SSH et telnet de version 9.x ASA sur l'exemple de configuration d'interfaces internes et externes

Contenu

Introduction

Ce document décrit comment configurer le Protocole Secure Shell (SSH) sur les interfaces internes et externes des versions 9.x et ultérieures d'appareils de Sécurité de gamme de Cisco. Quand vous devez configurer et surveiller l'appliance de sécurité adaptable Cisco (ASA) à distance avec le CLI, l'utilisation du telnet ou du SSH est exigée. Puisque des transmissions de telnet sont introduites le texte clair, qui peut inclure des mots de passe, le SSH est fortement recommandé. Le trafic de SSH est chiffré dans un tunnel et les aides protègent de ce fait des mots de passe et d'autres commandes de configuration sensibles contre l'interception.

L'ASA permet des connexions SSH aux dispositifs de sécurité pour la Gestion. L'appliance de sécurité permet un maximum de cinq connexions simultanées de SSH pour chaque contexte de sécurité, si disponible, et un maximum global de 100 connexions pour tous les contextes combinés.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 9.1.5 de logiciel pare-feu de Cisco ASA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> Remarque: La version SSH 2 (SSHv2) est prise en charge dans des versions 7.x et ultérieures ASA.

Produits connexes

Cette configuration peut également être utilisée avec l'appliance de Sécurité de gamme de Cisco ASA 5500 avec les versions de logiciel 9.x et plus tard.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

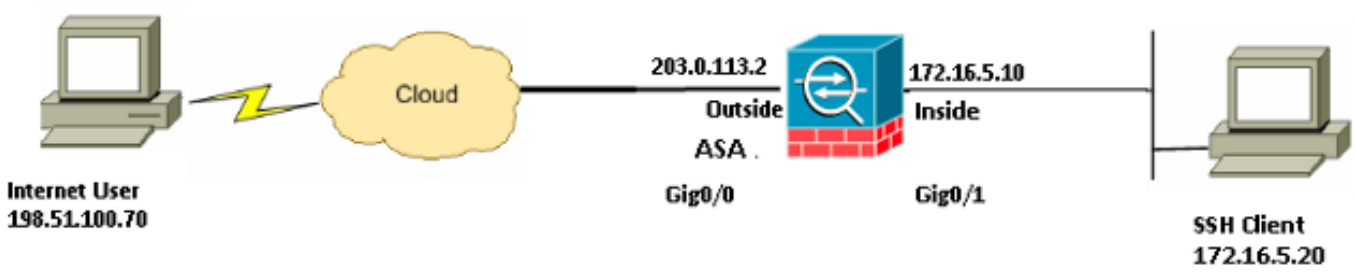
Configurez

Utilisez les informations qui sont fournies dans cette section afin de configurer les caractéristiques qui sont décrites dans ce document.

> Remarque: Chaque étape de configuration qui est décrite fournit les informations qui sont nécessaires afin d'utiliser le CLI ou l'Adaptive Security Device Manager (ASDM).

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



Dans cet exemple de configuration, l'ASA est considérée le serveur de SSH. Le trafic des clients SSH (198.51.100.70/32 et 172.16.5.20/24) au serveur de SSH est chiffré. L'appliance de Sécurité prend en charge la fonctionnalité à distance de shell de SSH qui est fournie dans les versions SSH 1 et 2 et prend en charge le Norme de chiffrement de données (DES) et les chiffrements 3DES. Les versions SSH 1 et 2 sont différentes et ne sont pas interopérables.

Configurations SSH

Ce document utilise les configurations suivantes :

- Accès SSH à l'appliance de sécurité
- Comment utiliser un client SSH
- Configuration ASA

Accès SSH à l'appliance de sécurité

Complétez ces étapes afin de configurer l'accès SSH à l'appliance de sécurité :

1. Les sessions de SSH exigent toujours une forme d'authentification telle qu'un nom d'utilisateur et mot de passe. Il y a deux méthodes que vous pouvez employer afin de répondre à cette exigence.

