Laboratório - Configurar dispositivos de rede com SSH

Topologia

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de Sub-Rede	Gateway padrão
R1	G0/0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Implementar as Configurações Básicas dos Dispositivos

Parte 2: Configurar o Roteador para o Acesso SSH

Parte 3: Configurar o Switch para o Acesso SSH

Parte 4: SSH da CLI no Switch

Histórico/cenário

No passado, o Telnet era o protocolo de rede mais comum usado para configurar remotamente dispositivos de rede. O Telnet não autentica ou criptografa as informações entre o cliente e o servidor. Isso permite que um sniffer de rede intercepte senhas e informações de configuração.

O Shell Seguro (SSH) é um protocolo de rede que estabelece uma conexão segura de emulação de terminal para um roteador ou outro dispositivo de rede. O SSH criptografa todas as informações que passam no link de rede e fornece autenticação do computador remoto. O SSH está substituindo rapidamente o Telnet como ferramenta de login remoto favorita dos profissionais de rede. SSH é mais frequentemente usado para fazer login em um dispositivo remoto e executar comandos. No entanto, também pode transferir arquivos usando os protocolos Secure FTP (SFTP) ou Secure Copy (SCP) associados.

Os dispositivos de rede que se comunicam devem ser configurados para suportar o SSH, para que ele funcione. Neste laboratório, você ativará o servidor SSH em um roteador e conectará ao roteador usando um computador com um cliente SSH instalado. Em uma rede local, a conexão é feita normalmente usando Ethernet e IP.

Nota: Os roteadores usados com laboratórios hands-on são Cisco 4221 com o Cisco Ios Xe Release 16.9.6 (imagem universalk9). Os switches usados nos laboratórios são Cisco Catalyst 2960 com a versão Cisco IOS 15.2 (7) (imagem lanbasek9). Outros roteadores, switches e versões do Cisco IOS podem ser usados. De acordo com o modelo e a versão do Cisco IOS, os comandos disponíveis e a saída produzida poderão variar em relação ao que é mostrado nos laboratórios. Consulte a Tabela de resumo de interfaces dos roteadores no final do laboratório para saber quais são os identificadores de interface corretos.

Nota: Verifique se os roteadores e comutadores foram apagados e se não há configurações de inicialização. Se tiver dúvidas, fale com o instrutor.

Recursos necessários

- 1 roteador (Cisco 4221 com a Liberação Cisco Xe 16.9.6 Imagem universal ou comparável com uma licença de pacote de tecnologia de segurança)
- 1 switch(Cisco 2960+ com a versão do Cisco IOS 15.2 (7) Imagem lanbasek9 ou comparável)
- 1 PC (SO Windows com um programa de emulação de terminal, como Tera Term ou PuTTy instalado)
- Cabos de console para configurar os dispositivos Cisco IOS
- Cabos ethernet conforme mostrado na topologia

Instruções

Parte 1: Implementar as Configurações Básicas do Dispositivo

Na Parte 1, você vai configurar a topologia de rede e definir as configurações básicas, como os endereços IP das interfaces, o acesso a dispositivos e as senhas no roteador.

Etapa 1: Instalar os cabos da rede conforme mostrado na topologia.

Etapa 2: Inicializar e recarregar o roteador e o switch.

Etapa 3: Configurar o roteador.

a. Use o console para se conectar ao roteador e ative o modo EXEC privilegiado.

b. Entre no modo de configuração.

c. Desative a pesquisa do DNS para evitar que o roteador tente converter comandos inseridos incorretamente como se fossem nomes de host.

d. Atribua **class** como a senha criptografada EXEC privilegiada usando o algoritmo de hash tipo 8 (PBKDF2).

e. Atribua **cisco** como a senha de console e habilite o login.

f. Atribua **cisco** como a senha VTY e ative o login.

g. Criptografe as senhas de texto sem formatação.

h. Crie um banner que avisará a qualquer pessoa que acessa o dispositivo que o acesso não autorizado é proibido.

i. Configure e ative a interface G0/0/1 no roteador usando as informações contidas na Tabela de Endereçamento.

j. Salve a configuração atual no arquivo de configuração inicial.

Etapa 4: Configure o PC-A.

a. Configure o PC-A com um endereço IP e uma máscara de sub-rede.

b. Configure um gateway padrão para o PC-A.

Etapa 5: Verificar a conectividade de rede.

Faça ping em R1 do PC-A. Se o ping falhar, solucione os problemas da conexão.

Parte 2: Configurar o Roteador para o Acesso SSH

Usar o Telnet para conectar-se a um dispositivo de rede é um risco à segurança, porque todas as informações são transmitidas em um formato de texto não criptografado. SSH criptografa os dados da sessão e fornece autenticação do dispositivo; Portanto, o SSH é recomendado para conexões remotas. Na Parte 2, você configurará o roteador para aceitar conexões SSH nas linhas VTY.

Etapa 1: Configurar a autenticação do dispositivo.

O nome do dispositivo e o domínio são usados como a parte da chave criptografada quando gerada. Portanto, esses nomes devem ser inseridos antes da emissão do comando de **crypto key**.

a. Configure o nome do dispositivo.

b. Configure o domínio do dispositivo.

Etapa 2: Configure o método de chave de criptografia.

Etapa 3: Configure um nome de usuário no banco de dados local.

a. Configure um nome de usuário usando o **admin** como o nome de usuário e o **Adm1nP@55** como a senha usando o algoritmo de hash do tipo 8 (PBKDF2).

