Configuración de ACL extendidas

Topología

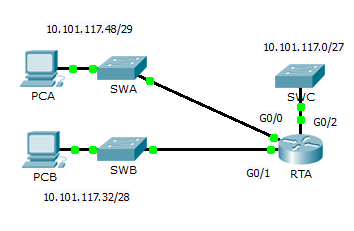


Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| RTA | G0/0 | 10.101.117.49 | 255.255.255.248 | N/D |
| G0/1 | 10.101.117.33 | 255.255.255.240 | N/D |
| G0/2 | 10.101.117.1 | 255.255.255.224 | N/D |
| PCA | NIC | 10.101.117.51 | 255.255.255.248 | 10.101.117.49 |
| PCB | NIC | 10.101.117.35 | 255.255.255.240 | 10.101.117.33 |
| SWC | VLAN1 | 10.101.117.2 | 255.255.255.224 | 10.101.117.1 |

Objetivos

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

Parte 2: Preguntas de reflexión

Aspectos básicos/situación

En esta situación, los dispositivos de una LAN pueden acceder de forma remota a los dispositivos de otra LAN mediante el protocolo Telnet. Aparte de ICMP, se deniega todo el tráfico de otras redes.

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

**Paso 1: Configurar la ACL extendida.**

Configure, aplique y verifique una ACL para que cumpla con la siguiente política:

1. Se permite el tráfico de Telnet desde los dispositivos de la red **10.101.117.32 /28** hasta los dispositivos en las redes **10.101.117.0 /27**. Utiliza el número de lista 199 para la ACL extendida.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Se permite el tráfico ICMP desde cualquier origen hasta cualquier destino. Utilice el mismo número de lista de acceso para permitir todo el tráfico ICMP, independientemente de la dirección de origen o de destino. NOTA: Utilice las palabras clave **any**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. El resto del tráfico a 10.101.117.0/27 está bloqueado. El resto del tráfico IP se deniega de manera predeterminada.

**Paso 2: Aplicar el ACL extendida.**

La regla general es colocar las ACL extendidas cerca del origen. Sin embargo, dado que la lista de acceso 199 afecta el tráfico que se origina de las dos redes, 10.101.117.48/29 y 10.101.117.32/28, la mejor ubicación de esta ACL podría ser en la interfaz gigabit Ethernet 0/2 en dirección saliente. ¿Cuál es el comando para aplicar la ACL 199 a la interfaz Gigabit Ethernet 0/2?

ip access-group 199 out

* 1. Verificar la implementación de la ACL extendida.
     1. Haga ping de la **PCB** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
     2. Desde la **PCB**, acceda al **SWC** mediante Telnet. La contraseña es **cisco**.
     3. Salga del servicio de Telnet del **SWC**.
     4. Haga ping de la **PCA** a todas las otras direcciones IP en la red. Si los pings no se realizan correctamente, verifique las direcciones IP antes de continuar.
     5. Desde la **PCA**, acceda al **SWC** mediante Telnet. La lista de acceso ocasiona que el router rechace la conexión.
     6. Desde la **PCA**, acceda al **SWB** mediante Telnet. La lista de acceso está colocada en **G0/2** y no afecta esta conexión.
     7. Una vez que inicie sesión en el **SWB**, no salga. Acceda al **SWC** mediante Telnet.

1. Preguntas de reflexión
   1. ¿Cómo pudo la PCA omitir la lista de acceso 199 y acceder al SWC mediante Telnet? Se siguieron dos pasos: primero, la PCA utilizó Telnet para acceder al SWB. Desde el SWB, pudo acceder al SWC mediante Telnet.
   2. ¿Qué se podría haber hecho para evitar que la PCA acceda indirectamente al SWC y, al mismo tiempo, permitir el acceso de la PCB al SWC por Telnet?La lista de acceso 199 debería haberse escrito para denegar el tráfico de Telnet de la red 10.101.117.48 /29 y permitir ICMP al mismo tiempo. Debería haberse colocado en G0/0 del RTA.

Tabla de puntuación sugerida

|  |  |  |  |
| --- | --- | --- | --- |
| Sección de la actividad | Ubicación de las preguntas | Puntos posibles | Puntos obtenidos |
| Parte 1: configurar, aplicar y verificar una ACL extendida numerada | Paso 1a | 4 |  |
| Paso 1b | 4 |  |
| Paso 2 | 4 |  |
| **Total de la parte 1** | | **12** |  |
| Parte 2: Preguntas de reflexión | Pregunta 1 | 4 |  |
| Pregunta 2 | 4 |  |
| **Total de la parte 2** | | **8** |  |
| **Puntuación de Packet Tracer** | | **80** |  |
| **Puntuación total** | | **100** |  |