Atividade PT 5.2.8: Configurando ACLs padrão

Diagrama de topologia

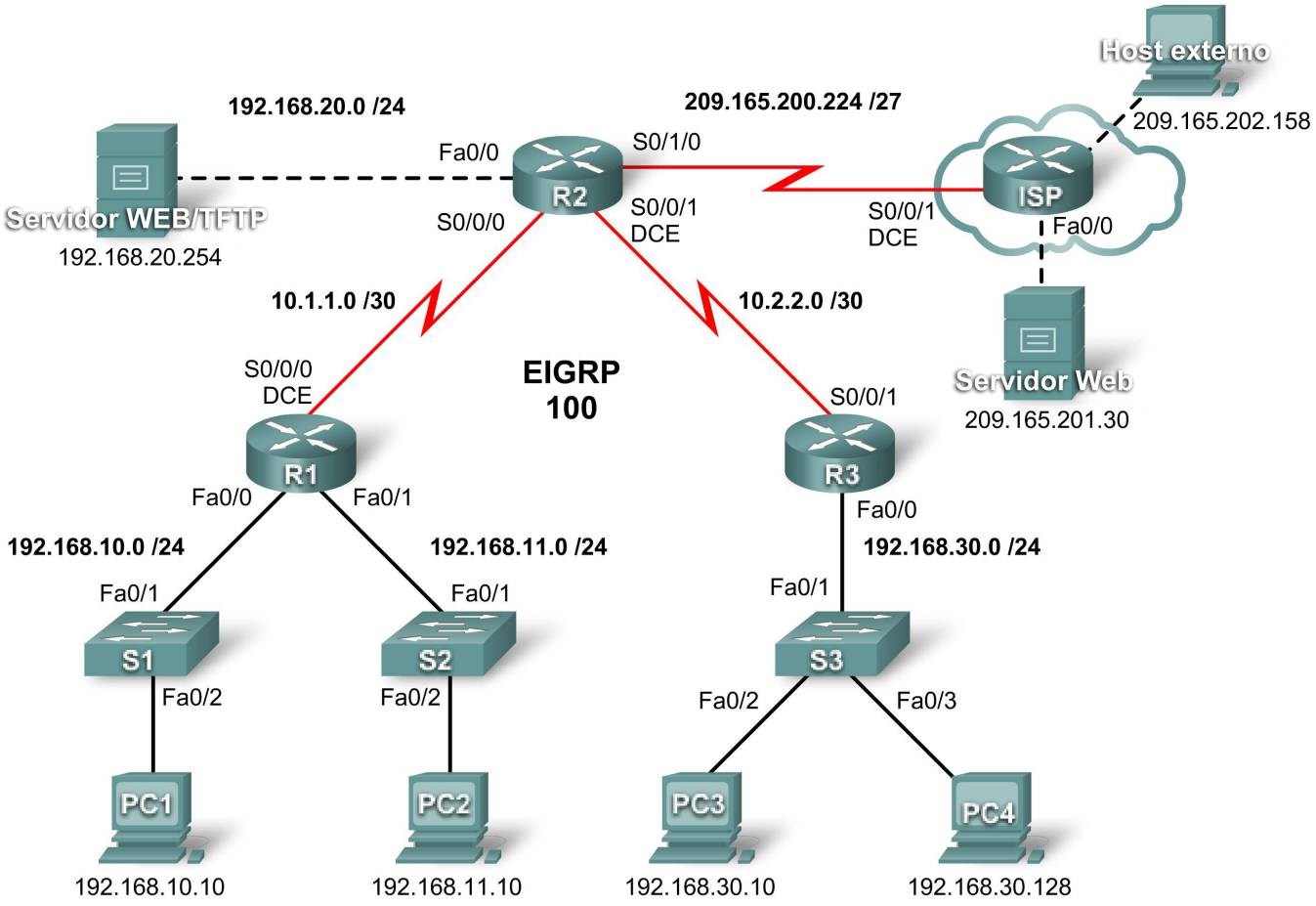

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**Placa de rede**	192.168.10.10	255.255.255.0
PC2	**Placa de rede**	192.168.11.10	255.255.255.0
PC3	**Placa de rede**	192.168.30.10	255.255.255.0
PC4	**Placa de rede**	192.168.30.128	255.255.255.0
Servidor WEB/TFTP	**Placa de rede**	192.168.20.254	255.255.255.0
Servidor WEB	**Placa de rede**	209.165.201.30	255.255.255.224
Host externo	**Placa de rede**	209.165.202.158	255.255.255.224

Objetivos de aprendizagem

- Investigue a configuração de rede atual.
- Avalie uma política de rede e planeje uma implementação ACL.
- Configure ACLs padrão numeradas.
- Configure ACLs padrão nomeadas.

