Versão ASA 9.x SSH e telnet no exemplo de configuração das interfaces internas e externas

Índice

Introdução

Este documento descreve como configurar o Shell Seguro (ssh) nas interfaces internas e externas das versões 9.x e mais recente da ferramenta de segurança do Cisco Series. Quando você deve configurar e monitorar a ferramenta de segurança adaptável de Cisco (ASA) remotamente com o CLI, o uso do telnet ou do SSH está exigido. Porque as comunicações de Telnet são enviadas no texto claro, que pode incluir senhas, o SSH é altamente recomendado. O tráfego SSH é cifrado em um túnel e desse modo as ajudas protegem senhas e outros comandos configuration sensíveis da intercepção.

O ASA permite conexões de SSH à ferramenta de segurança para propósitos do gerenciamento. A ferramenta de segurança permite um máximo de cinco conexões de SSH simultâneas para cada contexto de segurança, se disponível, e um máximo global de 100 conexões para todos os contextos combinados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 9.1.5 do software de firewall de Cisco ASA.

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) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

> Nota: A versão de SSH 2 (SSHv2) é apoiada nas versões ASA 7.x e mais tarde.

Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança do 5500 Series de Cisco ASA com versões de software 9.x e mais tarde.

Convenções

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

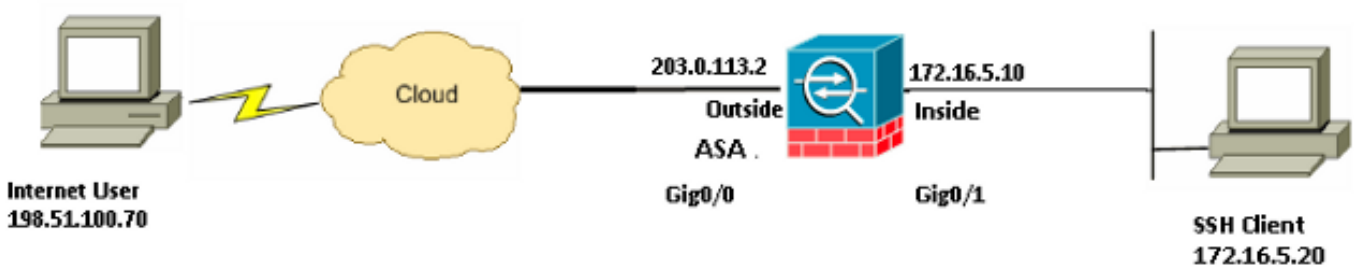
Configurar

Use a informação que é fornecida nesta seção a fim configurar as características que são descritas neste documento.

> Nota: Cada etapa de configuração que é descrita fornece a informação que é necessária a fim usar o CLI ou o Security Device Manager adaptável (ASDM).

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

Diagrama de Rede



Neste exemplo de configuração, o ASA é considerado ser o servidor de SSH. O tráfego dos clientes SSH (198.51.100.70/32 e 172.16.5.20/24) ao servidor de SSH é cifrado. A ferramenta de segurança apoia a funcionalidade do shell remoto SSH que é fornecida nas versões de SSH 1 e 2 e apoia o Data Encryption Standard (DES) e as cifras 3DES. As versões de SSH 1 e 2 são diferentes e não são interoperáveis.

Configurações SSH

Este documento utiliza as seguintes configurações:

- Acesso SSH à ferramenta de segurança
- Como usar um cliente SSH
- Configuração ASA

Acesso SSH à ferramenta de segurança

Termine estas etapas a fim configurar o acesso SSH à ferramenta de segurança:

1. As sessões SSH exigem sempre um formulário de autenticação tal como um nome de usuário e senha. Há dois métodos que você pode usar a fim cumprir esta exigência.

   O primeiro método que você pode usar a fim cumprir esta exigência é configurar um nome de usuário e senha com o uso do Authentication, Authorization, and Accounting (AAA):
   `ASA(config)#username username password password`
   `ASA(config)#aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}`Nota: Se você usa um TACACS+ ou um grupo de servidor Radius para a autenticação, você pode configurar a ferramenta de segurança de modo que use o base de dados local como um método da reserva se o servidor AAA é não disponível. Especifique o nome de grupo de servidor e então o **LOCAL** (o **LOCAL** é diferenciando maiúsculas e minúsculas). Cisco recomenda que você usa o mesmo nome de usuário e a senha no base de dados local e no servidor AAA, porque a alerta da ferramenta de segurança não dá nenhuma indicação do método que é usado.A fim especificar um **backup local** para o **TACACS+**, use esta configuração para a autenticação SSH:
   `ASA(config)#aaa authentication ssh console TACACS+ LOCAL`Você pode alternativamente usar o base de dados local como seu método principal da autenticação sem a reserva. A fim fazer isto, entre em sozinho **LOCAL**:
   `ASA(config)#aaa authentication ssh console LOCAL`**O segundo método** que você pode usar a fim cumprir esta exigência é usar o nome de usuário padrão do **ASA** e a senha telnet do padrão de **Cisco**. Você pode mudar a senha telnet com este comando:
   `ASA(config)#passwd password`Nota: **O comando password** pode igualmente ser usado nesta

situação, como ambos os comandos function similarmente.

