# PIX/ASA 7.x: Exemplo de Configuração de SSH/Telnet nas Interfaces Interna e Externa

## Índice



## Introdução

Este documento fornece um exemplo de configuração do Secure Shell (SSH) nas interfaces interna e externa do Cisco Series Security Appliance versão 7.x. A configuração remota do Security Appliance com a linha de comando envolve a utilização do Telnet ou do SSH. Como as comunicações de Telnet são enviadas em texto não criptografado, incluindo as senhas, o uso do SSH é altamente recomendável. O tráfego de SSH é criptografado em um túnel, o que ajuda a proteger as senhas e outros comandos de configuração contra a interceptação.

O Security Appliance permite conexões de SSH para fins de gerenciamento. O Security Appliance permite um máximo de cinco conexões de SSH simultâneas para cada contexto de segurança, se estiverem disponíveis, e um máximo global de 100 conexões para todos os contextos combinados.

Neste exemplo de configuração, o PIX Security Appliance é considerado como sendo o servidor SSH. O tráfego dos clientes SSH (10.1.1.2/24 e 172.16.1.1/16) até o servidor SSH é criptografado. O Security Appliance oferece suporte à funcionalidade de shell remoto SSH fornecida com as versões 1 e 2 do SSH e aos padrões de criptografia Data Encryption Standard (DES) e 3DES. As versões 1 e 2 do SSH são diferentes e não são interoperáveis.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações deste documento são baseadas no Cisco PIX Firewall Software Versão 7.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração padrão. Se a sua rede estiver em um ambiente de produção, esteja ciente do impacto potencial de qualquer comando.

### Produtos Relacionados

Esta configuração também pode ser utilizada com o Cisco ASA 5500 Series Security Appliance.

### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Configuração

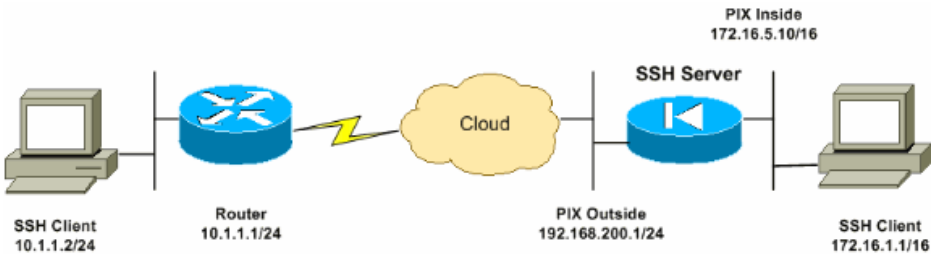
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Cada passo de configuração é apresentado com as informações necessárias para a utilização da linha de comando ou do Adaptive Security Device Manager (ASDM).

**Nota:** Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento usa esta configuração de rede:




## Configurações do SSH

Este documento utiliza estas configurações:

- Acesso de SSH ao Security Appliance
- Como Utilizar um Cliente SSH
- Configuração do PIX

### Acesso de SSH ao Security Appliance

Execute estes passos para configurar o acesso de SSH ao Security Appliance:

1. As sessões de SSH sempre necessitam de um nome de usuário e de uma senha para autenticação. Há duas maneiras de atender a este requisito:

   Configure um nome de usuário e uma senha e utilize o AAA:

   Sintaxe:

   ```
   pix(config)#username username password password

   pix(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL |
   server_group [LOCAL]}
   ```

   **Nota:** Se você usa um grupo de servidores TACACS+ ou RADIUS para a autenticação, é possível configurar o Security Appliance para usar o banco de dados local como método de fallback quando o servidor AAA não está disponível. Especifique o nome do grupo de servidores seguido por LOCAL (LOCAL diferencia maiúsculas de minúsculas). Recomendamos que você use no banco de dados local os mesmos nome de usuário e senha usados no servidor AAA porque o prompt do Security Appliance não fornece nenhuma indicação do método que é usado.

