Versión de ASA 9.x SSH y Telnet en el ejemplo de configuración de las interfaces interior y exterior

Contenido

Introducción

Este documento describe cómo configurar el Secure Shell (SSH) en las interfaces interior y exterior de las versiones 9.x del dispositivo de seguridad del Cisco Series y posterior. Cuando usted debe configurar y monitorear el dispositivo de seguridad adaptante de Cisco (ASA) remotamente con el CLI, el uso de Telnet o de SSH se requiere. Porque las comunicaciones Telnet se envían en el texto claro, que puede incluir las contraseñas, SSH se recomienda altamente. El tráfico de SSH se cifra en un túnel y de tal modo las ayudas protegen las contraseñas y otros comandos configuration sensibles contra la interceptación.

El ASA 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.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 9.1.5 del software de firewall de Cisco ASA.

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: El SSH versión 2 (SSHv2) se soporta en las Versiones de ASA 7.x y posterior.

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 9.x y posterior.

Convenciones

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

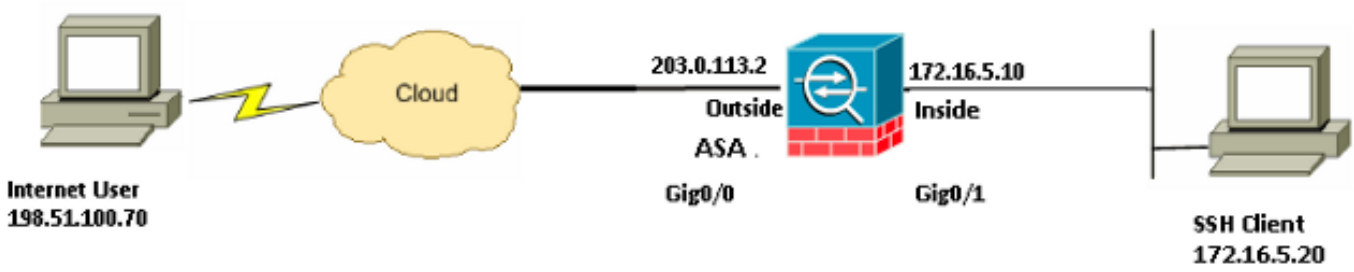
Configurar

Utilice la información que se proporciona en esta sección para configurar las características que se describen en este documento.

> Nota: Cada paso para la configuración se describe que proporciona la información que es necesaria para utilizar el CLI o al Administrador de dispositivos de seguridad adaptante (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 ejemplo de configuración, el ASA se considera ser el servidor SSH. El tráfico de los clientes SSH (198.51.100.70/32 y 172.16.5.20/24) al servidor SSH se cifra. El dispositivo de seguridad soporta las funciones de SSH shell remoto que se proporcionan en los SSH versión 1 y 2 y soporta el Data Encryption Standard (DES) y las cifras 3DES. Los SSH versión 1 y 2 son diferentes y no son interoperables.

Configuraciones SSH

En este documento, se utilizan estas configuraciones:

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

Acceso SSH al dispositivo de seguridad

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

1. Las sesiones SSH requieren siempre una forma de autenticación tal como un nombre de usuario y contraseña. Hay dos métodos que usted puede utilizar para cumplir este requisito.

   El primer método que usted puede utilizar para cumplir este requisito es configurar un nombre de usuario y contraseña con el uso del 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: Si usted utiliza un TACACS+ o a un grupo de servidor de RADIUS para la autenticación, usted puede configurar el dispositivo de seguridad de modo que utilice la base de datos local como método del retraso si el servidor de AAA es inasequible. Especifique el nombre de grupo de servidores y luego LOCAL (LOCAL distingue entre mayúsculas y minúsculas). Cisco recomienda que usted utiliza el mismo nombre de usuario y la contraseña en la base de datos local y el servidor de AAA, porque el prompt del dispositivo de seguridad no da ninguna indicación del método se utiliza que.Para especificar un **backup local** para el **TACACS+**, utilice esta configuración para la autenticación SSH:
   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```
   Puede alternativamente utilizar las bases de datos locales como tu método principal de autentificación sin el retraso. Para hacer

esto, ingrese solo **LOCAL**:

`ASA(config)#aaa authentication ssh console LOCAL`**El segundo método** que usted puede utilizar para cumplir este requisito es utilizar el nombre de usuario predeterminado del **ASA** y la contraseña de Telnet predeterminada de **Cisco**. Usted puede cambiar la contraseña de Telnet con este comando:

`ASA(config)#passwd password`Nota: **El comando password** puede también ser utilizado en esta situación, como ambos comandos function semejantemente.

2. Genere un par clave RSA para el Firewall ASA, que se requiere para SSH:

   `ASA(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. Un valor de 2048 se recomienda. El comando que se utiliza para generar un par clave RSA es diferente para las versiones de software ASA anterior que la versión 7.x. En las versiones anteriores, un Domain Name debe ser fijado antes de que usted pueda crear las claves. En el modo de contexto múltiple, usted debe generar las claves RSA para cada contexto.
3. Especifique los host que se permiten conectar con el dispositivo de seguridad. Este comando especifica la dirección de origen, el netmask, y la interfaz del host que se permite conectar con 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:

   ```
   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 paso es opcional. Por abandono, el dispositivo de seguridad permite el SSH versión 1 y la versión 2. ingresa este comando para restringir las conexiones a una versión específica:

   `ASA(config)# ssh version <version_number>`Nota: **El version_number** puede ser **1** o **2.**
5. Este paso es opcional. Por abandono, las sesiones SSH son cerradas después de cinco minutos de inactividad. Este descanso se puede configurar para durar entre 1 y 60 minutos:

   `ASA(config)#ssh timeout minutes`

Configuración ASA

Utilice esta información para configurar el ASA:

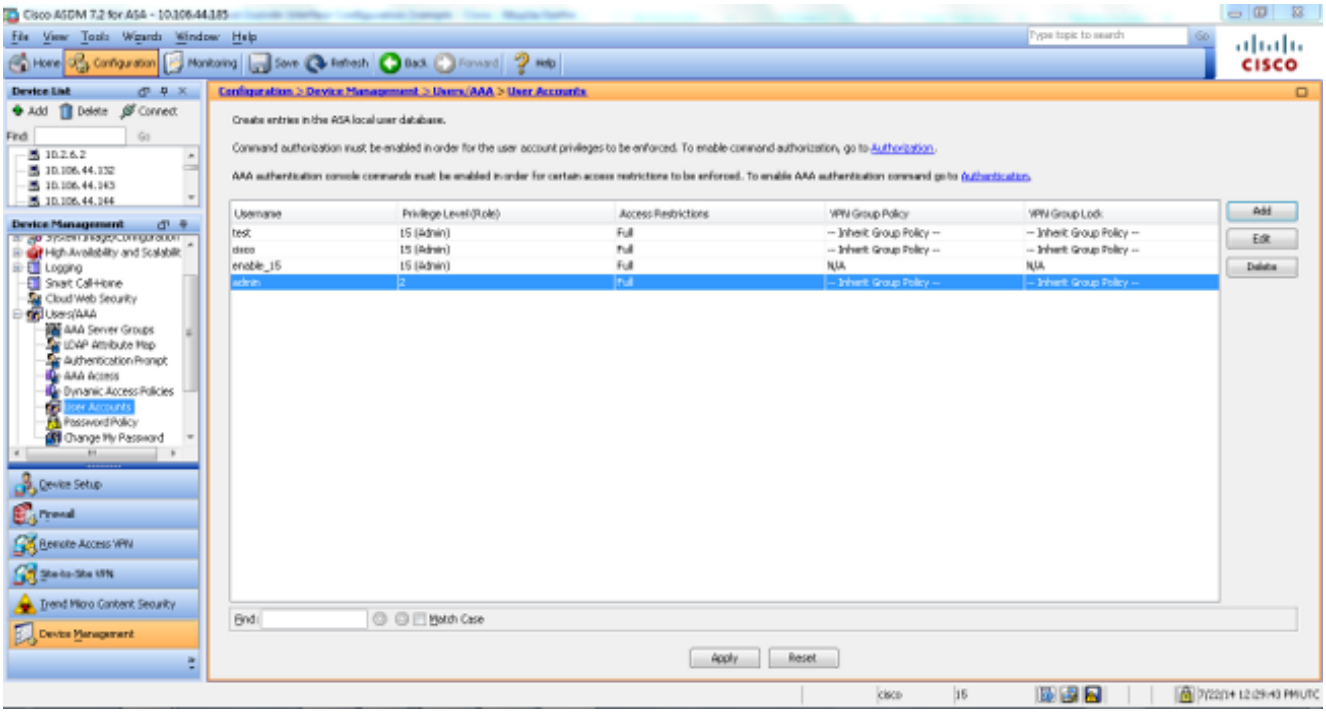
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

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
```

