PIX/ASA 7.x: SSH/Telnet en el ejemplo de configuración de las interfaces interior y exterior

Contenido

Introducción

Este documento proporciona un ejemplo de configuración del Secure Shell (SSH) en las interfaces interiores y exteriores de la versión 7.x y posterior del dispositivo de seguridad del Cisco Series. La configuración del Series Security Appliance de forma remota con la línea de comando implica el uso de Telnet o de SSH. Debido a que las comunicaciones Telnet se envían en el texto sin formato, que incluye las contraseñas, el SSH se recomienda altamente. El tráfico SSH se encripta en un túnel y de tal modo ayuda a proteger las contraseñas y otros comandos de configuración contra la interceptación.

El dispositivo de seguridad permite las conexiones SSH al dispositivo de seguridad para los fines de administración. El dispositivo de seguridad permite un máximo de cinco conexiones SSH simultáneas para cada contextos de seguridad, si está disponible, y un máximo global de 100

conexiones para todos los contextos combinados.

En este ejemplo de configuración, el dispositivo de seguridad PIX se considera el servidor SSH. El tráfico de los clientes SSH (10.1.1.2/24 y 172.16.1.1/16) al servidor SSH se encripta. El dispositivo de seguridad soporta las funciones SSH shell remoto proporcionadas en los SSH versión 1 y 2 y soporta la Data Encryption Standard (DES) y los cifrados 3DES. Los SSH versión 1 y 2 son diferentes y no son interoperables.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 7.1 y 8.0 del Cisco Pix Firewall Software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Nota: SSHv2 se soporta en la versión 7.x y posterior del PIX/ASA y no se soporta en las versiones anterior a 7.x.

Productos Relacionados

Esta configuración se puede también utilizar con el dispositivo de seguridad de las 5500 Series de Cisco ASA con las versiones de software 7.x y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

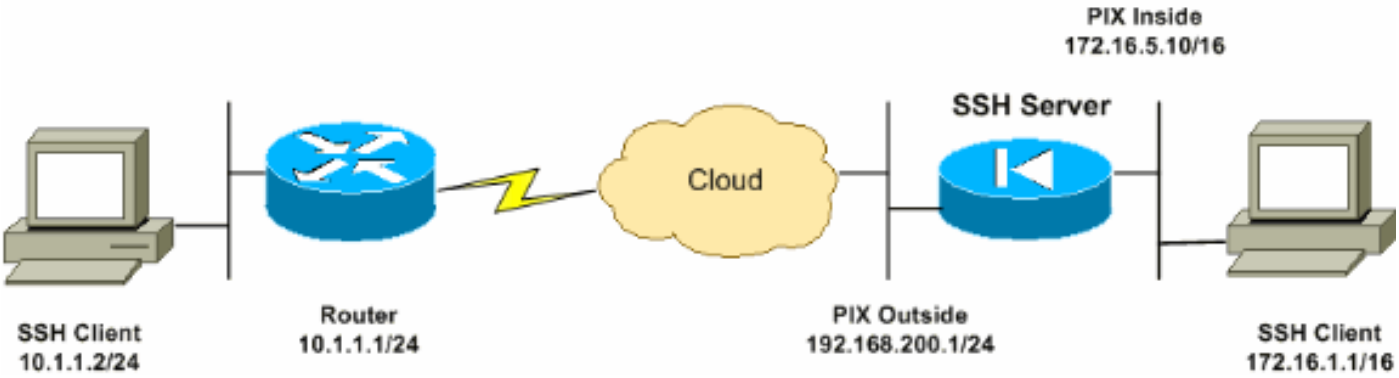
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Cada paso para la configuración se presenta con la información necesaria para utilizar la línea de comando o el administrador del Adaptive Security Device (ASDM).

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones SSH

En este documento, se utilizan estas configuraciones:

- Acceso SSH al dispositivo de seguridad
- Cómo utilizar a un cliente SSH
- Configuración de PIX

Acceso SSH al dispositivo de seguridad

Termina estos pasos para configurar el acceso SSH al dispositivo de seguridad:

1. Las sesiones SSH requieren siempre un nombre de usuario y contraseña para la autentificación. Hay dos maneras de cumplir este requisito.Configure un nombre de usuario y contraseña y use el AAA:Sintaxis:`pix(config)#`**`username`** *`username`* **`password`** *`password`*
`pix(config)#`**`aaa authentication {telnet | ssh | http | serial} console {LOCAL | server_group [LOCAL]}`** **Nota:** Si utiliza un TACACS+ o un grupo de servidor de radio para la autenticación, puede configurar el dispositivo de seguridad para utilizar las bases de datos locales como método del retraso si no se puede acceder al servidor de AAA . Especifique el nombre de grupo de servidores y luego LOCAL (LOCAL distingue entre mayúsculas y minúsculas). Recomendamos que use el mismo nombre de usuario y la contraseña en las bases de datos locales como el servidor de AAA, porque el prompt del dispositivo de seguridad no da ninguna indicación que el método se utilice.**Nota:** Ejemplo:`pix(config)#`**`aaa authentication ssh console TACACS+ LOCAL`** **Nota:** Puede alternativamente utilizar las bases de datos locales como tu método principal de autentificación sin el retraso. Para hacer esto, ingresa solo LOCAL.Ejemplo:`pix(config)#`**`aaa authentication ssh console LOCAL`** OUtiliza el nombre de usuario predeterminado del **pix** y la contraseña de Telnet predeterminada de **Cisco**. Usted puede cambiar la contraseña de Telnet con este comando:`pix(config)#`**`passwd`** *`password`*
Nota: El comando de la **contraseña** se puede también utilizar en esta situación. Ambos comandos hacen lo mismo.
2. Genere un par clave RSA para el firewall PIX, que se requiere para el SSH:`pix(config)#`**`crypto key generate rsa modulus`** *`modulus_size`* **Nota:** El modulus_size (en bits) puede ser 512, 768, 1024, o 2048. Cuanto más grande es el tamaño del módulo clave que especifique, mayor será el tiempo para generar el par clave RSA. El valor de 1024 se recomienda.**Nota:** El comando usado para generar un par clave RSA es diferente para las versiones de software PIX anterior que 7.x. En las versiones anteriores, debe determinarse

un nombre de dominio antes de crear las claves.**Nota:** En el modo de contexto múltiple, debe generar los claves RSA para cada contexto. Además, los comandos crypto no se soportan en el modo del contexto del sistema.

3. Especifica los ordenadores principal permitidos conectar con el dispositivo de seguridad.Este comando especifica la dirección de origen, el netmask y la interfaz de los host permitidos conectar con el SSH. Puede ser ingresado las épocas múltiples para los host múltiples, las redes, o las interfaces. En este ejemplo, un host en el interior y un host en el exterior se permiten.`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:** De forma predeterminada, el dispositivo de seguridad permite el SSH versión 1 y la versión 2. ingresa este comando para restringir las conexiones a una versión específica:`pix(config)#` **`ssh version`** *`<version_number>`* **Nota:** El version_number puede ser 1 o 2.
5. **Opcional:** De forma predeterminada, las sesiones SSH son cerradas después de cinco minutos de inactividad. Este descanso se puede configurar dura por entre 1 y 60 minutos.`pix(config)#`**`ssh timeout`** *`minutes`*

Cómo utilizar a un cliente SSH

Proporcione el nombre de usuario y la contraseña de inicio de sesión del dispositivo de seguridad de la serie PIX 500 mientras abre la sesión SSH. Cuando comienza una sesión SSH, las visualizaciones de un punto (.) en la consola del dispositivo de seguridad antes de que aparezca el prompt de la autenticación de usuario SSH:

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

La visualización del punto no afecta a las funciones del SSH. El punto aparece en la consola cuando se genera una clave del servidor o un mensaje se desencripta con las claves privadas durante el intercambio de claves SSH antes de que ocurra la autenticación de usuario. Estas tareas pueden tomar a dos minutos o más. El punto es un indicador de progreso que verifica que el dispositivo de seguridad esté ocupado y no haya colgado.

Los SSH versión 1.x y 2 son protocolos totalmente diversos y no son compatibles. Descargue a un cliente compatible. Para obtener más información consulte la sección Obtener un Cliente SSH en Configuraciones Avanzadas.