   **Nota:** Exemplo :

   ```
   pix(config)#aaa authentication ssh console TACACS+ LOCAL
   ```

   **Nota:** Você pode, de forma alternativa, utilizar o banco de dados local como método principal de autenticação sem fallback. Para fazer isso, insira LOCAL somente.

   Exemplo:

   ```
   pix(config)#aaa authentication ssh console LOCAL
   ```

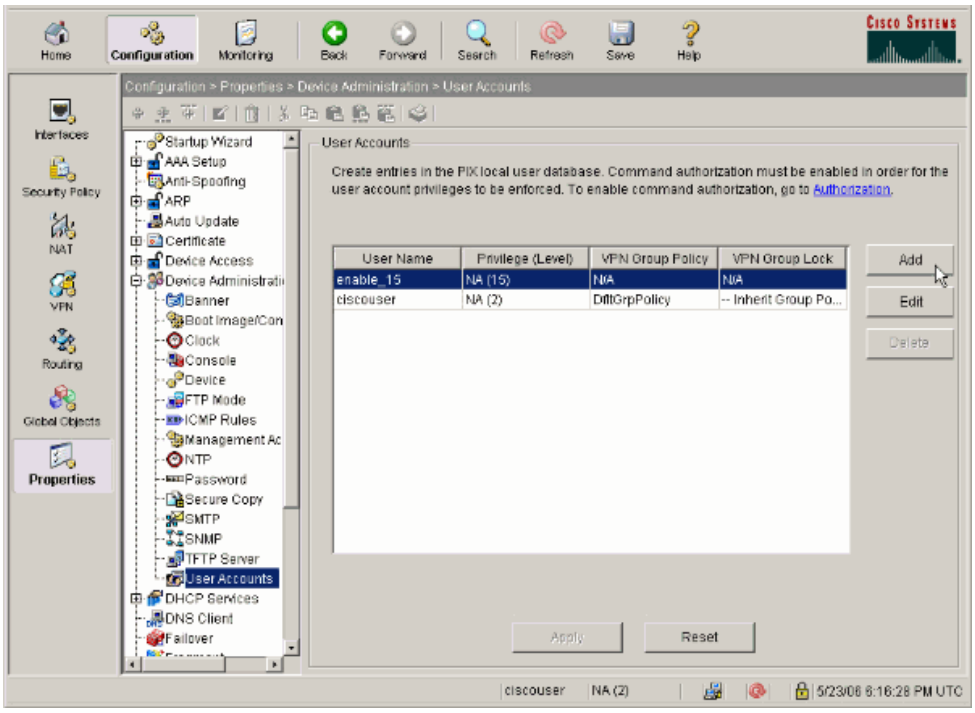
   **OU**

Use o nome de usuário padrão **pix** e a senha de Telnet padrão **cisco**. Você pode alterar a senha de Telnet com este comando:

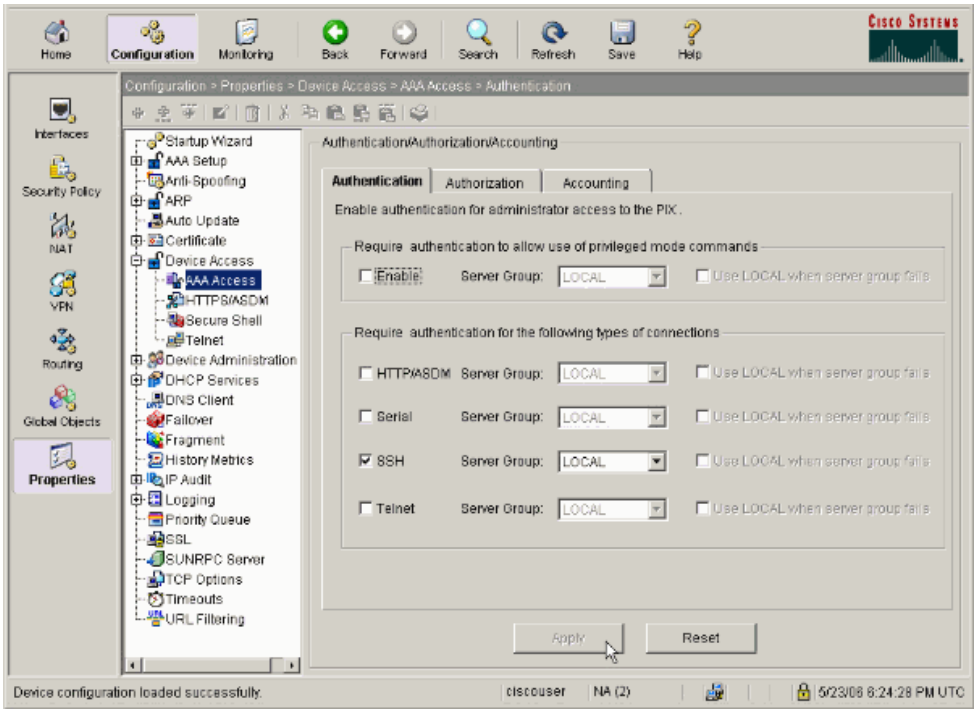
```
pix(config)#passwd password
```

**Nota:** O comando **password** também pode ser utilizado nessa situação. Ambos os comandos fazem a mesma coisa.

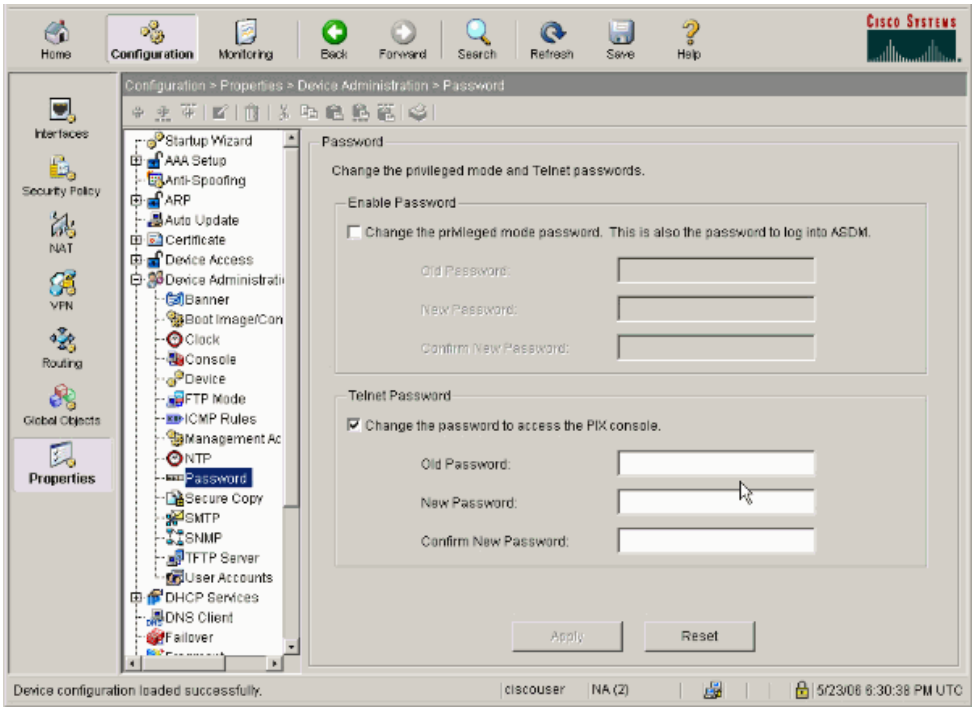
Selecione **Configuration > Properties > Device Administration > User Accounts** para adicionar um usuário com o ASDM.




Selecione **Configuration > Properties > Device Access > AAA Access > Authentication** para definir a autenticação AAA para o SSH com o ASDM.