   La première méthode que vous pouvez employer afin de répondre à cette exigence est de configurer un nom d'utilisateur et mot de passe avec l'utilisation de l'Authentification, autorisation et comptabilité (AAA) :
   ```
   ASA(config)#username username password password
   ASA(config)#aaa authentication {telnet | ssh | http | serial} console
   {LOCAL | server_group [LOCAL]}
   ```
   Remarque: Si vous utilisez un groupe de serveurs TACACS+ ou de RAYON pour l'authentification, vous pouvez configurer les dispositifs de sécurité de sorte qu'ils utilisent la base de données locale comme méthode de retour si le serveur d'AAA est indisponible. Spécifiez le nom du groupe de serveurs et puis LOCAL (LOCAL distingue les majuscules et minuscules). Cisco recommande que vous utilisiez le même nom d'utilisateur et mot de passe dans la base de données locale et le serveur d'AAA, parce que la demande de dispositifs de sécurité ne donne aucune indication de la méthode qui est utilisée.Afin de spécifier une sauvegarde **LOCALE** pour **TACACS+**, utilisez cette configuration pour l'authentification de SSH :
   ```
   ASA(config)#aaa authentication ssh console TACACS+ LOCAL
   ```
   Vous pouvez alternativement utiliser la base de données locale en tant que votre principale méthode d'authentification sans secours. Afin de faire ceci, entrez dans seuls les **GENS DU PAYS** :
   ```
   ASA(config)#aaa authentication ssh console LOCAL
   ```
   La deuxième méthode que vous pouvez

employer afin de répondre à cette exigence est d'utiliser le nom d'utilisateur par défaut de l'ASA et le mot de passe par défaut de telnet de Cisco. Vous pouvez changer le mot de passe Telnet avec cette commande :
`ASA(config)#passwd password`Remarque: La commande de mot de passe peut également être utilisée dans cette situation, en tant que chacun des deux fonction de commande pareillement.