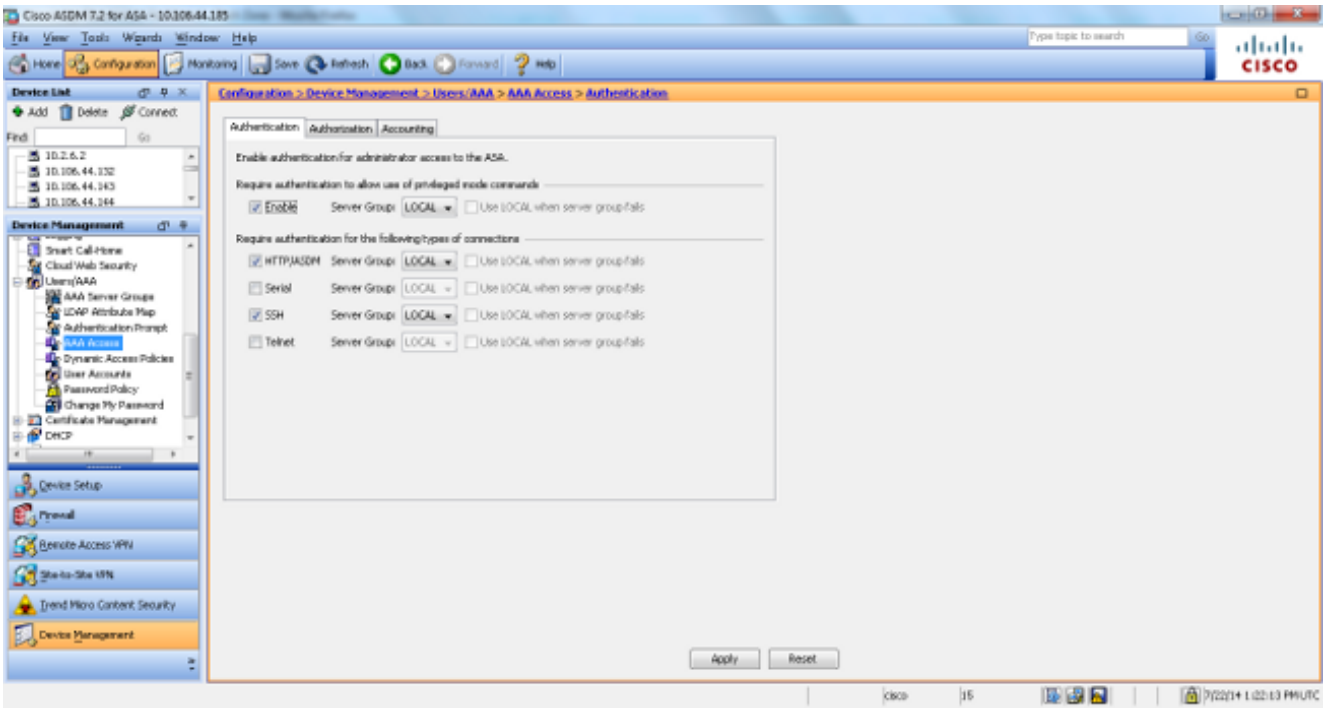
Configuración de la versión 7.2.1 del ASDM