Selecione **Configuration > Properties > Device Administration > Password** para alterar a senha de Telnet com o ASDM.



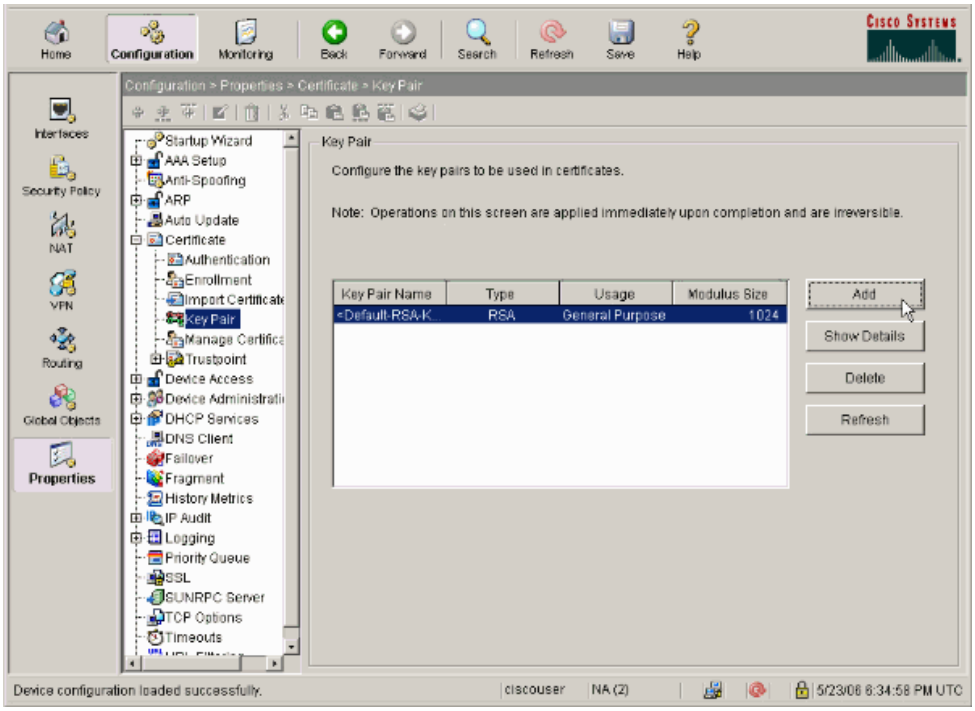

2. Gere um par de chaves de RSA para o PIX Firewall, o qual é necessário para o SSH.

```
pix(config)#crypto key generate rsa modulus modulus_size
```

**Nota:** O `modulus_size` (em bits) pode ser de 512, 768, 1024 ou 2048. Quanto maior o tamanho do módulo da chave especificado, mais tempo será necessário para a geração do par de chaves de RSA. O valor 1024 é o recomendado.

**Nota:** O comando utilizado para gerar um par de chaves de RSA é diferente nas versões de software do PIX anteriores à 7.x. Nas versões anteriores, um nome de domínio deve ser definido antes que as chaves possam ser criadas.

Selecione **Configuration > Properties > Certificate > Key Pair**, clique em **Add** e use as opções padrão apresentadas para gerar as mesmas chaves de RSA com o ASDM.




3. Especifique os hosts com permissão de conexão ao Security Appliance.

Este comando especifica o endereço de origem, a máscara de rede e a interface do(s) host(s) com permissão para conexão com o SSH. Ele pode ser inserido diversas vezes para vários hosts, redes ou interfaces. Neste exemplo, um host interno e um externo são permitidos.

```
pix(config)#ssh 172.16.1.1 255.255.255.255 inside
pix(config)#ssh 10.1.1.2 255.255.255.255 outside
```

4. **Opcional:** Por padrão, o Security Appliance permite tanto o SSH versão 1 quanto versão 2. Insira este comando para restringir as conexões a uma versão específica.

