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

# Contexto

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

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

### Etapa 1: Efetuar ping de dispositivos na rede local para verificar a conectividade.

a.     Do prompt de comando de **PC1**, ping **PC2**.

b.     Do prompt de comando de **PC1**, ping **PC3**.

#### Pergunta:

Os pings tiveram êxito?

Digite suas respostas aqui.

### Etapa 2: Executar ping em dispositivos em redes remotas para testar a funcionalidade ACL.

a.     Do prompt de comando de**PC1**, ping **PC4**.

b.     Do prompt de comando de **PC1**, ping o **DNS Server**.

#### Pergunta:

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

Digite suas respostas aqui.

## Parte 2: Remover ACL e repetir o teste

### Etapa 1: Use os comandos show para investigar a configuração ACL.

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

R1# **show access-lists ?**

<1-199> ACL number

WORD ACL name

  <cr>

Se você souber o número ou nome da ACL, pode filtrar a saída do **show** ainda mais. Contudo, **R1** tem apenas 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 da ACL impede que quaisquer pacotes originados no **192.168.10.0/24** rede, que inclui ecos do protocolo de mensagens de controle da Internet (ICMP) (solicitações de ping). A segunda linha da ACL permite que todo o outro tráfego de **ip** de **qualquer** origem atravesse o roteador.

b.     Para que uma ACL tenha impacto na 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 ver 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.

### Etapa 2: Remova a lista de acesso 11 da configuração.

Você pode remover ACLs da configuração emitindo 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.

a.     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**

b.     No modo de configuração global, remova a ACL digitando o seguinte comando:

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

c.     Verifique que o **PC1** agora pode realizar o ping para o **DNS Server** e o **PC4**.

Fim do documento