Complete estos pasos para configurar la versión 7.2.1 del ASDM:

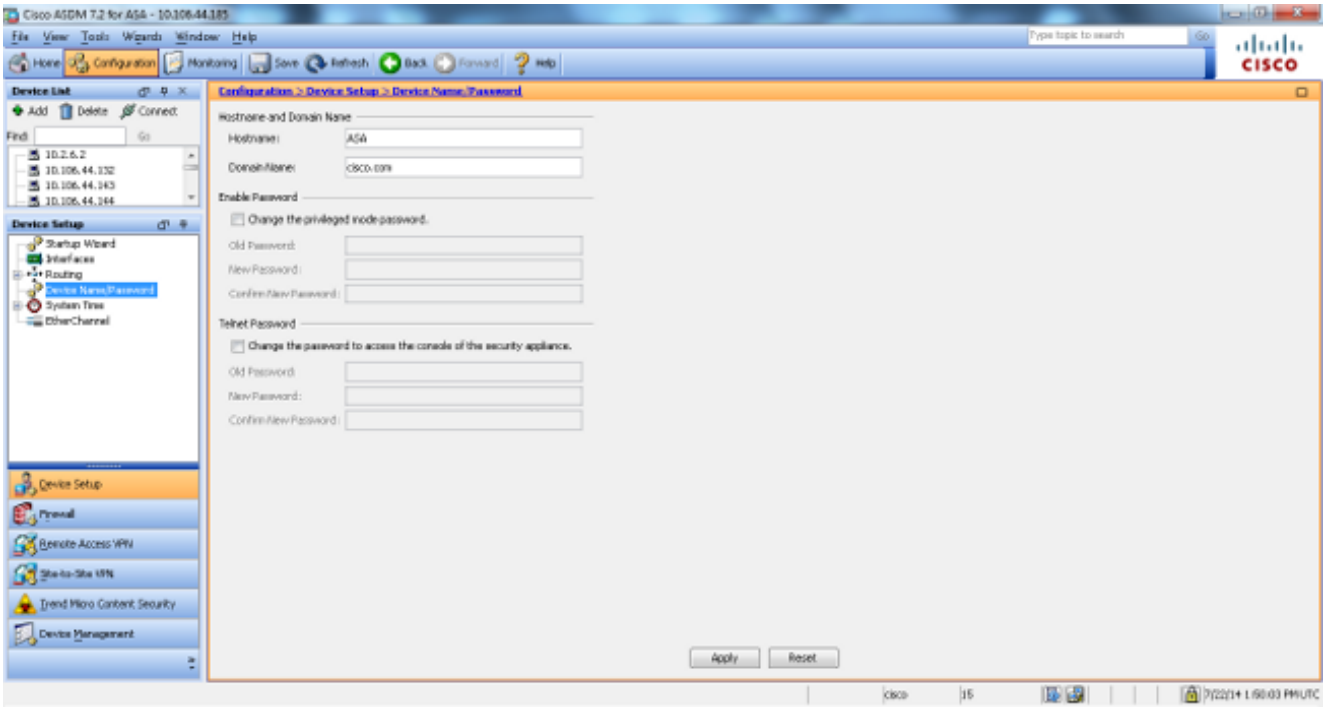
1. Navegue a la **configuración > a la Administración de dispositivos > a Users/AAA > a las cuentas de usuario** para agregar a un usuario con el ASDM.