2. Gerencia um par de chaves RSA para o Firewall ASA, que é exigido para o SSH:
   `ASA(config)#crypto key generate rsa modulus modulus_size`Nota: **O modulus_size** (nos bit) pode ser 512, 768, 1024, ou 2048. Maior o tamanho que chave do módulo você especificam, mais por muito tempo toma para gerar o par de chaves RSA. Um valor de 2048 é recomendado. O comando que é usado a fim gerar um par de chaves RSA é diferente para versões de software ASA mais cedo do que a versão 7.x. Nas versões anterior, um Domain Name deve ser ajustado antes que você possa criar as chaves. No modo de contexto múltiplo, você deve gerar as chaves RSA para cada contexto.
3. Especifique os anfitriões que são permitidos conectar à ferramenta de segurança. Este comando especifica o endereço de origem, o netmask, e a relação do host que é permitido conectar com o SSH. Pode ser entrado épocas múltiplas para host múltiplos, redes, ou relações. Neste exemplo, um host no interno e um host na parte externa são permitidos:
   ```
   ASA(config)#ssh 172.16.5.20 255.255.255.255 inside
   ASA(config)#ssh 198.51.10.70 255.255.255.255 outside
   ```
4. Este passo é opcional. À revelia, a ferramenta de segurança permite a versão de SSH 1 e a versão 2. incorpora este comando a fim restringir as conexões a uma versão específica:
   `ASA(config)# ssh version <version_number>`Nota: **O version_number** pode ser **1** ou **2.**
5. Este passo é opcional. À revelia, as sessões SSH são fechadas após cinco minutos da inatividade. Este intervalo pode ser configurado para durar entre 1 e 60 minutos:
   `ASA(config)#ssh timeout minutes`

Configuração ASA

Use esta informação a fim configurar o ASA:

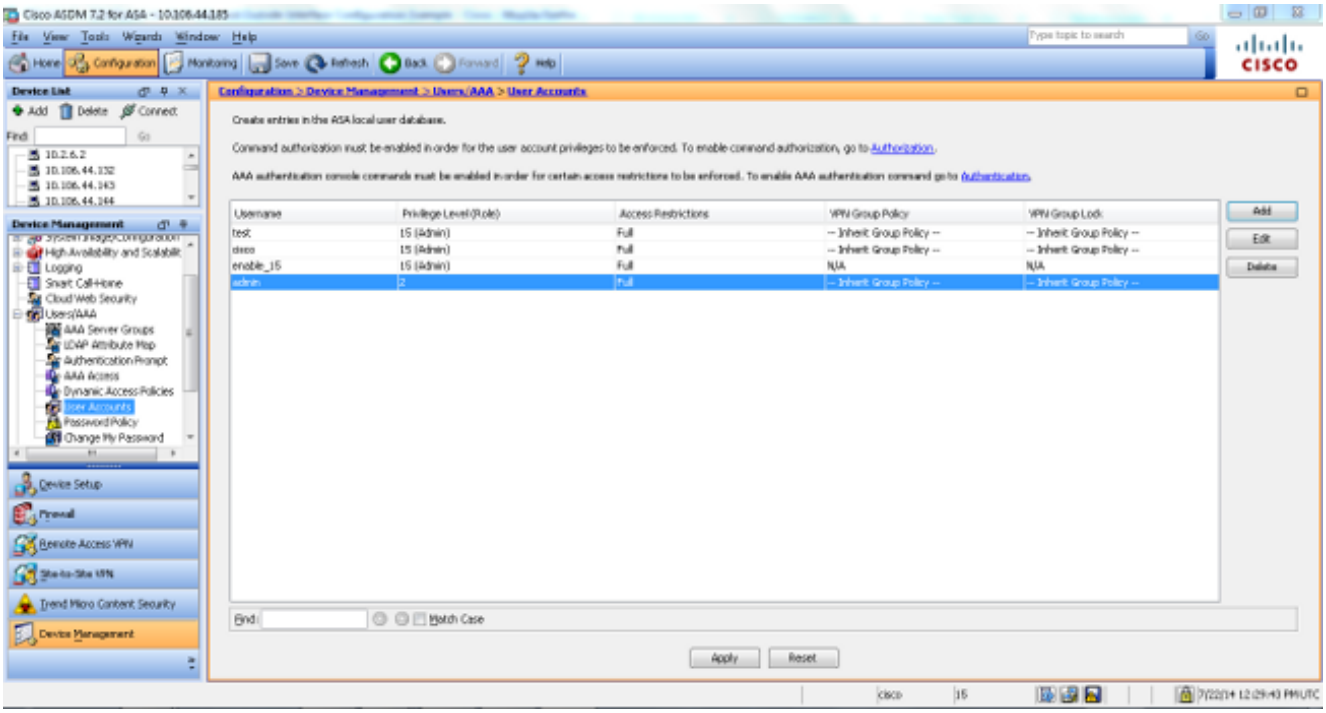
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.0