Configuración de PIX

Este documento usa esta configuración:

Configuración de 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
```

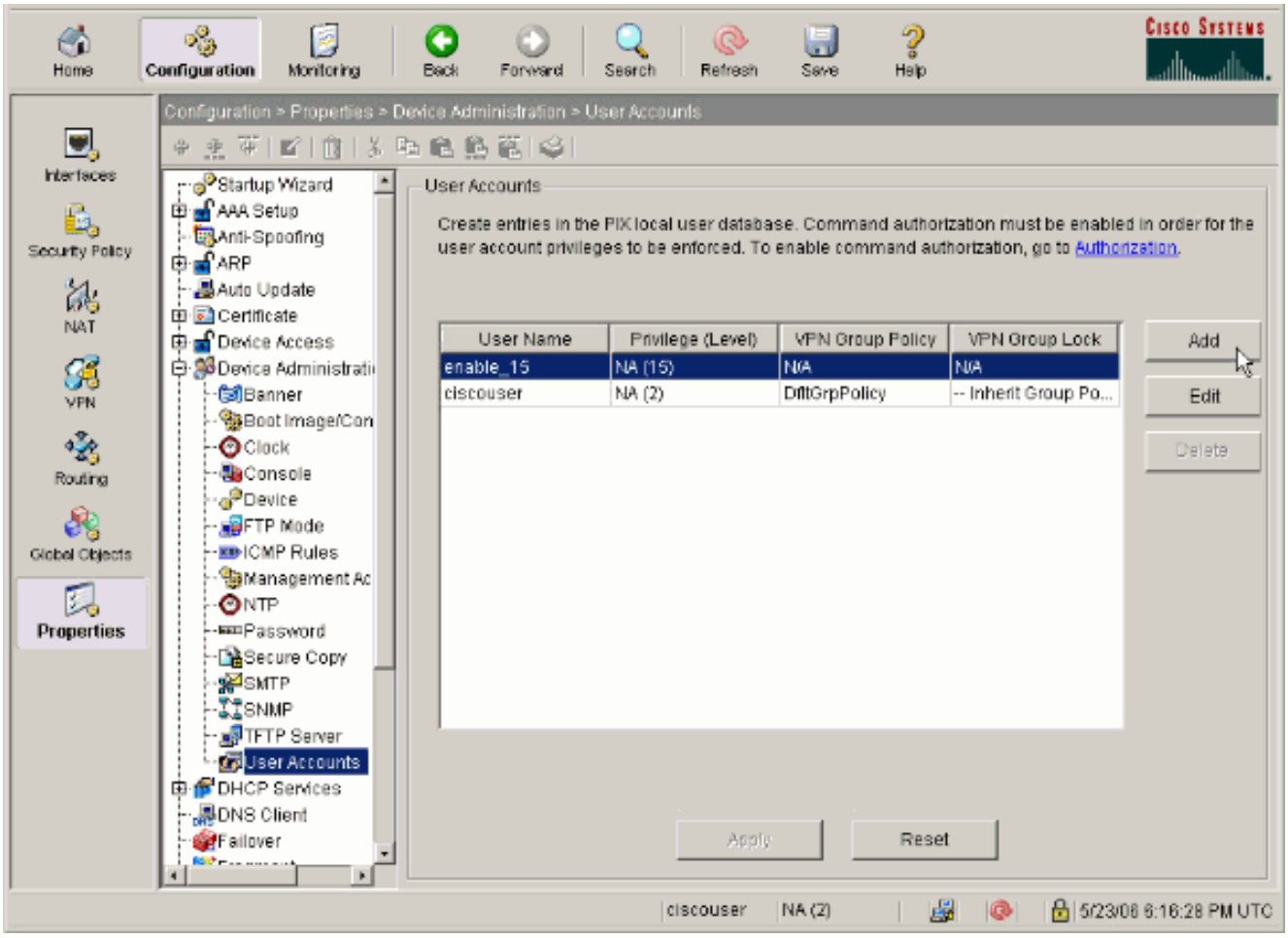
```
 nameif inside
 security-level 100
 ip address 172.16.5.10 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp permit any outside
no asdm history enable
arp timeout 14400
route outside 10.1.1.0 255.255.255.0 192.168.200.1 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 for the SSH configuration 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
!--- 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 10.1.1.2 255.255.255.255 outside !---
Allows the users on the host 172.161.1.1 !--- to access
