Packet Tracer – Demonstração de lista de controle de acesso

# Objetivos

Parte 1: Verificar a conectividade local e testar a lista de controle de acesso

Parte 2: Remover a lista de controle de acesso e repetir o teste

# Histórico

Nesta atividade, você observará como uma lista de controle de acesso (ACL) pode ser usada para impedir que um ping alcance hosts em redes remotas. Após remover a ACL da configuração, os pings terão êxito.

# Instruções

## Verificar a conectividade local e teste a lista de controle de acesso

### Execute o ping nos dispositivos na rede local para verificar a conectividade.

* + - 1. Do prompt de comando de **PC1**, execute ping para **PC2**.
      2. Do prompt de comando de **PC1**, execute ping para **PC3**.

#### Pergunta:

Os pings tiveram êxito?

Digite suas respostas aqui.

### Execute o ping nos dispositivos em redes remotas para testar a funcionalidade da ACL.

* + - 1. Do prompt de comando de **PC1**, execute ping para **PC4**.
      2. Do prompt de comando de **PC1**, execute ping para **Servidor DNS**.

#### Pergunta:

Por que o ping falhou? (Dica: use o modo de simulação ou visualize as configurações do roteador para investigar.)

Digite suas respostas aqui.

## Remover a ACL e repetir o teste

### Use comandos show para investigar a configuração de ACL.

* + - 1. Use os comandos **show run** e **show access-lists** para exibir as ACLs configuradas atualmente. Para ver rapidamente as ACLs atuais, use **show access-lists**. Insira o comando **show access-lists**, seguido por um espaço e um ponto de interrogação (?) para exibir as opções disponíveis:

R1# **show access-lists ?**

<1-199> ACL number

WORD ACL name

<cr>

Se você souber o número ou o nome da ACL, poderá filtrar ainda mais a saída de **show**. No entanto, **R1** tem somente uma ACL; portanto, o comando **show access-lists** será suficiente.

R1# **show access-lists**

Standard IP access list 11

10 deny 192.168.10.0 0.0.0.255

20 permit any

A primeira linha de ACL impede pacotes oriundos da rede**192.168.10.0/24**, que inclui Internet Control Message Protocol (ICMP) echoes (solicitações de ping). A segunda linha da ACL permite todo o tráfego **ip** restante de **qualquer** origem para atravessar o roteador.

* + - 1. Para uma ACL afetar a operação do roteador, ela deve ser aplicada a uma interface em uma direção específica. Neste cenário, a ACL é usada para filtrar o tráfego em uma interface. Portanto, todo o tráfego saindo da interface de R1 especificada será inspecionado contra ACL 11.

Embora você possa visualizar as informações de IP com o comando **show ip interface**, pode ser mais eficiente em algumas situações, simplesmente usar o comando **show run**.

#### Pergunta:

Usando um ou ambos os comandos, a que interface é aplicada a ACL?

Digite suas respostas aqui.

### Remova a lista de acesso 11 da configuração.

Você pode remover as ACLs da configuração executando o comando **no access-list** [*number of the ACL*]. O comando **no access-list** exclui todas as ACLs configuradas no roteador. O comando **no access-list** [*number of the ACL*] remove apenas uma ACL específica.

* + - 1. Na interface Serial0 / 0/0, remova a lista de acesso 11, anteriormente aplicada à interface como um filtro de **saída**:

R1(config)# **int se0/0/0**

R1(config-if)#**no ip access-group 11 out**

* + - 1. No modo de configuração global, remova a ACL inserindo o seguinte comando:

R1(config)# **no access-list 11**

* + - 1. Verifique se **PC1** agora pode executar ping do **Servidor DNS** e **PC4**.

Fim do documento