Packet Tracer - Firewalls de servidor e ACLs do roteador

Tabela de Endereçamento

Dispositivo	Endereço IP privado	Endereço IP público	Máscara de sub-rede	Site
Servidor Web	N/D	209,165.201,10	255.255.255.0	Internet

Objetivos

Parte 1: Conectar-se ao servidor da Web

Parte 2: Impedir sessões HTTP não criptografadas

Parte 3: Acessar o firewall no servidor de e-mail

Histórico

Nessa atividade, você acessará um usuário dentro do site do Metropolis e se conectará usando HTTP e HTTPS a um servidor da Web remoto. O endereçamento IP, a configuração de rede e as confirmações de serviço já foram realizados. Você usará um dispositivo cliente no site do Metropolis para testar a conectividade com um servidor da Web remoto e, depois, proteger o site do Metropolis, impedindo que sessões da Web não criptografadas se conectem com o mundo externo.

Parte 1: Conecte-se ao servidor da Web

Passo 1: Acesse o servidor Web HQ Internet no PC da Sally usando HTTP.

a. Clique no site **Metropolis Bank HQ** e clique no PC **Sally**.

b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Web Browser (Navegador Web)**.

c. Digite a URL de **http://www.cisco.corp** e clique em **Go (Ir)**.

d. Clique no link **Login Page (Página de login)**.

Um usuário deveria ficar preocupado ao enviar informações usando esse site da Web?

Passo 2: Acesse o servidor da Web HQ Internet no PC da Sally usando HTTPS.

a. Acesse o **Navegador da Web** no computador da Sally.

b. Digite a URL de **https://www.cisco.corp** e clique em Go (Ir).

c. Clique no link **Login Page (Página de login)**.

Um usuário deveria ficar pouco preocupado ao enviar informações usando esse site da Web?

d. Feche o computador da **Sally**.

Parte 2: Impedir sessões HTTP não criptografadas

Passo 1: Configure o HQ_Router.

a. No site **Metropolis Bank HQ**, clique no **HQ_Router**.

b. Clique na guia **CLI** e pressione **Enter**.

c. Use a senha **cisco** para fazer login no roteador.

d. Use o comando **enable** e, em seguida, o comando **configure terminal** para acessar o modo de configuração global.

Para evitar que tráfego HTTP não criptografado passe pelo roteador HQ, os administradores da rede podem criar e implantar ACLs (Access Control Lists, Listas de controle de acesso).

Os comandos a seguir estão além deste curso, mas são usados para demonstrar a habilidade para evitar que tráfego não criptografado passe pelo HQ_Router.

e. No modo de configuração global, **HQ_Router**(config)**#**, copie a configuração de lista de acesso a seguir e cole-a no **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Feche o **HQ_Router**.

Passo 2: Acesse o servidor Web HQ Internet no PC da Sally usando HTTP.

a. No site **Metropolis Bank HQ**, clique no PC **Sally**.

b. Clique na guia **Desktop (Área de Trabalho)** e depois clique em **Web Browser (Navegador Web)**.

c. Digite a URL de **http://www.cisco.corp** e clique em **Go (Ir)**.

O computador de **Sally** consegue acessar o servidor da Web HQ Internet usando HTTP?

Passo 3: Acesse o servidor da Web HQ Internet no PC da Sally usando HTTPS.

a. Acesse o **Navegador da Web** no computador da Sally.

b. Digite a URL de **https://www.cisco.corp** e clique em Go (Ir).

O computador da Sally consegue acessar o servidor da Web HQ Internet usando HTTP?

c. Feche o computador da **Sally**.

Parte 3: Acessar o firewall no servidor de e-mail

a. No site **Metropolis Bank HQ**, clique no servidor de **e-mail**.

b. Clique na guia **Desktop** (Área de Trabalho) e clique em **Firewall**. Não há regras de firewall implementadas.

Para evitar que tráfego não relacionado a e-mail seja enviado ou recebido do servidor de e-mail, os administradores de rede podem criar regras de firewall diretamente no servidor, ou como anteriormente mostrado, eles podem usar ACLs (Access Control Lists, Listas de controle de acesso) em um dispositivo de rede como um roteador.

Pontuação Sugerida

Seção da Atividade	Etapa da Pergunta	Pontos Possíveis	Pontos Obtidos
Parte 1: Conectar-se ao servidor da Web	Etapa 1	15	
	Etapa 2	15	
Parte 2: Impedir sessões HTTP não criptografadas	Etapa 2	15	
	Etapa 3	15	
	Perguntas	**60**	
	Pontuação do Packet Tracer	**40**	
	Pontuação Total	**100**	