!--- AAA for the SSH configuration

username ciscouser password 3USUcOPFUiMCO4Jk encrypted
aaa authentication ssh console LOCAL

http server enable
http 172.16.5.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstar
telnet timeout 5

!--- Enter this command for each address or subnet
!--- to identify the IP addresses from which
!--- the security appliance accepts connections.
```

```
!--- The security appliance accepts SSH connections from all interfaces.

ssh 172.16.5.20 255.255.255.255 inside
ssh 198.51.100.70 255.255.255.255 outside

!--- Allows the users on the host 172.16.5.20 on inside
!--- Allows SSH access to the user on internet 198.51.100.70 on outside
!--- to access the security appliance
!--- on the inside interface.

ssh 172.16.5.20 255.255.255.255 inside

!--- Sets the duration from 1 to 60 minutes
!--- (default 5 minutes) that the SSH session can be idle,
!--- before the security appliance disconnects the session.

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
```

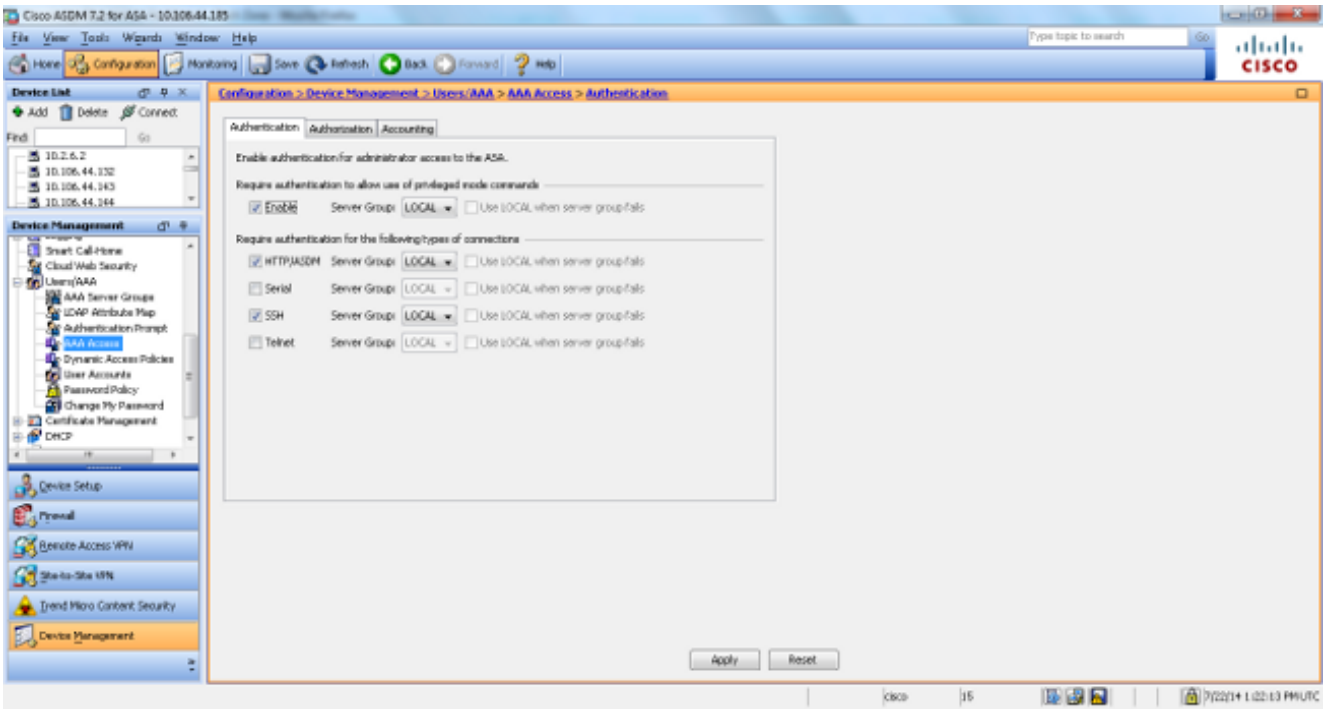
Configuração da versão 7.2.1 ASDM

Termine estas etapas a fim configurar a versão 7.2.1 ASDM:

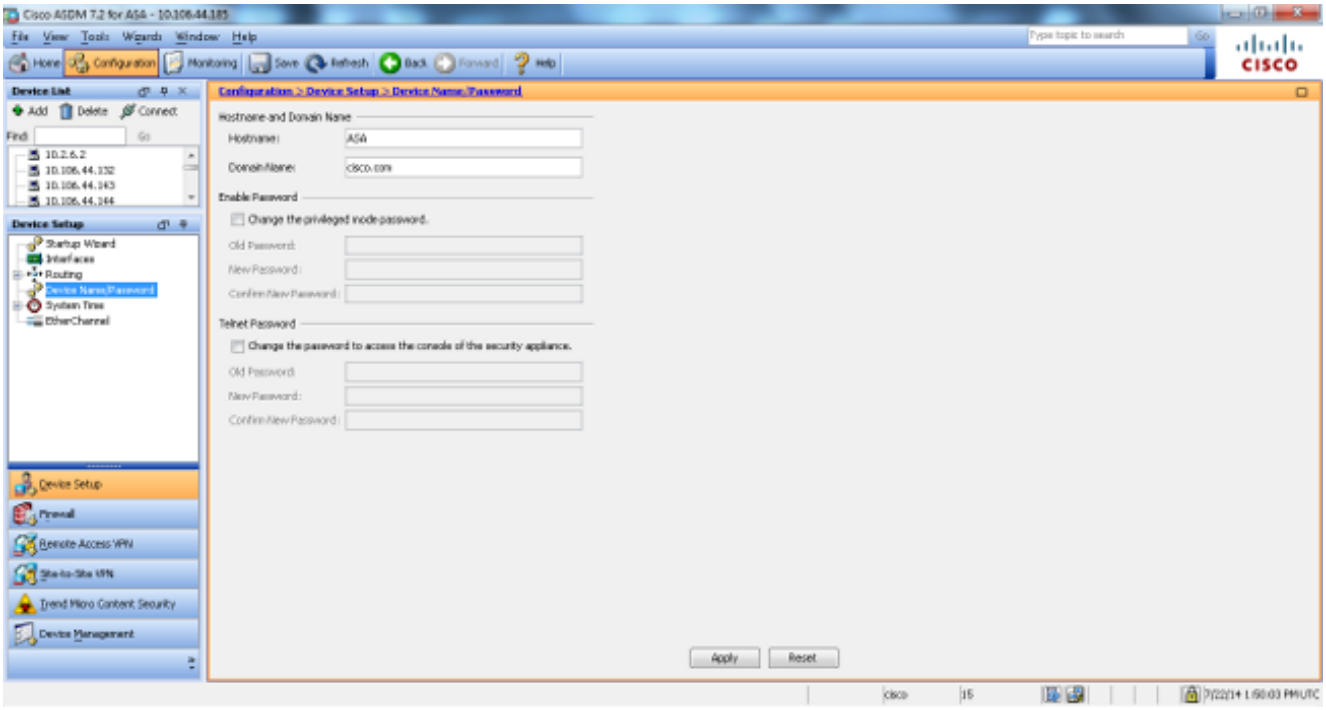
