Atividade PT 5.3.4: Configurando ACLs estendidas

Diagrama de topologia

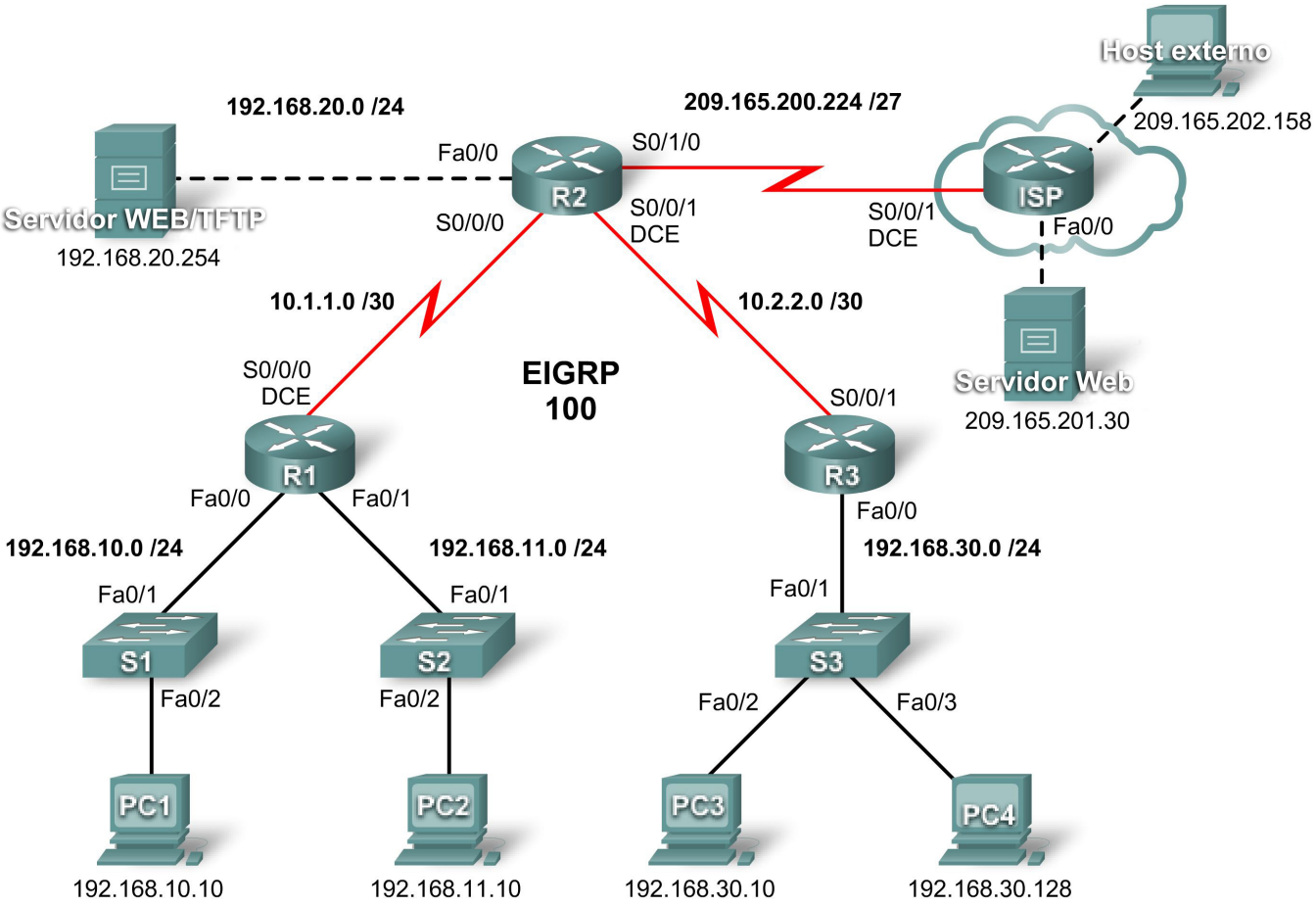

Tabela de endereçamento

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	10.2.2.2	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**	10.2.2.1	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 estendidas numeradas.
- Configure ACLs estendidas nomeadas.

Introduction

As ACLs estendidas são scripts de configuração de roteador que controlam se um roteador permite ou nega pacotes com base no endereço de origem ou de destino, bem como protocolos ou portas. As ACLs estendidas dão mais flexibilidade e granularidade do que as ACLs padrão. Esta atividade vai ensinar a definir critérios de filtragem, configurar as ACLs estendidas, 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, sendo 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 em sua rede antes de aplicar uma ACL, solucionar problemas será muito difícil.

Para assegurar conectividade em toda a rede, utilize os comandos **ping** e **tracert** entre vários dispositivos de rede para verificar as conexões.

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

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

- Para a rede 192.168.10.0/24, bloqueie o acesso Telnet a todos os locais e o acesso TFTP para o servidor Web/TFTP corporativo em 192.168.20.254. Todos os demais acessos são permitidos.
- Para a rede192.168.11.0/24, permita o acesso TFTP e o acesso à Web para o servidor Web/TFTP em 192.168.20.254. Bloqueie os demais tráfegos da rede 192.168.11.0/24 para a rede 192.168.20.0/24. Todos os demais acessos são permitidos.

