Exemple de configuration d'ASA version 9.x SSH et Telnet sur les interfaces internes et externes

Contenu

Introduction

Ce document décrit comment configurer Secure Shell (SSH) sur les interfaces internes et externes des versions 9.x et ultérieures des appliances de sécurité de la gamme Cisco. Lorsque vous devez configurer et surveiller le dispositif de sécurité adaptatif Cisco (ASA) à distance avec l'interface de ligne de commande, l'utilisation de Telnet ou de SSH est requise. Comme les communications Telnet sont envoyées en texte clair, qui peuvent inclure des mots de passe, SSH est fortement recommandé. Le trafic SSH est chiffré dans un tunnel et contribue ainsi à protéger les mots de passe et les autres commandes de configuration sensibles de l'interception.

L'ASA autorise les connexions SSH au dispositif de sécurité à des fins de 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.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Note**: SSH version 2 (SSHv2) est pris en charge dans ASA versions 7.x et ultérieures.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco ASA 5500 avec les versions 9.x et ultérieures du logiciel.

Conventions

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

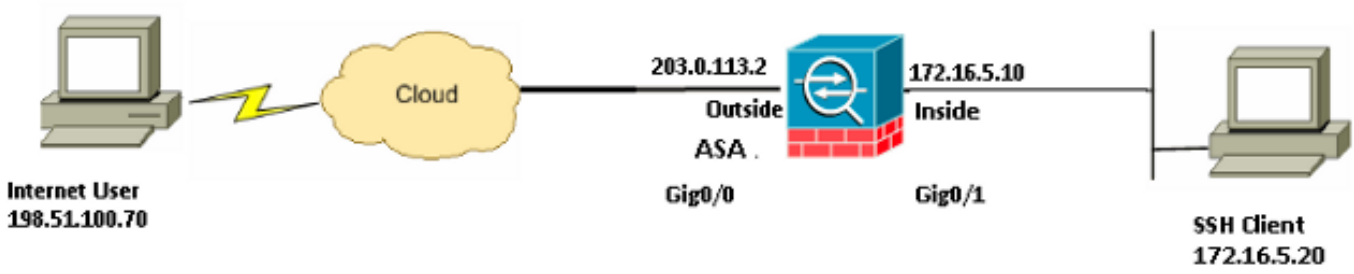
Configuration

Utilisez les informations fournies dans cette section afin de configurer les fonctionnalités décrites dans ce document.

> **Note**: Chaque étape de configuration décrite fournit les informations nécessaires pour utiliser l'interface de ligne de commande ou l'Adaptive Security Device Manager (ASDM).

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

Diagramme du réseau



Dans cet exemple de configuration, l'ASA est considéré comme le serveur SSH. Le trafic des clients SSH (198.51.100.70/32 et 172.16.5.20/24) vers le serveur SSH est chiffré. L'appliance de sécurité prend en charge la fonctionnalité SSH remote shell fournie dans SSH versions 1 et 2 et prend en charge les chiffrement DES (Data Encryption Standard) et 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 SSH nécessitent toujours une forme d'authentification telle qu'un nom d'utilisateur et un mot de passe. Vous pouvez utiliser deux méthodes pour répondre à cette exigence.

   La première méthode que vous pouvez utiliser pour satisfaire à cette exigence est de configurer un nom d'utilisateur et un 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]}
   ```

   Note: Si vous utilisez un groupe de serveurs TACACS+ ou RADIUS pour l'authentification, vous pouvez configurer l'appliance de sécurité de sorte qu'elle utilise la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs et puis LOCAL (LOCAL distingue les majuscules et minuscules). Cisco vous recommande d'utiliser le même nom d'utilisateur et mot de passe dans la base de données locale et le serveur AAA, car l'invite du dispositif de sécurité ne donne aucune indication de la méthode utilisée.Afin de spécifier une sauvegarde **LOCAL** pour **TACACS+**, utilisez cette configuration pour l'authentification 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 LOCAL seul:

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

La deuxième méthode que vous pouvez utiliser pour répondre à cette condition est d'utiliser le nom d'utilisateur par défaut d'**ASA** et le mot de passe Telnet par défaut de **cisco**. Vous pouvez changer le mot de passe Telnet avec cette commande :