Etapa 4: Habilitar o SSH nas linhas VTY.

a. Ative o SSH nas linhas vintas de entrada usando o comando **transport input**.

b. Altere o método de login para usar o banco de dados local para a verificação de usuário.

Etapa 5: Salve a configuração atual no arquivo de configuração inicial.

Etapa 6: Estabelecer uma conexão SSH para o roteador.

a. Inicie o Tera Term do PC-A.

b. Estabeleça uma sessão SSH com o R1. Use o nome de usuário **admin** e a senha **Adm1nP@55**. Você deve conseguir estabelecer uma sessão SSH com R1.

Parte 3: Configurar o Switch para o Acesso SSH

Na parte 3, você configurará o comutador para aceitar conexões SSH. Depois que o switch tiver sido configurado, estabeleça uma sessão SSH usando o Tera Term.

Etapa 1: Implementar as configurações básicas no switch.

a. Use o console para se conectar ao switch e ative o modo EXEC privilegiado.

b. Entre no modo de configuração.

c. Desative a pesquisa do DNS para evitar que o roteador tente converter comandos inseridos incorretamente como se fossem nomes de host.

d. Atribua **class** como a senha criptografada EXEC privilegiada usando o algoritmo de hash tipo 8 (PBKDF2).

e. Atribua **cisco** como a senha de console e habilite o login.

f. Atribua **cisco** como a senha VTY e ative o login.

g. Criptografe as senhas de texto simples.

h. Crie um banner que avisará a qualquer pessoa que acessa o dispositivo que o acesso não autorizado é proibido.

i. Configure e ative a interface VLAN 1 no switch de acordo com a Tabela de Endereçamento.

j. Salve a configuração atual no arquivo de configuração inicial.

Etapa 2: Configurar o switch para a conectividade SSH.

Utilize os mesmos comandos usados para configurar o SSH no roteador na Parte 2 para configurar o SSH para o switch.

a. Configure o nome do dispositivo conforme listado na Tabela de Endereçamento.

b. Configure o domínio do dispositivo.

c. Configure o método de chave de criptografia.

d. Configure um nome de usuário de banco de dados local usando o algoritmo de hash tipo 8 (PBKDF2).

e. Habilite o Telnet e o SSH nas linhas VTY.

f. Altere o método de login para usar o banco de dados local para a verificação de usuário.

Etapa 3: Estabelecer uma conexão SSH com o switch.

Inicie o Tera Term no PC-A, e o SSH na interface SVI de S1.

Você consegue estabelecer uma sessão SSH com o switch?

Sim. O SSH pode ser configurado em um switch usando os mesmos comandos que foram usados no roteador.

Parte 4: SSH da CLI no Switch

O cliente SSH é incorporado ao Cisco IOS e pode ser executado na CLI. Na Parte 4, você fará SSH para o roteador na CLI do switch.

Etapa 1: Exibir os parâmetros disponíveis para o cliente SSH do Cisco IOS.

Use o ponto de interrogação**(?)**Para exibir as opções de parâmetros disponíveis com o comando **ssh**.

```
S1# ssh ?
  -c Selecionar algoritmo de criptografia
  -l Iniciar sessão com este nome de utilizador
  -m Selecionar algoritmo HMAC
  -o Especificar opções
  -p Conectar a esta porta
  -v Especificar a versão do protocolo SSH
  -vrf Especificar o nome do vrf
  Endereço IP WORD ou nome de host de um sistema remoto
```

Etapa 2: SSH para R1 de S1.

a. Você deve usar a opção **–l admin** ao fazer o SSH para R1. Isso permite que você efetue login como usuário **admin**. Quando solicitado, digite **Adm1nP@55** para a senha.

```
S1# ssh -l admin 192.168.1.1
Senha:
Somente Usuários Autorizados!
R1>
```

b. Você pode retornar ao S1 sem fechar a sessão SSH para R1 pressionando **Ctrl**+**Shift**+**6**. Solte as teclas **Ctrl**+**Shift**+**6** e pressione **x**. O prompt do EXEC privilegiado do switch é exibido.

```
R1>
```



```
S1#
```

c. Para retornar à sessão SSH em R1, pressione Enter em uma linha CLI em branco. Pode ser necessário pressionar Enter uma segunda vez para ver o prompt CLI do roteador.

```
S1#
[Retomando a conexão 1 a 192.168.1.1... ]

R1>
```

d. Para finalizar a sessão SSH em R1, digite **exit** no prompt do roteador.

```
R1#exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Que versões de SSH são compatíveis com a CLI?

Perguntas para reflexão

Como você concederia acesso a um dispositivo de rede para vários usuários, cada um com seu próprio nome de usuário?

Tabela de Resumo das Interfaces dos Roteadores

Modelo do roteador	Interface Ethernet 1	Interface Ethernet 2	Interface serial 1	Interface serial 2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Nota: Para descobrir como o roteador está configurado, consulte as interfaces para identificar o tipo de roteador e quantas interfaces o roteador possui. Não há como listar efetivamente todas as combinações de configurações para cada classe de roteador. Esta tabela inclui identificadores para as combinações possíveis de Ethernet e Interfaces seriais no dispositivo. Esse tabela não inclui nenhum outro tipo de interface, embora um roteador específico possa conter algum. Um exemplo disso poderia ser uma interface ISDN BRI. O string entre parênteses é a abreviatura legal que pode ser usada em comandos do Cisco IOS para representar a interface.