Configurar Telnet, console e senhas de porta AUX em roteadores

Contents

Introduction

Esse documento fornece exemplos de configuração de proteção por senha para conexões EXEC de entrada, no roteador.

Prerequisites

Requirements

Para executar as tarefas descritas neste documento, você deve ter acesso EXEC privilegiado à Interface de Linha de Comando (CLI) do roteador. Para obter informações sobre como usar a linha de comando e entender os modos de comando, consulte Usando a Interface de Linha de Comando do Cisco IOS.

Para instruções sobre como conectar um console ao seu roteador, consulte a documentação que acompanha o roteador ou a documentação on-line para o seu equipamento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco 2509
- Cisco IOS® Software Versão 12.2(19)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

A utilização de proteção por senha para controlar ou restringir o acesso à interface à Interface de linha de comando (CLI) do roteador é um dos elementos fundamentais de um plano completo de segurança.

Proteger o roteador contra acesso remoto não autorizado, normalmente Telnet, é o aspecto de segurança mais comum que precisa de configuração, mas a proteção do roteador contra acesso local não autorizado também não pode ser negligenciada.

Observação: a proteção por senha é apenas uma das muitas etapas que você deve usar em um regime de segurança de rede eficaz e detalhado. Firewalls, listas de acesso e controle de acesso físico ao equipamento são outros elementos que devem ser considerados ao implementar seu plano de segurança.

O acesso de linha de comando ou EXEC a um roteador pode ser feito de diversas maneiras, mas em todos os casos a conexão de entrada para o roteador é feita em uma linha de TTY. Existem quatro tipos principais de linhas TTY, como pode ser visto neste exemplo de saída de show line:

```
2509#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY               -    -      -    -    -      0       0     0/0       -
     1 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     2 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     3 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     4 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     5 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     6 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     7 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     8 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     9 AUX   9600/9600   -    -      -    -    -      0       0     0/0       -
    10 VTY               -    -      -    -    -      0       0     0/0       -
    11 VTY               -    -      -    -    -      0       0     0/0       -
    12 VTY               -    -      -    -    -      0       0     0/0       -
    13 VTY               -    -      -    -    -      0       0     0/0       -
    14 VTY               -    -      -    -    -      0       0     0/0       -

2509#
```

O tipo de linha CTY é a porta do console. Em qualquer roteador, ela aparece na configuração do

roteador como line con 0 e na saída do comando show line como ctv. A porta do console é utilizada principalmente para acesso de sistema local, utilizando um terminal de console.

As linhas TTY são linhas assíncronas usadas para modems internos ou externos e conexões de terminal e podem ser vistas na configuração de um roteador ou servidor de acessos como linhas x. Os números de linha específicos são uma função de hardware incorporada ou instalada no roteador ou servidor de acesso.

A linha **AUX é a porta auxiliar, vista na configuração como line aux 0**.

As linhas **VTY são as linhas de Terminal virtual do roteador, usadas unicamente para controlar as conexões Telnet de entrada.** Elas são virtuais, pois são uma função do software - não há nenhum hardware associado a elas. Elas aparecem na configuração como a linha vty 0 4.

Cada um desses tipos de linha pode ser configurado com proteção de senha. As linhas podem ser configuradas para usar uma senha para todos os usuários ou para utilizar senhas específicas de usuários. As senhas específicas ao usuário podem ser configuradas localmente no roteador, ou você pode fornecer autenticação.usando um servidor de autenticação.

Não há nenhuma proibição contra a configuração de linhas diferentes com diferentes tipos de proteção de senha. Na verdade, é comum ver roteadores com uma única senha para o console e senhas de usuário específicas para outras conexões de entrada.

Abaixo há um exemplo de saída de roteador do comando running-config:

```
2509#show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

Configurar senhas na linha

Para especificar uma senha em uma linha, use o comando password no modo de configuração de linha. Para habilitar a verificação de senha no login, use o comando de login no modo configuração de linha.

Procedimento de configuração

Nesse exemplo, uma senha é configurada para todos os usuários que tentam usar o console.

1. A partir do prompt EXEC (ou "enable") privilegiado, entre no modo de configuração e, em seguida, mude para o modo de configuração de linha, usando os seguintes comandos. Observe que o prompt é alterado para refletir o modo atual.
   ```
   router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#line con 0
   router(config-line)#
   ```

2. Configure a senha e habilite a verificação de senha no login.
```
router(config-line)#password letmein
router(config-line)#login
```

3. Sair do modo de configuração.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
Observação: não salve as alterações de configuração no **line con 0** até que sua capacidade de fazer login tenha sido verificada.

Observação: na configuração do console de linha, **login** é um comando de configuração necessário para ativar a verificação de senha no login. A autenticação de console exige os comandos **password e login funcionem.**

Verificar a configuração

Examine a configuração do roteador para verificar se os comandos foram digitados corretamente:

- **show running-config – Exibe a configuração atual do roteador.**
```
router#show running-config
Building configuration...
...
!--- Lines omitted for brevity ! line con 0 password letmein
login
line 1 8
line aux 0
line vty 0 4
!
end
```
Para testar a configuração, desconecte o console e conecte-o novamente, usando a senha configurada para acessar o roteador.
```
router#exit

router con0 is now available

Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```
Observação: antes de executar este teste, verifique se você tem uma conexão alternativa no roteador, como Telnet ou dial-in, caso haja um problema ao fazer login novamente no roteador.

Solução de problemas de falha de login

Se você não conseguir efetuar login de volta no roteador e não tiver salvado a configuração, o recarregamento do roteador eliminará as alterações feitas nessa configuração.