```
ASA(config)#passwd password
```

Note: La commande **password** peut également être utilisée dans cette situation, car les deux commandes fonctionnent de la même manière.

2. Générer une paire de clés RSA pour le pare-feu ASA, qui est requise pour SSH :

```
ASA(config)#crypto key generate rsa modulusmodulus_size
```

Note: 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 utilisée pour générer une paire de clés RSA est différente pour les versions de logiciels ASA antérieures à la version 7.x. Dans les versions antérieures, un nom de domaine doit être défini avant de pouvoir créer les clés. En mode de contexte multiple, vous devez générer les clés RSA pour chaque contexte.

3. Spécifiez les hôtes autorisés à se connecter à l'appliance de sécurité. Cette commande spécifie l'adresse source, le masque de réseau et l'interface des hôtes autorisés à se connecter avec 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. This step is optional. Par défaut, l'appliance de sécurité autorise SSH version 1 et version 2. Entrez cette commande afin de restreindre les connexions à une version spécifique :

```
ASA(config)# ssh version
```

Note: Le **numéro_version** peut être **1** ou **2**.

5. This step is optional. Par défaut, les sessions SSH sont fermées après cinq minutes d'inactivité. Ce délai peut être configuré pour durer entre 1 et 60 minutes :

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

Configuration ASA

Utilisez ces informations afin de configurer l'ASA :

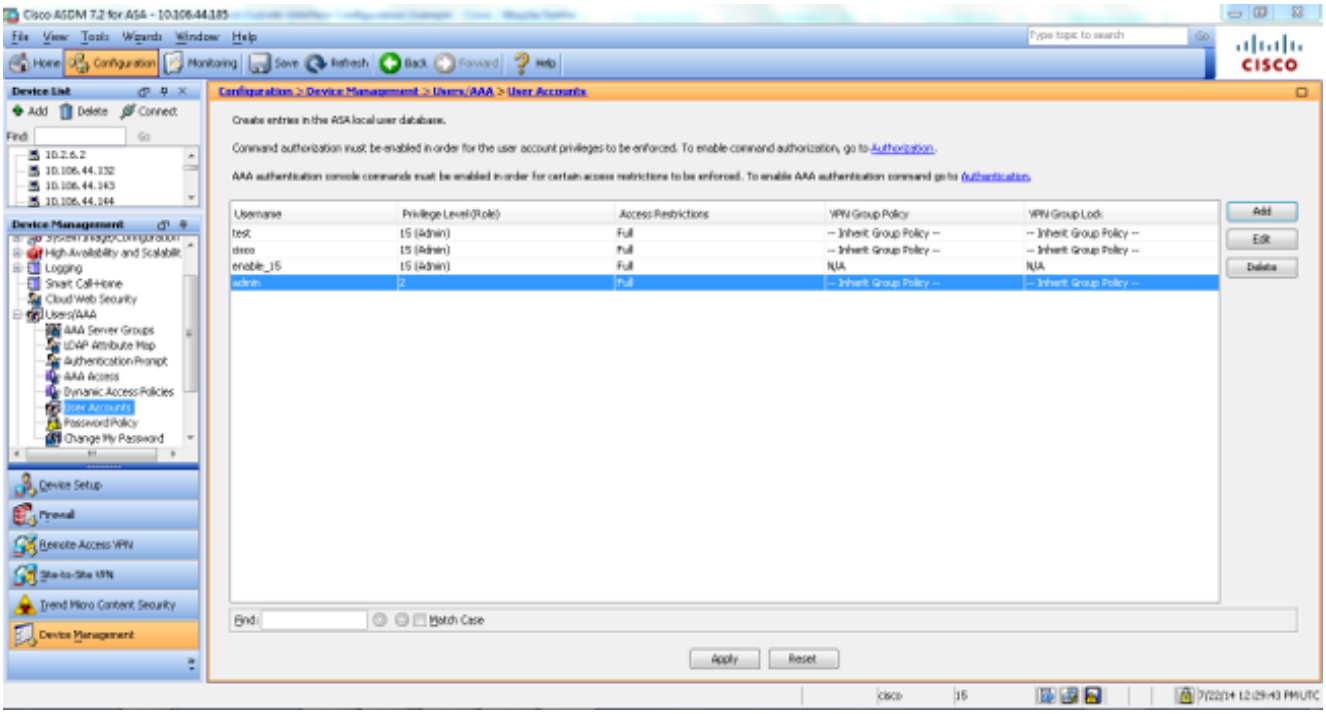
```
ASA Version 9.1(5)2
!
hostname ASA
domain-name cisco.com