Introdução

As ACLs padrão são scripts de configuração de roteador que controlam se um roteador permite ou nega pacotes com base no endereço de origem. Esta atividade vai ensinar a definir critérios de filtragem, configurar as ACLs padrão, aplicar as ACLs a interfaces de roteador e verificar e testar a implementação da ACL. Os roteadores já estão configurados, inclusive os endereços IP e o protocolo de roteamento de IGRP melhorado. A senha EXEC do usuário é **cisco** e a senha EXEC privilegiada é **class**.

Tarefa 1: Investigar a configuração de rede atual

Etapa 1. Exibir a configuração de execução nos roteadores.

Exibir as configurações de execução nos três roteadores que usam o comando **show running-config** enquanto eles estiverem no modo EXEC privilegiado. Observe que as interfaces e o roteamento estão totalmente configurados. Compare as configurações de endereço IP com as da Tabela de endereçamento acima. Não deve haver nenhuma ACL configurada nos roteadores neste momento.

O roteador ISP não exige nenhuma configuração durante este exercício. Suponhamos que o roteador ISP não esteja sob sua administração e seja configurado e mantido pelo administrador ISP.

Etapa 2. Confirmar se todos os dispositivos podem acessar todos os outros locais.

Antes de aplicar qualquer ACL a uma rede, é importante confirmar se você tem total conectividade. Sem testar a conectividade na rede antes de aplicar uma ACL, a identificação e solução de problemas pode ser muito mais difícil.

Uma etapa útil na conectividade de teste é exibir as tabelas de roteamento em cada dispositivo para certificar-se de que cada rede seja listada. Em R1, R2 e R3, utilize o comando **show ip route**. Você deve observar que cada dispositivo possui rotas conectadas para redes anexadas, e rotas dinâmicas para todas as outras redes remotas. Todos os dispositivos podem acessar todos os outros locais.

Embora a tabela de roteamento possa ser útil na avaliação do status da rede, você ainda deve testar a conectividade utilizando **ping**. Conclua os seguintes testes:

- Em PC1, execute ping em PC2.
- Em PC2, execute ping no host externo.
- Em PC4, execute ping no servidor Web/TFTP.

Todos os testes de conectividade devem ser bem-sucedidos.

Tarefa 2: Avaliar uma política de rede e planejar uma implementação de ACL

Etapa 1. Avaliar a política para as redes locais de R1.

- A rede 192.168.10.0/24 tem permissão para acessar todos os locais, exceto a rede 192.168.11.0/24.
- A rede 192.168.11.0/24 tem permissão para acessar todos os destinos, exceto redes conectadas ao ISP.

Etapa 2. Planejar a implementação de ACL nas redes locais de R1.

- Duas ACLs implementam completamente a política de segurança para as redes locais do R1.
- A primeira ACL em R1 nega tráfego da rede 192.168.10.0/24 para a rede 192.168.11.0/24, mas permite todo o restante do tráfego.
- Essa primeira ACL, aplicada na saída da interface Fa0/1, monitora todo o tráfego enviado para a rede 192.168.11.0.
- A segunda ACL em R2 nega o acesso da rede 192.168.11.0/24 ao ISP, mas permite todo o tráfego restante.
- O tráfego de saída da interface S0/1/0 é controlado.
- Coloque as instruções ACL na ordem da mais específica para a menos específica. Negar o acesso do tráfego de rede a outra rede vem antes de permitir todos os demais tráfegos.

Etapa 3. Avaliar a política para a rede local de R3.

- A rede 192.168.30.0/24 tem permissão para acessar todos os destinos.
- Host 192.168.30.128 não tem permissão de acesso fora da LAN.

Etapa 4. Planejar a implementação ACL da rede local R3.

- Uma ACL implementa completamente a política de segurança para a LAN R3.
- A ACL é colocada em R3 e nega acesso ao host 192.168.30.128 fora da rede local, mas permite o tráfego de todos os demais hosts na rede local.
- Aplicada na entrada da interface Fa0/0, essa ACL irá monitorar todo o tráfego que tenta deixar a rede 192.168.30.0/24.
- Coloque as instruções ACL na ordem da mais específica para a menos específica. Negar acesso ao host 192.168.30.128 vem antes de permitir todo o tráfego restante.

Tarefa 3: Configurar ACLs padrão numeradas

Etapa 1. Determinar a máscara curinga.