the security appliance !--- on the inside interface. ssh
172.16.1.1 255.255.255.255 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
Cryptochecksum:a6b05fd04f9fbd0a39f1ca7328de91f7 : end
```

Nota: Para acceder a la la interfaz de administración del ASA/PIX utilizando el SSH, emita este comando: `ssh 172.16.16.160 255.255.255.255 Management`

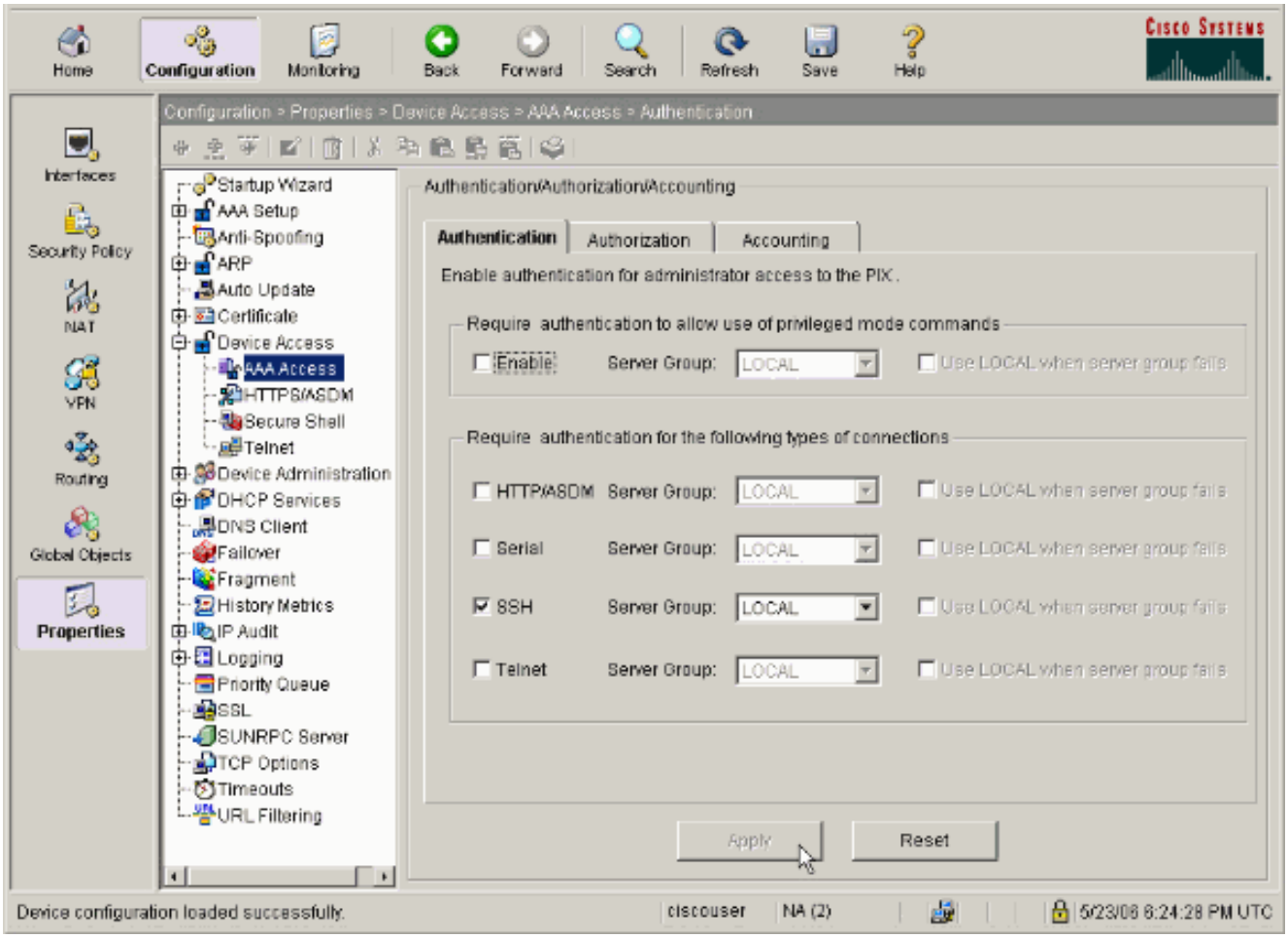
Configuración con el ASDM 5.x

Complete estos pasos de progresión para configurar el dispositivo para el SSH usando el ASDM:

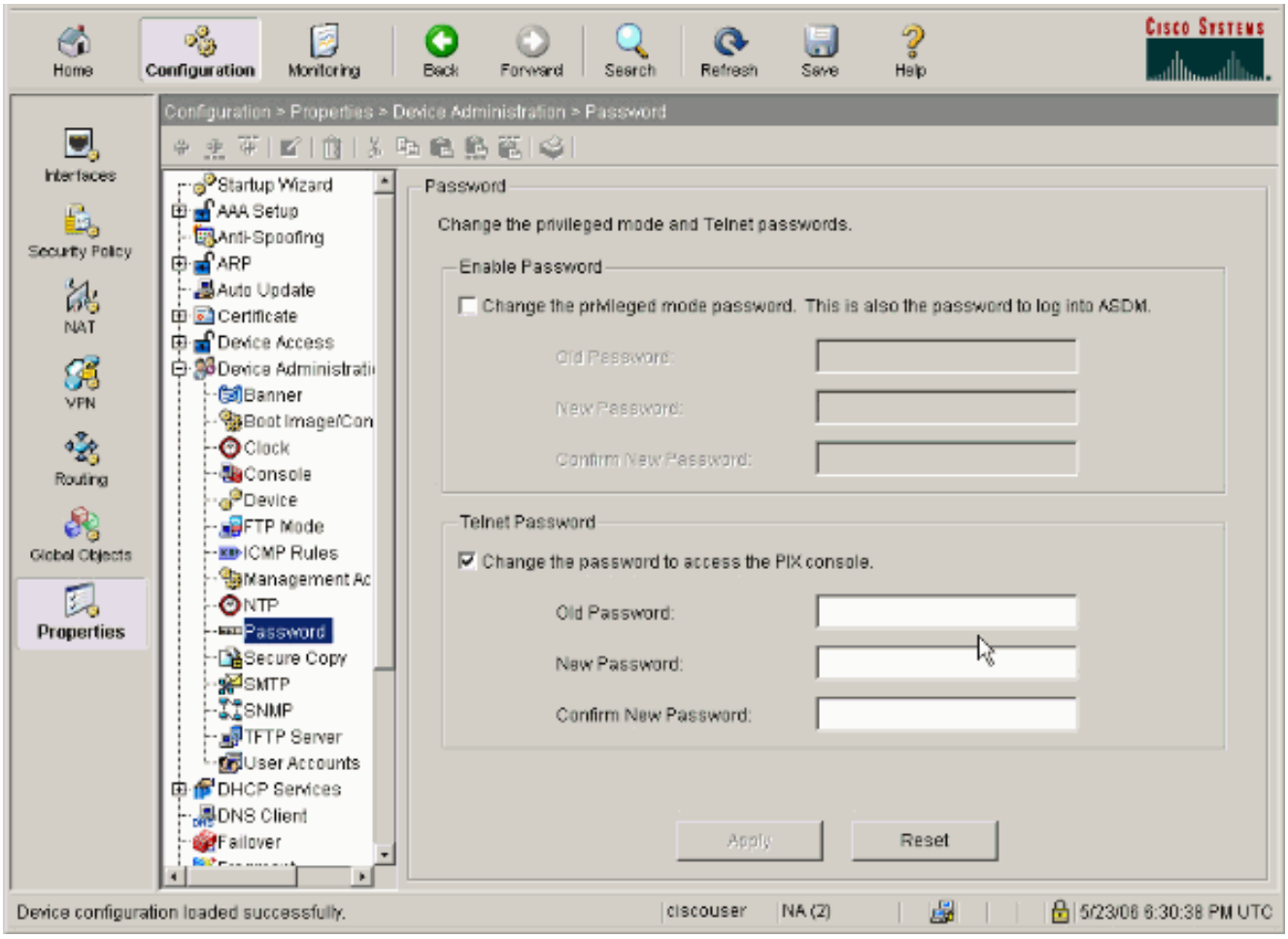
1. Elija **Configuration > Properties > Device Administration > User Accounts** para agregar un usuario con
   ASDM.



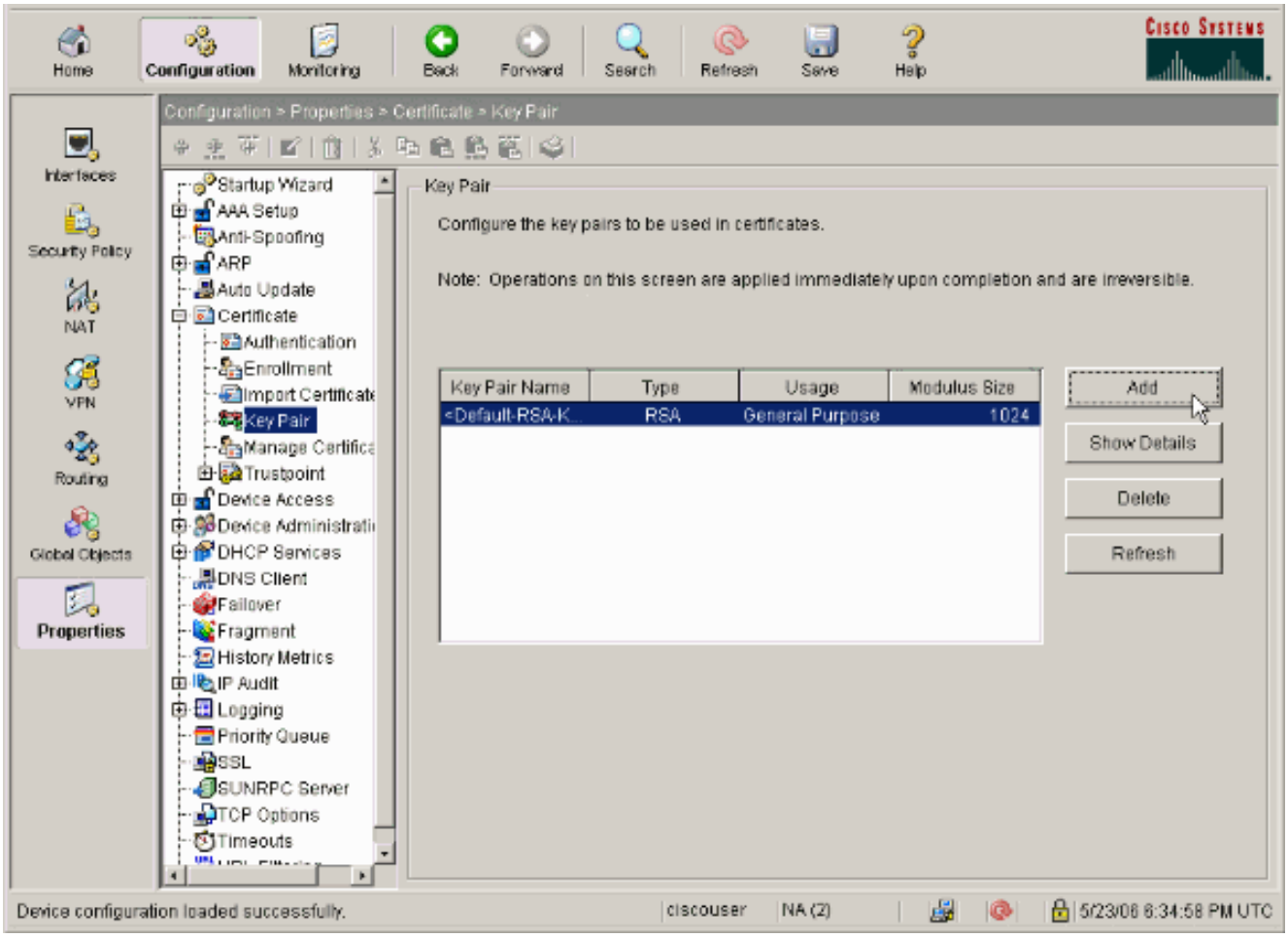