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
```

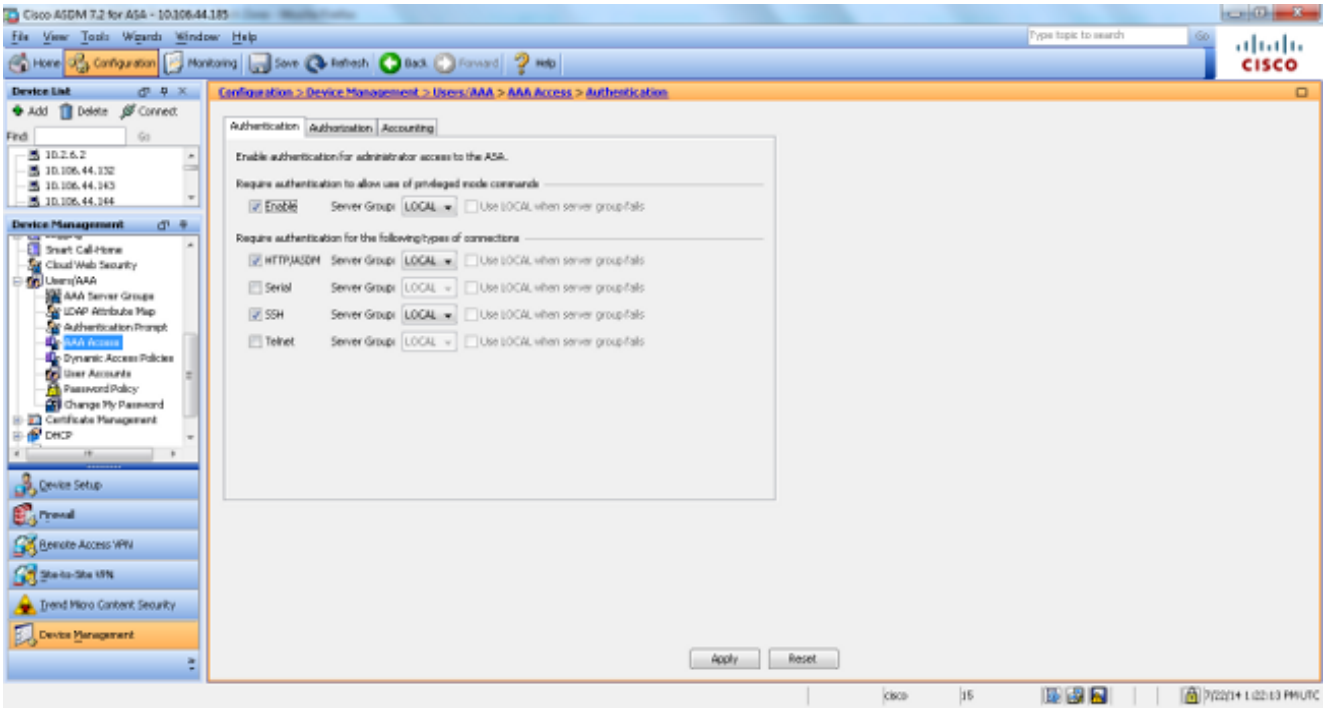
Configuration d'ASDM version 7.2.1

Complétez ces étapes afin de configurer la version 7.2.1 d'ASDM :

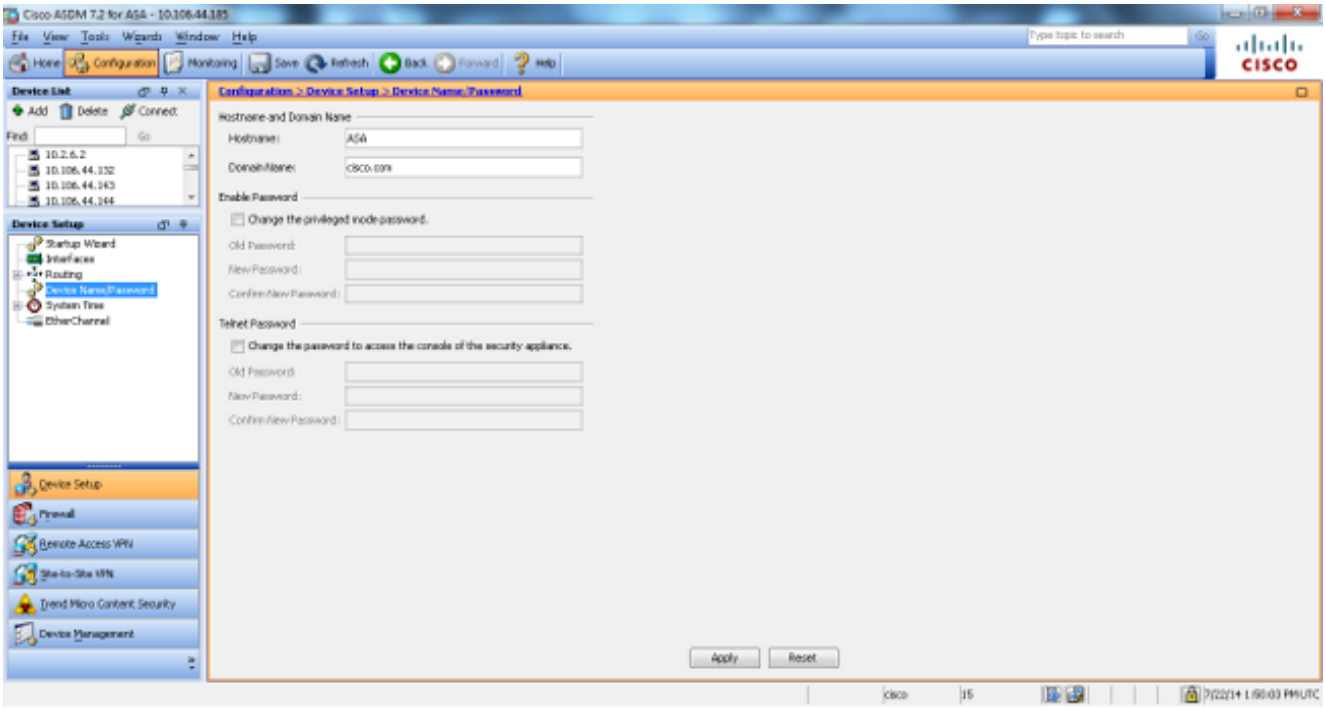
1. Accédez à **Configuration > Device Management > Users/AAA > User Accounts** afin d'ajouter un utilisateur avec ASDM.



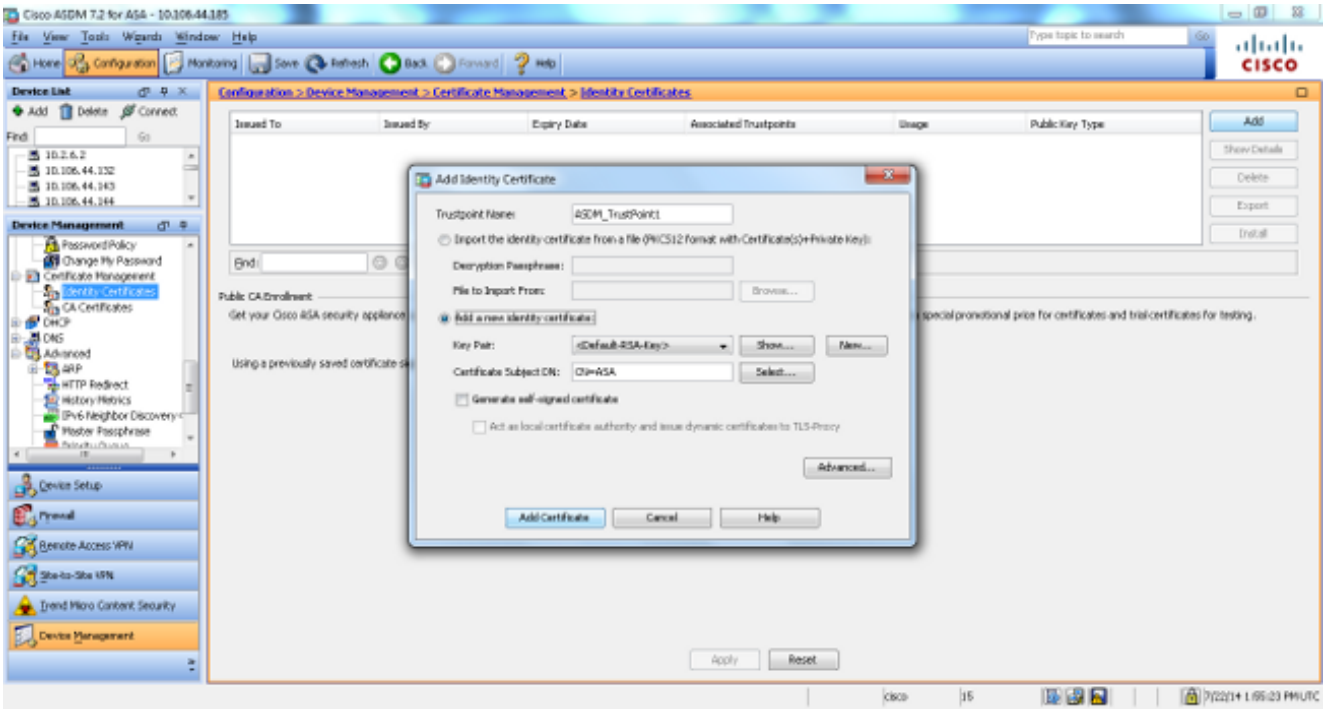
2. Accédez à **Configuration > Device Management > Users/AAA > AAA Access > Authentication** afin de configurer l'authentification AAA pour SSH avec ASDM.



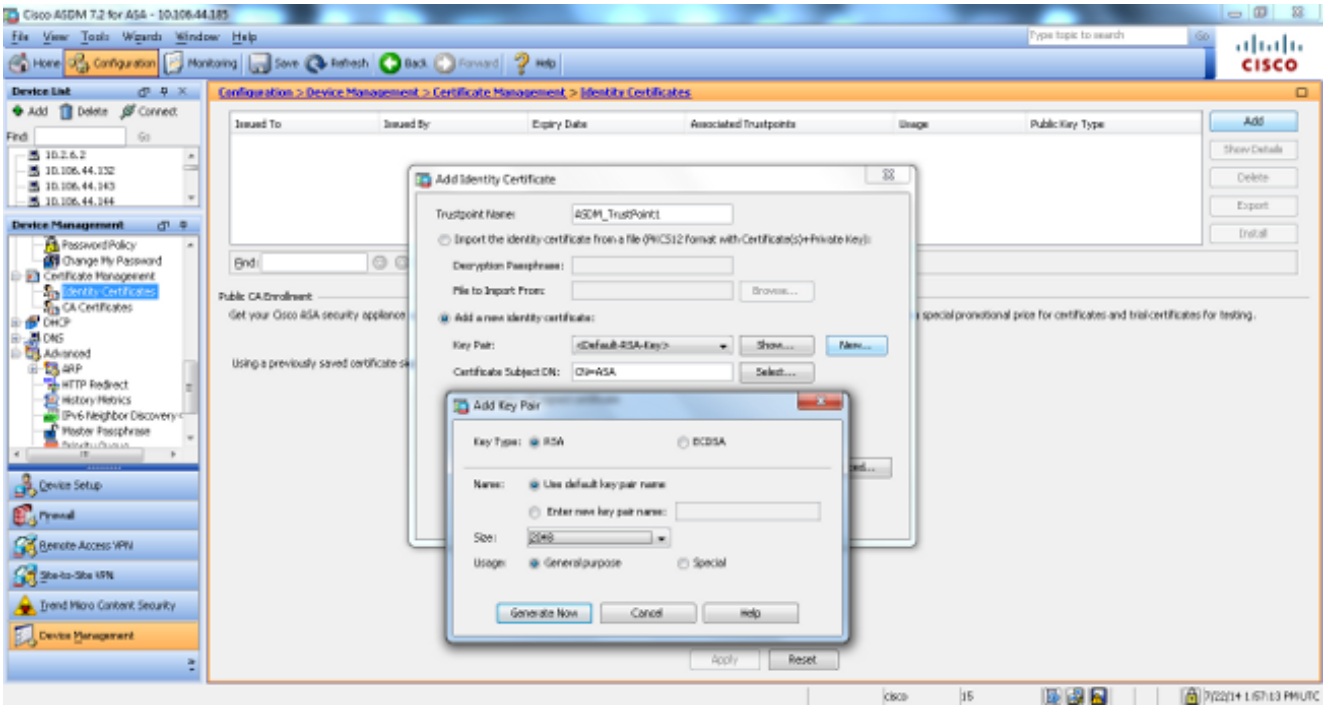
3. Accédez à **Configuration > Device Setup > Device Name/Password** afin de modifier le mot de passe Telnet avec ASDM.



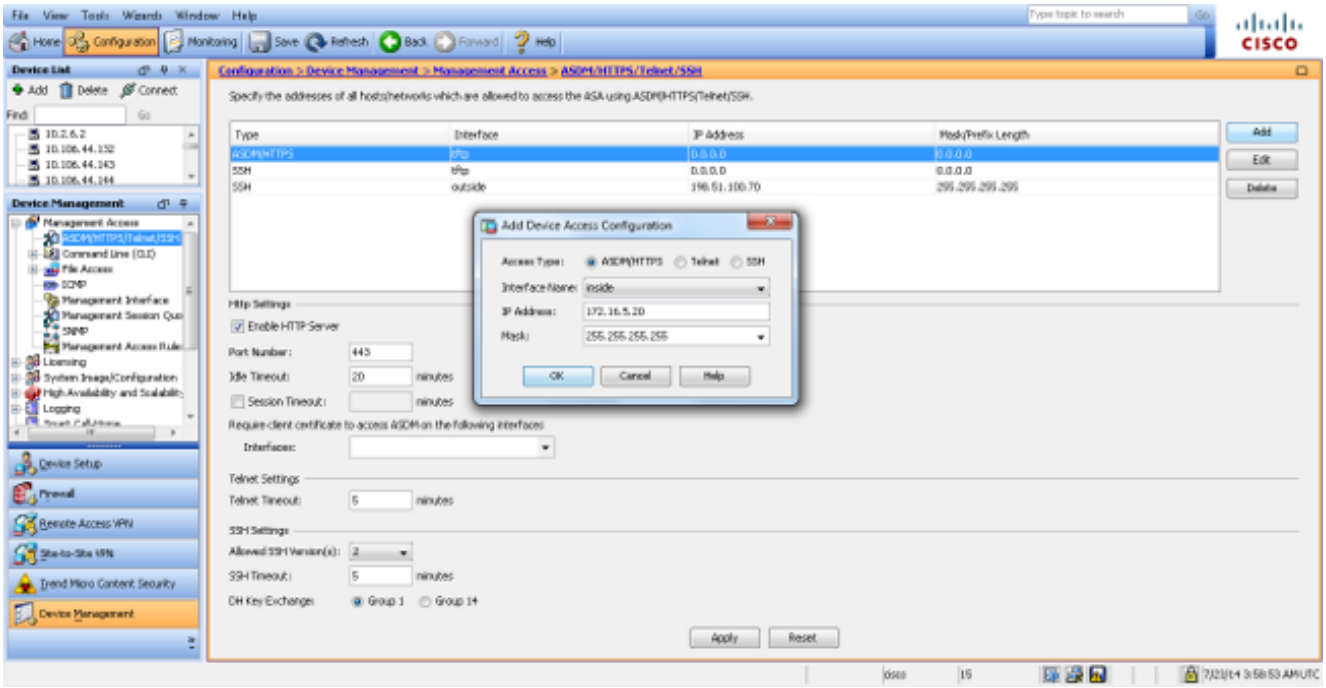
4. Accédez à **Configuration > Device Management > Certificate Management > Identity Certificates**, cliquez sur **Add** et utilisez les options par défaut disponibles afin de générer les mêmes clés RSA avec ASDM.