2. Générez une paire de clés RSA pour le Pare-feu ASA, qui est exigé pour le SSH :
`ASA(config)#crypto key generate rsa modulus modulus_size`Remarque: Le modulus_size (en bits) peut être 512, 768, 1024 ou 2048. Plus la taille de la clé modulus est grande, plus cela prend de temps pour produire la paire de clés RSA. Une valeur de 2048 est recommandée. La commande qui est utilisée afin de générer une paire de clés RSA est différente pour des versions de logiciel ASA plus tôt que la version 7.x. Dans les versions antérieures, un nom de domaine doit être placé avant que vous puissiez créer les clés. Dans le mode de contexte multiple, vous devez générer les clés RSA pour chaque contexte.
3. Spécifiez les hôtes qui sont permis pour se connecter aux dispositifs de sécurité. Cette commande spécifie l'adresse source, le netmask, et l'interface de l'hôte qui est permis pour se connecter au SSH. Elle peut être entrée plusieurs fois pour plusieurs hôtes, réseaux ou interfaces. Dans cet exemple, on permet un hôte sur l'intérieur et un hôte sur l'extérieur :
```
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. Cette étape est facultative. Par défaut, l'appliance de Sécurité permet la version SSH 1 et la version 2. sélectionnent cette commande afin de limiter les connexions à une version spécifique :
`ASA(config)# ssh version <version_number>`Remarque: Le version_number peut être 1 ou 2.
5. Cette étape est facultative. Par défaut, les sessions de SSH sont fermées après cinq minutes d'inactivité. Ce délai d'attente peut être configuré pour durer entre 1 et 60 minutes :
`ASA(config)#ssh timeout minutes`

Configuration ASA

Employez ces informations afin de configurer l'ASA :

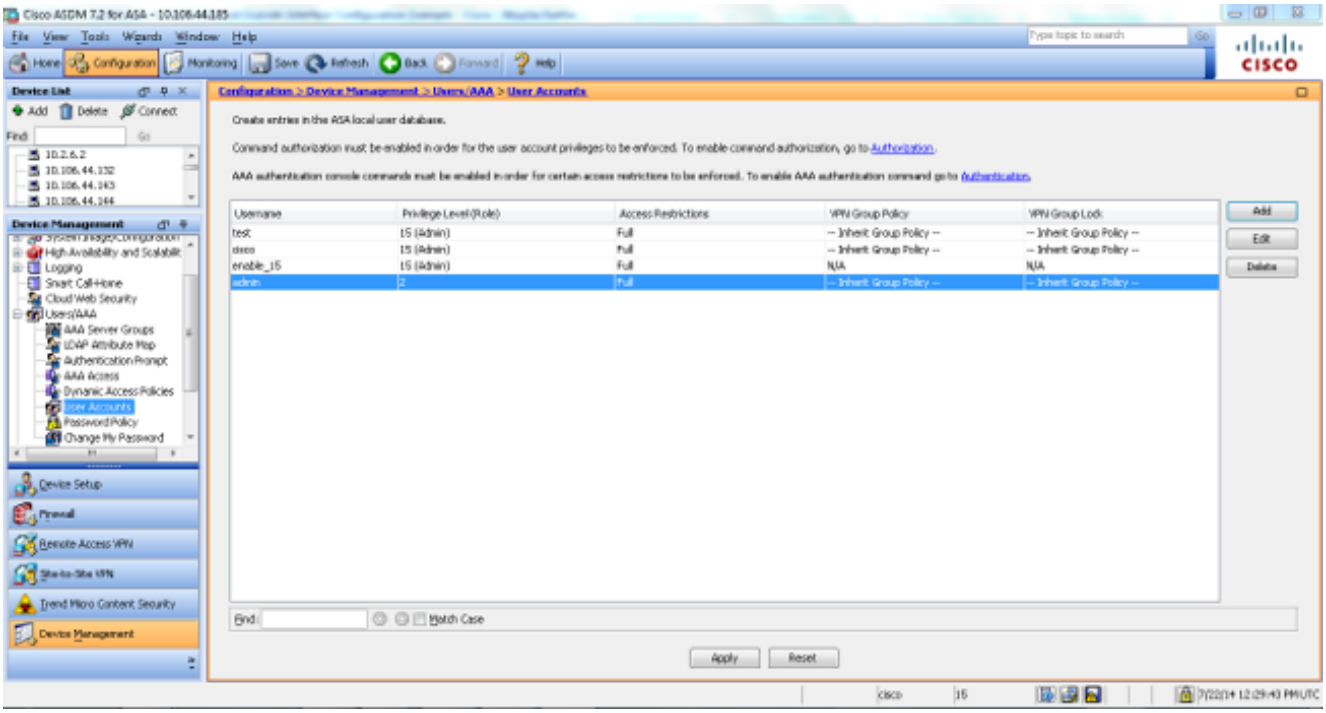
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

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
```