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

- Duas ACLs implementam completamente a política de segurança para as redes locais do R1.
- A primeira ACL oferece suporte à primeira parte da política, é configurada no R1 e aplicada à interface 0/0 Fast Ethernet.
- A segunda ACL oferece suporte à segunda parte da política, é configurada no R1 e aplicada à interface 0/1 Fast Ethernet.

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

- Todos os endereços IP da rede 192.168.30.0/24 são impedidas de acessar todos os endereços IP da rede 192.168.20.0/24.
- A primeira parte da 192.168.30.0/24 tem permissão para acessar todos os demais destinos.
- A segunda parte da rede 192.168.30.0/24 tem permissão para acessar as redes 192.168.10.0/24 e 192.168.11.0/24.
- A segunda parte da 192.168.30.0/24 tem permissão para acessar todos os demais destinos pela Web e por ICMP.
- Todos os demais acessos são negados explicitamente.

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

Esta etapa exige uma ACL configurada no R3 e aplicada à interface 0/0 Fast Ethernet.

Etapa 5. Avaliar a política quanto ao tráfego proveniente da Internet via ISP.

- Os hosts de saída podem estabelecer uma sessão de Web somente com o servidor Web interno na porta 80.

- Apenas as sessões TCP estabelecidas são permitidas.
- Apenas respostas ping são permitidas em R2.

Etapa 6. Planejar as implementações ACL considerando o tráfego proveniente da Internet via ISP.

Esta etapa exige uma ACL configurada no R2 e aplicada à interface serial 0/1/0.

Tarefa 3: Configurar ACLs estendidas numeradas

Etapa 1. Determinar as máscaras curinga.

São necessárias duas ACLs para reforçar a política de controle de acesso no R1. Ambas as ACLs serão criadas para negar uma rede da Classe C inteira. Você configurará uma máscara curinga que corresponda a todos os hosts em cada uma destas redes de Classe C.

Por exemplo, para que haja correspondência de toda a sub-rede 192.168.10.0/24, a máscara curinga é 0.0.0.255. Isso pode ser considerado como "verificar, verificar, verificar, ignorar" e, essencialmente, corresponde a toda a rede 192.168.10.0/24.

Etapa 2. Configurar a primeira ACL estendida de R1.

No modo de configuração global, configure a primeira ACL com o número 110. Primeiro, você deseja bloquear Telnet para qualquer local de todos os endereços IP na rede 192.168.10.0/24.

Ao escrever a instrução, verifique se você está atualmente no modo de configuração global.

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

A seguir, bloqueie todos os endereços IP na rede 192.168.10.0/24 no acesso TFTP para o host em 192.168.20.254.

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Por fim, permita todos os demais tráfegos.

```
R1(config)#access-list 110 permit ip any any
```

Etapa 3. Configurar a segunda ACL estendida para R1.

Configure a segunda ACL com o número 111. Permita WWW ao host em 192.168.20.254 para qualquer endereço IP na rede 192.168.11.0/24.

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

A seguir, deixe o TFTP ser o host em 192.168.20.254 para qualquer endereço IP na rede 192.168.11.0/24.

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Bloqueie os demais tráfegos da rede 192.168.11.0/24 para a rede 192.168.20.0/24.

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

Por fim, permita qualquer outro tráfego. Esta instrução garante que o tráfego para outras redes não seja bloqueado.

```
R1(config)#access-list 111 permit ip any any
```


Etapa 4. Verificar as configurações das ACL.

Confirme as configurações em R1, emitindo comando **show access-lists**. Sua saída de dados deve ter esta aparência.

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

Etapa 5. Aplicar os commandos às interfaces.

Para aplicar uma ACL a uma interface, entre no modo de configuração dessa interface. Configure o comando **ip access-group** *access-list-number* {**in** | **out**} para aplicar a ACL à interface.

Cada ACL filtra o tráfego de entrada. Aplique ACL 110 a Fast Ethernet 0/0 e ACL 111 a Fast Ethernet 0/1.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

Confirme se as ACLs são exibidas na configuração em execução de R1 e se elas foram aplicadas às interfaces corretas.

Etapa 6. Testar as ACLs configuradas em R1.

Agora que as ACLs foram configuradas e aplicadas, é muito importante testar se o tráfego está bloqueado ou é permitido como esperado.

- Em PC1, tente obter acesso Telnet a qualquer dispositivo. Isso deve ser bloqueado.
- Em PC1, tente acessar o servidor Web/TFTP corporativo via HTTP. Isso deve ser permitido.
- Em PC2, tente acessar o servidor Web/TFTP via HTTP. Isso deve ser permitido.
- Em PC2, tente acessar o servidor Web externo via HTTP. Isso deve ser permitido.

Com base na sua compreensão de ACLs, tente executar outros testes de conectividade em PC1 e PC2.

Etapa 7. Verifique os resultados.

Como o Packet Tracer não oferece suporte ao teste de acesso TFTP, você não poderá verificar essa política. No entanto, o seu percentual de conclusão deve ser de 50%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Configurar uma ACL estendida numerada para R3

Etapa 1. Determinar a máscara curinga.