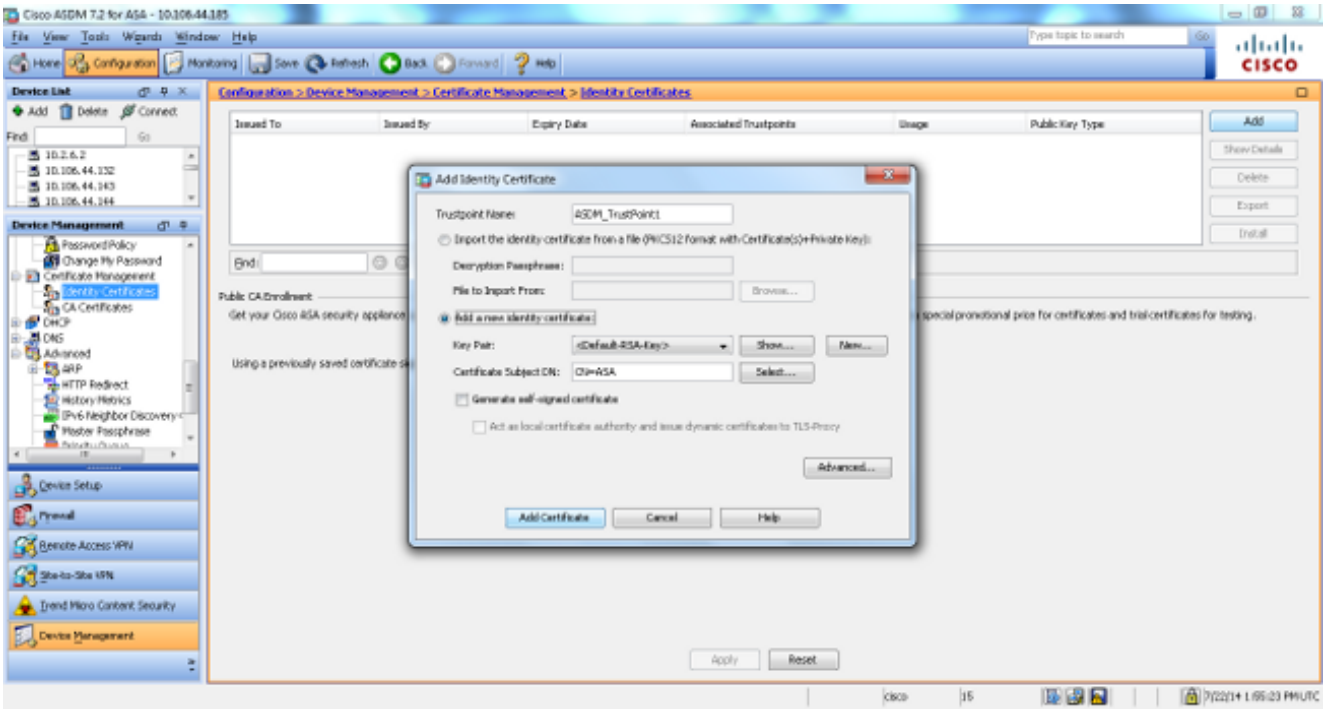
2. Navegue a la **configuración > a la Administración de dispositivos > al acceso > a la autenticación Users/AAA >AAA** para configurar la autenticación AAA para SSH con el ASDM.