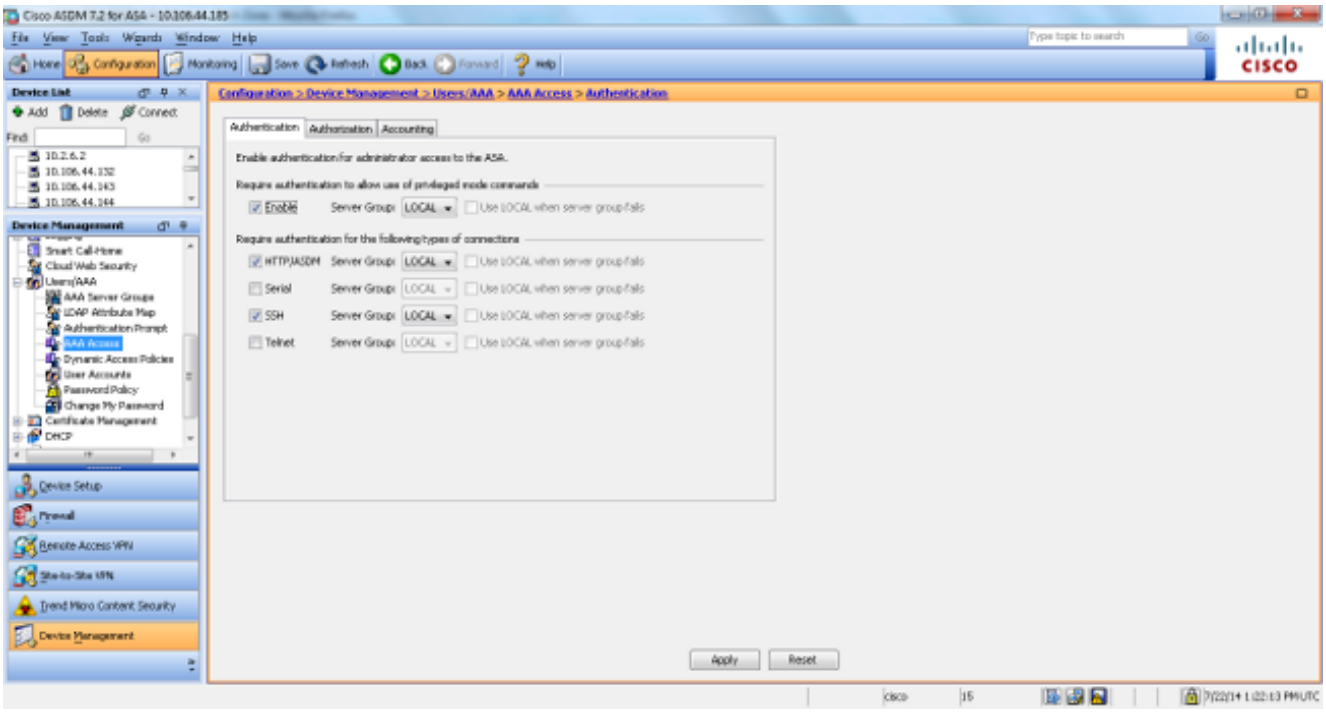
Configuration de version 7.2.1 ASDM

Terminez-vous ces étapes afin de configurer la version 7.2.1 ASDM :

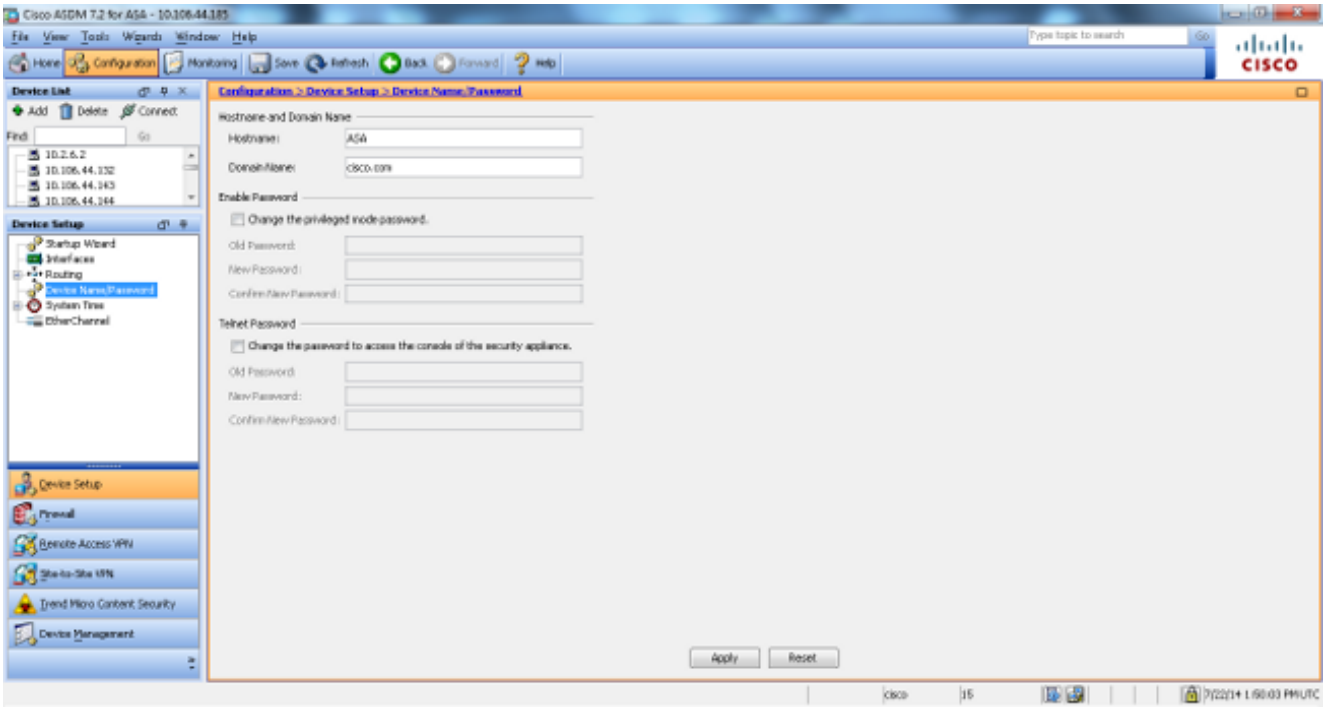
1. Naviguez vers le **Configuration > Device Management > Users/AAA > User Accounts** afin d'ajouter un utilisateur avec l'ASDM.