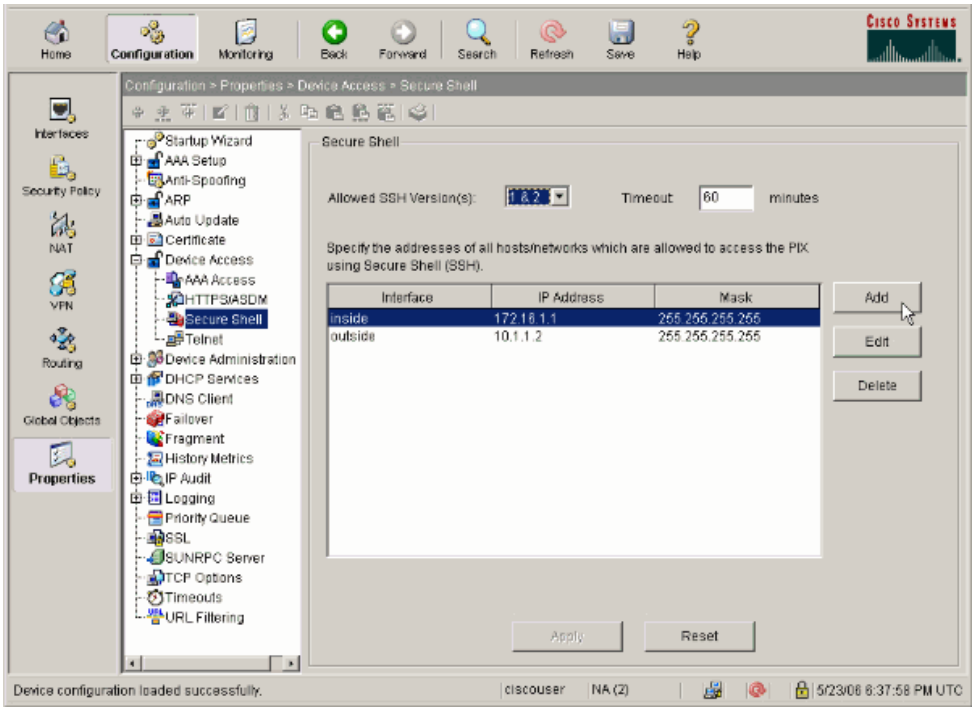
```
pix(config)# ssh version <version_number>
```

**Nota:** O `version_number` pode ser 1 ou 2.

5. **Opcional:** Por padrão, as sessões de SSH são encerradas após cinco minutos de inatividade. Esse timeout pode ser configurado para um valor entre 1 e 60 minutos.

```
pix(config)#ssh timeout minutes
```

Selecione **Configuration > Properties > Device Access > Secure Shell** para utilizar o ASDM para especificar os hosts com permissão para se conectarem com o SSH e para especificar as opções de versão e timeout.




**Como Utilizar um Cliente SSH**

Forneça o nome de usuário e a senha de login do PIX 500 Series Security Appliance ao abrir a sessão de SSH. Quando você inicia uma sessão de SSH, um ponto (.) é exibido no console do Security Appliance antes que o prompt de autenticação de usuário do SSH seja exibido.

```
hostname(config)# .
```

A exibição do ponto não afeta a funcionalidade do SSH. O ponto é exibido no console quando uma chave de servidor é gerada ou quando uma mensagem é descriptografada com chaves privadas durante uma troca de chaves de SSH antes que ocorra a autenticação do usuário. Essas tarefas podem durar até dois minutos ou mais. O ponto é um indicador de progresso que verifica que o Security Appliance está ocupado e não travou.

As versões 1.x e 2 do SSH têm protocolos completamente diferentes e não são compatíveis. Baixe um cliente compatível. Consulte a seção Obtenção de um Cliente SSH de Configurações Avançadas para obter mais informações.