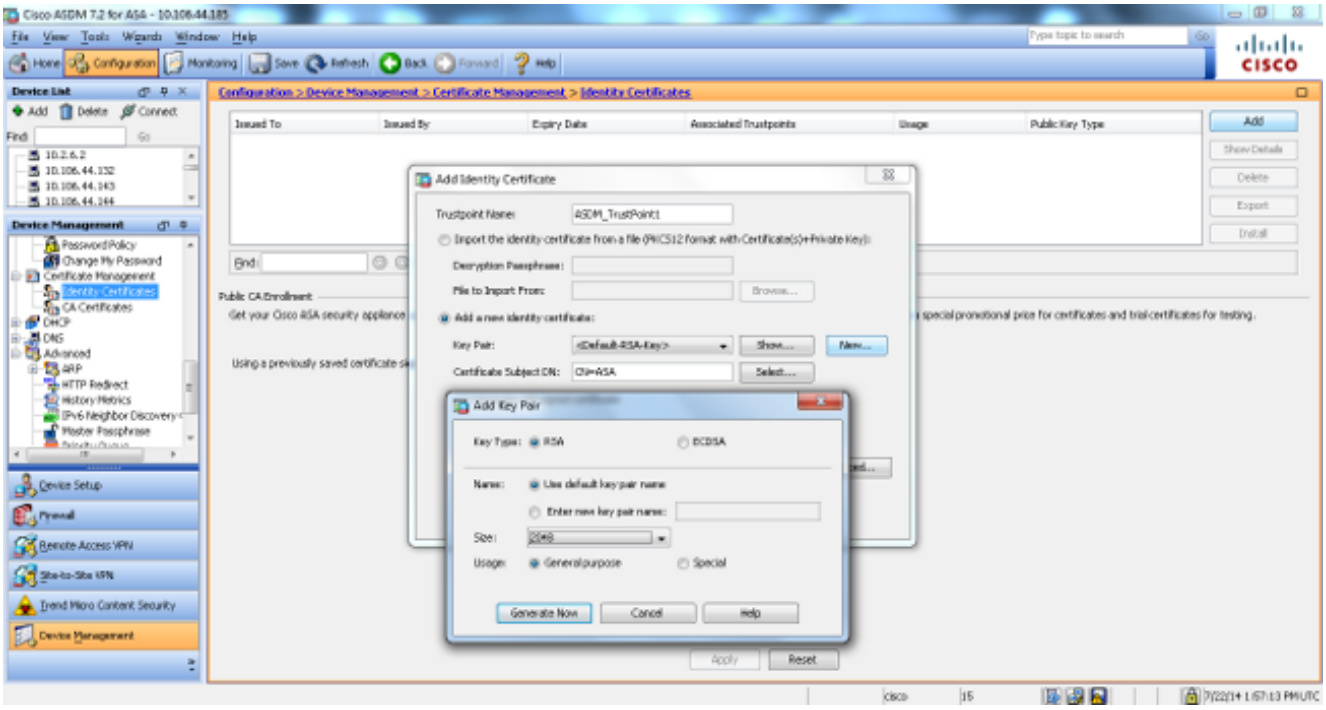
3. Navegue a la **configuración > a la configuración > al Nombre del dispositivo/a la contraseña de dispositivo** para cambiar la contraseña de Telnet con el ASDM.