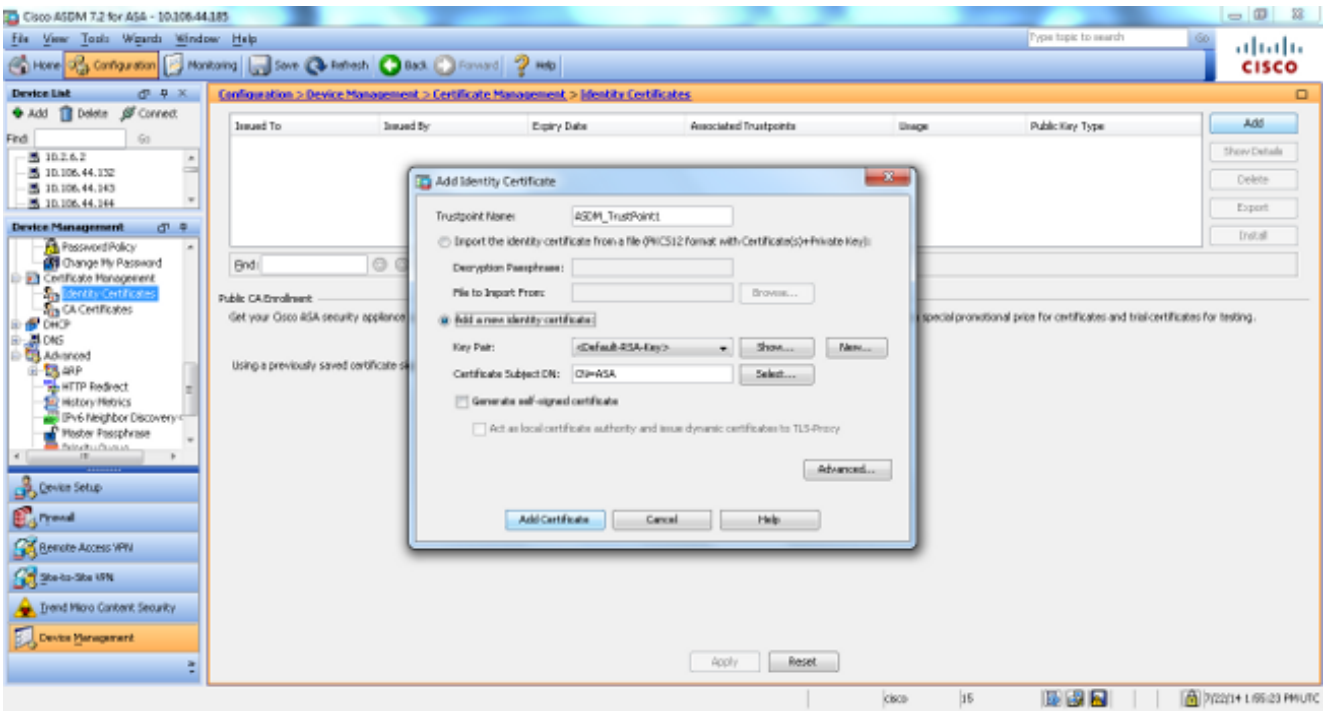
2. Naviguez vers le **Configuration > Device Management > Users/AAA > AAA Access > Authentication** afin d'installer l'authentification d'AAA pour le SSH avec l'ASDM.