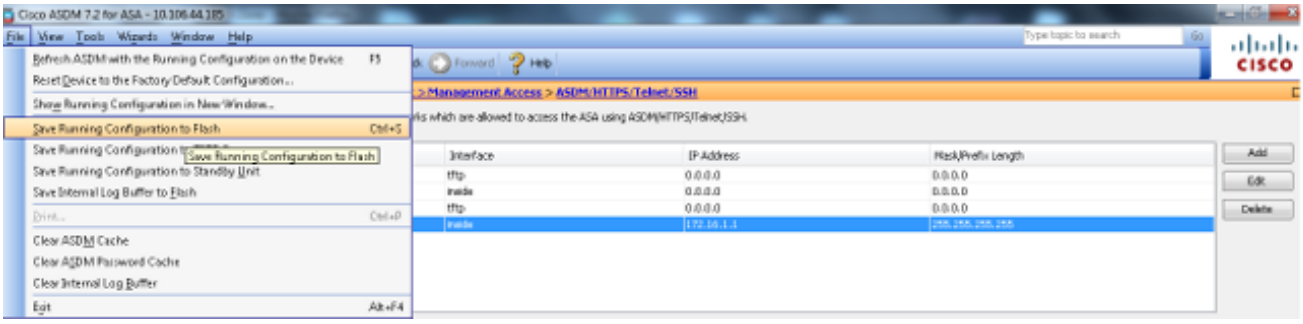
5. Cliquez sur la case d'option **Ajouter un nouveau certificat d'identité** et cliquez sur **Nouveau** afin d'ajouter une paire de clés par défaut, si elle n'existe pas. Une fois terminé, cliquez sur **Générer maintenant**.



6. Accédez à **Configuration > Device Management > Management Access > Command Line (CLI) > Secure Shell (SSH)** afin d'utiliser ASDM pour que vous puissiez spécifier les hôtes autorisés à se connecter avec SSH et pour spécifier les options de version et de délai d'attente.



7. Cliquez sur **Enregistrer** dans la fenêtre contextuelle afin d'enregistrer 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 Telnet à la console et de définir le délai d'inactivité, entrez 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** vous permet de spécifier les hôtes qui peuvent accéder à la console du dispositif de sécurité via Telnet.

