Packet Tracer: configuración de ACL extendidas, situación 3

Topología

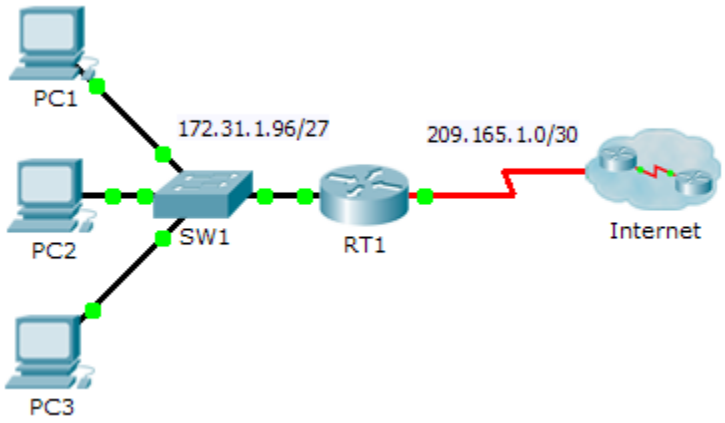

Tabla de direccionamiento

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	N/D
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: configurar una ACL extendida con nombre

Parte 2: aplicar y verificar la ACL extendida

Aspectos básicos/situación

En esta situación, se permite que determinados dispositivos de la LAN tengan acceso a varios servicios en servidores ubicados en Internet.

Parte 1: configurar una ACL extendida con nombre

Utilice una ACL con nombre para implementar la política siguiente:

- 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: a los fines de la puntuación, las instrucciones se deben configurar en el orden que se especifica en los siguientes pasos.

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

a. Cree una ACL de IP extendida con nombre que le deniegue a la **PC1** el acceso a los servicios HTTP y HTTPS del **Servidor1** y el **Servidor2**. Ya que no es posible observar directamente la subred de servidores en Internet, se necesitan cuatro reglas.

¿Cuál es el comando para iniciar la ACL con nombre?

b. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTP (puerto 80).

c. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor1** solo para HTTPS (puerto 443).

d. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTP.

e. Registre la instrucción que deniega el acceso de la **PC1** al **Servidor2** solo para HTTPS.

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

a. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor1** solo para FTP (puerto 21 únicamente).

b. Registre la instrucción que deniega el acceso de la **PC2** al **Servidor2** solo para FTP (puerto 21 únicamente).

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

a. Registre la instrucción que deniega el acceso ICMP de la **PC3** al **Servidor1**.

b. Registre la instrucción que deniega el acceso ICMP de la **PC3** al **Servidor2**.

Paso 4: permitir 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. ¿Qué comando permite el resto del tráfico?

Parte 2: aplicar y verificar 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 ubicación adecuada de la ACL también depende de la relación del tráfico con respecto al **RT1**.

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

a. ¿Cuáles son los comandos que necesita para aplicar la ACL a la interfaz apropiada en el sentido correcto?

Paso 2: probar el acceso de cada computadora.

a. Acceda a los sitios web del **Servidor1** y **Servidor2** mediante el navegador web de la **PC1** con los protocolos HTTP y HTTPS.

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

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

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