**Configuração do PIX**

Este documento usa esta configuração:

**Configuração do PIX**

```
PIX Version 7.1(1)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 192.168.200.1 255.255.255.0
```

```
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.5.10 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute


!--- AAA para a configuração de SSH

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.0.0 255.255.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5


!--- Insira este comando para cada endereço ou sub-rede
!--- para identificar o endereço IP do qual o
!--- Security Appliance aceita conexões.
!--- O Security Appliance aceita conexões de SSH de todas as interfaces.


ssh 10.1.1.2 255.255.255.255 outside


!--- Permite que os usuários no host 172.161.1.1
!--- acessem o Security Appliance
!--- na interface interna.


ssh 172.16.1.1 255.255.255.255 inside


!--- Define a duração entre 1 a 60 minutos
!--- (o padrão é 5 minutos) durante a qual a sessão de SSH poderá permanecer ociosa
!--- antes do Security Appliance desconectar a sessão.


ssh timeout 60

console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
```

```
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7
: end
```

**Nota:** Você pode acessar a interface de gerenciamento do ASA/PIX por SSH ao executar o comando - `ssh 172.16.16.160 255.255.255.255 Management`

## Configuração do Telnet

Para adicionar o acesso por Telnet ao console e definir o timeout por inatividade, execute o comando **telnet** no modo de configuração global. Por padrão, as sessões de Telnet em inatividade por cinco minutos são encerradas pelo Security Appliance. Para remover o acesso de Telnet de um endereço IP previamente definido, use a forma *no* deste comando.

```
telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}}

no telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeout number}}
```

O comando **telnet** permite que você especifique os hosts que podem acessar o console do Security Appliance por meio de Telnet. Você pode habilitar o Telnet ao Security Appliance em todas as interfaces. Entretanto, o Security Appliance faz com que todo o tráfego de Telnet até a interface externa seja protegido por IPsec. Para habilitar uma sessão de Telnet até a interface externa, configure o IPsec nessa interface para incluir o tráfego IP gerado pelo Security Appliance e ative o Telnet na interface externa.

**Nota:** O acesso ao Security Appliance por meio de sessão de Telnet não é recomendável. As informações das credenciais de autenticação, tais como as senha, são enviadas em texto não criptografado. As comunicações entre o servidor e o cliente Telnet são efetuadas somente com texto não criptografado. A Cisco recomenda a utilização do SSH para uma comunicação de dados mais segura.

Se você inserir um endereço IP, precisará inserir uma máscara de rede também. Não há máscara de rede padrão. Não use a máscara de sub-rede da rede interna. A máscara de rede é apenas uma máscara de bits para o endereço IP. Para limitar o acesso a um único endereço IP, use 255 em cada octeto, por exemplo, 255.255.255.255.

Se o IPsec estiver ativo, você pode especificar um nome de uma interface insegura, geralmente a interface externa. No mínimo, você pode configurar o comando **crypto map** para especificar um nome de interface com o comando **telnet**.

Execute o comando **password** para definir uma senha para o acesso por Telnet ao console. O padrão é cisco. Execute o comando **who** para ver que endereços IP estão acessando o console do Security Appliance no momento. Execute o comando **kill** para encerrar uma sessão ativa de Telnet no console.

Para habilitar uma sessão de Telnet até a interface interna, examine estes exemplos:

**Exemplo 1**

Este exemplo permite que somente o host 10.1.1.1 tenha acesso ao console do Security Appliance por Telnet:

```
pix(config)#telnet 10.1.1.1 255.255.255.255 inside
```

**Exemplo 2**

Este exemplo permite que somente a rede 10.0.0.0/8 tenha acesso ao console do Security Appliance por Telnet:

```
pix(config)#telnet 10.0.0.0 255.0.0.0 inside
```

**Exemplo 3**

Este exemplo permite que todas as redes tenham acesso ao console do Security Appliance por Telnet:

```
pix(config)#telnet 0.0.0.0 0.0.0.0 inside
```

Se você usar o comando **aaa** com a palavra-chave console, acesso ao console por Telnet deverá ser autenticado com um servidor de autenticação.