> **Note**: Vous pouvez activer Telnet à l'appliance de sécurité sur toutes les interfaces. Cependant, l'appliance de sécurité exige que tout le trafic Telnet vers l'interface externe soit protégé par IPsec. Afin d'activer une session Telnet à l'interface externe, configurez IPsec sur l'interface externe de sorte qu'il inclue le trafic IP généré par l'appliance de sécurité et activez Telnet sur l'interface externe.

> **Note**: En règle générale, si une interface dont le niveau de sécurité est inférieur ou égal à zéro, l'ASA n'autorise pas Telnet à cette interface.

> **Note**: Cisco ne recommande pas l'accès à l'appliance de sécurité via une session Telnet. Les informations d'identification d'authentification, telles que le mot de passe, sont envoyées en texte clair. Cisco vous recommande d'utiliser SSH pour une communication de données plus sécurisée.

Entrez la commande **password** afin de définir un mot de passe pour l'accès Telnet à la console. Le mot de passe par défaut est **cisco**. Entrez la commande **oms** afin d'afficher les adresses IP qui accèdent actuellement à la console du dispositif de sécurité. Entrez la commande **kill** afin de terminer une session de console Telnet active.

Exemples de scénarios Telnet

Afin d'activer une session Telnet sur l'interface interne, examinez les exemples fournis dans cette

section.

Exemple 1

Cet exemple montre comment autoriser uniquement l'hôte **172.16.5.20** à accéder à la console de l'appliance de sécurité via Telnet :

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

Exemple 2

Cet exemple montre comment autoriser uniquement le réseau **172.16.5.0/24** à accéder à la console de l'appliance de sécurité via Telnet :

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

Exemple 3

Cet exemple permet à tous les réseaux d'accéder à la console de l'appliance de sécurité via 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.

> **Note**: Si vous configurez la commande **aaa** afin d'exiger l'authentification pour l'appliance de sécurité et l'accès à la console Telnet, et que la demande de connexion à la console expire, vous pouvez accéder à l'appliance de sécurité à partir 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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

> **Note**: 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

Entrez la commande **debug ssh** afin d'activer le débogage SSH :

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

Ce résultat montre une tentative SSH d'une adresse IP interne (172.16.5.20) à l'interface interne de l'ASA. Ces débogages décrivent 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 incorrect est entré, par exemple **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

Entrez cette commande afin de vérifier le nombre de sessions SSH 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
```

