Atividade PT 5.6.1: Desafio: Integração das habilidades no Packet Tracer

Diagrama de topologia

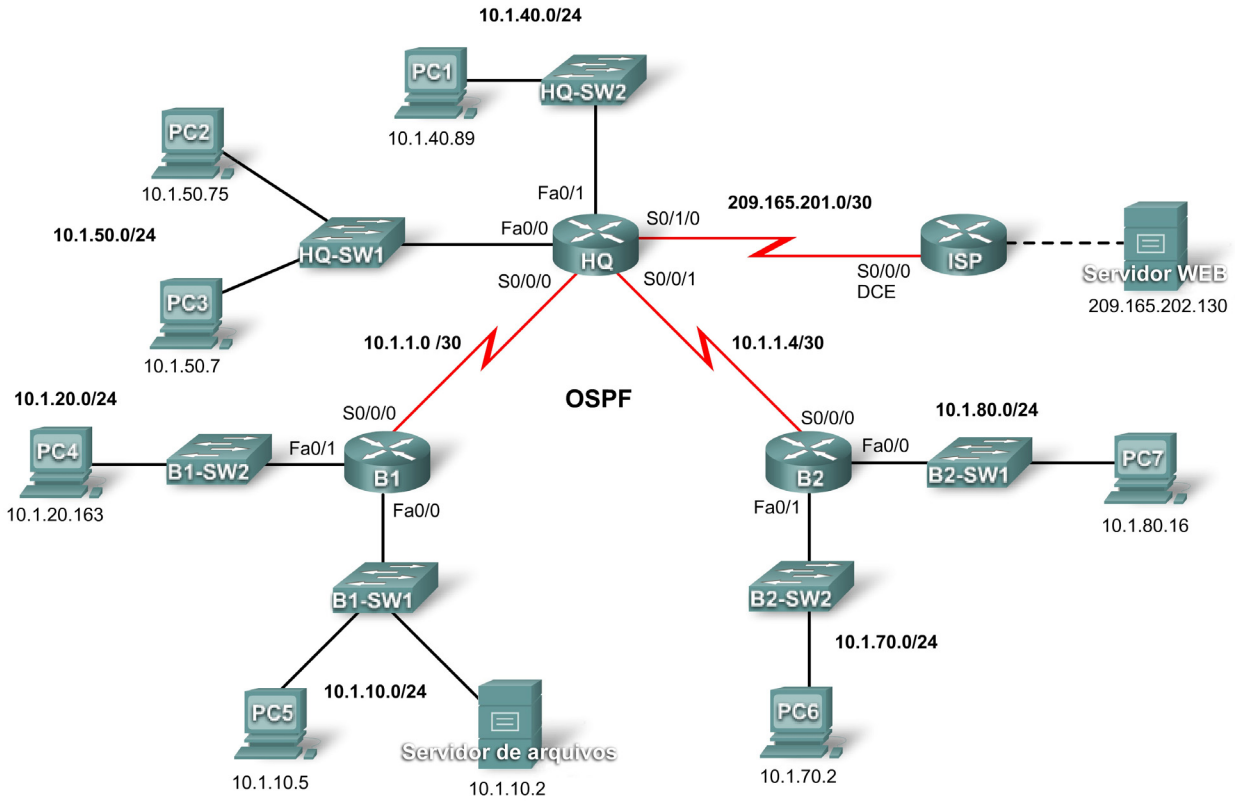

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
HQ	**S0/0/0**	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	**S0/0/0**	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	**S0/0/0**	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Servidor Web	**Placa de rede**	209.165.202.130	255.255.255.252

Objetivos de aprendizagem

- Configurar PPP com autenticação CHAP.
- Configurar roteamento padrão.
- Configure roteamento OSPF.
- Implementar e verificar várias políticas de segurança com ACL.

Introdução

Nesta atividade, você demonstrará a sua capacidade de configurar ACLs que aplicam cinco políticas de segurança. Além disso, você irá configurar o roteamento PPP e OSPF. Os dispositivos já estão configurados com endereçamento IP. A senha EXEC do usuário é **cisco** e a senha EXEC privilegiada é **class**.

Tarefa 1: Configurar PPP com autenticação CHAP

Etapa 1. Configurar o link entre HQ e B1 para utilizar o encapsulamento PPP com autenticação CHAP.

A senha para a autenticação de CHAP é **cisco123**.

Etapa 2. Configurar o link entre HQ e B2 para utilizar o encapsulamento PPP com autenticação CHAP.

A senha para a autenticação de CHAP é **cisco123**.

Etapa 3. Verificar se a conectividade foi restaurada entre os roteadores.

HQ deve ser capaz de executar ping em B1 e B2. Pode levar alguns minutos para que as interfaces sejam reativadas. Você pode alternar de um para outro entre os modos Realtime e Simulation para

agilizar o processo. Outra possível solução alternativa para este comportamento do Packet Tracer é usar os comandos **shutdown** e **no shutdown** nas interfaces.

Nota: as interfaces podem ser desativadas em pontos aleatórios durante a atividade devido a um bug do Packet Tracer. Normalmente, a interface é reativada automaticamente se você aguardar alguns segundos.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 29%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar roteamento padrão

Etapa 1. Configurar roteamento padrão de HQ para ISP.