**Nota:** Se você configurou o comando **aaa** para solicitar autenticação para o acesso ao console do Security Appliance por Telnet e a solicitação de login no console exceder o timeout, você poderá ter acesso ao Security Appliance a partir do console serial. Para fazer isso, insira o nome de usuário e a senha do Security Appliance definidas com o comando **enable password**.

Execute o comando **telnet timeout** para definir o tempo máximo que uma sessão de Telnet no console possa ficar inativa antes de ser desconectada pelo Security Appliance. Você não pode utilizar o comando **no telnet** com o comando **telnet timeout**.

Este exemplo mostra como alterar a duração máxima de inatividade da sessão:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

### Suporte a SSH/Telnet no ACS 4.x

Se você observar as funções do RADIUS, ele poderá ser usado RADIUS para a funcionalidade do SSH.

Quando uma tentativa de acesso ao Security Appliance com conexão de Telnet, SSH, HTTP ou console serial é feita e o tráfego atende a uma instrução de autenticação, o Security Appliance solicita um nome de usuário e uma senha. Ele envia então essas credenciais ao servidor RADIUS (ACS) e permite ou recusa o acesso à CLI com base na resposta dada pelo servidor.

Consulte a seção Suporte a Servidor AAA e a Banco de Dados Local de Configurando Servidores AAA e o Banco de Dados Local para obter mais informações.

Por exemplo, seu ASA Security Appliance 7.0 precisa de um endereço IP onde aceitar conexões, tal como:

```
hostname(config)#ssh source_IP_address mask source_interface
```

Consulte a seção Permitindo o Acesso de SSH de Configurando Servidores AAA e o Banco de Dados Local para obter mais informações.

## Verificação

Utilize esta seção para confirmar se a sua configuração está funcionando corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos **show**. Use a OIT para exibir uma análise da saída do comando **show**.

### Depuração do SSH

Execute o comando **debug ssh** para ativar a depuração do SSH.

```
pix(config)#debug ssh
  SSH debugging on
```

Esta saída mostra que a solicitação de autenticação do host 10.1.1.2 (externo ao PIX) para "pix" obteve êxito:

```
pix#
Device ssh opened successfully.
  SSH0: SSH client: IP = '10.1.1.2' interface # = 1
  SSH: host key initialised
  SSH0: starting SSH control process
  SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
  server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
  SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows
  client version string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0:
begin    ser ver key generation
  SSH0: complete server key generation, elapsed time = 1760 ms
SSH2 0: SSH2_MSG_KEXINIT sent
  SSH2 0: SSH2_MSG_KEXINIT received
  SSH2: kex: client->server aes128-cbc hmac-md5 none
  SSH2: kex: server->client aes128-cbc hmac-md5 none
  SSH2 0: expecting SSH2_MSG_KEXDH_INIT
  SSH2 0: SSH2_MSG_KEXDH_INIT received
  SSH2 0: signature length 143
  SSH2: kex_derive_keys complete
  SSH2 0: newkeys: mode 1
  SSH2 0: SSH2_MSG_NEWKEYS sent
  SSH2 0: waiting for SSH2_MSG_NEWKEYS
  SSH2 0: newkeys: mode 0
  SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method is
'no AAA', aaa server group ID = 0
  SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
 SSH2 0: authentication successful for pix

!--- A autenticação para o PIX foi bem-sucedida.

  SSH2 0: channel open request
  SSH2 0: pty-req request
```

```
  SSH2 0: requested tty: vt100, height 25, width 80
SSH2 0: shell request
  SSH2 0: shell message received
```

Se um usuário fornecer um nome de usuário errado, como, por exemplo, "pix1" em vez de "pix", o PIX Firewall rejeitará a autenticação. Esta saída de depuração mostra a autenticação com falha:

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL
 server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for Windows client version
    string:SSH-1.99-3.2.0 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1960 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix1): user authen method is
'no AAA', aaa server group ID = 0
SSH(pix1): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix1

!--- A autenticação para pix1 não foi bem-sucedida devido ao nome de usuário incorreto.
```

De forma similar, se o usuário fornecer uma senha errada, esta saída de depuração mostrará a autenticação com falha.

