Packet Tracer - Desafío de implementación de ACL IPv4

Tabla de asignación de direcciones

Dispositivo	Interfaz	Dirección IP
Sucursal	G0/0/0	192.168.1.1/26
	G0/0/1	192.168.1.65/29
	S0/1/0	192.0.2.1/30
	/1/1	192.168.3.1/30
HQ	G0/0/0	192.168.2.1/27
	G0/0/1	192.168.2.33/28
	/1/1	192.168.3.2/30
PC-1	NIC	192.168.1.10/26
PC-2	NIC	192.168.1.20/26
PC-3	NIC	192.168.1.30/26
Administrador	NIC	192.168.1.67/29
Servidor Web empresarial	NIC	192.168.1.70/29
Rama PC	NIC	192.168.2.17/27
Servidor de sucursal	NIC	192.168.2.45/28
Usuarios de Internet	NIC	198.51.100.218/24
Servidor web externo	NIC	203.0.113.73/24

Objetivos

- Configure un router con ACL estándar con nombre.
- Configure un router con ACL nombradas extendidas.
- Configure un router con ACL extendidas para cumplir requisitos de comunicación específicos.
- Configure una ACL para controlar el acceso a las líneas de terminal de dispositivos de red.

- Configure las interfaces de router adecuadas con ACL en la dirección apropiada.
- Verifique el funcionamiento de las ACL configuradas.

Antecedentes/Escenario

En esta actividad, configurará ACL extendidas, con nombre estándar y con nombre extendido para cumplir los requisitos de comunicación especificados.

Packet Tracer - Desafío de implementación de ACL IPv4

Instrucciones

Paso 1: Verificación de la conectividad en la red de la nueva empresa

Primero, pruebe la conectividad en la red tal como está antes de configurar las ACL. Todos los hosts deberían poder hacer ping a todos los demás hosts.

Paso 2: Configure ACL estándar y extendida según los requisitos.

Configure las ACL para que cumplan los siguientes requisitos:

Directrices importantes:

- **No** use la denegación explícita de ninguna declaración al final de sus ACL. ○ Utilice taquigrafía (**host** y **any**) siempre que sea posible.
- Escriba sus sentencias ACL para abordar los requisitos en el orden en que se especifican aquí.
- Coloque sus ACL en la ubicación y dirección más eficientes.

Requisitos de ACL 1 ○ Crear ACL **101**. ○ Bloquear explícitamente el acceso FTP a Enterprise Web Server desde Internet.

- No se debe permitir tráfico ICMP desde Internet a ningún host en HQ LAN 1 ○ Permitir el resto del tráfico.

Requisitos de ACL 2

- Usar el número ACL **111** ○ Ningún host de HQ LAN 1 debería poder acceder al servidor de sucursal.
- Todo otro tráfico debe ser permitido.

ACL 3: Requisitos ○ Cree una ACL estándar con nombre. Utilice el nombre **vty_block**. El nombre de su ACL debe coincidir exactamente con este nombre.

- Solo las direcciones de la red LAN 2 de HQ deben poder acceder a las líneas VTY del router HQ.

ACL 4: Requisitos ○ Cree una ACL extendida con nombre llamada **branch_to_hq**. El nombre de su ACL debe coincidir exactamente con este nombre.

- No se debe permitir que ningún host de ninguna de las LAN de sucursal acceda a la LAN 1 de HQ. Utilice una instrucción de lista de acceso para cada una de las LAN de sucursales.
- Todo otro tráfico debe ser permitido.

Paso 3: Verifique la operación ACL.

a. Realice las siguientes pruebas de conectividad entre dispositivos de la topología. Tenga en cuenta si tienen éxito o no.

Nota: Use el comando **show ip access-lists para verificar la operación de ACL. Utilice el** comando clear access list counters para restablecer los contadores de cruce.

Envíe una solicitud de ping desde Branch PC al Enterprise Web Server. ¿Tuvo éxito? Explique. FUE CORRECTO EL PING PORQUE EL ACL LO PERMITIO.

¿Qué declaración ACL permitió o denegó el ping entre estos dos dispositivos? Enumere el nombre o número de la lista de acceso, el router en el que se aplicó y la línea específica con la que coincidió el tráfico. LA ÚLTIMA LÍNEA EN LA ACL BRANCH_TO_HQ EN EL ENRUTADOR DE SUCURSAL ES PERMIT IP ANY.

Intente hacer ping desde PC-1 en la LAN 1 de HQ al servidor de sucursal. ¿Tuvo éxito? Explique. FUE CORRECTO EL PING PORQUE EL TRAFICO FUE BLOQUEADO POR UNA LISTA DE ACCESO

¿Qué declaración ACL permitió o denegó el ping entre estos dos dispositivos? LA DECLARACIÓN 10 EN LA LISTA DE ACCESO 111 EN EL ENRUTADOR HQ NIEGA TODO EL TRÁFICO AL SERVIDOR DE SUCURSAL.

Abra un explorador Web en el servidor externo e intente abrir una página Web almacenada en Enterprise Web Server. ¿Tuvo éxito? Explique. SÍ, EL SERVIDOR EXTERNO PUEDE ACCEDER A UNA PÁGINA WEB EN EL SERVIDOR WEB EMPRESARIAL. EL TRÁFICO HTTP NO ESTÁ BLOQUEADO AL SERVIDOR WEB EMPRESARIAL.

¿Qué declaración ACL permitió o denegó el ping entre estos dos dispositivos? LA LÍNEA 20 EN LA LISTA DE ACCESO 101 EN EL ENRUTADOR HQ PERMITIÓ ESTE TRÁFICO.

b. Probar conexiones a un servidor interno desde Internet.

Desde la línea de comandos del PC de usuario de Internet, intente realizar una conexión FTP con el servidor de sucursales. ¿Se ha realizado correctamente la conexión FTP? SÍ, LA CONEXIÓN FTP DESDE LA PC DEL USUARIO DE INTERNET AL SERVIDOR DE SUCURSAL SE REALIZÓ CORRECTAMENTE.

¿Qué lista de acceso se debe modificar para evitar que los usuarios de Internet realicen conexiones FTP al servidor de sucursales? LA LISTA DE ACCESO 101 EN EL ENRUTADOR HQ DEBE MODIFICARSE PARA DENEGAR ESTE TRÁFICO.

¿Qué instrucciones se deben agregar a la lista de acceso para denegar este tráfico? LA DECLARACIÓN "DENEGAR TCP CUALQUIER HOST 192.168.2.45 EQ 21" O "DENEGAR TCP CUALQUIER HOST 192.168.2.45 RANGO 20 21" DEBE AGREGARSE A LA LISTA DE ACCESO 101.