Packet Tracer - Configurar Senhas Seguras e SSH (Versão do Instrutor)

**Nota do Instrutor**: Cor vermelha da fonte ou realces em cinza indicam o texto que aparece apenas na cópia do instrutor.

# 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

## Implementar as Medidas Básicas de Segurança no Roteador

Abra um prompt de comando

* + 1. Configurae o endereçamento IP em **PCA** de acordo com a Tabela de Endereçamento.

Feche um prompt de comando

Abrir a janela de configuração

* + 1. ·        Acesse o console de [[R1Name]] com o terminal em PC-A.
    2. Configure o nome do host como **RTA**.
    3. Configure o endereçamento IP em **RTA** e ative a interface.
    4. Criptografe todas as senhas em texto simples.

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

* + 1. Configure o comprimento mínimo para senhas para 10

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

* + 1. 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.
    2. Desative a pesquisa de DNS.

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

* + 1. Configure o nome de domínio como **CCNA.com** (diferencie maiúsculas e minúsculas para pontuar no PT).

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

* + 1. Crie um usuário da escolha com uma senha forte.

RTA (config) # **nome de usuário *any\_user* secret *any\_password***

* + 1. 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**

* + 1. 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**

* + 1. 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**

* + 1. Defina o tempo limite do modo EXEC para 6 minutos nas linhas VTY.

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

* + 1. Salve a configuração na NVRAM.

Fechar janela de configuração

* + 1. Acesse o prompt de comando na área de trabalho do **PCA** para estabelecer uma conexão SSH com o **RTA** .

Abra um prompt de comando

C:\ > **ssh/?**

Packet Tracer PC SSH

Uso: **SSH -l username target**

C:\ >

Feche um prompt de comando

## 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.

* + 1. Clique em **SW1** e selecione a guia **CLI**.

Abra uma janela de configuração

* + 1. Configure o nome de host como **SW1**.
    2. Configure o endereçamento IP em SW1 **VLAN1** e ative a interface.
    3. Configure o endereço de gateway padrão.
    4. 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.

* + 1. Criptografe todas as senhas em texto simples.
    2. Configure uma senha secreta forte de sua escolha.
    3. Desative a pesquisa de DNS.
    4. Configure o nome de domínio como **CCNA.com** (diferencie maiúsculas e minúsculas para pontuar no PT).
    5. Crie um usuário da escolha com uma senha forte.
    6. Gere chaves RSA de 1024 bits.
    7. Configure as linhas VTY para o acesso por SSH e use os perfis locais de usuário local para autenticação.
    8. Defina o tempo limite do modo EXEC para 6 minutos em todas as linhas VTY.
    9. Salve a configuração na NVRAM.

Fechar uma janela de configuração

Fim do documento