A máscara curinga em uma instrução de ACL determina a proporção de uma origem de IP ou de um endereço de destino que deverá ser verificada. Um bit 0 significa uma correspondência desse valor com o endereço, enquanto um bit 1 ignora o valor no endereço. Lembre-se de as ACLs padrão só podem ser verificadas em endereços de origem.

- Como a ACL em R1 nega todo o tráfego da rede 192.168.10.0/24, qualquer IP de origem que comece com 192.168.10 é negado. Como o último octeto do endereço IP pode ser ignorado, a máscara curinga correta é 0.0.0.255. Cada octeto nesta máscara pode ser considerado “verificar, verificar, verificar, ignorar”.
- A ACL em R2 também nega o tráfego de rede de 192.168.11.0/24. A mesma máscara curinga pode ser aplicada, 0.0.0.255.

Etapa 2. Determinar as instruções.

- As ACLs são configuradas no modo de configuração global.
- Para ACLs padrão, utilize um número entre 1 e 99. O número **10** é utilizado para a lista em R1 para ajudar a se lembrar de que essa ACL está monitorando a rede 192.168.**10**.0.
- Como em R2, access list **11 negará** o tráfego da rede 192.168.**11**.0 a qualquer rede ISP, a opção **deny** será definida com a rede **192.168.11.0** e a máscara de rede **0.0.0.255**.
- Todo o tráfego restante deve ser permitido com a opção **permit** por conta do “deny any” implícito ao final das ACLs. A opção **any** especifica qualquer host de origem.

Configure o seguinte em R1:

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Nota: o Packet Tracer não avaliará como correta uma configuração de ACL até que todas as instruções sejam digitadas na ordem correta.

Agora crie uma ACL em R2 para negar a rede 192.168.11.0 e permitir todas as demais redes. Para esta ACL, utilize o número **11**. Configure o seguinte em R2:

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Etapa 3. Aplicar as instruções às interfaces.

Em R1, acesse o modo de configuração da interface Fa0/1.

Execute o comando **ip access-group 10 out** para aplicar a saída da ACL padrão na interface.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```


Em R2, acesse o modo de configuração da interface S0/1/0.

Execute o comando **ip access-group 11 out** para aplicar a saída da ACL padrão na interface.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Etapa 4. Verificar e testar ACLs.

Com as ACLs configuradas e aplicadas, o PC1 (192.168.10.10) não deve poder executar ping no PC2 (192.168.11.10), porque ACL 10 é aplicada na saída em Fa0/1 em R1.

PC2 (192.168.11.10) não deve ser capaz de executar ping no servidor Web (209.165.201.30) ou no host externo (209.165.202.158), mas deve ser capaz de executar ping em todos os demais lugares, porque a ACL 11 é aplicada externamente em S0/1/0 no R2. No entanto, PC2 não pode executar ping em PC1 porque a ACL 10 em R1 impede a resposta eco de PC1 para PC2.

Etapa 5. Verifique os resultados.

O percentual de conclusão deve ser 67%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Configurar uma ACL padrão nomeada

Etapa 1. Determinar a máscara curinga.

- A política de acesso para R3 declara que o host em 192.168.30.128 não deve ter permissão de acesso fora da rede local. Todos os demais hosts na rede 192.168.30.0 devem ter permissão de acesso a todos os outros locais.
- Para verificar um único host, todo o endereço IP precisa ser verificado, o que é realizado utilizando-se a palavra-chave **host**.
- Todos os pacotes que não correspondem à instrução do host são permitidos.

Etapa 2. Determinar as instruções.

- Em R3, acesse o modo de configuração global.
- Crie uma ACL nomeada chamada NO_ACCESS, através do comando **ip access-list standard NO_ACCESS**. Você entrará no modo de configuração de ACL. Todas as instruções de permissão e negação são configuradas neste modo de configuração.
- Negue tráfego do host 192.168.30.128 com a opção **host**.
- Permita todo o tráfego restante com **permit any**.

Configure a seguinte ACL nomeada em R3:

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Etapa 3. Aplicar as instruções à interface correta.

Em R3, entre no modo de configuração da interface Fa0/0.

Utilize o comando **ip access-group NO_ACCESS in** para aplicar a ACL nomeada na entrada na interface. Este comando faz com que todo o tráfego que entra na interface Fa0/0 da rede local 192.168.30.0/24 seja comparado à ACL.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```


Etapa 4. Verificar e testar ACLs.

Clique em **Check Results** e na guia **Connectivity Tests**. Os testes a seguir devem falhar:

- PC1 para PC2
- PC2 para host de saída
- PC2 para servidor Web
- Todos os pings de/para PC4, exceto os entre PC3 e PC4

Etapa 5. Verifique os resultados.

O percentual de conclusão deve ser 100%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

