Packet Tracer - Configurar AAA Local para Console e Acesso VTY

.

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão	Porta do Switch
R1	G0/1	192.168.1.1	255.255.255.0	N/D	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/D	N/D
R2	G0/0	192.168.2.1	255.255.255.0	N/D	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/D	N/D
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/D	N/D
R3	G0/1	192.168.3.1	255.255.255.0	N/D	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/D	N/D
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objetivos

- Configurar uma conta de usuário local no R1 e configurar autenticar no console e nas linhas vty usando o AAA local.
- Verifique a autenticação AAA local do console R1 e do cliente PC-A.

Histórico/Cenário

A topologia de rede mostra os roteadores R1, R2 e R3. Atualmente, toda a segurança administrativa é baseada no conhecimento da senha secreta de habilitação. Sua tarefa é configurar e testar soluções AAA locais e baseadas em servidor.

Você criará uma conta de usuário local e configurará o AAA local no roteador R1 para testar os logins do console e do vty.

- Conta de usuário: **Admin1** e senha **admin1pa55**

Os roteadores também foram pré-configurados com o seguinte:

- Enable secret password: **ciscoenpa55**
- Protocolo de roteamento OSPF com autenticação MD5 usando senha: **MD5pa55**

Nota: O console e as linhas vty não foram pré-configuradas.

Nota: As imagens IOS mais novas usam o algoritmo de hashing de criptografia mais seguro; contudo, a versão IOS apoiada atualmente no Packet Tracer usa MD5. Use sempre a opção mais segura disponível no seu equipamento físico.

Parte 1: Configurar a autenticação AAA local para o acesso de console no R1

Etapa 1: Configure um nome de usuário local em R1.

Configurar um nome de usuário de **Admin1** com uma senha secreta de **admin1pa55**.

Etapa 2: Configurar a autenticação AAA local para o acesso de console no R1.

Permita o AAA no R1 e configure a autenticação AAA para que o início de uma sessão do console use o base de dados local.

Etapa 3: Configurar o console de linha para usar o método de autenticação AAA definido.

Permita o AAA no **R1** e configure a autenticação AAA para que o início de uma sessão do console use a lista de métodos padrão.

Etapa 4: Verify the AAA authentication method.

Verifique o login EXEC do usuário usando o banco de dados local.

Parte 2: Configurar a autenticação AAA local para linhas vty no R1

Etapa 1: Configurar o nome de domínio e a chave de criptografia para uso com SSH.

a. Use **netsec.com** como o nome de domínio no R1.

b. Create an RSA crypto key using 1024 bits.

Etapa 2: Configurar um método de autenticação AAA da lista nomeada para as linhas vty no R1.

Configurar uma lista nomeada chamada **SSH-LOGIN** para autenticar logins usando AAA local.

Etapa 3: Configurar as linhas vty para usar o método de autenticação AAA definido.

Configurar as linhas vty para usar o método AAA nomeado e permitir somente o SSH para o acesso remoto.

Etapa 4: Verifique o método de autenticação AAA.

Verifique a configuração SSH SSH ao **R1** do prompt de comando do **PC-A**.

```
PC> ssh –l Admin1 192.168.1.1
Aberto(s)
Password: admin1pa55
```