Se as alterações de configuração forem salvas e não for possível acessar o roteador, você terá que executar uma recuperação de senha. Consulte Password Recovery Procedures (Procedimentos de recuperação de senha) para obter instruções sobre a sua plataforma específica.

Configure senhas específicas de usuário local

Para estabelecer um sistema de autenticação com base em nome de usuário, utilize o comando username no modo de configuração global. Para habilitar a verificação de senha no login, use o comando login local no modo de configuração de linha.

Procedimento de configuração

Nesse exemplo, as senhas são configuradas para usuários que tentam se conectar ao roteador nas linhas VTY usando o Telnet.

1. No prompt EXEC (ou "ativar") privilegiado, entre no modo de configuração e digite as combinações de nome de usuário/senha, uma para cada usuário com permissão de acesso ao roteador:
```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#username russ password montecito
router(config)#username cindy password belgium
router(config)#username mike password rottweiler
```

2. Comute para o modo de configuração usando os seguintes comandos. Observe que o prompt é alterado para refletir o modo atual.
```
router(config)#line vty 0 4
router(config-line)#
```
3. Configure a verificação de senha no login.
```
router(config-line)#login local
```

4. Sair do modo de configuração.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
Observação: para desabilitar o Telnet automático quando você digita um nome na CLI, configure **nenhum registro preferido** na linha usada. Embora **transport preferred none forneça a mesma saída, também desativa o Telnet automático para o host definido configurado com o comando ip host .** Essa opção é diferente do comando **no logging preferred, que para em hosts indefinidos e permite que ele funcione nos definidos.**

Verificar a configuração

Examine a configuração do roteador para verificar se os comandos foram digitados corretamente:

- **show running-config – Exibe a configuração atual do roteador.**
```
router#show running-config
Building configuration...
!
!--- Lines omitted for brevity ! username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
!
end
```

Para testar essa configuração, faça uma conexão Telnet ao roteador. Isso pode ser feito conectando a partir de um host diferente na rede, mas também é possível testar a partir do próprio roteador realizando um Telnet para o endereço IP de qualquer interface no roteador que esteja em um estado up/up, conforme visto na saída do comando show interfaces.Veja abaixo um exemplo no qual o endereço da interface ethernet 0 é 10.1.1.1:

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open


User Access Verification


Username: mike
Password:
!--- Password entered here is not displayed by the router router
```

Solucione problemas de falha de senha específicas do usuário

Os nomes de usuários e as senhas fazem distinção entre maiúsculas e minúsculas. Os usuários que tentarem efetuar logon com um nome de usuário ou senha armazenada incorretamente serão recusados.

Se os usuários não puderem fazer login no roteador com suas senhas específicas, reconfigure o nome de usuário e a senha no roteador.

Configurar a senha de linha AUX

Para especificar uma senha na linha AUX, emita o **comando password no modo de configuração de linha.** Para habilitar a verificação de senha no início da sessão, execute o **comando login no modo de configuração de linha.**

Procedimento de configuração

Neste exemplo, uma senha é configurada para todos os usuários que tentam usar a porta AUX.

1. Emita o **comando show line para verificar a linha usada pela porta AUX.**

```
R1#show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                   -    -     -    -    -     0      0     0/0       -
    65 AUX  9600/9600    -    -     -    -    -    0     1     0/0             -
    66 VTY                  -    -     -    -    -     0      0     0/0       -
    67 VTY                  -    -     -    -    -     0      0     0/0       -
```

2. Neste exemplo, a porta AUX é na linha 65. Execute estes comandos para configurar a linha AUX do roteador:

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

Verifique a configuração

Examine a configuração do roteador para verificar se os comandos foram inseridos corretamente:

- O **comando show running-config exibe a configuração atual do roteador:**

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

Configurar autenticação AAA para logon

Para habilitar a autenticação AAA (autenticação, autorização e relatório) para logons, use o comando login authentication no modo de configuração de linha. Os serviços AAA também devem ser configurados.

Procedimento de configuração

Nesse exemplo, o roteador está configurado para recuperar as senhas dos usuários de um servidor TACACS+ quando os usuários tentam se conectar ao roteador.

Observação: configurar o roteador para usar outros tipos de servidores AAA (RADIUS, por exemplo) é semelhante. Consulte Configuração da Autenticação para obter informações adicionais.

Observação: este documento não aborda a configuração do próprio servidor AAA.

1. A partir do prompt EXEC privilegiado (ou de "habilitar"), insira o modo de configuração e informe os comandos para configurar o roteador de forma a usar os serviços AAA para autenticação:

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. Comute para o modo de configuração de linha usando os seguintes comandos. Observe que o prompt é alterado para refletir o modo atual.

```
router(config)#line 1 8
router(config-line)#
```

3. Configure a verificação de senha no login.

```
router(config-line)#login authentication my-auth-list
```

4. Sair do modo de configuração.

```
router(config-line)#end
```

```
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Verificar a configuração

Examine a configuração do roteador para verificar se os comandos foram digitados corretamente:

- **show running-config – Exibe a configuração atual do roteador.**

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
 login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

Para testar essa configuração específica, uma conexão de entrada ou saída deve ser feita para a linha. Consulte Modem Guia de conexão do roteador para obter informações especificas sobre configuração de linhas assíncronas para conexões de modem.

Como alternativa, você pode configurar uma ou mais linhas VTY para executar a autenticação AAA e seus testes posteriores.

Solução de problema de falha no início de sessão de AAA

Antes de emitir comandos debug, consulte Informações importantes sobre comandos debug.

Para solucionar uma tentativa de login com falha, use o comando de depuração apropriado para a sua configuração:

- debug aaa authentication
- debug radius
- debug kerberos

Informações Relacionadas

- Referência de debug command do Cisco IOS
- Suporte Técnico - Cisco Systems