

Packet Tracer - Configurar Senhas Seguras e SSH

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
RTA	G0/0	172.16.1.1	255.255.255.0	N/D
PCA	Placa de rede	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Cenário

O administrador de redes pediu que você prepare o **RTA** e **SW1** para implantação. Antes de conectá-lo à rede, você deve ativar medidas de segurança.

Intrusões

Etapa 1: Implementar as Medidas Básicas de Segurança no Roteador

- a. Configure o endereçamento IP em **PCA** de acordo com a Tabela de Endereçamento.
- b. Acesse o console de [[R1Name]] com o terminal em PC-A.
- c. Configure o nome do host como **RTA**.
- d. Configure o endereçamento IP em **RTA** e ative a interface.
- e. Criptografe todas as senhas em texto simples.

```
RTA(config)# service password-encryption
```

- f. Configure o comprimento mínimo para senhas para 10

```
RTA(config)# security passwords min-length 10
```

- g. Configure uma senha secreta forte de sua escolha. **Observação:** escolha uma senha que você se lembre ou você precisará redefinir a atividade se estiver bloqueado no dispositivo.

- h. Desative a pesquisa de DNS.

```
RTA(config)#no ip domain-lookup
```

- i. Configure o nome de domínio como **CCNA.com** (diferencie maiúsculas e minúsculas para pontuar no PT).

```
RTA(config)# ip domain-name CCNA.com
```

- j. Crie um usuário da escolha com uma senha forte.

```
RTA (config) # nome de usuário any_user secret any_password
```

- k. Gere chaves RSA de 1024 bits.

Observação: no Packet Tracer, insira o comando crypto key generate rsa, e pressione Enter para continuar.

```
RTA(config)# crypto key generate rsa
```

O nome para as chaves será: **RTA.CCNA.com**

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: **1024**

- I. Bloqueie durante três minutos qualquer pessoa que não conseguiu fazer log in depois de quatro tentativas em um período de dois minutos.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

- m. Configure as linhas VTY para o acesso por SSH e use os perfis locais de usuário local para autenticação.

```
RTA (configuração) # linha vty 0 4
RTA(config-line)# transport input ssh
R1(config-line)# login local
```

- n. Defina o tempo limite do modo EXEC para 6 minutos nas linhas VTY.

```
RTA(config-line)# exec-timeout 6
```

- o. Salve a configuração na NVRAM.

- p. Acesse o prompt de comando na área de trabalho do **PCA** para estabelecer uma conexão SSH com o **RTA**.

```
C:\ > ssh/?
Packet Tracer PC SSH
Uso: SSH -l username target
C:\ >
```

Etapa 2: Implementar as Medidas Básicas de Segurança no Switch

Configure o switch **SW1** com as medidas de segurança correspondentes. Consulte as etapas de configuração no roteador se precisar de assistência adicional.

- a. Clique em **SW1** e selecione a guia **CLI**.
- b. Configure o nome de host como **SW1**.
- c. Configure o endereçamento IP em **SW1 VLAN1** e ative a interface.
- d. Configure o endereço de gateway padrão.
- e. Desative todas as portas não utilizadas.

Observação: Em um switch, é uma boa prática de segurança desabilitar portas não utilizadas. Um método para fazer isso é simplesmente desligar cada porta com o comando '**shutdown**'. Isso exigiria acessar cada porta individualmente. Existe um método de atalho para fazer modificações em várias portas ao mesmo tempo usando o **comando interface range**. No **SW1**, todas as portas, exceto FastEtherNet0/1 e GigabitEthernet0/1, podem ser desativadas com o seguinte comando:

```
SW1(config)# interface range F0/2-24, G0/2
SW1 (config-if-range) # shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
<Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
```

O comando usou o intervalo de portas de 2-24 para as portas FastEthernet e, em seguida, um único intervalo de porta de GigabitEtherNet0/2.

- f. Criptografe todas as senhas em texto simples.
- g. Configure uma senha secreta forte de sua escolha.
- h. Desative a pesquisa de DNS.
- i. Configure o nome de domínio como **CCNA.com** (diferencie maiúsculas e minúsculas para pontuar no PT).
- j. Crie um usuário da escolha com uma senha forte.
- k. Gere chaves RSA de 1024 bits.
- l. Configure as linhas VTY para o acesso por SSH e use os perfis locais de usuário local para autenticação.
- m. Defina o tempo limite do modo EXEC para 6 minutos em todas as linhas VTY.
- n. Salve a configuração na NVRAM.