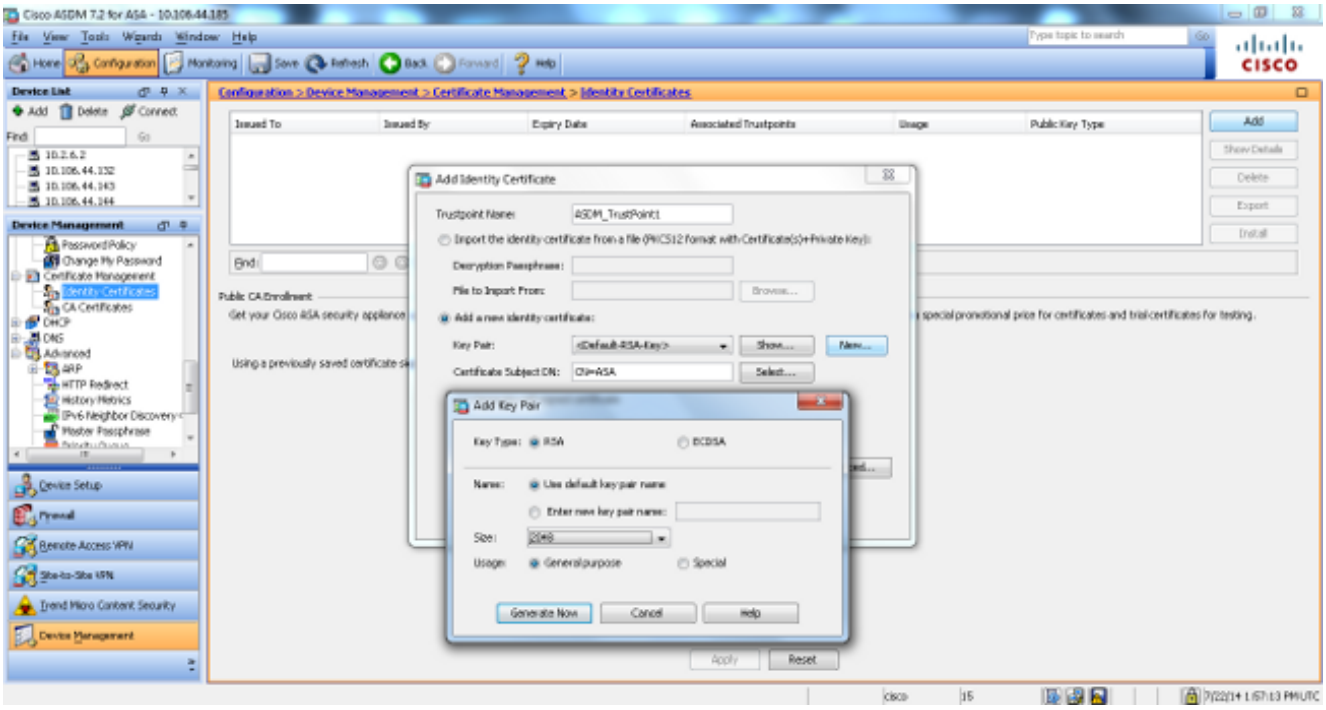
3. Naviguez vers le **Configuration > Device Setup > Device Name/Password** afin de changer le mot de passe de telnet avec l'ASDM.



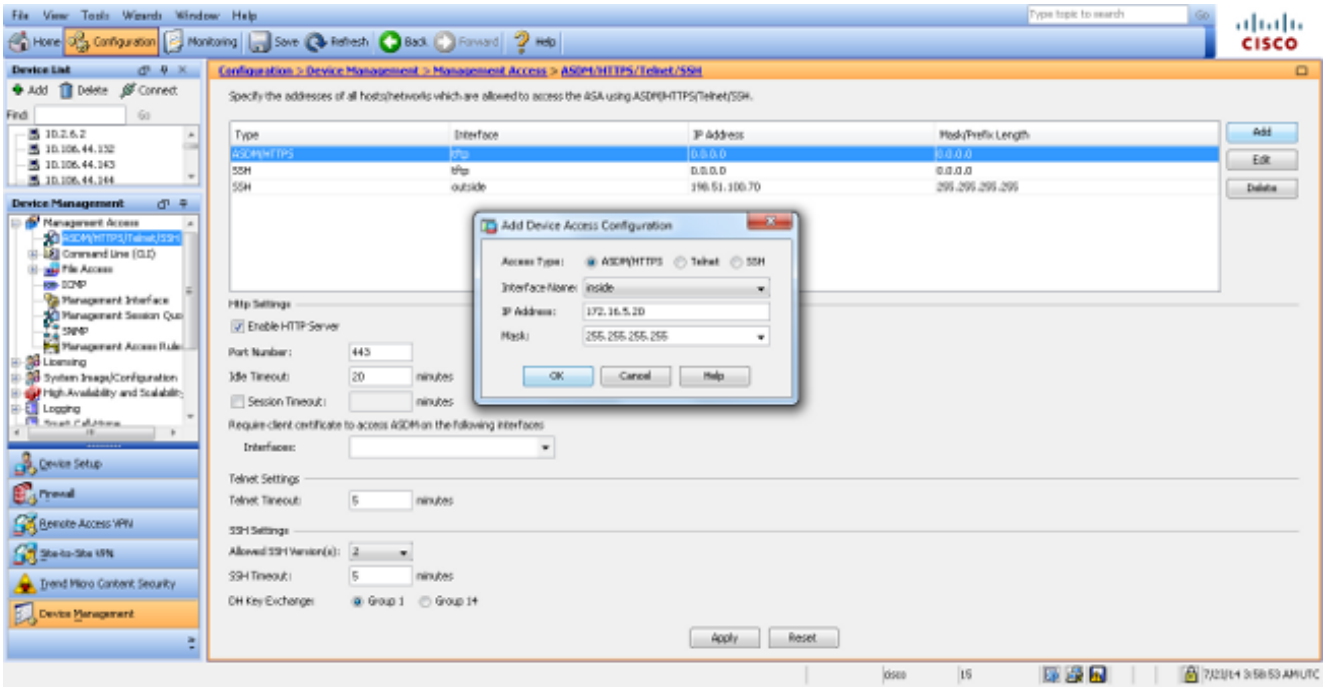
4. Naviguez vers le **Configuration > Device Management > Certificate Management > Identity Certificates**, cliquez sur Add, et utilisez les options par défaut qui sont disponibles afin de générer les mêmes clés RSA avec l'ASDM.