Accédez à **Surveillance > Propriétés > Accès aux périphériques > Sessions Shell sécurisées** afin d'afficher les sessions avec ASDM.

Entrez la commande **show asp table socket** 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
```

Afficher les clés RSA publiques

Entrez cette commande afin d'afficher la partie publique des clés RSA sur l'appliance 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
```

Accédez à **Configuration > Properties > Certificate > Key Pair** et cliquez sur **Show Details** afin d'afficher les clés RSA avec ASDM.

Dépannage

Cette section fournit des renseignements qui vous permettront de régler les problèmes de configuration.

Supprimer les clés RSA de l'ASA

Dans certaines situations, par exemple lorsque vous mettez à niveau le logiciel ASA ou modifiez la version SSH dans l'ASA, vous devrez peut-être supprimer et recréer les clés RSA. Entrez cette commande afin de supprimer la paire de clés RSA de l'ASA :

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

Accédez à **Configuration > Properties > Certificate > Key Pair** et cliquez sur **Delete** afin de supprimer les clés RSA avec 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.
```

Il s'agit du message d'erreur qui apparaît sur l'ordinateur client SSH :

```
Selected cipher type
```

Afin de résoudre ce problème, supprimez et recréez les clés RSA. Entrez cette commande afin de supprimer la paire de clés RSA de l'ASA :

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

Entrez cette commande afin de générer la nouvelle clé :

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