Configure uma rota padrão em HQ utilizando o argumento *exit interface* do comando *ip route* para enviar todo o tráfego padrão para o ISP.

Etapa 2. Testar conectividade com o servidor Web.

HQ deve ser capaz de executar ping com êxito no servidor Web em 209.165.202.130, desde que a origem do ping esteja a interface Serial0/1/0.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 32%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurar roteamento OSPF

Etapa 1. Configurar OSPF em HQ.

- Configure OSPF usando o processo ID 1.
- Anuncie todas as sub-redes, exceto a rede 209.165.201.0.
- Propague a rota padrão para vizinhos OSPF.
- Desabilite atualizações OSPF nas redes locais ISP e HQ.

Etapa 2. Configurar OSPF em B1 e B2.

- Configure OSPF usando o processo ID 1.
- Em cada roteador, configure as sub-redes apropriadas.
- Desabilite atualizações OSPF para as redes locais.

Etapa 3. Testar conectividade em toda a rede.

Agora a rede deve ter uma conectividade fim-a-fim completa. Todos os dispositivos devem ser capazes de executar ping em todos os demais dispositivos com êxito, inclusive o servidor Web em 209.165.202.130.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 76%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Implementar várias políticas de segurança ACL

Etapa 1. Implementar o número da política de segurança 1.

Impeça a rede 10.1.10.0 de acessar a rede 10.1.40.0. Qualquer outro acesso a 10.1.40.0 é permitido. Configure a ACL em HQ utilizando a ACL número 10.

- Usar uma ACL padrão ou estendida? _____
- Aplicar a ACL a que interface? _____
- Aplicar a ACL em que direção? _____

_____

_____

_____

_____

_____

Etapa 2. Verificar se o número da política de segurança 1 foi implementado.

Deve haver falha em um ping de PC5 em PC1.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 80%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Etapa 4. Implementar a política de segurança de número 2.

O host 10.1.10.5 não tem permissão para acessar o host 10.1.50.7. Todos os outros hosts têm permissão para acessar 10.1.50.7. Configure a ACL em B1 utilizando a ACL número 115.

- Usar uma ACL padrão ou estendida? _____
- Aplicar a ACL a que interface? _____
- Aplicar a ACL em que direção? _____

_____

_____

_____

_____

_____

Etapa 5. Verificar se o número da política de segurança 2 foi implementado.

Deve haver falha em um ping de PC5 em PC3.

Etapa 6. Verifique os resultados.

O percentual de conclusão deve ser 85%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Etapa 7. Implementar o número da política de segurança 3.

Os hosts 10.1.50.1 até 10.1.50.63 não têm permissão de acesso web no servidor da Intranet em 10.1.80.16. Todos os demais acessos são permitidos. Configure a ACL no roteador apropriado e utilize a ACL número 101.

- Usar uma ACL padrão ou estendida? _____
- Configurar a ACL em que roteador? _____
- Aplicar a ACL a que interface? _____
- Aplicar a ACL em que direção? _____

Etapa 8. Verificar se a política de segurança de número 3 foi implementada.

Para testar essa política, clique em PC3, na guia **Desktop** e em **Web Browser**. Para o URL, digite o endereço IP do servidor da Intranet, 10.1.80.16, e pressione **Enter**. Depois de alguns segundos, você deve receber uma mensagem Request Timeout. PC2 e qualquer outro PC na rede devem ser capazes de acessar o servidor da Intranet.

Etapa 9. Verifique os resultados.

O percentual de conclusão deve ser 90%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Etapa 10. Implementar a política de segurança de número 4.

Utilize o nome **NO_FTP** para configurar uma ACL nomeada que impeça a rede 10.1.70.0/24 de acessar serviços FTP (porta 21) no servidor de arquivos em 10.1.10.2. Todos os demais acessos devem ser permitidos.

Nota: os nomes diferenciam maiúsculas de minúsculas.

- Usar uma ACL padrão ou estendida? _____
- Configurar a ACL em que roteador? _____
- Aplicar a ACL a que interface? _____
- Aplicar a ACL em que direção? _____

Etapa 11. Verifique os resultados.

Como o Packet Tracer não dá suporte ao teste de acesso FTP, você não poderá verificar essa política. No entanto, o seu percentual de conclusão deve ser de 95%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Etapa 12. Implementar o número da política de segurança 5.

Como o ISP representa a conectividade com a Internet, configure uma ACL chamada **FIREWALL** na seguinte ordem:

1. Só permita respostas ping de entrada em ISP e em qualquer origem além dele.
2. Só permita sessões TCP estabelecidas em ISP e em qualquer origem além dele.
3. Bloqueie explicitamente todo o acesso de entrada do ISP e qualquer origem além do ISP.

- Usar uma ACL padrão ou estendida? _____
- Configurar a ACL em que roteador? _____
- Aplicar a ACL a que interface? _____
- Aplicar a ACL em que direção? _____

_____

_____

_____

_____

_____

Etapa 13. Verificar se a política de segurança de número 5 foi implementada.

Para testar essa política, qualquer PC deve ser capaz de executar ping no ISP ou no servidor Web. No entanto, nem o ISP nem o servidor Web devem ser capazes de executar ping em HQ ou em qualquer outro dispositivo atrás da ACL **FIREWALL**.

Etapa 14. 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.