2. Elija **Configuration > Properties > Device Access > AAA Access > Authentication** para configurar la autenticación AAA para SSH con ASDM.



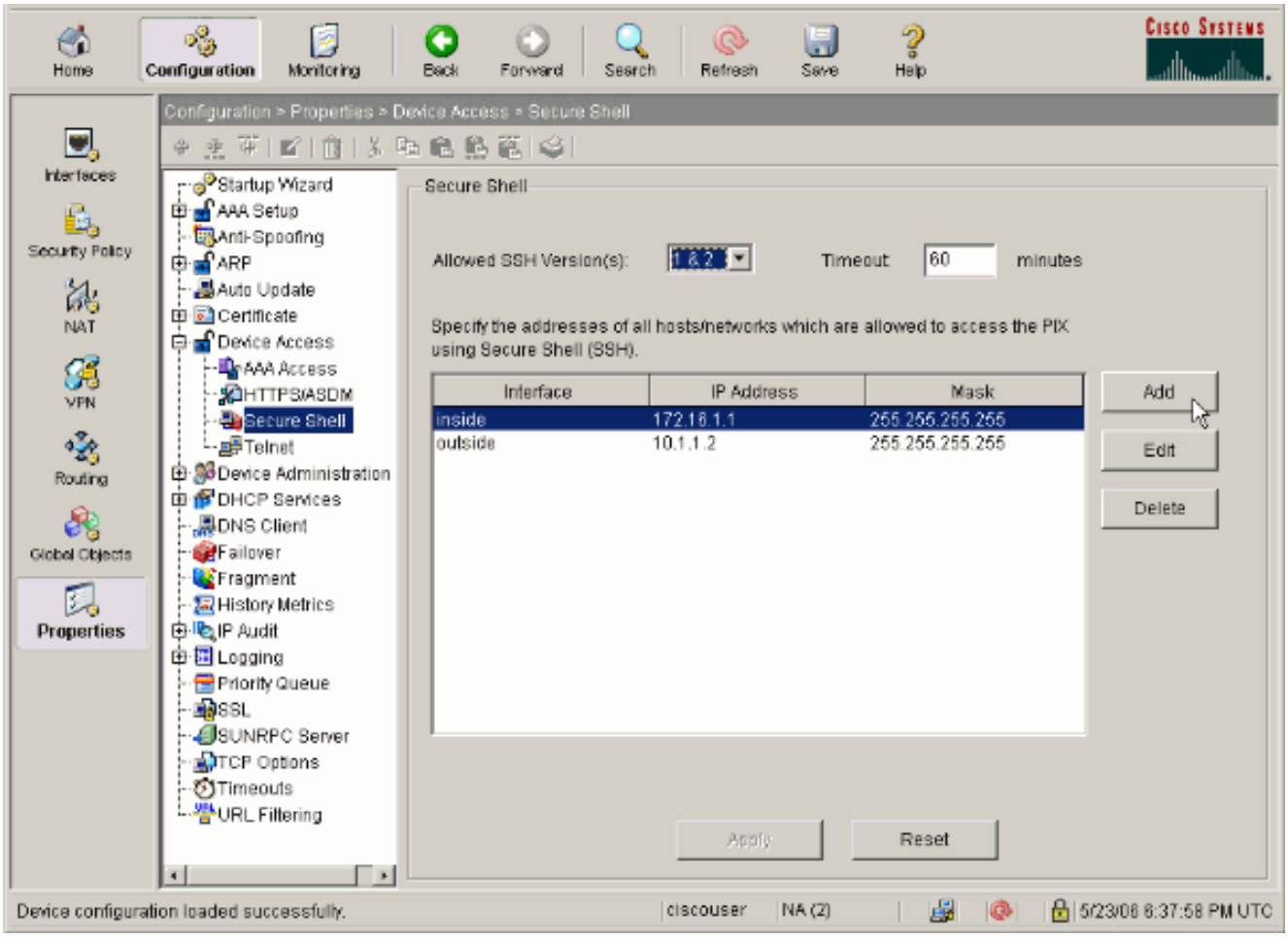
3. Elija **Configuration > Properties > Device Administration > Password** para cambiar la contraseña Telnet con
ASDM.



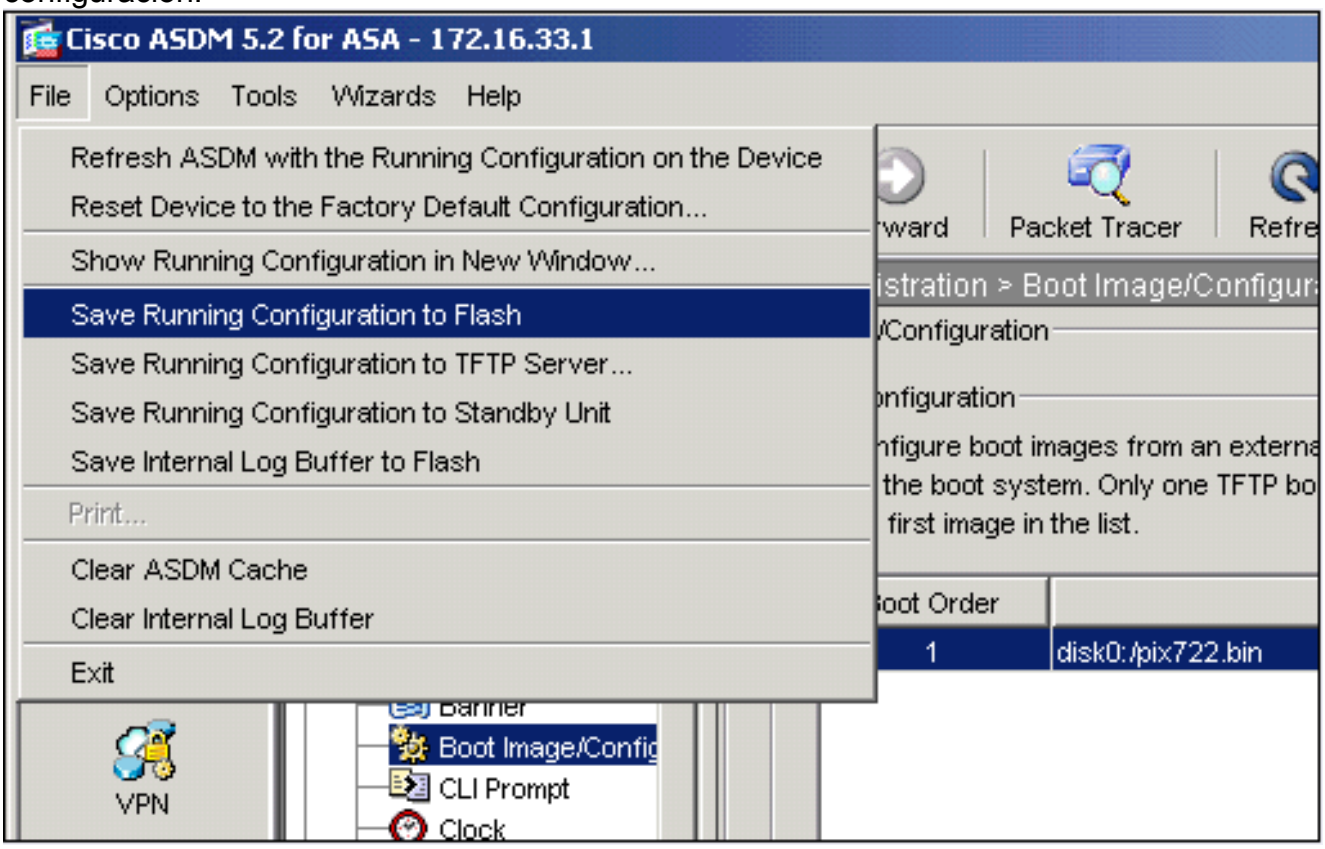
4. Elija **Configuration > Properties > Certificate > Key Pair**, haga clic en **Agregar** y use las opciones predeterminadas presentadas para generar las mismas claves RSA con ASDM.



5. Elija **Configuration > Properties > Device Access > Secure Shell** para usar ASDM y especificar los hosts permitidos para conectar con SSH y para especificar la versión y las opciones de tiempo de