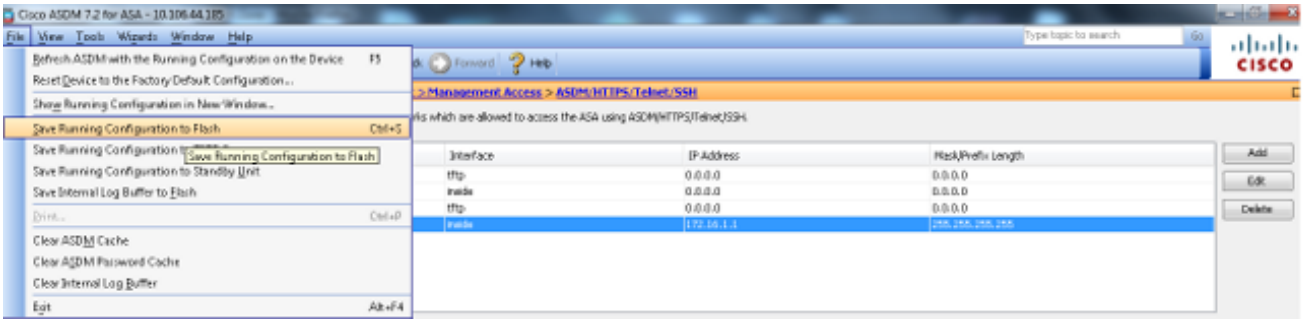
5. Cliquez sur l'**ajouter une nouvelle** case d'option de **certificat d'identité** et cliquez sur New afin d'ajouter une paire de clé par défaut, si on n'existe pas. Une fois complet, le clic **se produisent maintenant**.



6. Naviguez vers le **Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)** afin d'utiliser l'ASDM de sorte que vous puissiez spécifier les hôtes qui sont permis pour connecter au SSH et afin de spécifier les options de version et de délai d'attente.



7. **Sauvegarde de** clic de la fenêtre externe afin de sauvegarder la configuration.



8. Une fois invité à sauvegarder la configuration sur flash, choisissez **Apply** afin de sauvegarder la configuration.

Configuration Telnet

Afin d'ajouter l'accès de telnet à la console et placer le délai d'attente de veille, sélectionnez la **commande telnet** en mode de configuration globale. Par défaut, les sessions Telnet qui sont laissées en attente pendant cinq minutes sont fermées par l'appliance de sécurité. Afin de supprimer l'accès Telnet d'une adresse IP précédemment définie, employez la forme *aucune* de cette commande.

```
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}}
```

La commande telnet te permet pour spécifier les hôtes qui peuvent accéder à la console de dispositifs de sécurité par l'intermédiaire du telnet.

> Remarque: Vous pouvez activer Telnet à l'appliance de sécurité sur toutes les interfaces. Cependant, les dispositifs de sécurité exigent que tout le trafic de telnet à l'interface extérieure soit protégé par IPsec. Afin d'activer une session de telnet à l'interface extérieure, configurez IPsec sur l'interface extérieure de sorte qu'elle inclue le trafic IP qui est générée par les dispositifs de sécurité et le telnet d'enable sur l'interface extérieure.

> Remarque: Généralement si aucune interface qui a un niveau de Sécurité de zéro ou diminue que n'importe quelle autre interface, l'ASA ne permet le telnet à cette interface.

> Remarque: Cisco ne recommande pas l'accès aux dispositifs de sécurité par une session de telnet. Les informations de créance d'authentification, telles que le mot de passe, sont envoyées en tant que texte clair. Cisco recommande que vous utilisiez le SSH pour une communication de données plus sécurisée.