1. Navegue à **configuração > ao Gerenciamento de dispositivos > ao Users/AAA > às contas de usuário** a fim adicionar um usuário com ASDM.



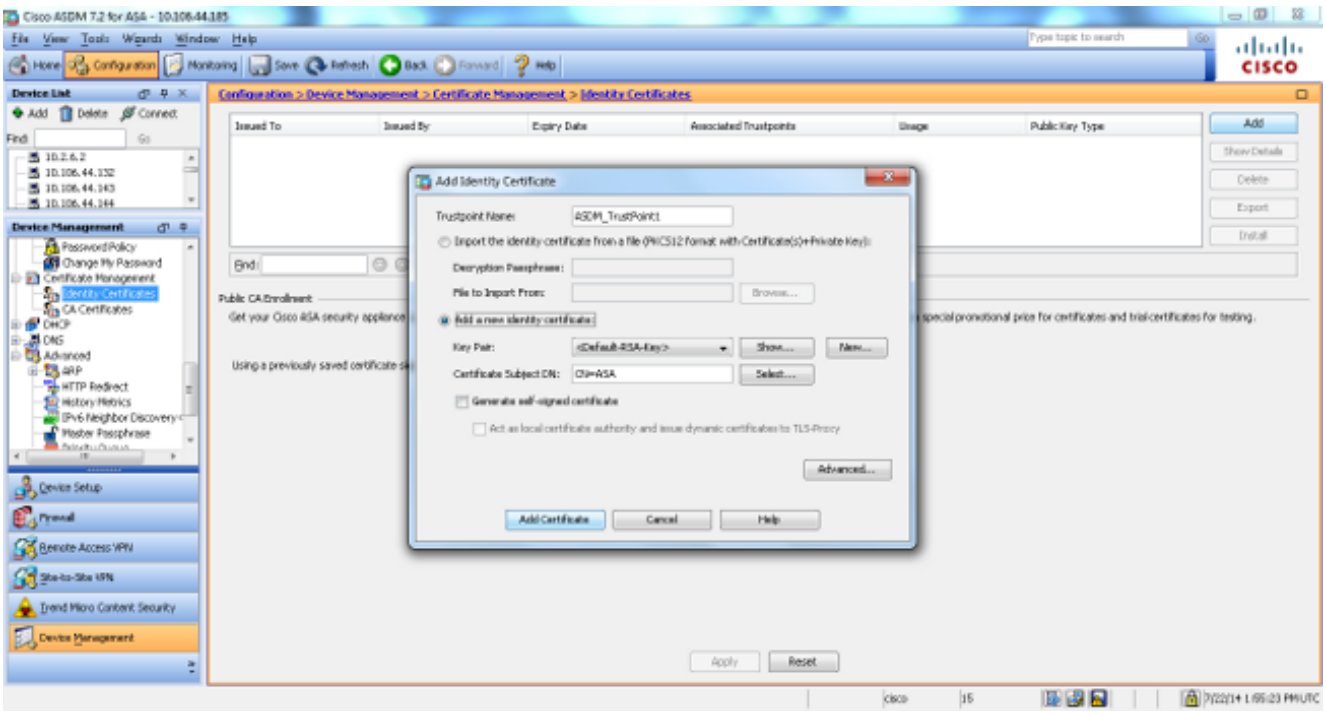
2. Navegue à **configuração > ao Gerenciamento de dispositivos > ao Users/AAA > ao acesso > à autenticação AAA** a fim estabelecer a autenticação de AAA para o SSH com ASDM.



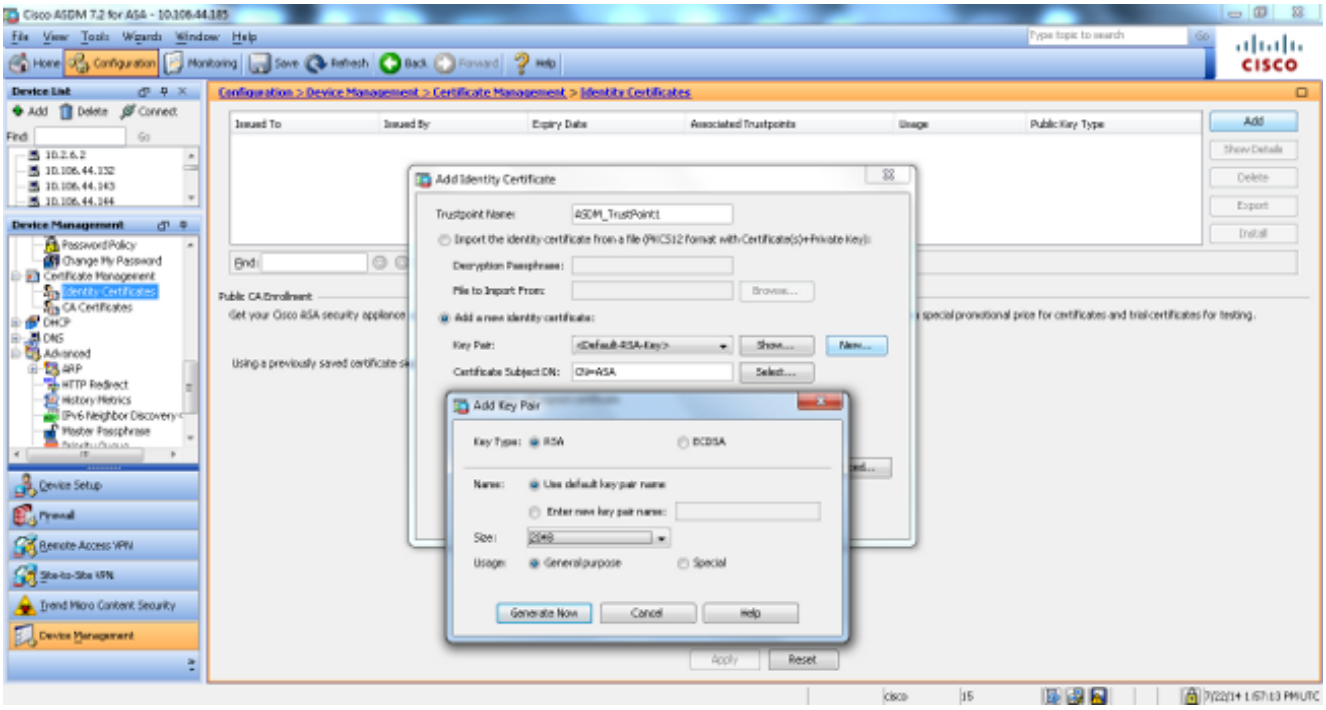
3. Navegue à **configuração > à instalação > ao nome de dispositivo/senha de dispositivo** a fim mudar a senha telnet com ASDM.



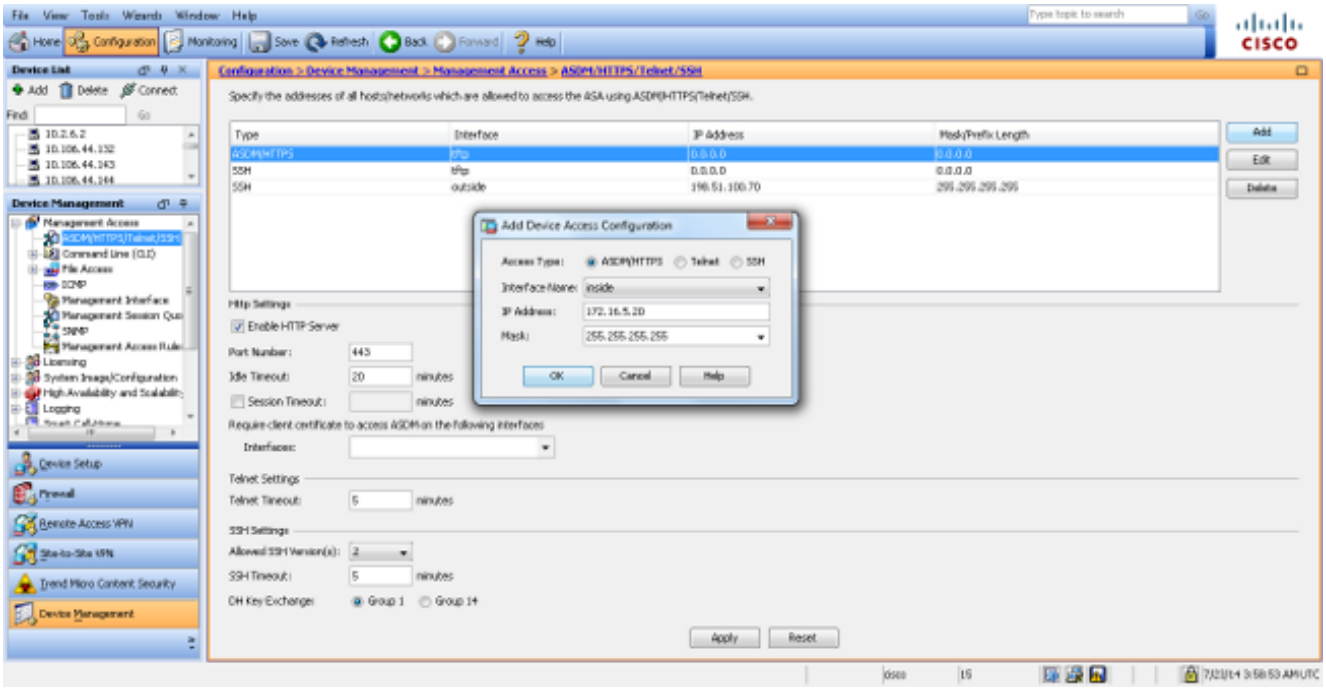
4. Navegue à **configuração > ao > gerenciamento de certificado > aos certificados de identidade do Gerenciamento de dispositivos**, o clique **adiciona**, e usa as opções padrão que estão disponíveis a fim gerar as mesmas chaves RSA com ASDM.



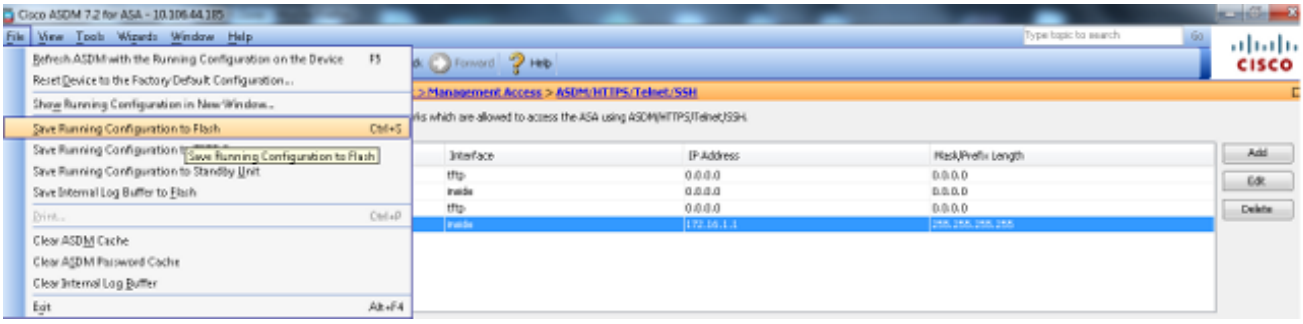
5. Clique **adicionar um** botão de rádio **novo do certificado de identidade** e clique-o **novo** a fim adicionar um par de chave padrão, se um não existe. Uma vez que completo, o clique **gerencie agora**.



