Packet Tracer - Firewalls de Servidor e ACLs de Router

Tabela de Endereçamento

Dispositivo	Endereço IP Privado	Endereço IP Público	Máscara de sub-rede	Local
Servidor Web	N/A	209.165.201.10	255.255.255.0	Internet

Objetivos

Parte 1: Ligação ao Servidor Web

Parte 2: Impedir sessões HTTP não Cifradas

Parte 3: Aceder ao Firewall no Servidor de Email

Contextualização

Nesta atividade, irá aceder a um utilizador dentro do site Metropolis, usando HTTP e HTTPS para se ligar a um servidor Web remoto. O endereçamento IP, a configuração de rede e a configuração do serviço já foram realizados. Utilizará um dispositivo cliente no site Metropolis para testar a conectividade a um servidor Web remoto e, de seguida, proteger o site Metropolis, impedindo que sessões web não cifradas se liguem ao mundo exterior.

Parte 1: Ligação ao Servidor Web

Passo 1: Aceder ao servidor Web HQ Internet no PC da Sally usando HTTP.

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

b. Clique na aba **Desktop** e de seguida clique em **Navegador Web**.

c. Introduza o URL **http://www.cisco.corp** e clique em **Ir**.

d. Clique no link **Página de Login**.

Porque é que um utilizador se deveria preocupar ao enviar informações usando este site?

_____

Passo 2: Aceder ao servidor Web HQ Internet no PC da Sally usando HTTPS.

a. Aceda ao **Navegador Web** no computador da Sally.

b. Introduza o URL **https://www.cisco.corp** e clique em **Ir**.

c. Clique no link **Página de Login**.

Porque que é que um utilizador deve estar menos preocupado ao enviar informações usando este site?

_____

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

Parte 2: Impedir Sessões HTTP Não Cifradas

Passo 1: Configurar o HQ_Router.

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

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

c. Use a palavra-passe **cisco** para entrar no router.

d. Use o comando **enable** e de seguida o comando **configure terminal** para entrar no modo de configuração global.

A fim de impedir que o tráfego HTTP não cifrado viaje através do router HG, os administradores de rede podem criar e distribuir listas de controle de acesso (ACLs).

Os comandos seguintes estão além deste curso, mas são usados para demonstrar a capacidade de impedir que o tráfego não cifrado seja movido através do **HQ_Router**.

e. Dentro do modo de configuração global **HQ_Router(config) #** copie a seguinte configuração da lista de acesso em baixo 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: Aceder ao servidor Web HQ Internet no PC da Sally usando HTTP.

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

b. Clique na aba **Desktop** e de seguida clique em **Navegador Web**.

c. Introduza o URL **http://www.cisco.corp** e clique em **Ir**.

O computador da **Sally** é capaz de aceder ao Servidor Web Internet HQ usando HTTP?

_____

Passo 3: Aceder ao servidor Web HQ Internet no PC da Sally usando HTTPS.

a. Aceda ao **Web Browser** no computador da Sally.

b. Introduza o URL **https://www.cisco.corp** e clique em **Ir**.

O computador da Sally é capaz de aceder ao Servidor Web Internet HQ usando HTTP?

_____

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

Parte 3: Aceder ao Firewall no Servidor de Email

a. Dentro do site **Metropolis Bank HQ**, clique no servidor de **Email**.

b. Clique na aba **Área de Trabalho** e, de seguida, clique em **Firewall**. Não estão implementadas regras de firewall.

A fim impedir que o tráfego não relacionado com tráfego email seja enviado ou recebido do servidor de Email, os administradores de rede podem criar regras do firewall diretamente no server, ou como mostrado antes, podem usar listas de controle de acesso (ACLs) num dispositivo de rede como um router.

Pontuação Sugerida

Secção da Atividade	Localização da Questão	Pontos Possíveis	Pontos Ganhos
Parte 1: Ligação ao Servidor Web	Passo 1	15	
	Passo 2	15	
Parte 2: Impedir Sessões HTTP não Criptografadas	Passo 2	15	
	Passo 3	15	
	Perguntas	**60**	
	Pontuação do Packet Tracer	**40**	
	Pontuação Total	**100**	