configure, Apliqye y Verifique una ACL extendida con nombre

Paso 1: Configure una ACL para permitir el acceso HTTP e ICMP desde la PC2 LAN.

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.

```
R1(config)# ip access-list ?
  extended Extended Access List
  standard Standard Access List
```

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. (Para la puntuación Packet Tracer, el nombre distingue entre mayúsculas y minúsculas y las sentencias de lista de acceso deben ser el orden correcto.)

```
R1(config)# ip access-list extended HTTP_ONLY
```

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.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 ?
  A.B.C.D Source wildcard bits
```

d. Otra manera de calcular el valor de una wildcard es restar la máscara de subred a 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
= 0.  0.  0. 15
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15
```

e. Para finalizar la instrucción, especifique la dirección del servidor como hizo en la parte 1 y filtre el tráfico **www**.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq 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.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

g. El resto del tráfico se deniega de manera predeterminada. Salga del modo de configuración de ACL con nombre extendido.

h. **Ejecute el comando show access-list** y verifique que access list **HTTP_ONLY** contenga las instrucciones correctas.

```
R1# show access-lists
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

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

Desde la perspectiva de **R1**el tráfico al que se aplica la lista de acceso **HTTP_ONLY** es entrante desde la red conectada a la interfaz Gigabit Ethernet 0/1. Ingrese al modo de configuración de interfaz y aplique la ACL.

Nota: En una red operativa real, no es una buena práctica aplicar una lista de acceso no probada a una interfaz activa. Debe evitarse si es posible.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Paso 3: Verifique la implementación de la ACL.

a. Haga ping desde la **PC2** al **servidor**. Si el ping no tiene éxito, verifique las direcciones IP antes de continuar.

b. Desde la PC2, abra un navegador web e ingrese la dirección IP del servidor. Debe mostrarse la página web del servidor.

c. Desde la **PC2,** acceda mediante FTP al **Servidor**. La conexión debería fallar. Si no es así, solucione los problemas de las sentencias de lista de acceso y las configuraciones de grupo de acceso en las interfaces.