6. Navegue à **configuração > ao Gerenciamento de dispositivos > ao acesso de gerenciamento > à linha de comando (CLI) > Shell Seguro (ssh)** a fim usar o ASDM de modo que você possa especificar os anfitriões que são permitidos conectar com o SSH e a fim especificar a versão e as opções de timeout.



7. Clique a **salvaguarda da** janela pop-up a fim salvar a configuração.



8. Quando alertado para salvar a configuração no flash, escolha **aplicam-se** a fim salvar a configuração.

Configuração do telnet

A fim adicionar o acesso do telnet ao console e ajustar o idle timeout, inscreva o **comando telnet no** modo de configuração global. À revelia, as sessões de Telnet que são deixadas inativas por cinco minutos são fechadas pela ferramenta de segurança. A fim remover o acesso do telnet de um endereço IP de Um ou Mais Servidores Cisco ICM NT previamente ajustado, não use **nenhum** formulário 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 anfitriões que podem alcançar o console da ferramenta de segurança através do telnet.

> Nota: Você pode permitir o telnet à ferramenta de segurança em todas as relações. Contudo, a ferramenta de segurança exige que todo o tráfego do telnet à interface externa esteja protegido pelo IPsec. A fim permitir uma sessão de Telnet à interface externa, configurar o IPsec na interface externa de modo que inclua o tráfego IP que é gerado pela ferramenta de segurança e permita o telnet na interface externa.

> Nota: Geralmente, se nenhuma relação que tiver um nível de segurança de zero ou o abaixar do que toda a outra relação, o ASA não permite o telnet a essa relação.

> Nota: Cisco não recomenda o acesso à ferramenta de segurança através de uma sessão de Telnet. A informação das credenciais de autenticação, tal como a senha, é enviada como o texto claro. Cisco recomenda que você usa o SSH para uma comunicação de dados mais fixada.

Inscreva o **comando password** a fim ajustar uma senha para o acesso do telnet ao console. A senha padrão é **Cisco**. Inscreva o **comando who** a fim ver os endereços IP de Um ou Mais Servidores Cisco ICM NT que alcançam atualmente o console da ferramenta de segurança. Inscreva o **comando kill** a fim terminar uma sessão de console ativa do telnet.

Exemplos de cenário do telnet

A fim permitir uma sessão de Telnet à interface interna, reveja os exemplos que são fornecidos

nesta seção.

Exemplo 1

Este exemplo permite que somente o host **172.16.5.20** aceda ao console da ferramenta de segurança com o telnet:

```
ASA(config)#telnet 172.16.5.20 255.255.255.255 inside
```

Exemplo 2

Este exemplo permite que somente a rede **172.16.5.0/24** aceda ao console da ferramenta de segurança com o telnet:

```
ASA(config)#telnet 172.16.5.0 255.255.255.0 inside
```

Exemplo 3

Este exemplo permite que todas as redes acedam ao console da ferramenta de segurança com o telnet:

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

Se você usa o **comando aaa** com a palavra-chave do console, o acesso de console do telnet deve ser autenticado com um Authentication Server.

> Nota: Se você configura o **comando aaa** a fim exigir para fora a autenticação para a ferramenta de segurança e o acesso de console do telnet, e os tempos do pedido do console de login, você pode aceder à ferramenta de segurança do console serial. A fim fazer isto, incorpore o username da ferramenta de segurança e a senha que é ajustada com o **comando enable password**.

Emita o comando do **Timeout da Telnet** a fim ajustar o tempo máximo que uma sessão de Telnet do console pode ser inativa antes que esteja terminado pela ferramenta de segurança. Você não pode não usar **nenhum comando telnet** com o comando do **Timeout da Telnet**.

Este exemplo mostra como mudar a duração da quietude da sessão máxima:

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

> Nota: A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Debugar o SSH

Inscreva o **comando debug ssh** a fim permitir a eliminação de erros SSH:

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

Esta saída mostra uma tentativa SSH de um endereço IP de Um ou Mais Servidores Cisco ICM NT interno (172.16.5.20) à interface interna do ASA. Estes debugam descrevem uma conexão bem sucedida e uma autenticação:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication successful for cisco

!--- Authentication for the ASA was successful.

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 nome de usuário errado é incorporado, como **cisco1** em vez de **Cisco**, o Firewall ASA rejeita a autenticação. Este resultado do debug mostra a autenticação falha:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA1 was not successful due to the wrong username.
```