```
pix#
Device ssh opened successfully.
SSH0: SSH client: IP = '10.1.1.2'  interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.99-Cisco-1.25
SSH0: send SSH message: outdata is NULL server version string:
SSH-1.99-Cisco-1.25SSH0: receive      SSH message: 83 (83)
SSH0: client version is - SSH-1.99-3.2.0 SSH Secure Shell for
Windows client version string:SSH-1.99-3.2.0
 SSH Secure Shell for WindowsSSH0: begin server key generation
SSH0: complete server key generation, elapsed time = 1920 ms
SSH2 0: SSH2_MSG_KEXINIT sent
SSH2 0: SSH2_MSG_KEXINIT received
SSH2: kex: client->server aes128-cbc hmac-md5 none
SSH2: kex: server->client aes128-cbc hmac-md5 none
SSH2 0: expecting SSH2_MSG_KEXDH_INIT
SSH2 0: SSH2_MSG_KEXDH_INIT received
SSH2 0: signature length 143
SSH2: kex_derive_keys complete
SSH2 0: newkeys: mode 1
SSH2 0: SSH2_MSG_NEWKEYS sent
SSH2 0: waiting for SSH2_MSG_NEWKEYS
SSH2 0: newkeys: mode 0
SSH2 0: SSH2_MSG_NEWKEYS receivedSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
    SSH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pixSSH(pix): user authen method
is 'no AAA', aaa server group ID = 0
SSH2 0: authentication failed for pix

!--- A autenticação para o PIX não foi bem-sucedida devido à senha de usuário incorreta.
```

## Exibição das Sessões Ativas de SSH

Execute este comando para verificar o número de sessões de SSH que estão conectadas e o estado da conexão ao PIX:

```
pix#show ssh session
```

```
SID Client IP       Version Mode Encryption Hmac     State            Username
0   10.1.1.2        1.99    IN   aes128-cbc md5      SessionStarted   pix
                            OUT  aes128-cbc md5      SessionStarted   pix
```

Selecione **Monitoring > Properties > Device Access > Secure Shell Sessions** para exibir as sessões com o ASDM.

### Exibição da Chave Pública de RSA

Execute este comando para exibir a porção pública das chaves de RSA no Security Appliance:

```
pix#show crypto key mypubkey rsa

Key pair was generated at: 19:36:28 UTC May 19 2006
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c172f4
 95f66c34 2c2ced37 aa3442d8 12158c93 131480dd 967985ab 1d7b92d9 5290f695
 8e9b5b0d d88c0439 6169184c d8fb951c 19023347 d6b3f939 99ac2814 950f4422
 69b67328 f64916b1 82e15341 07590da2 390fbefd 38758888 7319196c de61aef1
 165c4bab 03d081d5 ddaf15cc c9ddb204 c2b451e0 f19ce0f3 485b1d69 8b020301 0001
```

Selecione **Configuration > Properties > Certificate > Key Pair**, escolha o par de chaves a exibir e clique em **Show Details** para ver as chaves de RSA com o ASDM.

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Como Remover as Chaves de RSA do PIX

Em certas situações, como quando você atualiza o software do PIX ou altera a versão do SSH no PIX, pode ser necessário remover e recriar as chaves de RSA. Execute este comando para remover o par de chaves de RSA do PIX:

```
pix(config)#crypto key zeroize rsa
```

Selecione **Configuration > Properties > Certificate > Key Pair**, escolha o par de chaves a exibir e clique em **Delete** para remover as chaves de RSA com o ASDM.

---



Data da Geração do PDF: 1 Julho 2009

http://www.cisco.com/cisco/web/support/BR/106/1067/1067710_ssh-inside-out-pix7x.html