Packet Tracer - Configure ACL extendidas de IPv4 - Escenario 2

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
RT1	G0/0	172.31.1.126	255.255.255.224	N/D
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Servidor1	NIC	64.101.255.254		
Servidor2	NIC	64.103.255.254		

Objetivos

Parte 1: Configure una ACL extendida con nombre

Parte 2: Aplique y verifique la ACL extendida

Aspectos básicos/Escenario

En este escenario, se permiten dispositivos específicos en la LAN a varios servicios en servidores ubicados en Internet.

Instrucciones

Parte 1: Configure una ACL extendida y nombrada

Configure una ACL con nombre para implementar la siguiente política:

- Bloquee el acceso HTTP y HTTPS desde la **PC1** hasta el **Servidor1** y el **Servidor2**. Los servidores están dentro de la nube, y solo conoce sus direcciones IP.
- Bloquee el acceso FTP desde la **PC2** hasta el **Servidor1** y el **Servidor2.**
- Bloquee el acceso ICMP desde la **PC3** hasta el **Servidor1** y el **Servidor2.**

Nota: Para fines de puntuación, debe configurar las declaraciones en el orden especificado en los siguientes pasos.

Paso 1: Deniegue el acceso de la PC1 a los servicios HTTP y HTTPS en el Servidor1 y el Servidor2.

a. Cree una lista de acceso IP extendida nombrada en el router RT1 que denegará el acceso de la **PC1** a los servicios HTTP y HTTPS de **Servidor1** y **Servidor2**. Se requieren cuatro declaraciones de control de acceso.

¿Cuál es el comando para comenzar la configuración de una lista de acceso extendido con el nombre **ACL**?.

b. Comience la configuración de ACL con una declaración que niega el acceso de la **PC1** al **Servidor1**, solo para HTTP (puerto 80). Consulte la tabla de direccionamiento para conocer la dirección IP de **PC1** y **Servidor1**.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
```

c. Luego, ingrese la declaración que niega el acceso de la **PC1** al **Servidor1**, solo para HTTPS (puerto 443).

```
RT1 (config-ext-nacl) # deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
```

d. Ingrese la declaración que niega el acceso de la **PC1** al **Servidor2**,solo para HTTP. Consulte la tabla de direccionamiento para conocer la dirección IP del **Servidor 2.**

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
```

e. Ingrese la declaración que niega el acceso de la **PC1** al **Servidor2**, solo para HTTPS.

```
RT1 (config-ext-nacl) # deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Paso 2: Deniegue a la PC2 el acceso a los servicios FTP en el Servidor1 y el Servidor2.

Consulte la tabla de direccionamiento para la dirección IP de **PC2**.

a. Ingrese la declaración que niega el acceso de la **PC2** al **Servirdor1**, solo para FTP (solo el puerto 21).

```
RT1 (config-ext-nacl) # deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
```

b. Ingrese la declaración que niega el acceso de la **PC2** al **Servidor2**, solo para FTP (solo el puerto 21).

```
RT1 (config-ext-nacl) # deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```

Paso 3: Deniegue a la PC3 que haga ping al Servidor1 y al Servidor2.

Consulte la tabla de direccionamiento para la dirección IP de **PC3.**

a. Ingrese la declaración que niega el acceso ICMP de **PC3** al **Servidor1**.

```
RT1 (config-ext-nacl) # deny icmp host 172.31.1.103 host 64.101.255.254
```

b. Ingrese la declaración que niega el acceso ICMP de **PC3** al **Servidor2**.

```
RT1 (config-ext-nacl) # deny icmp host 172.31.1.103 host 64.103.255.254
```

Paso 4: Permita todo el tráfico IP restante.

De manera predeterminada, las listas de acceso deniegan todo el tráfico que no coincide con alguna regla de la lista. Escriba el comando que permita todo el tráfico que no coincida con ninguna de las instrucciones de lista de acceso configuradas.

Paso 5: Verifique la configuración de la lista de acceso antes de aplicarla a una interfaz.

Antes de aplicar cualquier lista de acceso, la configuración debe verificarse para asegurarse de que no hay errores tipográficos y de que las instrucciones están en el orden correcto. Para ver la configuración actual de la lista de acceso, utilice el comando **show access-lists** o el comando **show running-config** .

```
RT1# show access-lists
Extended IP access list ACL
       10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
       20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
       30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
```

```
        40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
        50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
        60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
        70 deny icmp host 172.31.1.103 host 64.101.255.254
        80 deny icmp host 172.31.1.103 host 64.103.255.254
        90 permit ip any any

RT1# show running-config | begin access-list
ip access-list extended ACL
      deny tcp host 172.31.1.101 host 64.101.255.254 eq www
      deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
      deny tcp host 172.31.1.101 host 64.103.255.254 eq www
      deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
      deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
      deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
      deny icmp host 172.31.1.103 host 64.101.255.254
      deny icmp host 172.31.1.103 host 64.103.255.254
      permit ip any any
```

Nota: La diferencia entre la salida del **comando show access-lists** y la salida del comando **show running-config** es que el comando **show access-lists incluye los números de secuencia asignados al** comando instrucciones de configuración. Estos números de secuencia permiten la edición, eliminación e inserción de líneas individuales dentro de la configuración de lista de acceso. Los números de secuencia también definen el orden de procesamiento de las sentencias de control de acceso individuales, comenzando por el número de secuencia más bajo.

Parte 2: Aplique y Verifique la ACL extendida

El tráfico que se filtrará proviene de la red 172.31.1.96/27 y tiene como destino las redes remotas. La colocación apropiada de ACL depende de la relación del tráfico con respecto a **RT1**. En general, las listas de acceso extendido deben colocarse en la interfaz más cercana al origen del tráfico.

Paso 1: Aplique la ACL a la interfaz apropiada en el sentido correcto.

Nota: En una red operativa real, nunca se debe aplicar una ACL no probada a una interfaz activa. Esta no es una buena práctica y puede interrumpir el funcionamiento de la red.

¿En qué interfaz se debe aplicar la ACL nombrada y en qué dirección?

Ingrese los comandos de configuración para aplicar la ACL a la interfaz.

Paso 2: Pruebe el acceso de cada computadora.

a. Acceda a los sitios web del **Servidor1** y **Servidor2** utilizando el navegador web de **PC1.** Utilice los protocolos HTTP y HTTPS. Utilice el comando **show access-lists** para ver qué instrucción de lista de acceso permitió o denegó el tráfico. El resultado del comando **show access-lists** muestra el número de paquetes que coinciden con cada sentencia desde la última vez que se borraron los contadores o se reinició el router.

   Nota: Para borrar los contadores de una lista de acceso, utilice el comando clear access-list counters.

```
RT1#show ip access-lists
Extended IP access list ACL
10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))
20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
```

```
30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
70 deny icmp host 172.31.1.103 host 64.101.255.254
80 deny icmp host 172.31.1.103 host 64.103.255.254
90 permit ip any any
```

b. Acceda al **Servidor1** y el **Servidor2** mediante FTP con la **PC1**. El nombre de usuario y la contraseña son **cisco**.

c. Haga ping al **Servidor1** y al **Servidor2** desde la **PC1**.

d. Repita los pasos del 2a al 2c con **PC2** y **PC3** para verificar la correcta operación de la lista de acceso.