Similarmente, se a senha incorreta é fornecida, a autenticação falha. Este resultado do debug mostra a autenticação falha:

```
Device ssh opened successfully.
SSH0: SSH client: IP = '172.16.5.20' interface # = 1
SSH: host key initialised
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-2.0-Cisco-1.25
SSH0: send SSH message: outdata is NULL
server version string:SSH-2.0-Cisco-1.25
SSH0: receive SSH message: 83 (83)
SSH0: client version is - SSH-2.0-PuTTY_Release_0.62
SSH Secure Shell for Windows
client version string:SSH-2.0-PuTTY_Release_0.62
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 received
SSH(cisco): user authen method is 'use AAA', aaa server group ID = 1
SSH2 0: authentication failed for cisco1

!--- Authentication for ASA was not successful due to the wrong password.
```

Sessões SSH ativa da vista

Incorpore este comando a fim verificar o número de sessões SSH que são conectadas (e o estado de conexão) ao ASA:

```
ASA(config)# show ssh sessions

SID Client IP    Version Mode Encryption Hmac State           Username
0   172.16.5.20 2.0     IN   aes256-cbc sha1 SessionStarted  cisco
                        OUT  aes256-cbc sha1 SessionStarted  cisco
```

Navegue à **monitoração > propriedades > sessões do acesso de dispositivo > do Secure Shell** a fim ver as sessões com o ASDM.

Inscreva o **comando socket da tabela asp da mostra** a fim verificar que a sessão de TCP está estabelecida:

```
ASA(config)# show asp table socket

Protocol Socket State Local Address Foreign Address

SSL 02444758 LISTEN 203.0.113.2:443 0.0.0.0:*
TCP 02448708 LISTEN 203.0.113.2:22 0.0.0.0:*
SSL 02c75298 LISTEN 172.16.5.10:443 0.0.0.0:*
TCP 02c77c88 LISTEN 172.16.5.10:22 0.0.0.0:*
TCP 02d032d8 ESTAB 172.16.5.10:22 172.16.5.20:52234
```

Veja chaves públicas RSA

Incorpore este comando a fim ver a parcela pública das chaves RSA na ferramenta de segurança:

```
ASA(config)#show crypto key mypubkey rsa
Key pair was generated at: 23:23:59 UTC Jul 22 2014
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Key:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 00aa82d1 f61df1a4 7cd1ae05 c92322c1 1ce490e3 c9db00fd d75afe77 1ea0b2c2
 3325576f a7dc5ffe a6166bf5 7f0f2551 25b8cb23 a8908b49 81c42618 c98e3aea
 ce6f9e42 367974d1 5c2ea6b1 e7aac40b 44a6c0a5 23c4d845 a57d4c04 6de49dbb
 2c6f074e 25e3b19e 7c5da809 ac7d775c 0c01bb9d 211b7078 741094b4 94056e75
 72d5e938 c59baaec 12285005 ee6abf81 90822610 cf7ee4c1 ae8093d9 6943bde3
 16d8748c d86b5f66 1a6ccf33 9cde0432 b3cabab5 938b1874 c3d7c13e 43a95a8f
 ed36db2e f9ca5d2c 0c65858e 3e513723 2d362b47 7984d845 faf22579 654113d1
 24d59f27 55d2ddf3 20af3b65 62f039cb a3aafc31 d92a3d9b 14966eb3 cb6ca249
 55020301 0001
```

Navegue à **configuração > às propriedades > ao certificado > ao par de chaves** e clique **detalhes da mostra** a fim ver as chaves RSA com o ASDM.

Troubleshooting

Esta seção fornece a informação que você pode usar a fim pesquisar defeitos sua configuração.

Remova as chaves RSA do ASA

Em determinadas situações, como quando você promove o software ASA ou muda a versão de SSH no ASA, você pôde ser exigido remover e recrear as chaves RSA. Incorpore este comando a fim remover o par de chaves RSA do ASA:

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

Navegue à **configuração > às propriedades > ao certificado > ao par de chaves** e clique a **supressão** a fim remover as chaves RSA com o ASDM.

Conexão de SSH falhada

Você recebe este Mensagem de Erro no ASA:

```
%ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
```

Este é o Mensagem de Erro que aparece na máquina de cliente SSH:

```
Selected cipher type <unknown> not supported by server.
```

A fim resolver esta edição, remova e recreie as chaves RSA. Incorpore este comando a fim remover o par de chaves RSA do ASA:

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

Incorpore este comando a fim gerar a chave nova:

```
ASA(config)# crypto key generate rsa modulus 2048
```