espera.



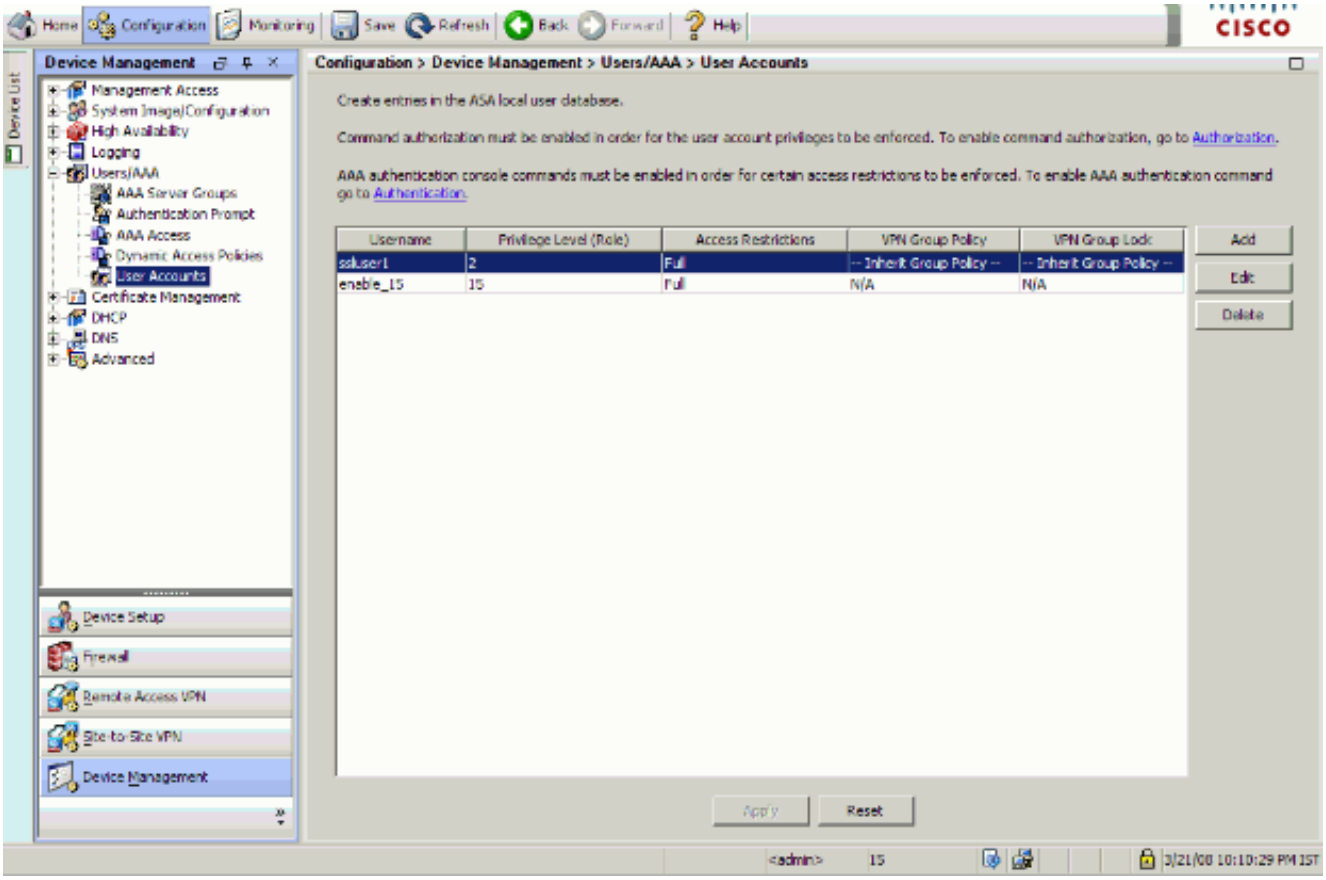
6. Haga clic en **Archivo > Guardar Configuración Actual en Memoria Flash** para guardar la configuración.



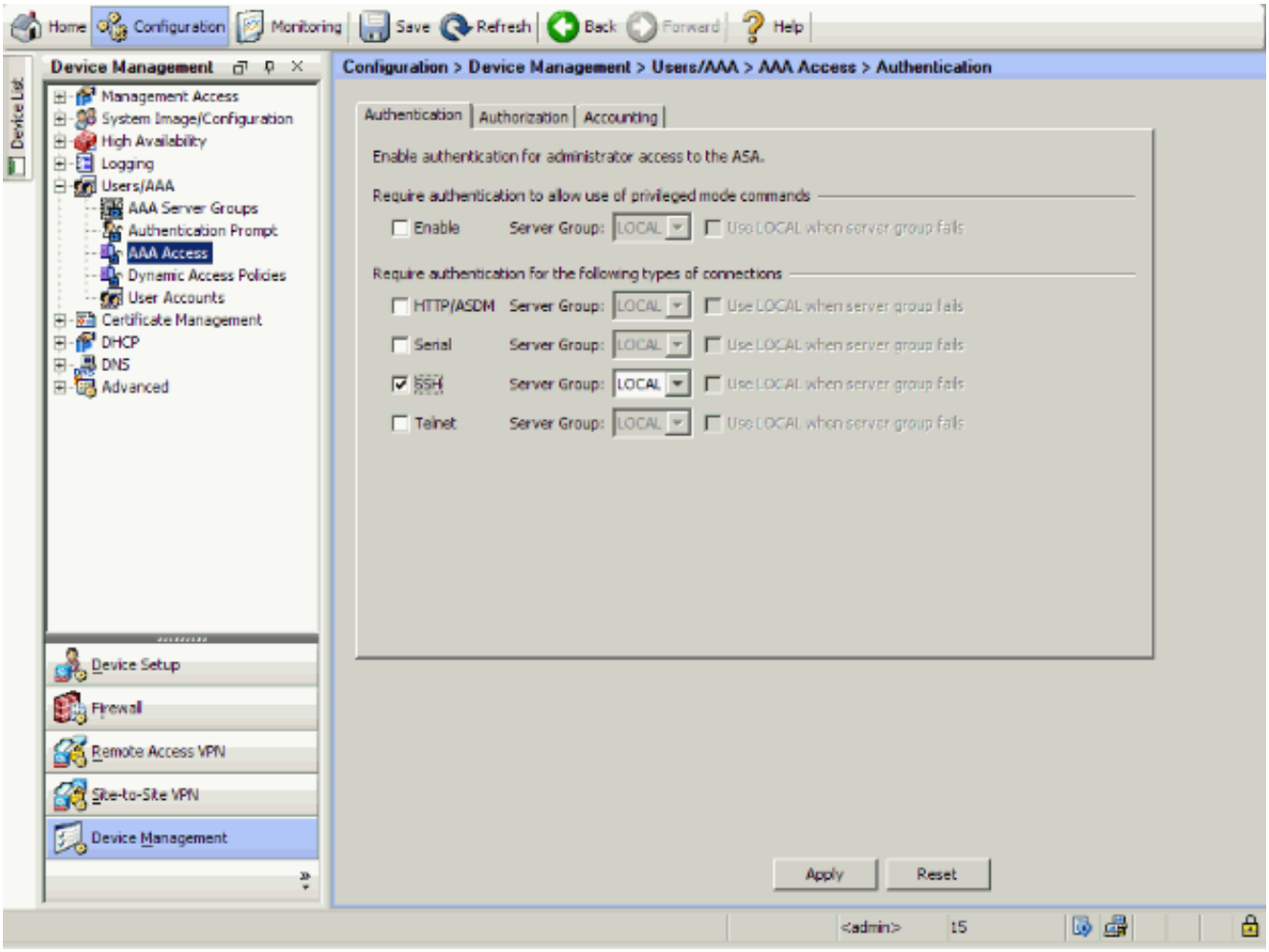
Configuración con el ASDM 6.x

Complete estos pasos:

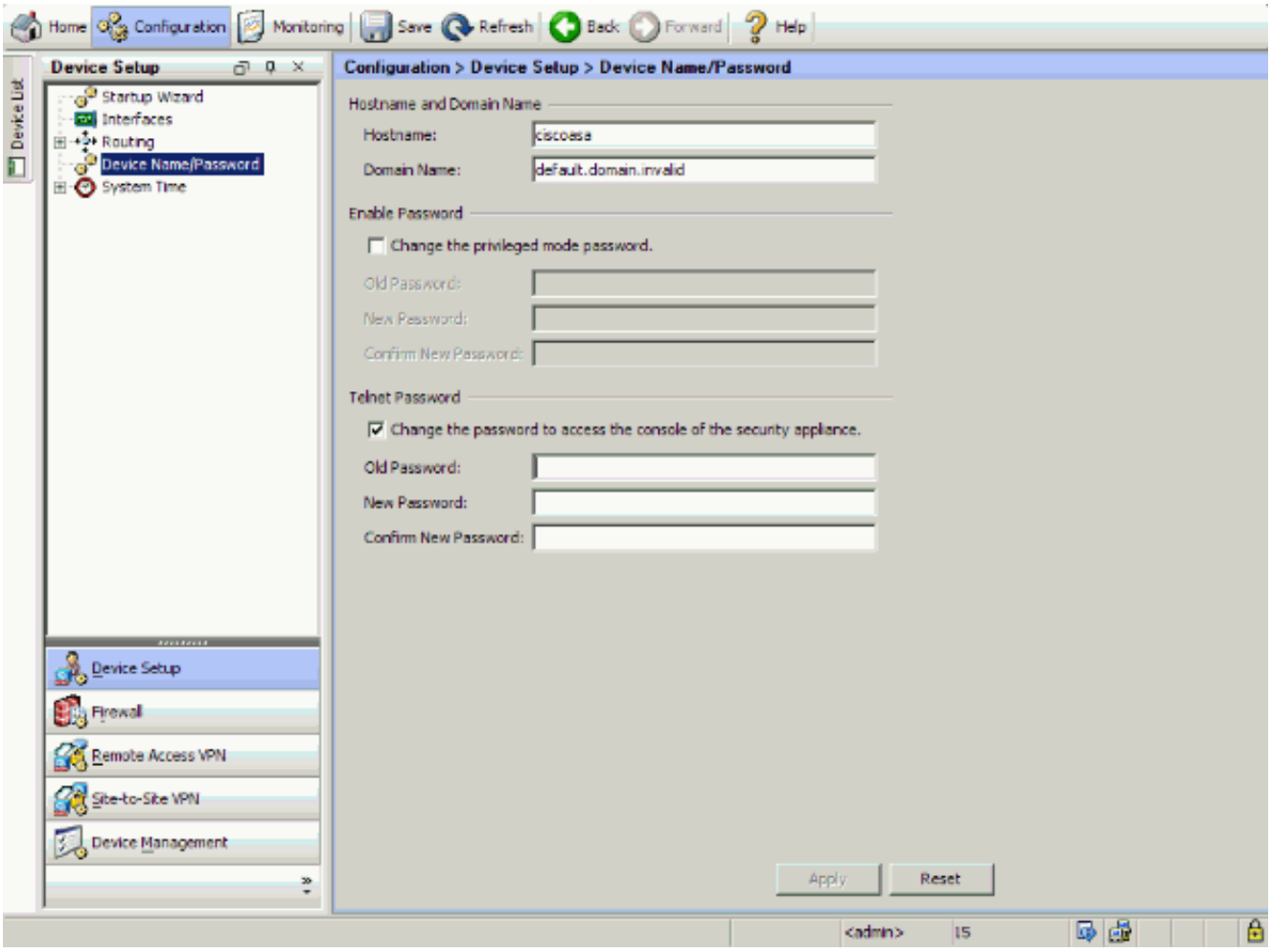
1. Elija **Configuration > Device Management > Users/AAA > User Accounts** para agregar un usuario con
ASDM.



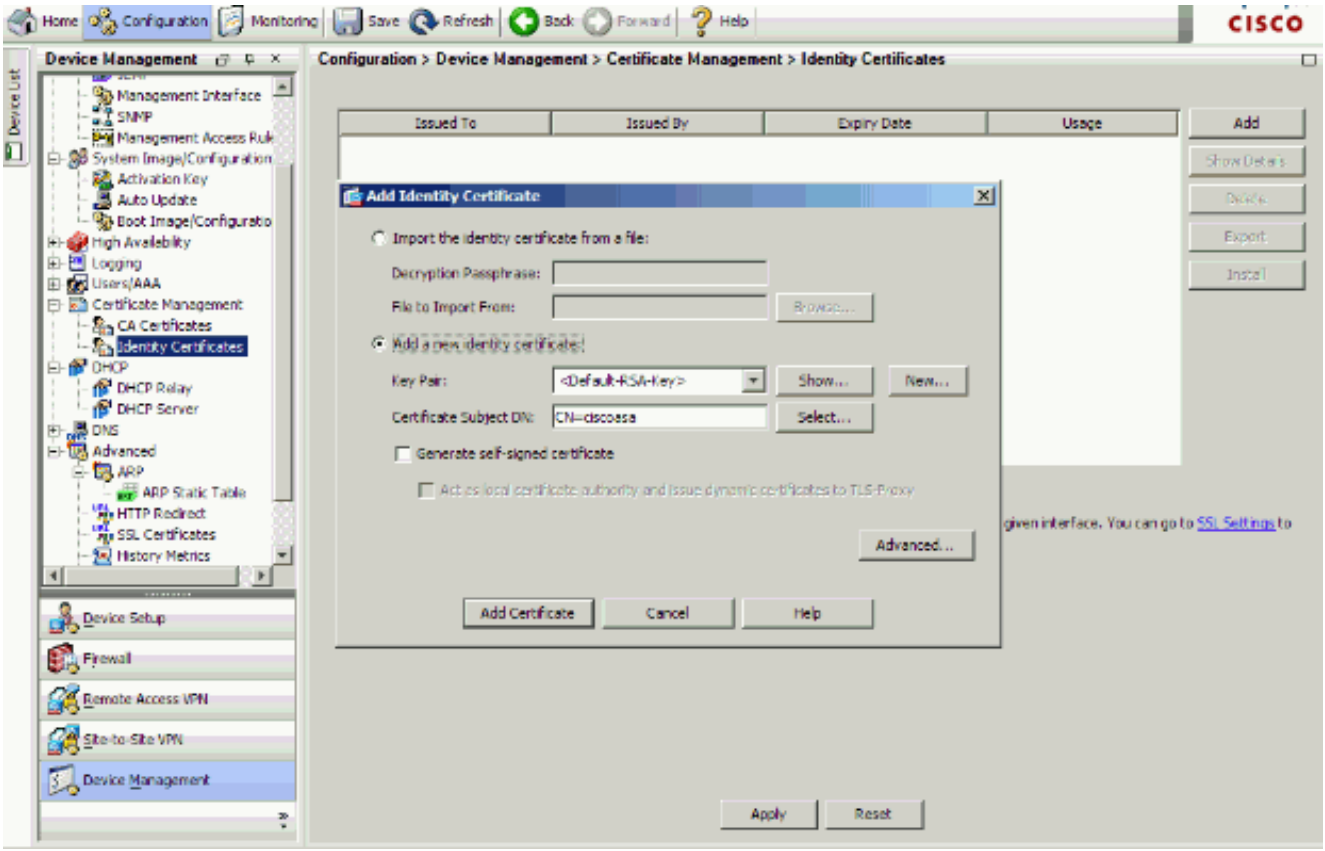
2. Elija **Configuration > Device Management > Users/AAA > AAA Access > Authentication** para configurar autenticación AAA para SSH con
ASDM.



3. Elija **Configuration > Device Setup > Device Name/Password** para cambiar la contraseña de Telnet con
ASDM.