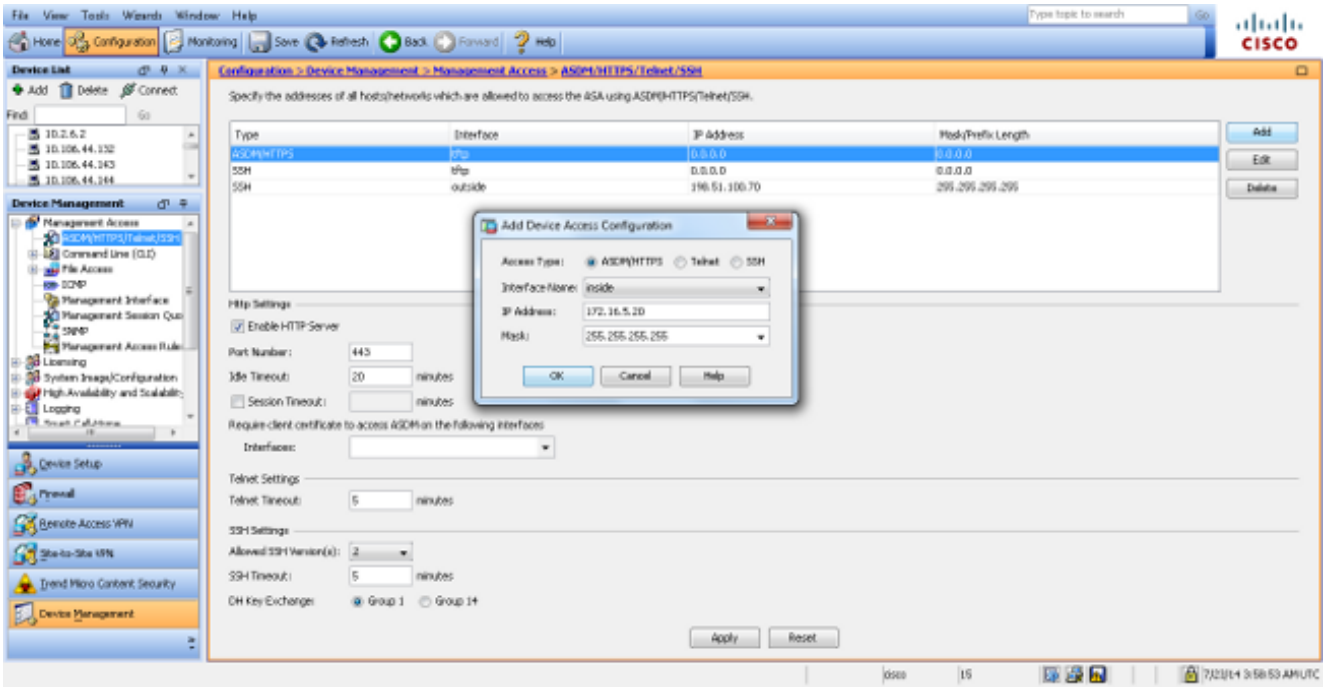
4. Navegue a la **configuración > al Certificate Management (Administración de certificados) > a los certificados de identidad de la Administración de dispositivos**, el tecleo **agrega**, y utiliza las opciones predeterminadas que están disponibles para generar las mismas claves RSA con el ASDM.



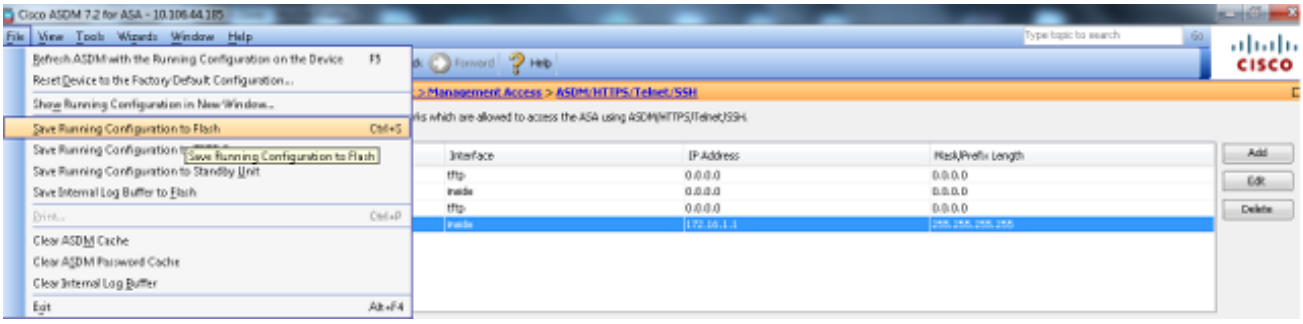
5. Haga clic el **agregar un nuevo** botón de radio del **certificado de identidad** y haga clic **nuevo** para agregar un par de clave predeterminada, si no existe uno. Complete una vez, tecleo **ahora generan**.



6. Navegue a la **configuración > a la Administración de dispositivos > al Acceso de administración > a la línea de comando (CLI) > Secure Shell (SSH)** para utilizar el ASDM de modo que usted pueda especificar los host que se permiten conectar con SSH y para especificar la versión y las opciones de tiempo de espera.