A política de acesso da segunda parte dos endereços IP na rede 192.168.30.0/24 exige:

- Negar acesso à rede 192.168.20.0/24
- Dê acesso a todos os demais destinos

A parte superior dos endereços IP na rede 192.168.30.0/24 apresenta as seguintes restrições:

- Dê acesso a 192.168.10.0 e 192.168.11.0

- Negar acesso a 192.168.20.0
- Permita Web e ICMP a todos os demais locais

Para determinar a máscara curinga, leve em conta quais bits precisam ser verificados para que a ACL corresponda aos endereços IP 0–127 (parte inferior) ou 128–255 (parte superior).

Lembre-se de que uma maneira de determinar a máscara curinga é subtrair a máscara de rede normal de 255.255.255.255. A máscara normal dos endereços IP 0–127 e 128–255 de um endereço de Classe C é 255.255.255.128. Com o uso do método de subtração, a máscara curinga correta é:

```
   255.255.255.255
 - 255.255.255.128
-----------------
     0.  0.  0.127
```

Etapa 2. Configurar a ACL estendida em R3.

Em R3, acesse o modo de configuração global e configure a ACL que usa 130 como o número da lista de acesso.

A primeira instrução bloqueia o acesso de 192.168.30.0/24 a todos os endereços da rede 192.168.20.0/24.

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

A segunda instrução permite que a metade inferior da rede 192.168.30.0/24 acesse todos os outros destinos.

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

As instruções restantes permitem explicitamente que a metade superior da rede 192.168.30.0/24 acesse essas redes e os serviços permitidos pela política de rede.

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

Etapa 3. Aplicar o comando à interface.

Para aplicar uma ACL a uma interface, entre no modo de configuração dessa interface. Configure o comando **ip access-group** *access-list-number* {**in** | **out**} para aplicar a ACL à interface.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

Etapa 4. Verificar e testar as ACLs.

Agora que a ACL foi configurada e aplicada, é muito importante testar se o tráfego está bloqueado ou é permitido como esperado.

- Em PC3, execute ping no servidor Web/TFTP. Isso deve ser bloqueado.
- Em PC3, execute ping em outro dispositivo. Isso deve ser permitido.
- Em PC4, execute ping no servidor Web/TFTP. Isso deve ser bloqueado.
- Em PC4, execute telnet em R1 em 192.168.10.1 ou 192.168.11.1. Isso deve ser permitido.
- Em PC4, execute ping em PC1 e em PC2. Isso deve ser permitido.
- Em PC4, execute telnet em R2 em 10.2.2.2. Isso deve ser bloqueado.

Depois que os testes forem realizados e produzirem os resultados corretos, utilize o comando **show access-lists** no modo EXEC privilegiado em R3 para verificar se as ACL apresentam correspondências.

Com base na sua compreensão de ACLs, realize outros testes para verificar se cada instrução corresponde ao tráfego correto.

Etapa 5. Verifique os resultados.

O percentual de conclusão deve ser 75%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 5: Configurar uma ACL estendida nomeada

Etapa 1. Configurar uma ACL estendida nomeada em R2.

Lembre-se de que a política em R2 será criada para filtrar tráfego de Internet. Como R2 tem a conexão com o ISP, esse é o melhor local para a ACL.

Configure uma ACL nomeada chamada FIREWALL em R2 utilizando o comando **ip access-list extended** *name*. Este comando coloca o roteador em modo de configuração de ACL de nomenclatura estendida. Observe o prompt de roteador alterado.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

No modo de configuração ACL, adicione as instruções para filtrar o tráfego conforme descrito na política:

- Os hosts de saída podem estabelecer uma sessão de Web somente com o servidor Web interno na porta 80.
- Apenas as sessões TCP estabelecidas são permitidas.
- Respostas ping são permitidas por meio de R2.

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

Depois de configurar a ACL em R2, utilize o comando **show access-lists** para confirmar se a ACL tem as instruções corretas.

Etapa 2. Aplicar a instrução à interface.

Utilize o comando **ip access-group** *name* {**in** | **out**} para aplicar a ACL de entrada ao ISP voltado para a interface de R2.

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

Etapa 3. Verificar e testar as ACLs.

Realize os seguintes testes para garantir que a ACL esteja funcionando como esperado:

- No host externo, abra uma página da Web no servidor Web/TFTP interno. Isso deve ser permitido.
- No host externo, execute ping no servidor Web/TFTP interno. Isso deve ser bloqueado.
- No host externo, execute ping em PC1. Isso deve ser bloqueado.
- Em PC1, execute ping no servidor Web externo em 209.165.201.30. Isso deve ser permitido.
- Em PC1, abra uma página da Web no servidor externo. Isso deve ser permitido.

Depois que os testes forem realizados e produzirem os resultados corretos, utilize o comando **show access-lists** no modo EXEC privilegiado em R2 para verificar se as ACL apresentam correspondências.

Com base na sua compreensão de ACLs, realize outros testes para verificar se cada instrução corresponde ao tráfego correto.

Etapa 4. 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.