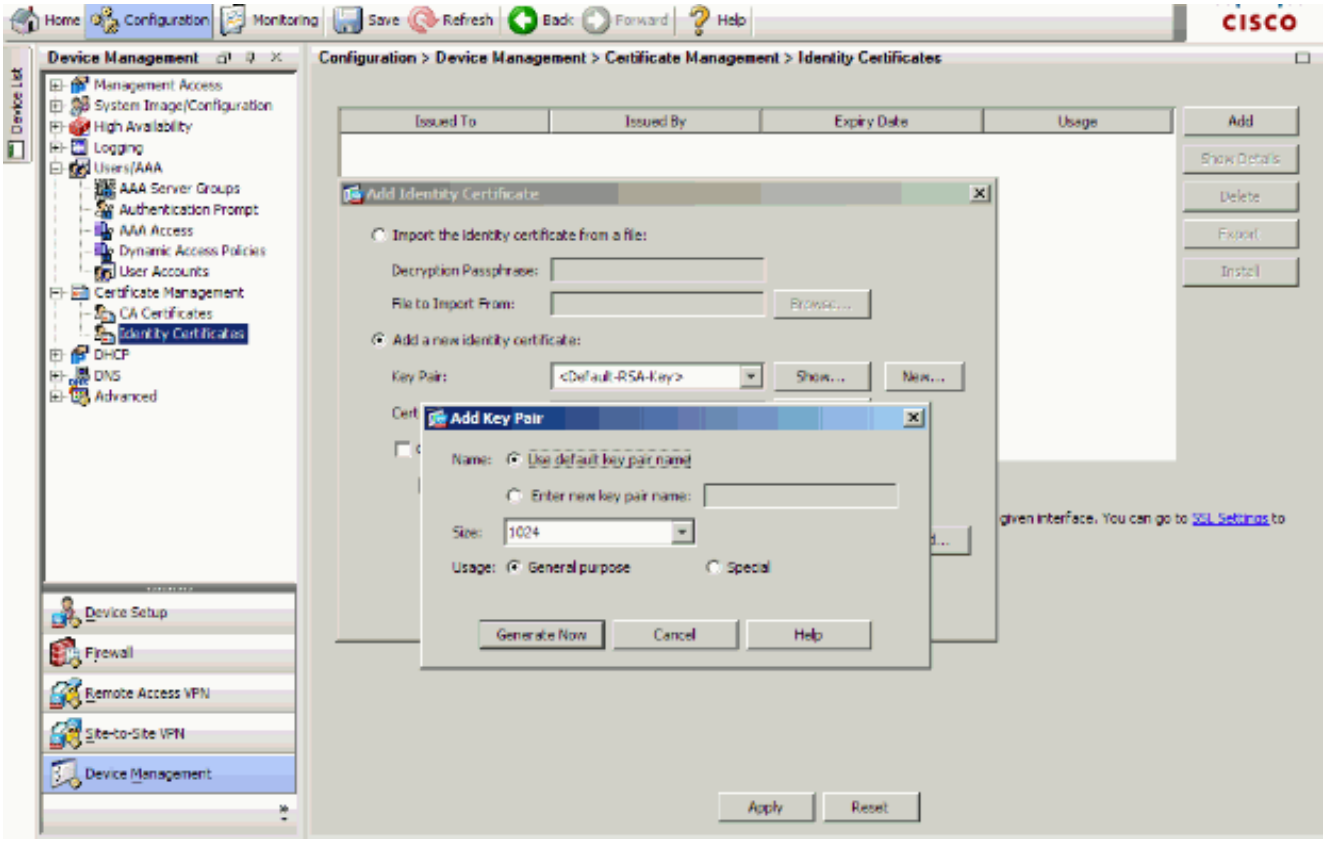


4. Elija **Configuration > Device Management > Certificate Management > Identity Certificates**, haga clic en **Agregar** y use las opciones predeterminadas presentadas para generar las mismas claves RSA con
ASDM.

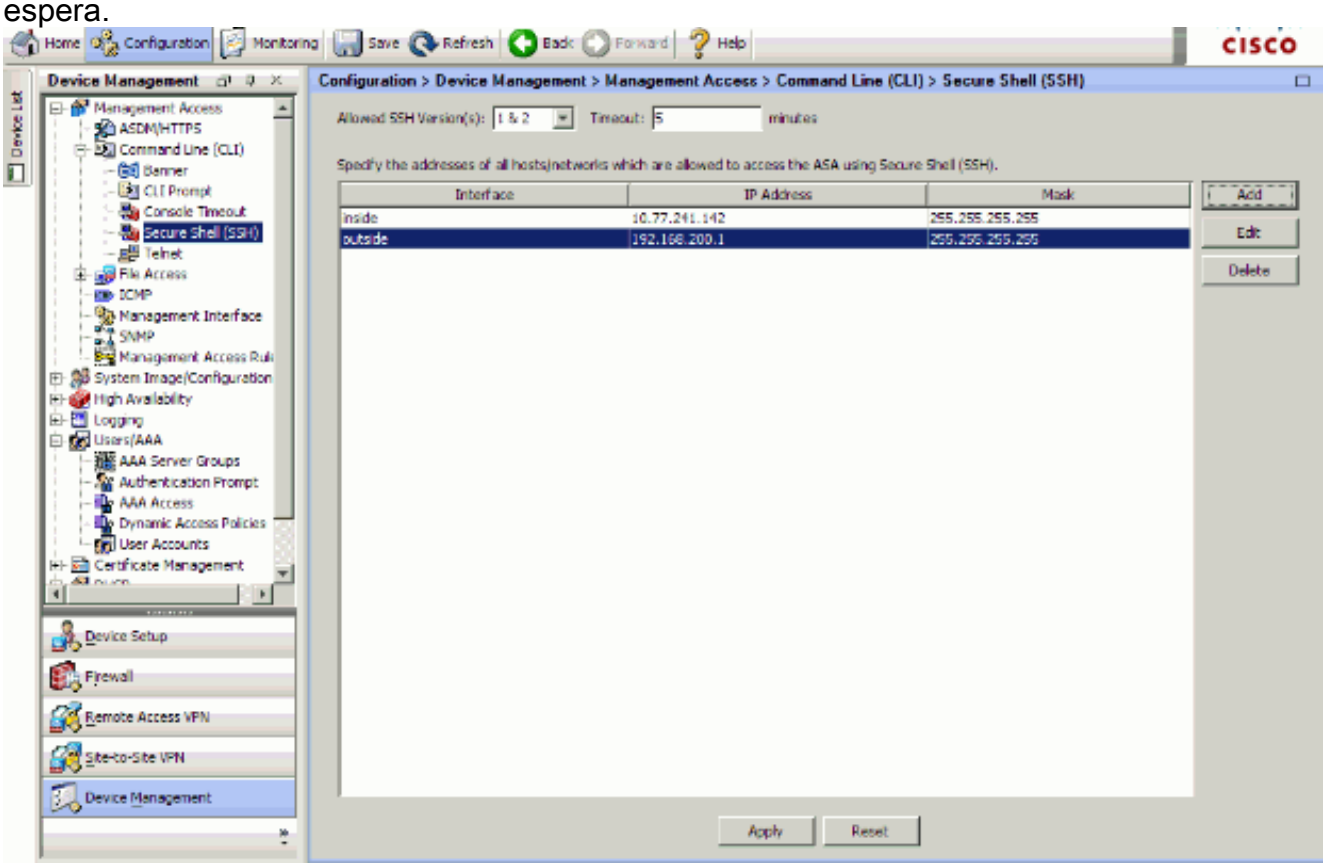


5. Bajo **agregue un nuevo** tecleo del **certificado de identidad nuevo** para agregar un par de

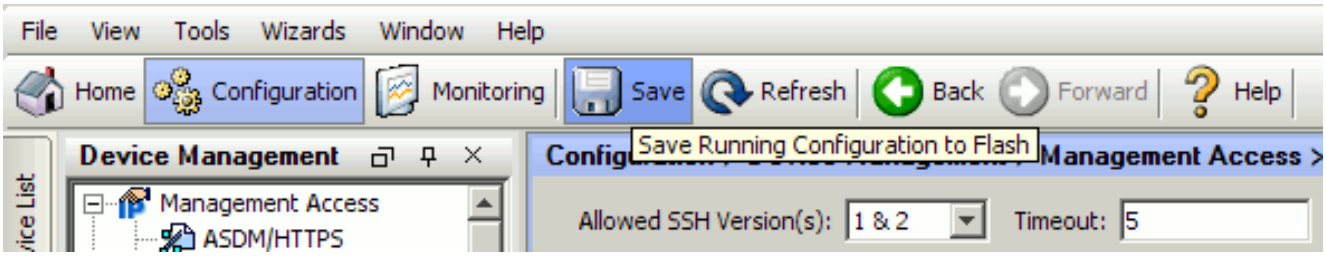
clave predeterminada si no lo hace existe uno. Entonces, haga clic en **Generar ahora**.



6. Elija **Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)** para usar ASDM y especificar hosts permitidos para conectarse con SSH y especificar la versión y las opciones de tiempo de espera.



7. Haga clic en **Guardar** e la parte superior de la ventana para guardar la configuración.



8. Cuando se le pregunte si desea guardar la configuración en la memoria flash, elija **Aplicar** para guardar la configuración.

Configuración Telnet

Para agregar acceso telnet a la consola y establecer el tiempo de espera de inactividad, emita el **comando telnet** en el modo de configuración global. De forma predeterminada, el dispositivo de seguridad cierra las sesiones telnet que se quedan inactivas durante cinco minutos. Para quitar el acceso telnet de un dirección IP previamente fijado, no utilices la *ninguna* forma de este 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}}
```