7. Haga clic la **salvaguardia de la** ventana emergente para salvar 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 el acceso telnet a la consola y fijar el tiempo de inactividad, ingrese 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 permite que usted especifique los host que pueden acceder la consola del dispositivo de seguridad vía Telnet.

> Nota: Puede habilitar el telnet al dispositivo de seguridad en todas las interfaces. Sin embargo, el dispositivo de seguridad requiere que todo el tráfico de Telnet a la interfaz exterior sea protegido por el IPSec. Para habilitar a una sesión telnet a la interfaz exterior, IPSec de la configuración en la interfaz exterior de modo que incluya el tráfico IP que es generado por el dispositivo de seguridad y el permiso Telnet en la interfaz exterior.

> Nota: Generalmente si ninguna interfaz que tenga un nivel de seguridad de cero o baja que cualquier otra interfaz, el ASA no permite Telnet a esa interfaz.

> Nota: Cisco no recomienda el acceso al dispositivo de seguridad a través de una sesión telnet. La información del credencial de autenticación, tal como la contraseña, se envía como texto claro. Cisco recomienda que usted utiliza SSH para una comunicación de datos asegurada.

Ingrese el **comando password** para fijar una contraseña para el acceso telnet a la consola. La contraseña predeterminada es **Cisco**. Ingrese el **comando who** para ver los IP Addresses que accede actualmente la consola del dispositivo de seguridad. Ingrese el **comando kill** para terminar a una sesión de consola activa telnet.

Ejemplos de escenario de Telnet

Para habilitar a una sesión telnet a la interfaz interior, revise los ejemplos que se proporcionan en esta sección.

Ejemplo 1

Este ejemplo permite que solamente el host **172.16.5.20** acceda a la consola del dispositivo de seguridad con Telnet:

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

Ejemplo 2

Este ejemplo permite que solamente la red **172.16.5.0/24** acceda a la consola del dispositivo de seguridad con Telnet:

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

Ejemplo 3

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

```
ASA(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 usted configura el **comando aaa** para requerir la autenticación para el dispositivo de seguridad y el acceso a la consola de Telnet, y los tiempos de la petición del acceso a la consola hacia fuera, usted 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

> Nota: 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

Ingrese el **comando debug ssh** para habilitar el debugging SSH:

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

Esta salida muestra una tentativa de SSH de una dirección IP interior (172.16.5.20) a la interfaz interior del ASA. Estos debugs representan una conexión satisfactoria y una autenticación:

```
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
```

Si un nombre de usuario incorrecto se ingresa, por ejemplo **cisco1** en vez de **Cisco**, el Firewall ASA rechaza la autenticación. Esta salida de los debugs muestra la autenticación fallida:

```
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.
```

Semejantemente, si se proporciona la contraseña incorrecta, la autenticación falla. Esta salida de los debugs muestra la autenticación fallida:

```
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.
```

Cómo ver las sesiones SSH activas

Ingrese este comando para verificar el número de sesiones SSH que estén conectadas (y el estado de la conexión) con el 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 a **monitorear > las propiedades > las sesiones del acceso del dispositivo > del shell seguro** para ver las sesiones con el ASDM.

Ingrese el **comando socket de la tabla de la demostración ASP** para verificar que establecen a la

sesión TCP:

```
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
```

Vea las claves públicas RSA

Ingrese este comando para ver la porción pública de las claves RSA en el dispositivo de seguridad:

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

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Quite las claves RSA del ASA

En ciertas situaciones, por ejemplo cuando usted actualiza el software ASA o cambia el SSH versión en el ASA, usted puede ser que sea requerido quitar y reconstruir las claves RSA. Ingrese este comando para quitar el par clave RSA del ASA:

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

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

Conexión SSH fallada

Usted recibe este mensaje de error en el ASA:

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

Éste es el mensaje de error que aparece en la máquina de cliente SSH:

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

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

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

Ingrese este comando para generar la nueva clave:

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