Sélectionnez la commande de **mot de passe** afin de placer un mot de passe pour l'accès de telnet à la console. Le mot de passe par défaut est **Cisco**. Entrez dans **qui** commandent afin de visualiser les adresses IP qui accèdent à actuellement la console de dispositifs de sécurité. Sélectionnez la commande de **mise à mort** afin de terminer une session de console active de telnet.

Exemples de scénario de telnet

Afin d'activer une session de telnet à l'interface interne, examinez les exemples qui sont fournis dans cette section.

Exemple 1

Cet exemple permet seulement à l'hôte **172.16.5.20** pour accéder à la console de dispositifs de sécurité par le telnet :

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

Exemple 2

Cet exemple permet seulement au réseau **172.16.5.0/24** pour accéder à la console de dispositifs de sécurité par le telnet :

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

Exemple 3

Cet exemple permet à tous les réseaux pour accéder à la console de dispositifs de sécurité par le telnet :

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

Si vous utilisez la commande **AAA** avec le mot clé console, l'accès à la console par Telnet doit être authentifié avec un serveur d'authentification.

> Remarque: Si vous configurez la commande d'**AAA** afin d'avoir besoin de l'authentification pour les dispositifs de sécurité et l'accès de console de telnet, et les temps de demande d'ouverture de session de console, vous pouvez accéder aux dispositifs de sécurité de la console série. Afin de faire ceci, entrez le nom utilisateur et le mot de passe de l'appliance de sécurité qui sont définis avec la commande **activer le mot de passe**.

Émettez la commande **telnet timeout** afin de définir la durée maximale du délai d'attente d'une session Telnet de la console avant qu'elle soit déconnectée par l'appliance de sécurité. Vous ne pouvez pas utiliser la commande **no telnet** avec la commande **telnet timeout**.

Cet exemple montre comment changer la durée d'attente maximale d'une session :

```
hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

> Remarque: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Débogage SSH

Sélectionnez la commande de **ssh de débogage** afin d'activer l'élimination des imperfections de SSH :

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

Cette sortie affiche une tentative de SSH d'une adresse IP intérieure (172.16.5.20) à l'interface interne de l'ASA. Ceux-ci met au point dépeignent une connexion et une authentification réussies :

```
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 nom d'utilisateur erroné est écrit, comme **cisco1** au lieu de **Cisco**, le Pare-feu ASA rejette l'authentification. Cette sortie de débogage montre l'échec de l'authentification :

```
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.
```

De même, si le mot de passe incorrect est fourni, l'authentification échoue. Cette sortie de débogage montre l'échec de l'authentification :

```
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.
```

Affichage sessions actives SSH

Sélectionnez cette commande afin de vérifier le nombre de sessions de SSH qui sont connectées (et l'état de connexion) à l'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
```

Naviguez vers le **Monitoring > Properties > Device Access > Secure Shell Sessions** afin de visualiser les sessions avec l'ASDM.

Sélectionnez la commande de **socket de table d'asp d'exposition** afin de vérifier que la session TCP est établie :

```
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
```

Clés publiques RSA de vue

Sélectionnez cette commande afin de visualiser la partie publique des clés RSA sur les dispositifs de sécurité :

```
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
```

Naviguez vers le **Configuration > Properties > Certificate > Key Pair** et cliquez sur les **détails d'exposition** afin de visualiser les clés RSA avec l'ASDM.

Dépannez

Cette section fournit les informations que vous pouvez employer afin de dépanner votre configuration.

Retirez les clés RSA de l'ASA

Dans certaines situations, comme quand vous améliorez le logiciel ASA ou changez la version SSH dans l'ASA, vous pourriez être requis de retirer et recréer les clés RSA. Sélectionnez cette commande afin de retirer la paire de clés RSA de l'ASA :

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

Naviguez vers le **Configuration > Properties > Certificate > Key Pair** et cliquez sur Delete afin de retirer les clés RSA avec l'ASDM.

La connexion SSH a échoué ?

Vous recevez ce message d'erreur sur l'ASA :

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

C'est le message d'erreur qui apparaît sur l'ordinateur de client SSH :

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

Afin de résoudre ce problème, retirez et recréez les clés RSA. Sélectionnez cette commande afin de retirer la paire de clés RSA de l'ASA :

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

Sélectionnez cette commande afin de générer la nouvelle clé :

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