El comando telnet te deja especificar qué ordenadores principal pueden accesar la consola del dispositivo de seguridad con el telnet.

Nota: Puede habilitar el telnet al dispositivo de seguridad en todas las interfaces. Sin embargo, el dispositivo de seguridad hace que todo el tráfico telnet a la interfaz exterior esté protegido por el IPSec. Para habilitar una sesión telnet a la interfaz exterior, el IPSec de la configuración en la interfaz exterior para incluir el tráfico IP que es generada por el dispositivo de seguridad y para habilitar el telnet en la interfaz exterior.

Nota: Generalmente, si ninguna interfaz tiene un nivel de seguridad 0 o menor que cualquier otra interfaz, entonces PIX/ASA no permite Telnet en esa interfaz.

Nota: No se recomienda para acceder al dispositivo de seguridad a través de una sesión telnet. La información de los credenciales de autenticación, tal como contraseña, se envía como texto claro. El servidor Telnet y la Comunicación del cliente sucede solamente con el texto sin formato. Cisco recomienda utilizar el SSH para una comunicación de datos segura.

Si ingresa una dirección IP, debe también ingresar un netmask. No hay una máscara de red predeterminada. No utilices la máscara del red secundaria de la red interna. La máscara de red es solamente una máscara de bits para la dirección IP. Para limitar el acceso a una sola dirección IP, use 255 en cada octeto; por ejemplo, 255.255.255.255.

Si el IPSec actúa, puede especificar un nombre no seguro de la interfaz, que es típicamente la interfaz exterior. Como mínimo, puede configurar el comando de **mapa crypto** para especificar un nombre de la interfaz con el **comando telnet**.

Emita el comando **password** para fijar una contraseña que le otorgue acceso telnet a la consola. El valor predeterminado es cisco. Emita el comando **who** para ver qué dirección IP accede actualmente la consola del dispositivo de seguridad. Emita el comando **kill** para terminar una sesión de consola Telnet activa.

Para habilitar una sesión telnet a la interfaz interior, revise estos ejemplos:

Ejemplo 1

Este ejemplo permite que solamente el host 10.1.1.1 acceda a la consola del dispositivo de seguridad a través del telnet:

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

Ejemplo 2

Este ejemplo permite que solamente la red 10.0.0.0/8 acceda a la consola del dispositivo de seguridad a través del telnet:

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

Ejemplo 3

Este ejemplo permite que todas las redes accedan a la consola del dispositivo de seguridad a través del telnet:

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

Si usa el comando **aaa** con la palabra clave de la consola, el acceso a la consola telnet se debe autenticar con un servidor de autenticación.

Nota: Si ha configurado el comando **aaa** para requerir la autentificación para el acceso a la consola telnet del dispositivo de seguridad y el acceso a la consola pide un tiempo hacia fuera, puede acceder al dispositivo de seguridad de la consola en serie. Para hacer esto, ingresa el nombre de usuario del dispositivo de seguridad y la contraseña que se fija con el comando **enable password**.

Emita el comando **telnet timeout** para fijar el tiempo máximo que una sesión telnet de la consola puede estar inactiva antes de que sea terminado una sesión por el dispositivo de seguridad. No puede utilizar el **no telnet comand** con el comando **telnet timeout**.

Este ejemplo muestra cómo cambiar la duración de la marcha lenta de la sesión máxima:

```
hostname(config)#telnet timeout 10 hostname(config)#show running-config telnet timeout telnet timeout 10 minutes
```

Soporte SSH/Telnet en el ACS 4.x

Si mira las funciones RADIUS, puede utilizar RADIUS para las funciones SSH.

Cuando se intenta acceder el dispositivo de seguridad con el telnet, SSH, HTTP, o una conexión de la consola en serie y el tráfico corresponde con una sentencia de autenticación, el dispositivo de seguridad pide un nombre de usuario y contraseña. Entonces envía estas credenciales al servidor RADIUS (ACS), y concede o niega el acceso CLI basado en la respuesta del servidor.

Para obtener más información consulte la sección Soporte del Servidor de AAA y de Bases de Datos Locales de Cómo configurar Servidores de AAA y Bases de Datos Locales.

Por ejemplo, su dispositivo de seguridad 7.0 ASA necesita una dirección IP de la cual pueda aceptar conexiones, como por ejemplo:

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

Consulte la sección de accesso SSH que permite de configurar los servidores de AAA y las bases

de datos locales para más información.

Consulte PIX/ASA: Consulte Cut-through Proxy para Network Access con TACACS+ y RADIUS Server para más información sobre cómo configurar el acceso SSH/Telnet a PIX con autenticación ACS.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Debug SSH

Emita el comando **debug ssh** para activar el debugging SSH.

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

Esta salida muestra que el pedido de autenticación del host 10.1.1.2 (afuera al PIX) al “pix” es acertado:

```
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 !--- Authentication for the PIX 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
```

Si un usuario da un nombre de usuario incorrecto, por ejemplo, el "pix1" en vez del “pix”, el firewall PIX rechaza la autenticación. Esta salida de los debugs muestra la autenticación fallida:

```
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 !--- Authentication for pix1 was not successful due to
the wrong username.
```

De forma similar, si el usuario proporciona la contraseña incorrecta, este ouput del debug le muestra la autenticación fallida.

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

Cómo ver las sesiones SSH activas

Emita este comando para marcar el número de sesiones SSH que estén conectadas y del estado

de la conexión al 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
```

Elija **Monitoring > Properties > Device Access > Secure Shell Sessions** para ver las sesiones con ASDM.

Cómo ver la clave pública RSA

Emita este comando para ver la porción pública de los claves RSA en el dispositivo de seguridad:

```
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
```

Elija la **configuración > las propiedades > el certificado > el par clave**, y haga clic los **detalles de la demostración** para ver las claves RSA con el ASDM.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Cómo quitar los claves RSA del PIX

Ciertas situaciones, por ejemplo cuando actualiza el sofware PIX o cambias el SSH versión en el PIX, pueden requerirte quitar y reconstruir los claves RSA. Emita este comando para quitar el par clave RSA del PIX:

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

Elija la **configuración > las propiedades > el certificado > el par clave**, y haga clic la **cancelación** para quitar las claves RSA con el ASDM.

Conexión SSH fallada

Mensaje de error en el PIX/ASA:

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

El mensaje de error correspondiente en la máquina de cliente SSH:

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

Para resolver este problema, quite y reconstruya las claves RSA. Publique este comando para quitar el par clave RSA del ASA:

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

Publique este comando para generar la nueva clave:

```
ASA(config)# crypto key generate rsa modulus 1024
```

Incapaz de acceder el ASA con SSH

Mensaje de error:

```
ssh_exchange_identification: read: Connection reset by peer
```

Complete estos pasos para resolver el problema:

1. Recargue el ASA o quite todos los config relacionados SSH y las claves RSA.
2. Configure de nuevo los comands de SSH y regenere las claves RSA.

Incapaz de acceder el ASA secundario usando SSH

Cuando el ASA está en el modo de fallas, no es posible a SSH al ASA espera a través del túnel VPN. Esto es porque el tráfico de la contestación para SSH toma la interfaz exterior del ASA espera.

Información Relacionada

- Dispositivos de seguridad Cisco PIX de la serie 500
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Configuración de las conexiones SSH - Routeres Cisco y Concentradores Cisco
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems