Accès de gestion

Ce chapitre décrit comment accéder à l'ASA pour la gestion de systèmes par le biais de Telnet, SSH et HTTPS (à l'aide d'ASDM), authentifier et autoriser les utilisateurs, et créer des bannières de connexion.

Configurer l'accès de gestion à distance

Cette section décrit comment configurer l'accès ASA pour ASDM, Telnet ou SSH, et d'autres paramètres de gestion tels qu'une bannière de connexion.

Configurer l'accès SSH

Lignes directrices relatives à SSH

- Pour accéder à l'interface ASA pour l'accès SSH, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès SSH conformément à cette section.
- L'accès SSH à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte SSH est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN (uniquement prise en charge par la pile ASA SSH). Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 15.
- L'ASA permet un maximum de cinq connexions SSH simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes. Cependant, comme les commandes de configuration peuvent obtenir des verrouillages sur les ressources en cours de modification, vous devez apporter des modifications à une session SSH à la fois pour vous assurer que toutes les modifications sont appliquées correctement.
- Par défaut, l'ASA utilise la pile CiscoSSH, qui est basée sur OpenSSH. Vous pouvez choisir d'activer à la place la pile ASA SSH propriétaire. CiscoSSH prend en charge :
  - Conformité FIPS

- Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre.

Notez que la pile CiscoSSH ne prend pas en charge :

- SSH vers une interface différente sur VPN (accès de gestion)
- Paire de clés EDDSA
- Paire de clés RSA en mode FIPS

Si vous avez besoin de ces fonctionnalités, vous devez utiliser la pile SSH ASA.

- Pour utiliser la commande **copy** de l'ASA afin de copier un fichier vers ou depuis un serveur SCP, vous devez :
  - (Pile CiscoSSH uniquement) Activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**.
  - Générer une paire de clés (pour les ASA physiques uniquement) à l'aide de la commande **crypto key generate**.
- Le nom d'utilisateur SSH par défaut n'est plus pris en charge. Vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur **pix** ou **asa** et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL**; puis définissez un utilisateur local en saisissant la commande **username**. Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.
- Seule la version 2 du protocole SSH est prise en charge.

Pour configurer l'accès SSH à l'ASA, activez le serveur SSH et identifiez les adresses IP autorisées. Pour authentifier les utilisateurs, vous pouvez utiliser les méthodes suivantes :

- Nom d'utilisateur et mot de passe utilisant la base de données locale ou un serveur AAA.
- Nom d'utilisateur et clé publique utilisant la base de données locale.

Activer le serveur SSH

Activez le serveur SSH et spécifiez les adresses IP autorisées à se connecter. Vous pouvez également configurer d'autres paramètres du serveur SSH.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 (Facultatif) Utilisez la pile ASA SSH au lieu de la pile CiscoSSH par défaut.

no ssh stack ciscossh

Pour revenir à la pile CiscoSSH, utilisez **ssh stack ciscossh**.

En mode de contexte multiple, utilisez cette commande dans l'espace d'exécution du système. Pour passer du contexte à la configuration système, saisissez **changeto system**.

Étape 2 Identifiez les adresses IP à partir lesquelles l'ASA accepte les connexions pour chaque adresse ou sous-réseau, et l'interface sur laquelle vous pouvez utiliser SSH.

ssh *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 15), spécifiez l'interface BVI nommée.

Contrairement à Telnet, vous pouvez utiliser SSH sur l'interface de niveau de sécurité le plus bas.

Exemple :

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

Étape 3 (Facultatif) Définissez la durée d'inactivité d'une session SSH avant que l'ASA ne déconnecte la session.

ssh timeout *minutes*

Exemple :

```
ciscoasa(config)# ssh timeout 30
```

Définissez le délai entre une et 60 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et doit être augmentée jusqu'à ce que tous les tests et dépannages de pré-production soient terminés.

Étape 4 (Facultatif) Activez le serveur Secure Copy (SCP)

ssh scopy enable

Le serveur SCP ne prend pas en charge les répertoires. L'absence de prise en charge des répertoires limite l'accès des clients à distance aux fichiers internes de l'ASA.

Le serveur SCP ne prend pas en charge les bannières ni les caractères génériques.

Étape 5 (Facultatif) Configurez les algorithmes de chiffrement SSH :

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

Exemple :

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

La valeur par défaut est **medium**. Les chiffrements sont utilisés dans l'ordre dans lequel ils sont répertoriés. Pour les listes prédéfinies, ils sont répertoriés du plus haut au plus bas niveau de sécurité.

- Le mot clé **all** spécifie l'utilisation de tous les chiffrements : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- Le mot clé **custom** spécifie une chaîne de configuration de chiffrement personnalisée, séparée par des deux-points.

- Le mot clé **fips** spécifie uniquement les chiffrements conformes à la norme FIPS : aes128-cbc aes256-cbc
- Le mot clé **high** spécifie uniquement les chiffrements de force élevée : aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- Le mot clé **low** spécifie les chiffrements de force faible, moyenne et élevée : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- Le mot clé **medium** spécifie les chiffrements de force moyenne et élevée (par défaut) : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

Étape 6 (Facultatif) Configurez les algorithmes d'intégrité de chiffrement SSH :

ssh cipher integrity {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_integrity_ciphers*}

Exemple :

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

La valeur par défaut est **high**.

- Le mot clé **all** spécifie l'utilisation de tous les chiffrements : hmac-sha1 hmac-sha1-96 (obsolète) hmac-md5 (obsolète) hmac-md5-96 (obsolète) hmac-sha2-256
- Le mot clé **custom** spécifie une chaîne de configuration de chiffrement personnalisée, séparée par des deux-points.
- Le mot clé **fips** spécifie uniquement les chiffrements conformes à la norme FIPS : hmac-sha1 hmac-sha2-256
- Le mot clé **high** spécifie uniquement les chiffrements de force élevée (par défaut) : hmac-sha2-256
- Le mot clé **low** spécifie les chiffrements de force faible, moyenne et élevée : hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- Le mot clé **medium** spécifie les chiffrements de force moyenne et élevée : hmac-sha1 hmac-sha1-96 (obsolète) hmac-sha2-256

Étape 7 (Facultatif) (Contexte d'administration uniquement) Définissez le mode d'échange de clés Diffie-Hellman (DH) :

ssh key-exchange group {**curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256**}

Exemple :

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

La valeur par défaut est **dh-group14-sha256**.

L'échange de clés DH fournit un secret partagé qui ne peut être déterminé par aucune des parties à elles seules. L'échange de clé est combiné à une signature et à la clé de l'hôte pour authentifier l'hôte. Cette méthode d'échange de clés fournit une authentification explicite du serveur. Pour en savoir plus sur l'utilisation des

méthodes d'échange de clés DH, consultez la RFC 4253. Vous ne pouvez définir l'échange de clés que dans le contexte d'administration; cette valeur est utilisée par tous les contextes.

Exemples

L'exemple suivant montre une session SCP vers l'ASA. À partir d'un client sur l'hôte externe, effectuez un transfert de fichiers SCP. Par exemple, dans Linux, saisissez la commande suivante :

scp -v -pw *password* [*path*/]*source_filename*
*username@asa_address***:** {**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

L'option **-v** correspond à verbose (détaillé), et si **-pw** n'est pas spécifié, vous serez invité à saisir un mot de passe.

Configurer SSH pour l'accès par mot de passe

Configurez l'authentification SSH à l'aide d'un nom d'utilisateur et d'un mot de passe.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Générez une paire de clés, requise pour SSH (pour les ASA physiques uniquement).

Pour l'ASA virtuel, les paires de clés sont automatiquement créées après le déploiement.

a) Générez la paire de clés.

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

Exemple :

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519** : la taille de clé est de 256 bits. Non pris en charge avec la pile CiscoSSH.
- **ecdsa elliptic-curve** *size* : la taille en bits est de 256, 384 ou 521.
- **rsa modulus** *size* : la taille en bits est de 2048, 3072 ou 4096.

Plus la taille de clé que vous spécifiez est grande, plus la génération d'une paire de clés prend du temps. SSH essaie les clés dans l'ordre suivant : EdDSA, ECDSA, puis RSA. Affichez les clés à l'aide de la commande **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**}. Les clés utilisées par SSH sont appelées <Default-*type*-Key>.

b) (Facultatif) Si vous ne souhaitez pas utiliser l'ordre de clés par défaut (EdDSA, ECDSA, puis RSA), identifiez la paire de clés que vous souhaitez utiliser.

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

Si vous choisissez RSA, vous devez utiliser une taille de clé de 2048 ou plus. Pour des raisons de compatibilité de mise à niveau, les clés plus petites ne sont prises en charge que lorsque vous utilisez l'ordre de clés par défaut.

Exemple :

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

Étape 2 Enregistrez les clés dans la mémoire flash persistante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 3 Créez un utilisateur dans la base de données locale ou sur un serveur AAA qui peut être utilisé pour l'accès SSH. Consultez la commande suivante pour ajouter un nom d'utilisateur local (conseillé).

username *name* **password** *password* **privilege** *level*

Vous pouvez utiliser l'authentification par clé publique ou l'authentification par mot de passe pour le même utilisateur local. L'authentification par clé publique n'est pas prise en charge par un serveur AAA.

Exemple :

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

Par défaut, le niveau de privilège est 2; entrez un niveau compris entre 0 et 15, où 15 a tous les privilèges.

Étape 4 Activez l'authentification du serveur local ou AAA pour l'accès SSH.

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

Cette commande n'affecte pas l'authentification par clé publique locale pour les noms d'utilisateur pour lesquels la commande **ssh authentication** est définie. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette commande n'affecte que les noms d'utilisateur locaux avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette commande pour autoriser l'accès par mot de passe.

Exemple :

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

Configurer SSH pour l'accès par clé publique

Configurez l'authentification SSH à l'aide d'une clé publique.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Générez une paire de clés, requise pour SSH (pour les ASA physiques uniquement).

Pour l'ASA virtuel, les paires de clés sont automatiquement créées après le déploiement.

a) Générez la paire de clés.

crypto key generate {**eddsa edwards-curve ed25519** | **ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

Exemple :

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **eddsa edwards-curve ed25519** : la taille de clé est de 256 bits. Non pris en charge avec la pile CiscoSSH.
- **ecdsa elliptic-curve** *size* : la taille en bits est de 256, 384 ou 521.
- **rsa modulus** *size* : la taille en bits est de 2048, 3072 ou 4096.

Plus la taille de clé que vous spécifiez est grande, plus la génération d'une paire de clés prend du temps. SSH essaie les clés dans l'ordre suivant : EdDSA, ECDSA, puis RSA. Affichez les clés à l'aide de la commande **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**}. Les clés utilisées par SSH sont appelées <Default-*type*-Key>.

b) (Facultatif) Si vous ne souhaitez pas utiliser l'ordre de clés par défaut (EdDSA, ECDSA, puis RSA), identifiez la paire de clés que vous souhaitez utiliser.

ssh key-exchange hostkey {**rsa** | **eddsa** | **ecdsa**}

Si vous choisissez RSA, vous devez utiliser une taille de clé de 2048 ou plus. Pour des raisons de compatibilité de mise à niveau, les clés plus petites ne sont prises en charge que lorsque vous utilisez l'ordre de clés par défaut.

Exemple :

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

Étape 2 Enregistrez les clés dans la mémoire flash persistante.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Étape 3 Créez un utilisateur dans la base de données locale qui peut être utilisé pour l'accès SSH.

username *nom* [**password** *mot de passe*] **privilege** *niveau*

Exemple :

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

Par défaut, le niveau de privilège est 2; entrez un niveau compris entre 0 et 15, où 15 a tous les privilèges. Vous pouvez créer un utilisateur sans mot de passe si vous souhaitez forcer l'utilisateur à utiliser l'authentification par clé publique (**ssh authentication**) au lieu de l'authentification par mot de passe. Si vous configurez l'authentification par clé publique ainsi qu'un mot de passe dans la commande **username**, l'utilisateur peut se connecter en utilisant l'une ou l'autre des méthodes si vous configurez explicitement l'authentification AAA dans Configurer SSH pour l'accès par mot de passe, à la page 5. **Remarque :** N'utilisez pas la commande **username** l'option **nopassword**; l'option **nopassword** permet de saisir *n'importe quel* mot de passe, et non pas aucun mot de passe.

Étape 4 Autorisez l'authentification par clé publique pour un utilisateur au lieu de/ou l'authentification par mot de passe, et saisissez la clé publique sur l'ASA :

username *nom* **attributes**

ssh authentication {**pkf** | **publickey** *key*}

Exemple :

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

Pour un **username** local, vous pouvez activer l'authentification par clé publique au lieu de l'authentification par mot de passe. Vous pouvez générer une paire de clés publiques/privées à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats). Saisissez la clé publique sur l'ASA. Le client SSH utilise ensuite la clé privée (et la phrase secrète que vous avez utilisée pour créer la paire de clés) pour se connecter à l'ASA.

Pour une clé **pkf**, vous êtes invité à coller une clé au format PKF, jusqu'à 4096 bits. Utilisez ce format pour les clés trop importantes pour les coller en ligne au format base64. Par exemple, vous pouvez générer une clé de 4096 bits à l'aide de ssh keygen, puis la convertir en PKF, et utiliser le mot clé **pkf** pour être invité à saisir la clé. **Remarque :** Vous pouvez utiliser l'option **pkf** avec le basculement, mais la clé PKF n'est pas automatiquement répliquée sur le système de secours. Vous devez saisir la commande **write standby** pour synchroniser la clé PKF.

Pour la valeur **publickey** *key*, la clé est une clé publique codée en Base64. Vous pouvez générer la clé à l'aide de n'importe quel logiciel de génération de clés SSH (comme ssh keygen) qui peut générer des clés brutes ssh-rsa, ssh-ed25519 ou ecdsa-sha2-nistp (sans certificats).

Exemples

L'exemple suivant montre comment s'authentifier à l'aide d'une clé au format PKF :

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)#
```

L'exemple suivant génère une clé partagée pour SSH sur un système Linux ou Macintosh et l'importe dans l'ASA :

1. Générez les clés publiques et privées RSA pour 4 096 bits sur votre ordinateur :

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. Convertissez la clé au format PKF :

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. Copiez la clé dans votre presse-papiers.
4. Dans ASDM, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**, sélectionnez le nom d'utilisateur, puis cliquez sur **Edit** (Modifier). Cliquez sur **Public Key Using PKF** (Clé publique utilisant PKF) et collez la clé dans la fenêtre :
5. Vérifiez que l'utilisateur peut se connecter par SSH à l'ASA. Pour le mot de passe, saisissez le mot de passe de la clé SSH que vous avez spécifié lors de la création de la paire de clés.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

La boîte de dialogue suivante s'affiche pour que vous puissiez saisir votre phrase secrète :

Pendant ce temps, dans la session de terminal :

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Configurer l'accès Telnet

Pour identifier les adresses IP clients autorisées à se connecter à l'ASA à l'aide de Telnet, procédez comme suit. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès Telnet, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès Telnet conformément à cette section.
- L'accès Telnet à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte Telnet est situé sur l'interface externe, vous ne pouvez initier une connexion Telnet que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 15.
- Vous ne pouvez pas utiliser Telnet sur l'interface de sécurité la plus basse, sauf si vous utilisez Telnet dans un tunnel VPN.
- L'ASA permet un maximum de cinq connexions Telnet simultanées par contexte/mode unique, avec un maximum de 100 connexions réparties entre tous les contextes.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.
- Pour accéder à l'interface de ligne de commande d'ASA à l'aide de Telnet, saisissez le mot de passe de connexion défini par la commande **password**. Vous devez définir manuellement le mot de passe avant d'utiliser Telnet.

Procédure

Étape 1 Identifiez les adresses IP à partir desquelles l'ASA accepte les connexions pour chaque adresse ou sous-réseau sur l'interface spécifiée.

telnet *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 15), spécifiez l'interface BVI nommée.

S'il n'existe qu'une seule interface, vous pouvez configurer Telnet pour accéder à cette interface tant que son niveau de sécurité est de 100.

Exemple :

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

Étape 2 Définissez la durée d'inactivité d'une session Telnet avant que l'ASA ne déconnecte la session.

telnet timeout *minutes*

Exemple :

```
ciscoasa(config)#  telnet timeout 30
```

Définissez le délai entre une et 1 440 minutes. La valeur par défaut est 5 minutes. La durée par défaut est trop courte dans la plupart des cas et devrait être augmentée jusqu'à ce que tous les tests de pré-production et le dépannage soient terminés.

Exemples

L'exemple suivant montre comment autoriser un hôte sur l'interface interne avec l'adresse 192.168.1.2 à accéder à l'ASA :

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

L'exemple suivant montre comment autoriser tous les utilisateurs du réseau 192.168.3.0 à accéder à l'ASA sur l'interface interne :

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

Configurer l'accès HTTPS pour ASDM, autres clients

Pour utiliser ASDM ou d'autres clients HTTPS tels que CSM, vous devez activer le serveur HTTPS et autoriser les connexions HTTPS à l'ASA. L'accès HTTPS est activé dans le cadre de la configuration d'usine par défaut. Pour configurer l'accès HTTPS, procédez comme suit. Consultez les consignes suivantes :

- Pour accéder à l'interface ASA pour l'accès HTTPS, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès HTTPS conformément à cette section. Si, toutefois, vous configurez la redirection HTTP pour rediriger automatiquement les connexions HTTP vers HTTPS, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.
- L'accès de gestion à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre hôte de gestion est situé sur l'interface externe, vous ne pouvez initier une connexion de gestion que directement à l'interface externe. La seule exception à cette règle est une connexion VPN. Consultez Configurer l'accès de gestion sur un tunnel VPN, à la page 15.
- En mode de contexte unique, vous pouvez avoir un maximum de 5 sessions ASDM simultanées. En mode de contexte multiple, vous pouvez avoir un maximum de 5 sessions ASDM simultanées par contexte, avec un maximum de 200 instances ASDM parmi tous les contextes.

  Les sessions ASDM utilisent deux connexions HTTPS: une pour la surveillance qui est toujours présente et une pour apporter des modifications de configuration qui est présente uniquement lorsque vous apportez des modifications. Par exemple, la limite système en mode de contexte multiple de 200 sessions ASDM représente une limite de 400 sessions HTTPS.
- L'ASA permet un maximum de 6 sessions HTTPS non ASDM simultanées en mode de contexte unique ou par contexte, si disponible, avec un maximum de 100 sessions HTTPS parmi tous les contextes.

- Si vous avez activé SSL (**webvpn** > **enable** *interface*) et l'accès HTTPS sur la même interface, vous pouvez accéder à Secure Client (services client sécurisés) à partir de l'adresse **https://***ip_address* et à ASDM à partir de l'adresse **https://***ip_address*/**admin**, tous deux sur le port 443. Si vous activez également **aaa authentication http console**, vous devez alors spécifier un port différent pour l'accès à ASDM.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, saisissez **changeto context** *name*.

Procédure

Étape 1 Identifiez les adresses IP à partir desquelles l'ASA accepte les connexions HTTPS pour chaque adresse ou sous-réseau sur l'interface spécifiée.

http *source_IP_address mask source_interface*

- *source_interface* : spécifiez n'importe quelle interface nommée. Pour les groupes de ponts, spécifiez l'interface membre du groupe de ponts. Pour l'accès à la gestion du VPN uniquement (voir Configurer l'accès de gestion sur un tunnel VPN, à la page 15), spécifiez l'interface BVI nommée.

Exemple :

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

Étape 2 Activez le serveur HTTPS.

http server enable [*port*]

Exemple :

```
ciscoasa(config)# http server enable 444
```

Par défaut, le port est 443. Si vous modifiez le numéro de port, veillez à l'inclure dans l'URL d'accès ASDM. Par exemple, si vous définissez le numéro de port à 444, saisissez l'URL suivante :

https://10.1.1.1:444

Étape 3 Autorisez les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés.

http server basic-auth-client *user_agent*

- *user_agent* : spécifie la chaîne User-Agent du client dans l'en-tête HTTP de la requête HTTP. Vous pouvez spécifier la chaîne complète ou une chaîne partielle; les chaînes partielles doivent correspondre au début de la chaîne User-Agent. Nous conseillons d'utiliser des chaînes complètes pour une meilleure sécurité. Notez que la chaîne est sensible à la casse.

  Par exemple, **curl** correspondra à la chaîne User-Agent suivante :

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

curl ne correspond *pas* à la chaîne User-Agent suivante :

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL ne correspond *pas* à la chaîne User-Agent suivante :

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic
ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

Saisissez chaque chaîne client à l'aide d'une commande distincte.De nombreux clients spécialistes (par exemple, les bibliothèques python, curl et wget) ne prennent pas en charge l'authentification basée sur le jeton Cross-site Request Forgery (CSRF). Vous devez donc autoriser expressément ces clients à utiliser la méthode d'authentification de base de l'ASA. Pour des raisons de sécurité, vous ne devez autoriser que les clients requis.

Exemple :

```
ciscoasa(config)# http server basic-auth-client curl
```

Étape 4 (Facultatif) Définissez les délais de connexion et de session.

http server idle-timeout*minutes*

http server session-timeout*minutes*

http connection idle-timeout*seconds*

- **http server idle-timeout** *minutes* : définissez le délai d'inactivité pour les connexions ASDM, de 1 à 1 440 minutes. La valeur par défaut est 20 minutes. L'ASA déconnecte une connexion ASDM qui est inactive pendant la période définie.
- **http server session-timeout** *minutes* : définissez le session expirée pour les sessions ASDM, de 1 à 1 440 minutes. Ce délai est désactivé par défaut. L'ASA déconnecte une session ASDM qui dépasse la période définie.
- **http connection idle-timeout** *seconds* : définissez le délai d'inactivité pour toutes les connexions HTTPS, y compris ASDM, WebVPN et d'autres clients, de 10 à 86 400 secondes. Ce délai est désactivé par défaut. L'ASA déconnecte une connexion qui est inactive pendant la période définie. Si vous définissez les commandes **http server idle-timeout** et **http connection idle-timeout**, la commande **http connection idle-timeout** prévaut.

Exemple :

```
ciscoasa(config)# http server idle-timeout 30
ciscoasa(config)# http server session-timeout 120
```

Exemples

L'exemple suivant montre comment activer le serveur HTTPS et autoriser un hôte sur l'interface interne avec l'adresse 192.168.1.2 à accéder à ASDM :

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

L'exemple suivant montre comment autoriser tous les utilisateurs du réseau 192.168.3.0/24 à accéder à ASDM sur l'interface interne :

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

Configurer la redirection HTTP pour l'accès ASDM ou le SSL VPN sans client

Vous devez utiliser HTTPS pour vous connecter à l'ASA à l'aide d'ASDM ou du SSL VPN sans client. Pour plus de commodité, vous pouvez rediriger les connexions de gestion HTTP vers HTTPS. Par exemple, en redirigeant HTTP, vous pouvez saisir **http://10.1.8.4/admin/** ou **https://10.1.8.4/admin/** et arriver toujours à la page de lancement d'ASDM à l'adresse HTTPS.

Vous pouvez rediriger le trafic IPv4 et IPv6.

Avant de commencer

Normalement, vous n'avez pas besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Cependant, pour la redirection HTTP, vous devez activer un critère d'accès pour autoriser HTTP; sinon, l'interface ne peut pas être à l'écoute du port HTTP.

Procédure

Activez la redirection HTTP :

http redirect *interface_name* [*port*]

Exemple :

```
ciscoasa(config)# http redirect outside 88
```

Le *port* identifie le port à partir duquel l'interface redirige les connexions HTTP. La valeur par défaut est 80.

Configurer l'accès de gestion sur un tunnel VPN

Si votre tunnel VPN se termine sur une interface, mais que vous souhaitez gérer l'ASA en accédant à une autre interface, vous devez identifier cette interface comme une interface d'accès de gestion. Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSHou Telnet; ou vous pouvez envoyer un message Ping à l'interface interne en entrant à partir de l'interface externe.

Remarque Cette fonctionnalité n'est pas prise en charge pour SSH si vous utilisez la pile CiscoSSH, qui est la valeur par défaut.

Remarque Cette fonctionnalité n'est pas prise en charge pour SNMP. Pour SNMP sur VPN, nous vous recommandons d'activer SNMP sur une interface de boucle avec retour. Vous n'avez pas besoin d'activer la fonctionnalité d'accès de gestion pour utiliser SNMP sur l'interface de boucle avec retour. La boucle avec retour fonctionne également pour SSH.

L'accès VPN à une interface autre que celle à partir de laquelle vous avez saisi l'ASA n'est pas pris en charge. Par exemple, si votre accès VPN se trouve sur l'interface externe, vous pouvez uniquement initier une connexion directement à l'interface externe. Vous devez activer le VPN sur l'interface directement accessible de l'ASA et utiliser la résolution de noms pour ne pas avoir à vous souvenir de plusieurs adresses.

L'accès de gestion est disponible par les types de tunnel VPN suivants : clients IPsec, IPsec de site à site, Easy VPN et le SSL VPN Secure Client (services client sécurisés).

Avant de commencer

- Cette fonctionnalité n'est pas prise en charge sur les interfaces de gestion uniquement.
- Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité, vous devez configurer la NAT avec l'option de recherche de routage. Pour en savoir plus, consultez la section « Accès à la gestion de la NAT et du VPN » dans le chapitre *Exemples de NAT et référence* dans la version appropriée du Guide de configuration de l'interface de ligne de commande du pare-feu ASA.

Procédure

Précisez le nom de l'interface de gestion à laquelle vous souhaitez accéder lorsque vous saisissez l'ASA à partir d'une autre interface.

management-access *management_interface*

Pour les tunnels Easy VPN et Site à site, vous pouvez spécifier une BVI nommée (en mode routé).

Exemple :

```
ciscoasa(config)# management-access inside
```

Configurer l'accès de gestion pour FXOS sur les interfaces de données en mode plateforme Firepower 2100

Si vous souhaitez gérer FXOS sur le Firepower 2100 en mode plateforme à partir d'une interface de données, vous pouvez configurer l'accès SSH, HTTPS et SNMP. Cette fonctionnalité est utile si vous souhaitez gérer le périphérique à distance, mais que vous souhaitez conserver la gestion 1/1, qui est la méthode d'accès native à FXOS, sur un réseau isolé. Si vous activez cette fonctionnalité, vous pouvez continuer à utiliser l'interface de gestion Management 1/1 pour l'accès local uniquement. Cependant, vous ne pouvez pas autoriser l'accès *à distance* depuis ou vers l'interface de gestion Management 1/1 pour FXOS en même temps que l'utilisation de cette fonctionnalité. Cette fonctionnalité nécessite le transfert du trafic vers les interfaces de données ASA

à l'aide d'un chemin interne (valeur par défaut), et vous ne pouvez spécifier qu'une seule passerelle de gestion FXOS.

L'ASA utilise des ports non standard pour l'accès FXOS; le port standard est réservé à l'utilisation par l'ASA sur la même interface. Lorsque l'ASA transfère le trafic vers FXOS, il traduit le port de destination non standard en port FXOS pour chaque protocole (ne modifiez pas le port HTTPS dans FXOS). L'adresse IP de destination du paquet (qui est l'adresse IP de l'interface ASA) est également convertie en une adresse interne pour l'utilisation par FXOS. L'adresse source reste inchangée. Pour renvoyer le trafic, l'ASA utilise sa table de routage de données pour déterminer la bonne interface de sortie. Lorsque vous accédez à l'adresse IP de données ASA pour l'application de gestion, vous devez vous connecter en utilisant un nom d'utilisateur FXOS; les noms d'utilisateur ASA ne s'appliquent qu'à l'accès de gestion ASA.

Vous pouvez également activer l'*initiation* du trafic de gestion FXOS sur les interfaces de données ASA. Cette fonction est requise pour les alertes SNMP ou pour l'accès au serveur NTP et DNS, par exemple. Par défaut, l'initiation du trafic de gestion FXOS est activée pour l'interface externe ASA pour la communication avec les serveurs DNS et NTP (cette fonctionnalité est requise pour la communication avec les licences Smart).

Avant de commencer

- Mode contexte unique seulement.
- Exclut les interfaces de gestion ASA uniquement.
- Vous ne pouvez pas utiliser un tunnel VPN pour l'interface de données ASA et accéder directement à FXOS. Comme solution de contournement pour SSH, vous pouvez faire appel au VPN vers l'ASA, accéder à l'interface de ligne de commande de l'*ASA*, puis utiliser la commande **connect fxos** pour accéder à l'interface de ligne de commande de FXOS. Notez que SSH, HTTPS et SNMPv3 sont/peuvent être chiffrés, de sorte qu'une connexion directe à l'interface de données est sécurisée.
- Assurez-vous que la passerelle FXOS est configurée pour acheminer le trafic vers les interfaces de données ASA (par défaut). Consultez le guide de démarrage pour en savoir plus sur la configuration de la passerelle.

Procédure

Étape 1 Activez la gestion à distance FXOS.

fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address/prefix_length*} *interface_name*

Exemple :

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

Étape 2 (Facultatif) Modifiez le port par défaut pour le service.

fxos {**https** | **ssh** | **snmp**} **port** *port*

Consultez les paramètres par défaut suivants :

- Port HTTPS par défaut : 3443

- Port SNMP par défaut : 3061
- Port SSH par défaut : 3022

Exemple :

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

Étape 3 Permettez à FXOS d'initier des connexions de gestion à partir de l'interface ASA.

ip-client *interface_name*

Par défaut, l'interface externe est activée.

Exemple :

```
ciscoasa(config)# ip-client outside
ciscoasa(config)# ip-client services
```

Étape 4 Connectez-vous à Firewall Chassis Manager sur l'interface de gestion Management 1/1 (par défaut https://192.168.45.45, avec le nom d'utilisateur : **admin** et le mot de passe : **Admin123**).

Étape 5 Cliquez sur l'onglet **Platform Settings** (paramètres de plateforme) et activez **SSH**, **HTTPS** ou **SNMP**.

SSH et HTTPS sont activés par défaut.

Étape 6 Configurez une liste d'accès (**Access List**) dans l'onglet des paramètres de la plateforme (**Platform Settings**) pour autoriser vos adresses de gestion. SSH et HTTPS autorisent uniquement le réseau de gestion Management 1/1 192.168.45.0 par défaut. Vous devez autoriser toutes les adresses que vous avez spécifiées dans la configuration de gestion à distance FXOS (**FXOS Remote Management**) sur l'ASA.

Modifier le délai d'expiration de la console

Le délai d'expiration de la console définit combien de temps une connexion peut rester en mode d'exécution privilégié ou en mode de configuration; une fois le délai d'expiration atteint, la session passe en mode EXEC de l'utilisateur. Par défaut, la session n'expire pas. Ce paramètre n'a pas d'incidence sur la durée de votre connexion au port de console, qui n'expire jamais.

Procédure

Spécifiez le délai d'inactivité en minutes (0 à 60) après quoi la session privilégiée se termine.

console timeout *number*

Exemple :

```
ciscoasa(config)# console timeout 0
```

La valeur d'expiration par défaut est 0, ce qui signifie que la session n'expire pas.

Personnaliser une invite de l'interface de ligne de commande

La possibilité d'ajouter des renseignements à une invite vous permet de voir en un coup d'œil à quel ASA vous êtes connecté lorsque vous avez plusieurs modules. Lors d'un basculement, cette fonctionnalité est utile lorsque les deux ASA ont le même nom d'hôte.

En mode de contexte multiple, vous pouvez afficher l'invite étendue lorsque vous vous connectez à l'espace d'exécution du système ou au contexte d'administration. Dans un contexte de non-administration, vous ne voyez que l'invite par défaut, qui est le nom d'hôte et le nom de contexte.

Par défaut, l'invite affiche le nom d'hôte de l'ASA. En mode de contexte multiple, l'invite affiche également le nom du contexte. Vous pouvez afficher les éléments suivants dans l'invite de l'interface de ligne de commande :

cluster-unit	Affiche le nom de l'unité de grappe. Chaque unité d'une grappe peut avoir un nom unique.
context	(Mode multiple uniquement) Affiche le nom du contexte actuel.
domaine	Affiche le nom de domaine.
hostname	Affiche le nom d'hôte.
priority	Affiche la priorité de basculement comme pri (principal) ou sec (secondaire).
state	Affiche l'état de transmission du trafic ou le rôle de l'unité. Pour le basculement, les valeurs suivantes sont affichées pour le mot clé d'état : • **act** : le basculement est activé et l'unité transmet activement le trafic. • **stby** : le basculement est activé et l'unité ne transmet pas de trafic et est en veille, en panne ou dans un autre état non actif. • **actNoFailover** : le basculement n'est pas activé et l'unité transmet activement le trafic. • **stbyNoFailover** : le basculement n'est pas activé et l'unité ne transmet pas de trafic. Cela pourrait se produire en cas de défaillance d'interface au-dessus du seuil sur l'unité en veille. Pour la mise en grappe, les valeurs du contrôle et des données sont affichées.

Procédure

Personnalisez l'invite de l'interface de ligne de commande en saisissant la commande suivante :

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

Exemple :

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

L'ordre dans lequel vous saisissez les mots clés détermine l'ordre des éléments dans l'invite, qui sont séparés par une barre oblique (/).

Configurer une bannière de connexion

Vous pouvez configurer un message pour qu'il s'affiche lorsqu'un utilisateur se connecte à l'ASA, avant qu'un utilisateur ne se connecte ou avant qu'un utilisateur n'entre en mode d'exécution privilégié.

Avant de commencer

- Du point de vue de la sécurité, il est important que votre bannière dissuade les accès non autorisés. N'utilisez pas les mots « bienvenue » ou « s'il vous plaît », car ils semblent inviter des intrus à entrer. La bannière suivante donne le bon ton en cas d'accès non autorisé :

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- Après l'ajout d'une bannière, les sessions Telnet ou SSH à l'ASA peuvent se fermer si :
  - La mémoire système est insuffisante pour traiter les messages sur bannière.
  - Une erreur d'écriture TCP se produit lors de la tentative d'affichage des messages sur bannière.
- Consultez la RFC 2196 pour connaître les lignes directrices relatives aux messages sur bannière.

Procédure

Ajoutez une bannière à afficher à l'un des trois moments suivants : lorsqu'un utilisateur se connecte pour la première fois (message du jour (motd)), lorsqu'un utilisateur se connecte (connexion) et lorsqu'un utilisateur accède au mode d'exécution privilégié (exec).

banner {**exec** | **login** | **motd**} *texte*

Exemple :

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).
```

Lorsqu'un utilisateur se connecte à l'ASA, la bannière message-du-jour s'affiche en premier, suivie de la bannière de connexion et des invites. Une fois que l'utilisateur a bien été connecté à l'ASA, la bannière d'exécution s'affiche.

Pour ajouter plusieurs lignes, précédez chaque ligne par la commande **banner**.

Pour le texte de la bannière :

- Les espaces sont autorisés, mais les onglets ne peuvent pas être saisis à l'aide de l'interface de ligne de commande.
- Il n'y a aucune limite de longueur de bannière autre que celles de la RAM et de la mémoire flash.

- Vous pouvez ajouter de manière dynamique le nom d'hôte ou le nom de domaine de l'ASA en incluant les chaînes **$(hostname)** et **$(domain)**.
- Si vous configurez une bannière dans la configuration système, vous pouvez utiliser ce texte de bannière dans un contexte en utilisant la chaîne **$(system)** dans la configuration du contexte.

Exemples

Les exemples suivants montrent comment ajouter une bannière de message du jour :

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

Définir un quota de sessions de gestion

Vous pouvez établir un nombre maximum de sessions ASDM, SSH et Telnet simultanées qui sont autorisées sur l'ASA. Si le maximum est atteint, aucune session supplémentaire n'est autorisée et un message de journal système est généré. Pour empêcher un verrouillage du système, le mécanisme de quota de sessions de gestion ne peut pas bloquer une session de console.

Remarque En mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions ASDM, où le maximum est fixe à 5 sessions.

Remarque Si vous définissez également une limite de ressources par contexte pour le nombre maximum de sessions administratives (SSH, etc.), la valeur la plus basse sera utilisée.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez le contexte **changeto context** *name*.

Procédure

Étape 1 Entrez la commande suivante :

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

- **ssh** : définit le nombre maximum de sessions SSH, entre 1 et 5. La valeur par défaut est égale à 5.
- **telnet** : définit le nombre maximum de sessions Telnet, entre 1 et 5. La valeur par défaut est égale à 5.

- **http** : définit le nombre maximum de sessions HTTPS (ASDM), entre 1 et 5. La valeur par défaut est égale à 5.
- **user** : définit le nombre maximum de sessions par utilisateur, entre 1 et 5. La valeur par défaut est égale à 5.
- *number* : définit le nombre de sessions. Lorsqu'il est saisi sans autre mot clé, cet argument définit le nombre agrégé de sessions entre 1 et 15. La valeur par défaut est de 15.

Exemple :

```
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

Étape 2 Affichez les sessions actuellement utilisées.

show quota management-session [**ssh** | **telnet** | **http** | **user**]

Exemple :

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                 Username
1                              SSH                     cisco
2                              TELNET                  cisco
1                              SSH                     cisco1
```

Configurer AAA pour les administrateurs système

Cette section décrit comment configurer l'authentification, l'autorisation de gestion et l'autorisation de commande pour les administrateurs système.

Configurer l'authentification de gestion

Configurez l'authentification pour l'accès à l'interface de ligne de commande et à ASDM.

À propos de l'authentification de gestion

La façon dont vous vous connectez à l'ASA dépend de si vous activez ou non l'authentification.

À propos de l'authentification SSH

Consultez le comportement suivant pour l'accès SSH avec et sans authentification :

- Aucune authentification : SSH n'est pas disponible sans authentification.
- Authentification : lorsque vous activez l'authentification SSH, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Pour l'authentification par clé publique, l'ASA ne prend en charge que la base de données locale. Si vous

configurez l'authentification par clé publique SSH, l'ASA utilise implicitement la base de données locale. Il vous suffit de configurer explicitement l'authentification SSH lorsque vous utilisez un nom d'utilisateur et un mot de passe pour vous connecter. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification Telnet

Consultez le comportement suivant pour l'accès Telnet avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour Telnet, vous ne saisissez pas de nom d'utilisateur; vous saisissez le mot de passe de connexion (défini avec la commande **password**). Il n'y a pas de mot de passe par défaut, vous devez donc en définir un avant de pouvoir vous connecter à l'ASA via Telnet. Vous accédez au mode EXEC de l'utilisateur.
- Authentification : si vous activez l'authentification Telnet, vous saisissez le nom d'utilisateur et le mot de passe définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'authentification ASDM

Consultez le comportement suivant pour l'accès ASDM avec et sans authentification. Vous pouvez également configurer l'authentification par certificat, avec ou sans authentification AAA.

- Aucune authentification : par défaut, vous pouvez vous connecter à ASDM avec un nom d'utilisateur vide et le mot de passe d'activation défini par la commande **enable password**, qui est vide par défaut. Nous vous suggérons de modifier le mot de passe d'activation dès que possible afin qu'il ne reste pas vide; voir Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet. Lorsque vous saisissez la commande **enable** au niveau de l'interface de ligne de commande pour la première fois, vous êtes invité à modifier le mot de passe; ce comportement n'est pas appliqué lorsque vous vous connectez à ASDM. Notez que si vous saisissez un nom d'utilisateur et un mot de passe à l'écran de connexion (au lieu de laisser le nom d'utilisateur vide), ASDM vérifie la base de données locale à la recherche d'une correspondance.
- Authentification par certificat : (mode unique et routé uniquement) Vous pouvez exiger que l'utilisateur ait un certificat valide. Saisissez le nom d'utilisateur et le mot de passe du certificat pour que l'ASA valide le certificat par rapport au point de confiance PKI.
- Authentification AAA : lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données locale des utilisateurs. Vous ne pouvez plus utiliser ASDM avec un nom d'utilisateur vide et le mot de passe d'activation.
- Authentification AAA plus authentification par certificat : (mode unique et routé uniquement) Lorsque vous activez l'authentification ASDM (HTTPS), vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Si le nom d'utilisateur et le mot de passe sont différents pour l'authentification par certificat, vous êtes invité à les saisir également. Vous pouvez choisir de préremplir le nom d'utilisateur dérivé de votre certificat.

À propos de l'authentification série

Consultez le comportement suivant pour l'accès au port de console série avec et sans authentification :

- Aucune authentification : si vous n'activez aucune authentification pour l'accès en série, vous ne saisissez pas de nom d'utilisateur ni de mot de passe. Vous accédez au mode EXEC de l'utilisateur.

- Authentification : si vous activez l'authentification pour l'accès en série, vous saisissez le nom d'utilisateur et le mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Vous accédez au mode EXEC de l'utilisateur.

À propos de l'activation de l'authentification

Pour passer en mode d'exécution privilégié après la connexion, saisissez la commande **enable**. Le fonctionnement de cette commande dépend de si vous activez ou non l'authentification.

- Aucune authentification : si vous ne configurez pas l'authentification, saisissez le mot de passe d'activation du système lorsque vous saisissez la commande **enable** (défini par la commande **enable password**), qui est vide par défaut. La première fois que vous saisissez la commande **enable**, vous devez modifier le mot de passe. Cependant, si vous n'utilisez pas l'activation de l'authentification, après avoir saisi la commande **enable**, vous n'êtes plus connecté en tant qu'utilisateur particulier, ce qui peut affecter les fonctionnalités basées sur l'utilisateur telles que l'autorisation de commande. Pour conserver votre nom d'utilisateur, utilisez l'activation de l'authentification.
- Authentification : si vous configurez l'activation de l'authentification, l'ASA vous invite à entrer votre nom d'utilisateur et mot de passe comme définis sur le serveur AAA ou la base de données des utilisateurs locale. Cette fonctionnalité est particulièrement utile lorsque vous effectuez une autorisation de commande, dans laquelle les noms d'utilisateur sont importants pour déterminer les commandes qu'un utilisateur peut saisir.

Pour activer l'authentification à l'aide de la base de données locale, vous pouvez utiliser la commande **login** au lieu de la commande **enable**. La commande **login** conserve le nom d'utilisateur, mais ne nécessite aucune configuration pour activer l'authentification.

⚠

Mise en garde Si vous ajoutez à la base de données locale des utilisateurs qui peuvent accéder à l'interface de ligne de commande et que vous ne souhaitez pas entrer en mode d'exécution privilégié, vous devez configurer l'autorisation de commande. Sans autorisation de commande, les utilisateurs peuvent accéder au mode d'exécution privilégié (et à toutes les commandes) au niveau de l'interface de ligne de commande en utilisant leur propre mot de passe si leur niveau de privilège est de 2 ou plus (2 est la valeur par défaut). Vous pouvez également décourager l'utilisation de la commande login en utilisant un serveur AAA pour l'authentification au lieu de la base de données locale, ou vous pouvez définir tous les utilisateurs locaux au niveau 1 afin de pouvoir contrôler qui peut utiliser le mot de passe d'activation du système pour accéder au mode d'exécution privilégié.

Sessions du système d'exploitation hôte vers l'ASA

Certaines plateformes prennent en charge l'exécution de l'ASA en tant qu'application distincte : par exemple l'ASA sur le Firepower 4100/9300. Pour les sessions du système d'exploitation hôte à l'ASA, vous pouvez configurer l'authentification série et Telnet, selon le type de connexion. Par exemple, la commande **connect asa** dans FXOS sur le Firepower 2100 en mode plateforme utilise un port série.

En mode de contexte multiple, vous ne pouvez pas configurer de commandes AAA dans la configuration système. Cependant, si vous configurez l'authentification Telnet ou série dans le contexte d'administration, l'authentification s'applique également à ces sessions. Le serveur AAA du contexte d'administration ou la base de données locale des utilisateurs est utilisé dans cette instance.

Configurer l'authentification pour l'interface de ligne de commandeet ASDM Access

Avant de commencer

- Configurez l'accès Telnet, SSH ou HTTP.
- Pour l'authentification extérieure, configurez un groupe de serveurs AAA. Pour l'authentification locale, ajoutez des utilisateurs à la base de données locale.
- L'authentification de gestion HTTP ne prend pas en charge le protocole SDI pour un groupe de serveurs AAA.
- Cette fonctionnalité n'affecte pas l'authentification par clé publique SSH pour les noms d'utilisateur locaux avec la commande **ssh authentication**. L'ASA utilise implicitement la base de données locale pour l'authentification par clé publique. Cette fonctionnalité n'affecte que les noms d'utilisateur avec mots de passe. Si vous souhaitez autoriser l'authentification par clé publique ou l'utilisation du mot de passe par un utilisateur local, vous devez configurer explicitement l'authentification locale à l'aide de cette procédure pour autoriser l'accès par mot de passe.

Procédure

Authentifiez les utilisateurs pour l'accès de la gestion.

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

Exemple :

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

Le mot clé **telnet** contrôle l'accès Telnet. Le mot clé **ssh** contrôle l'accès SSH (mot de passe uniquement; l'authentification par clé publique utilise implicitement la base de données locale). Le mot clé **http** contrôle l'accès ASDM. Le mot clé **serial** contrôle l'accès au port de la console. Pour Firepower 2100 en mode plateforme, ce mot clé affecte la console virtuelle accessible à partir de FXOS à l'aide de la commande **connect asa**.

Si vous utilisez un groupe de serveurs AAA pour l'authentification, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs suivi de **LOCAL** (qui est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée. Vous pouvez également utiliser la base de données locale comme méthode d'authentification principale (sans système de secours) en saisissant **LOCAL** uniquement.

Configurer l'activation de l'authentification (mode d'exécution privilégié)

Vous pouvez authentifier les utilisateurs lorsqu'ils saisissent la commande **enable**.

Avant de commencer

Consultez À propos de l'activation de l'authentification, à la page 24.

Procédure

Choisissez l'une des options suivantes pour l'authentification des utilisateurs :

- Pour authentifier les utilisateurs auprès d'un serveur AAA ou de la base de données locale, saisissez la commande suivante :

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  Exemple :

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  Un nom d'utilisateur et un mot de passe seront demandés à l'utilisateur.

  Si vous utilisez un groupe de serveurs AAA pour l'authentification, vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur AAA n'est pas disponible. Spécifiez le nom du groupe de serveurs suivi de **LOCAL** (qui est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur AAA, car l'invite ASA n'indique pas quelle méthode est utilisée.

  Vous pouvez également utiliser la base de données locale comme méthode d'authentification principale (sans système de secours) en saisissant **LOCAL** uniquement.

- Pour vous connecter en tant qu'utilisateur à partir de la base de données locale, saisissez la commande suivante :

  login

  Exemple :

  ```
  ciscoasa# login
  ```

  L'ASA vous demande votre nom d'utilisateur et votre mot de passe. Après avoir saisi votre mot de passe, l'ASA vous place au niveau de privilège spécifié par la base de données locale.

  Les utilisateurs peuvent se connecter avec leur nom d'utilisateur et mot de passe pour accéder au mode d'exécution privilégié. Vous n'avez donc pas à fournir le mot de passe d'activation du système à tout le monde. Pour permettre aux utilisateurs d'accéder au mode d'exécution privilégié (et à toutes les commandes) lorsqu'ils se connectent, définissez le niveau de privilège de l'utilisateur de 2 (par défaut) à 15. Si vous configurez l'autorisation de commande locale, l'utilisateur ne peut entrer que les commandes attribuées à ce niveau de privilège ou à un niveau inférieur.

Configurer l'authentification par certificat ASDM

Vous pouvez exiger l'authentification par certificat, avec ou sans authentification AAA. L'ASA valide le certificat par rapport au point de confiance PKI.

Avant de commencer

Cette fonctionnalité est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Activez l'authentification par certificat :

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

Exemple :

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name emailAddress www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

Vous configurez l'authentification par certificat pour chaque interface, de sorte que les connexions sur une interface de confiance/interne n'ont pas à fournir de certificat. Vous pouvez utiliser la commande plusieurs fois pour activer l'authentification par certificat sur plusieurs interfaces.

Pour exiger que le certificat corresponde à une carte de certificat, spécifiez le mot clé **match** et le nom de la carte. Configurez la carte à l'aide de la commande **crypto ca certificate map**.

Étape 2 (Facultatif) Définissez l'attribut utilisé par ASDM pour dériver le nom d'utilisateur à partir du certificat :

http username-from-certificate{*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

Exemple :

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

Par défaut, ASDM utilise les attributs CN OU.

- L'argument *primary-attr* spécifie l'attribut à utiliser pour dériver le nom d'utilisateur. L'argument *secondary-attr* spécifie un attribut supplémentaire à utiliser avec l'attribut principal pour dériver le nom d'utilisateur. Vous pouvez utiliser les attributs suivants :
  - C : Pays
  - CN : nom commun
  - DNQ : qualificateur de nom distinctif
  - emailAddress : adresse courriel
  - GENQ : qualificatif générationnel
  - GN : prénom
  - I : initiales
  - L : localité
  - N : nom
  - O : organisation
  - OU : unité organisationnelle

- SER : numéro de série
- SN : nom de famille
- SP : État/province
- T : titre
- UID : identifiant de l'utilisateur
- UPN : nom principal de l'utilisateur

- Le mot clé **use-entire-name** utilise le nom complet du DN.
- Le mot clé **use-script** utilise un script Lua généré par ASDM.
- Le mot clé **pre-fill-username** préremplit le nom d'utilisateur lorsque l'authentification est demandée. Si le nom d'utilisateur est différent de celui que vous avez initialement saisi, une nouvelle boîte de dialogue s'affiche avec le nom d'utilisateur prérempli. Vous pouvez ensuite saisir le mot de passe pour l'authentification.

Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion

L'ASA vous permet de distinguer les utilisateurs administratifs et d'accès à distance lorsqu'ils s'authentifient. La différence des rôles d'utilisateur peut empêcher les utilisateurs du VPN d'accès à distance et de l'accès réseau d'établir une connexion administrative à l'ASA.

Avant de commencer

Utilisateurs RADIUS ou LDAP (mappés)

Lorsque les utilisateurs sont authentifiés par LDAP, les attributs LDAP natifs et leurs valeurs peuvent être mappés aux attributs ASA pour fournir des fonctionnalités d'autorisation spécifiques. Configurez Cisco VSA CVPN3000-Privilege-Level avec une valeur comprise entre 0 et 15, puis mappez les attributs LDAP à Cisco VAS CVPN3000-Privilege-Level à l'aide de la commande **ldap map-attributes**.

L'attribut **service-type** IETF RADIUS, lorsqu'il est envoyé dans un message d'acceptation de l'accès à la suite d'une demande d'authentification et d'autorisation RADIUS, est utilisé pour désigner le type de service accordé à l'utilisateur authentifié.

L'attribut **privilege-level** RADIUS Cisco VSA (ID de fournisseur 3076, sous-ID 220), lorsqu'il est envoyé dans un message d'acceptation de l'accès, est utilisé pour désigner le niveau de privilège de l'utilisateur.

Utilisateurs TACACS+

L'autorisation est demandée par « service=shell », et le serveur répond par PASS (réussite) ou FAIL (échec).

Utilisateurs locaux

Définissez la commande **service-type** pour un nom d'utilisateur donné. Par défaut, le type de service est admin, ce qui permet un accès complet à tous les services spécifiés par la commande **aaa authentication console**.

Attributs d'autorisation de gestion

Consultez le tableau suivant pour connaître les types de serveurs AAA et les valeurs valides pour l'autorisation de gestion. L'ASA utilise ces valeurs pour déterminer le niveau d'accès de gestion.

Niveau de gestion	Attributs RADIUS/LDAP (mappés)	Attributs TACACS+	Attributs de la base de données locale
Accès complet : permet un accès complet à tous les services spécifiés par les commandes **aaa authentication console**	Type de service 6 (Administrateur), niveau de privilège 1	PASS (réussite), privilège de niveau 1	admin
Accès partiel : permet l'accès à l'interface de ligne de commande ou à ASDM lorsque vous configurez les commandes **aaa authentication console** . Cependant, si vous configurez l'authentification **enable** avec la commande **aaa authentication enable console** option, l'utilisateur de l'interface de ligne de commande ne peut pas accéder au mode d'exécution privilégié à l'aide de la commande **enable**.	Type de service 7 (invite NAS), niveau de privilège 2 et supérieur Les types de service Framed (2) et Login (1) sont traités de la même manière.	PASS (réussite), niveau de privilège 2 et supérieur	nas-prompt
Aucun accès : refuse l'accès de gestion. L'utilisateur ne peut pas utiliser les services spécifiés par les commandes **aaa authentication console** (à l'exception du mot clé **serial** option; l'accès en série est autorisé). Les utilisateurs d'accès à distance (IPsec et SSL) peuvent toujours s'authentifier et mettre fin à leurs sessions d'accès à distance. Tous les autres types de services (voix, FAX, etc.) sont traités de la même manière.	Type de service 5 (sortant)	ÉCHEC	remote-access

Directives supplémentaires

- L'accès à la console de série n'est pas inclus dans l'autorisation de gestion.
- Vous devez également configurer l'authentification AAA pour l'accès de gestion afin d'utiliser cette fonctionnalité. Consultez Configurer l'authentification pour l'interface de ligne de commandeet ASDM Access, à la page 25.
- Si vous utilisez l'authentification extérieure, vous devez préconfigurer un groupe de serveurs AAA avant d'activer cette fonctionnalité.
- L'autorisation HTTP est prise en charge uniquement en mode routé simple.

Procédure

Étape 1 Activez l'autorisation de gestion pour Telnet et SSH :

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

Le mot clé **auto-enable** permet aux administrateurs disposant de privilèges d'autorisation suffisants de passer automatiquement en mode d'exécution privilégié lorsqu'ils se connectent.

Exemple :

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

Étape 2 Activez l'autorisation de gestion pour HTTPS (ASDM) :

aaa authorization http console {**authentication-server** | **LOCAL**}

Exemple :

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

Étape 3

Exemples

L'exemple suivant montre comment définir une carte d'attributs LDAP. Dans cet exemple, la stratégie de sécurité précise que les utilisateurs authentifiés par LDAP mappent les champs d'enregistrement d'utilisateur ou le titre des paramètres et la société au type de service et au niveau de privilège IETF-RADIUS, respectivement.

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

L'exemple suivant applique une carte d'attributs LDAP à un serveur LDAP AAA :

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

Configurer l'autorisation de commande

Si vous souhaitez contrôler l'accès aux commandes, l'ASA vous permet de configurer l'autorisation de commande, dans laquelle vous pouvez déterminer quelles commandes sont disponibles pour un utilisateur. Par défaut, lorsque vous vous connectez, vous pouvez accéder au mode EXEC de l'utilisateur, qui n'offre que des commandes minimales. Lorsque vous saisissez la commande **enable** (ou la commande **login** lorsque vous utilisez la base de données locale), vous pouvez accéder au mode d'exécution privilégié et aux commandes avancées, y compris les commandes de configuration.

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux
- Niveaux de privilèges du serveur TACACS+

À propos de l'autorisation de commande

Vous pouvez activer l'autorisation de commande pour que seuls les utilisateurs autorisés puissent saisir des commandes.

Méthodes d'autorisation de commande prises en charge

Vous pouvez utiliser l'une des deux méthodes d'autorisation de commande suivantes :

- Niveaux de privilèges locaux : configurez les niveaux de privilège de commande sur l'ASA. Lorsqu'un utilisateur local, RADIUS ou LDAP (si vous mappez des attributs LDAP aux attributs RADIUS) s'authentifie pour l'accès à l'interface de ligne de commande, l'ASA place cet utilisateur au niveau de privilège défini par la base de données locale, RADIUS ou le serveur LDAP. L'utilisateur peut accéder aux commandes au niveau de privilège attribué et en dessous. Notez que tous les utilisateurs accèdent au mode EXEC lorsqu'ils se connectent pour la première fois (commandes au niveau 0 ou 1). L'utilisateur doit s'authentifier de nouveau avec la commande **enable** pour accéder au mode d'exécution privilégié (commandes de niveau 2 ou supérieur), ou il peut se connecter avec la commande **login** (base de données locale uniquement).

Remarque Vous pouvez utiliser l'autorisation de commande locale sans aucun utilisateur dans la base de données locale et sans interface de ligne de commande ni authentification **enable**. Au lieu de cela, lorsque vous saisissez la commande **enable**, vous saisissez le mot de passe d'activation du système et l'ASA vous place au niveau 15. Vous pouvez ensuite créer des mots de passe d'activation pour chaque niveau, de sorte que lorsque vous entrez **enable** *n* (2 à 15), l'ASA vous place au niveau *n*. Ces niveaux ne sont pas utilisés, sauf si vous activez l'autorisation de commande locale.

- Niveaux de privilège du serveur TACACS+ : sur le serveur TACACS+, configurez les commandes qu'un utilisateur ou un groupe peut utiliser après s'être authentifié pour l'accès à l'interface de ligne de commande. Chaque commande qu'un utilisateur saisit au niveau de l'interface de ligne de commande est validée auprès du serveur TACACS+.

Contextes de sécurité et autorisation de commande

Les paramètres AAA sont distincts par contexte et ne sont pas partagés entre les contextes.

Lors de la configuration de l'autorisation de commande, vous devez configurer chaque contexte de sécurité séparément. Cette configuration vous offre la possibilité d'appliquer différentes autorisations de commande pour différents contextes de sécurité.

Lorsqu'ils passent d'un contexte de sécurité à l'autre, les administrateurs doivent savoir que les commandes autorisées pour le nom d'utilisateur spécifié lors de la connexion peuvent être différentes dans la nouvelle session de contexte ou que l'autorisation de commande peut ne pas être configurée du tout dans le nouveau contexte. Ne pas comprendre que les autorisations de commande peuvent différer d'un contexte de sécurité à l'autre peut dérouter un administrateur.

Remarque L'espace d'exécution du système ne prend pas en charge les commandes AAA; par conséquent, l'autorisation de commande n'est pas disponible dans l'espace d'exécution du système.

Niveaux de privilège de commande

Par défaut, les commandes suivantes sont affectées au niveau de privilège 0. Toutes les autres commandes sont affectées au niveau de privilège 15.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Si vous déplacez des commandes de mode de configuration à un niveau inférieur à 15, veillez également à déplacer la commande **configure** à ce niveau, sinon l'utilisateur ne pourra pas entrer en mode de configuration.

Configurer l'autorisation de commande locale

L'autorisation de commande locale vous permet d'affecter des commandes à l'un des 16 niveaux de privilège (0 à 15). Par défaut, chaque commande est affectée au niveau de privilège 0 ou 15. Vous pouvez définir chaque utilisateur comme étant à un niveau de privilège spécifique, et chaque utilisateur peut saisir n'importe quelle commande au niveau de privilège attribué ou en dessous. L'ASA prend en charge les niveaux de privilège d'utilisateur définis dans la base de données locale, un serveur RADIUS ou un serveur LDAP (si vous mappez des attributs LDAP aux attributs RADIUS).

Procédure

Étape 1 Attribuez une commande à un niveau de privilège.

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** *command*

Exemple :

```
ciscoasa(config)# privilege show level 5 command filter
```

Répétez cette commande pour chaque commande que vous souhaitez réaffecter.

Les options de cette commande sont les suivantes :

- **show** | **clear** | **cmd** : ces mots clés facultatifs vous permettent de définir les privilèges uniquement pour la forme show, clear ou configure de la commande. La forme configure de la commande est généralement la forme qui entraîne une modification de configuration, soit sous forme de commande non modifiée (sans le préfixe **show** ou **clear**), soit sous la forme **no**. Si vous n'utilisez pas l'un de ces mots clés, toutes les formes de commande sont affectées.
- **level** *level* : un niveau compris entre 0 et 15.
- **mode** {**enable** | **configure**} : si une commande peut être saisie en mode d'exécution privilégié ainsi qu'en mode de configuration et que la commande effectue des actions différentes dans chaque mode, vous pouvez définir le niveau de privilège pour ces modes séparément :
  - **enable** : spécifie le mode EXEC de l'utilisateur et le mode d'exécution privilégié.
  - **configure** : spécifie le mode de configuration, accessible à l'aide de la commande **configure terminal**.
- **command** *command* : la commande que vous configurez. Vous pouvez uniquement configurer le niveau de privilège de la commande *principale*. Par exemple, vous pouvez configurer le niveau de toutes les commandes **aaa**, mais pas le niveau des commandes **aaa authentication** et **aaa authorization** séparément.

Étape 2 (Facultatif) Activez les utilisateurs AAA pour l'autorisation de commande. Sans cette commande, l'ASA ne prend en charge que les niveaux de privilège des utilisateurs de base de données locaux et définit par défaut tous les autres types d'utilisateurs au niveau 15.

aaa authorization exec authentication-server [auto-enable]

Exemple :

```
ciscoasa(config)# aaa authorization exec authentication-server
```

Cette commande active également l'autorisation de gestion. Consultez Contrôler l'interface de ligne de commande et l'accès ASDM avec l'autorisation de gestion, à la page 28.

Étape 3 Activez l'utilisation des niveaux de privilège de commande locaux :

aaa authorization command LOCAL

Exemple :

```
ciscoasa(config)# aaa authorization command LOCAL
```

Lorsque vous définissez des niveaux de privilège de commande, l'autorisation de commande n'a pas lieu, sauf si vous configurez l'autorisation de commande avec cette commande.

Exemples

La commande **filter** a les formes suivantes :

- **filter** (représenté par l'option **configure**)
- **show running-config filter**

- **clear configure filter**

Vous pouvez définir le niveau de privilège séparément pour chaque formulaire ou définir le même niveau de privilège pour tous les formulaires en omettant cette option. L'exemple suivant montre comment définir chaque formulaire séparément :

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

Sinon, l'exemple suivant montre comment définir toutes les commandes de filtre au même niveau :

```
ciscoasa(config)# privilege level 5 command filter
```

La commande **show privilege** sépare les formulaires dans l'affichage.

L'exemple suivant montre l'utilisation du mot clé **mode**. La commande **enable** doit être saisie à partir du mode EXEC de l'utilisateur, tandis que la commande **enable password**, qui est accessible en mode de configuration, requiert le niveau de privilège le plus élevé :

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

L'exemple suivant montre une commande supplémentaire, la commande **configure**, qui utilise le mot clé **mode** :

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

Remarque Cette dernière ligne est pour la commande **configure terminal**.

Configurer les commandes sur le serveur TACACS+

Vous pouvez configurer des commandes sur un serveur TACACS+ Cisco Secure Access Control Server (ACS) en tant que composant de profil partagé, pour un groupe ou pour des utilisateurs individuels. Pour les serveurs TACACS+ tiers, consultez la documentation de votre serveur pour en savoir plus sur la prise en charge des autorisations de commandes.

Consultez les lignes directrices suivantes pour la configuration des commandes dans Cisco Secure ACS version 3.1; la plupart de ces lignes directrices s'appliquent également aux serveurs tiers :

- L'ASA envoie les commandes à autoriser en tant que commandes shell; veuillez donc configurer les commandes sur le serveur TACACS+ en tant que commandes shell.

Remarque Cisco Secure ACS peut inclure un type de commande appelé « pix-shell ». N'utilisez pas ce type pour l'autorisation de commande ASA.

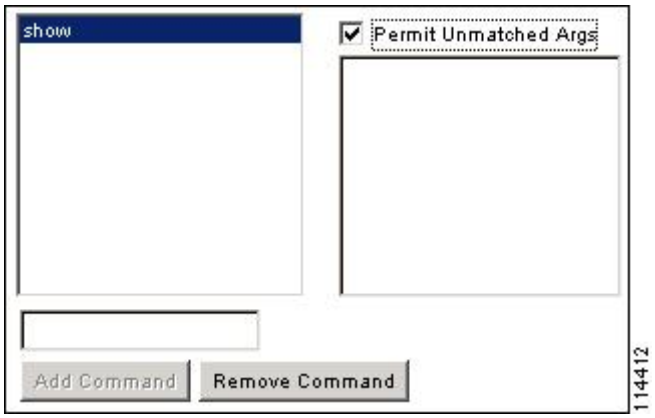
- Le premier mot de la commande est considéré comme la commande principale. Tous les mots supplémentaires sont considérés comme des arguments, qui doivent être précédés de **permit** ou **deny**.

  Par exemple, pour autoriser la commande **show running-configuration aaa-server**, ajoutez **show running-configuration** dans le champ de la commande et saisissez **permit aaa-server** dans le champ des arguments.

- Vous pouvez autoriser tous les arguments d'une commande que vous ne refusez pas explicitement en cochant la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance).

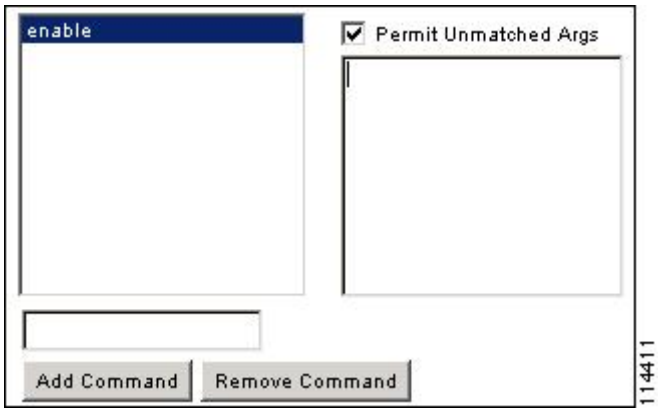
  Par exemple, vous pouvez configurer uniquement la commande **show**. Toutes les commandes **show** sont autorisées. Nous vous conseillons d'utiliser cette méthode pour que vous n'ayez pas à anticiper chaque variante d'une commande, y compris les abréviations et un point d'interrogation, qui indique l'utilisation de l'interface de ligne de commande (voir la figure suivante).

Illustration 1 : Autoriser toutes les commandes associées



- Pour les commandes composées d'un seul mot, vous *devez* autoriser des arguments sans correspondance, même s'il n'y a aucun argument pour la commande, par exemple **enable** ou **help** (voir la figure suivante).

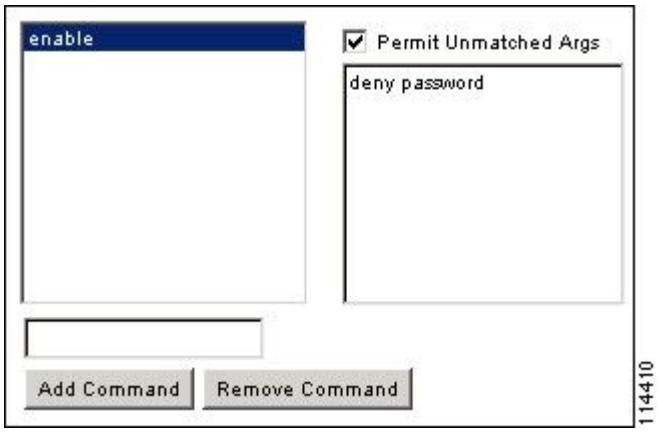
Illustration 2 : Autorisation des commandes à un seul mot



- Pour interdire certains arguments, entrez les arguments précédés de **deny**.

  Par exemple, pour autoriser **enable**, mais pas **enable password**, saisissez **enable** dans le champ des commandes et **deny password** dans le champ des arguments. Assurez-vous de cocher la case **Permit Unmatched Args** (Autoriser les arguments sans correspondance) pour que **enable** soit toujours autorisé (voir la figure suivante).

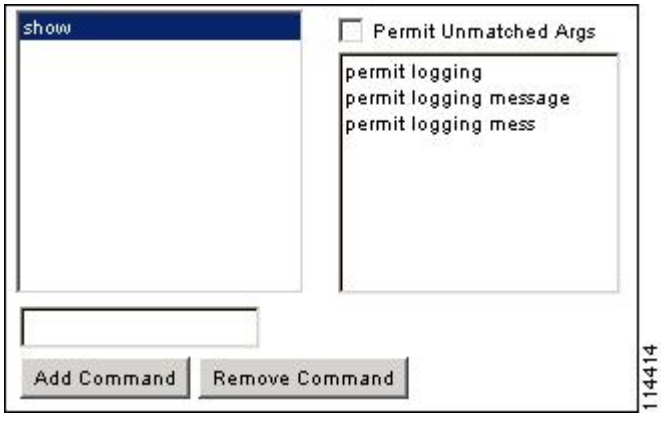
  Illustration 3 : Interdire les arguments



- Lorsque vous abrégez une commande dans la ligne de commande, l'ASA développe le préfixe et la commande principale en texte intégral, mais envoie des arguments supplémentaires au serveur TACACS+ au fur et à mesure que vous les saisissez.

  Par exemple, si vous saisissez **sh log**, l'ASA envoie la commande complète au serveur TACACS+, **show logging**. Cependant, si vous saisissez **sh log mess**, l'ASA envoie **show logging mess** au serveur TACACS+, et non la commande étendue **show logging message**. Vous pouvez configurer plusieurs orthographes du même argument afin d'anticiper les abréviations (voir la figure suivante).

  Illustration 4 : Spécifier les abréviations



- Nous vous conseillons d'autoriser les commandes de base suivantes pour tous les utilisateurs :
  - **show checksum**
  - **show curpriv**
  - **enable**

- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

Configurer l'autorisation de commande TACACS+

Si vous activez l'autorisation de commande TACACS+ et qu'un utilisateur saisit une commande au niveau de l'interface de ligne de commande, l'ASA envoie la commande et le nom d'utilisateur au serveur TACACS+ pour déterminer si la commande est autorisée.

Avant d'activer l'autorisation de commande TACACS+, assurez-vous d'être connecté à l'ASA en tant qu'utilisateur défini sur le serveur TACACS+ et de disposer de l'autorisation de commande nécessaire pour continuer à configurer l'ASA. Par exemple, vous devez vous connecter en tant qu'utilisateur admin avec toutes les commandes autorisées. Sinon, vous pourriez vous retrouver involontairement bloqué.

N'enregistrez pas votre configuration avant d'être sûr qu'elle fonctionne comme vous le souhaitez. Si vous êtes bloqué par erreur, vous pouvez généralement récupérer l'accès en redémarrant l'ASA.

Assurez-vous que votre système TACACS+ est complètement stable et fiable. Le niveau de fiabilité nécessaire exige généralement que vous ayez un système de serveurs TACACS+ entièrement redondant et une connectivité entièrement redondante à l'ASA. Par exemple, dans votre ensemble de serveurs TACACS+, incluez un serveur connecté à l'interface 1 et un autre à l'interface 2. Vous pouvez également configurer l'autorisation de commande locale comme méthode de secours si le serveur TACACS+ n'est pas disponible.

Pour configurer l'autorisation de commande à l'aide d'un serveur TACACS+, procédez comme suit :

Procédure

Entrez la commande suivante :

aaa authorization command *tacacs+_server_group* [**LOCAL**]

Exemple :

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

Vous pouvez configurer l'ASA pour utiliser la base de données locale comme méthode de secours si le serveur TACACS+ n'est pas disponible. Pour activer le basculement, précisez le nom du groupe de serveurs suivi de **LOCAL** (**LOCAL** est sensible à la casse). Nous vous conseillons d'utiliser le même nom d'utilisateur et le même mot de passe dans la base de données locale que sur le serveur TACACS+, car l'invite ASA n'indique

pas quelle méthode est utilisée. Assurez-vous de configurer les utilisateurs dans la base de données locale et les niveaux de privilège de commande.

Configurer une politique de mot de passe pour les utilisateurs de base de données locale

Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe telles qu'une longueur minimum et le nombre minimum de modifications de caractères.

La politique de mot de passe s'applique uniquement aux utilisateurs administratifs qui utilisent la base de données locale et non aux autres types de trafic qui peuvent utiliser la base de données locale, comme le VPN ou l'AAA pour l'accès au réseau, et non aux utilisateurs authentifiés par un serveur AAA.

Après avoir configuré la politique de mot de passe, lorsque vous modifiez un mot de passe (le vôtre ou celui d'un autre utilisateur), la politique de mot de passe s'applique au nouveau mot de passe. Tous les mots de passe existants sont conservés. La nouvelle politique s'applique à la modification du mot de passe avec la commande **username** et la commande **change-password**.

Avant de commencer

- Configurez l'authentification AAA pour l'accès de l'interface de ligne de commande ou ASDM à l'aide de la base de données locale.
- Spécifiez les noms d'utilisateurs dans la base de données locale.

Procédure

Étape 1 (Facultatif) Définissez l'intervalle en jours après lequel les mots de passe expirent pour les utilisateurs distants.

password-policy lifetime *days*

Exemple :

```
ciscoasa(config)# password-policy lifetime 180
```

Remarque
Les utilisateurs au niveau du port de console ne sont jamais verrouillés en raison de l'expiration du mot de passe.

Les valeurs valides sont comprises entre 0 et 65536 jours. La valeur par défaut est 0 jour, une valeur indiquant que les mots de passe n'expireront jamais.

Sept jours avant l'expiration du mot de passe, un message d'avertissement s'affiche. À l'expiration du mot de passe, l'accès au système est refusé aux utilisateurs distants. Pour y accéder après l'expiration, effectuez l'une des opérations suivantes :

- Demandez à un autre administrateur de modifier votre mot de passe à l'aide de la commande **username**.

- Connectez-vous au port de console physique pour modifier votre mot de passe.

Étape 2 (Facultatif) Définissez le nombre minimum de caractères que vous devez modifier entre l'ancien et le nouveau mot de passe.

password-policy minimum-changes *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-changes 2
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0.

La correspondance des caractères est indépendante de la position, ce qui signifie que les caractères du nouveau mot de passe ne sont considérés comme modifiés que s'ils n'apparaissent nulle part dans le mot de passe actuel.

Étape 3 (Facultatif) Définissez la longueur minimum des mots de passe.

password-policy minimum-length *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-length 8
```

Les valeurs valides sont comprises entre 3 et 64 caractères. Nous conseillons un mot de passe d'une longueur minimum de 8 caractères.

Étape 4 (Facultatif) Définissez le nombre minimum de caractères majuscules que les mots de passe doivent contenir.

password-policy minimum-uppercase *value*

Exemple :

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 5 (Facultatif) Définissez le nombre minimum de caractères minuscules que les mots de passe doivent contenir.

password-policy minimum-lowercase *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 6 (Facultatif) Définissez le nombre minimum de caractères numériques que les mots de passe doivent contenir.

password-policy minimum-numeric *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-numeric 1
```

Les valeurs valides sont comprises entre 0 et 64 caractères. La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 7 (Facultatif) Définissez le nombre minimum de caractères spéciaux que les mots de passe doivent contenir.

password-policy minimum-special *value*

Exemple :

```
ciscoasa(config)# password-policy minimum-special 2
```

Les valeurs valides sont comprises entre 0 et 64 caractères. Les caractères spéciaux sont les suivants : !, @, #, $, %, ^, &, *, « (» et «) ». La valeur par défaut est 0, ce qui signifie qu'il n'y a pas de minimum.

Étape 8 Interdire la réutilisation d'un mot de passe :

password-policy reuse-interval *value*

Exemple :

```
ciscoasa(config)# password-policy reuse-interval 5
```

Vous pouvez interdire la réutilisation d'un mot de passe correspondant aux mots de passe utilisés précédemment, entre 2 et 7 mots de passe précédents. Les mots de passe précédents sont stockés dans la configuration sous chaque nom d'utilisateur sous forme chiffrée à l'aide de la commande **password-history**; cette commande n'est pas configurable par l'utilisateur.

Étape 9 Interdire un mot de passe correspondant à un nom d'utilisateur :

password-policy username-check

Étape 10 (Facultatif) Définissez si les utilisateurs doivent modifier leur mot de passe à l'aide de la commande **change-password**, au lieu de permettre aux utilisateurs de modifier leur mot de passe avec la commande **username**.

password-policy authenticate enable

Exemple :

```
ciscoasa(config)# password-policy authenticate enable
```

Le paramètre par défaut est désactivé : un utilisateur peut utiliser l'une ou l'autre des méthodes pour modifier son mot de passe.

Si vous activez cette fonctionnalité et essayez de modifier votre mot de passe à l'aide de la commande **username**, le message d'erreur suivant s'affiche :

```
ERROR: Changing your own password is prohibited
```

Vous ne pouvez pas non plus supprimer votre propre compte avec la commande **clear configure username**. Si vous essayez, le message d'erreur suivant s'affiche :

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

Changer votre mot de passe

Si vous configurez une durée de validité du mot de passe dans la politique de mot de passe, vous devez changer votre mot de passe lorsque l'ancien mot de passe expire. Cette méthode de modification du mot de passe est requise si vous activez l'authentification par politique de mot de passe. Si l'authentification par politique de mot de passe n'est pas activée, vous pouvez utiliser cette méthode ou vous pouvez modifier directement votre compte d'utilisateur.

Pour modifier votre mot de passe d'utilisateur, procédez comme suit :

Procédure

Entrez la commande suivante :

change-password [**old-password** *old_password* [**new-password** *new_password*]]

Exemple :

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

Si vous ne saisissez pas l'ancien et le nouveau mot de passe dans la commande, l'ASA vous invite à les saisir.

Activer et afficher l'historique de connexion

Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours.

Avant de commencer

- L'historique de connexion n'est enregistré que par unité; dans les environnements de basculement et de mise en grappe, chaque unité conserve uniquement son propre historique de connexion.
- Les données de l'historique de connexion ne sont pas conservées pendant les rechargements.
- Cette fonctionnalité s'applique aux noms d'utilisateur dans la base de données locale ou à partir d'un serveur AAA lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion de l'interface de ligne de commande (SSH, Telnet, console série). Les connexions à ASDM ne sont pas enregistrées dans l'historique.

Procédure

Étape 1 Définissez la durée de l'historique de connexion :

aaa authentication login-history duration *days*

Exemple :

```
ciscoasa(config)# aaa authentication login-history duration 365
```

Vous pouvez définir les *jours* entre 1 et 365. La valeur par défaut est 90. Pour désactiver l'historique de connexion, saisissez **no aaa authentication login-history**.

Lorsqu'un utilisateur se connecte, il voit son propre historique de connexion, comme cet exemple SSH :

```
cugel@10.86.194.108's password:
The privilege level for user cugel is 15.  The privilege level at the previous login was
2.
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

Étape 2 Affichez l'historique de connexion :

show aaa login-history [**user** *name*]

Exemple :

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

Configurer la traçabilité de l'accès de gestion

Vous pouvez envoyer des messages de traçabilité au serveur de comptabilité TACACS+ lorsque vous saisissez une commande autre que les commandes **show** au niveau de l'interface de ligne de commande. Vous pouvez configurer la comptabilisation lorsque les utilisateurs se connectent, lorsqu'ils saisissez la commande **enable** ou lorsqu'ils émettent des commandes.

Pour la traçabilité des commandes, vous pouvez uniquement utiliser des serveurs TACACS+.

Pour configurer l'accès de gestion et activer la traçabilité des commandes, procédez comme suit :

Procédure

Étape 1 Entrez la commande suivante :

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

Exemple :

```
ciscoasa(config)# aaa accounting telnet console group_1
```

Les protocoles de groupe de serveurs valides sont RADIUS et TACACS+.

Étape 2 Activez la traçabilité des commandes. Seuls les serveurs TACACS+ prennent en charge la traçabilité des commandes.

aaa accounting command [**privilege** *level*] *server-tag*

Exemple :

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

La paire mot clé-argument **privilege** *level* est le niveau de privilège minimum et l'argument *server-tag* est le nom du groupe de serveurs TACACS+ auquel l'ASA doit envoyer des messages de traçabilité des commandes.

Récupérer d'un verrouillage

Dans certaines circonstances, lorsque vous activez l'autorisation de commande ou l'authentification de l'interface de ligne de commande, vous pouvez être verrouillé hors de l'interface de ligne de commande de l'ASA. Vous pouvez généralement récupérer l'accès en redémarrant l'ASA. Cependant, si vous avez déjà enregistré votre configuration, vous pourriez être verrouillé.

Le tableau suivant répertorie les conditions de verrouillage courantes et la façon dont vous pouvez y remédier.

Tableau 1 : Scénarios de verrouillage de l'authentification de l'interface de ligne de commande et de l'autorisation de commande

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Authentification de l'interface de ligne de commande locale	Aucun utilisateur n'a été configuré dans la base de données locale.	Si vous n'avez aucun utilisateur dans la base de données locale, vous ne pouvez pas vous connecter ni ajouter d'utilisateurs.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et ajouter un utilisateur.

Fonctionnalités	Condition de verrouillage	Description	Solution de contournement : mode unique	Solution de contournement : mode multiple
Autorisation de commande TACACS+ Authentification de l'interface de ligne de commande TACACS+ Authentification de l'interface de ligne de commande RADIUS	Le serveur est en panne ou inaccessible et vous n'avez pas configuré la méthode de secours.	Si le serveur est inaccessible, vous ne pouvez pas vous connecter ni saisir de commandes.	1. Connectez-vous et réinitialisez les mots de passe et les commandes AAA. 2. Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.	1. Si le serveur est inaccessible en raison d'une configuration de réseau incorrecte sur l'ASA, connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et reconfigurer vos paramètres réseau. 2. Configurez la base de données locale comme méthode de secours afin de ne pas être verrouillé lorsque le serveur est en panne.
Autorisation de commande TACACS+	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants ou en tant qu'utilisateur qui n'existe pas.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Corrigez le compte d'utilisateur du serveur TACACS+. Si vous n'avez pas accès au serveur TACACS+ et que vous devez configurer l'ASA immédiatement, connectez-vous à la partition de maintenance et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et terminer les modifications de configuration. Vous pouvez également désactiver l'autorisation de commande jusqu'à ce que vous corrigiez la configuration TACACS+.
Autorisation de commande locale	Vous êtes connecté en tant qu'utilisateur sans privilèges suffisants.	Vous activez l'autorisation de commande, mais vous constatez ensuite que l'utilisateur ne peut plus saisir de commandes.	Connectez-vous et réinitialisez les mots de passe et les commandes **aaa**.	Connectez-vous à l'ASA à partir du commutateur. À partir de l'espace d'exécution du système, vous pouvez modifier le contexte et changer le niveau d'utilisateur.

Accès au moniteur

Consultez les commandes suivantes pour surveiller l'accès au périphérique :

- **show running-config all privilege all**

  Cette commande affiche les niveaux de privilège de toutes les commandes.

Pour la commande **show running-config all privilege all**, l'ASA affiche l'affectation actuelle de chaque commande de l'interface de ligne de commande à un niveau de privilège. Voici un exemple de sortie de cette commande :

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** *level*

  Cette commande affiche les commandes pour un niveau de privilège précis. L'argument level est un nombre entier compris entre 0 et 15.

  L'exemple suivant montre les affectations de commandes pour le niveau de privilège 10 :

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** *command*

  Cette commande affiche le niveau de privilège d'une commande en particulier.

  L'exemple suivant montre les affectations de commandes pour la commande **access-list** :

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  Cette commande affiche l'utilisateur actuellement connecté.

  Voici un exemple de sortie de la commande **show curpriv** :

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  Le tableau suivant décrit la sortie de la commande **show curpriv**.

Tableau 2 : Description de la sortie de la commande show curpriv

Champ	Description
Username	Nom d'utilisateur. Si vous êtes connecté en tant qu'utilisateur par défaut, le nom est enable_1 (utilisateur EXEC) ou enable_15 (EXEC privilégié).
Niveau de privilège actuel	Les niveaux vont de 0 à 15. À moins que vous ne configuriez l'autorisation de commande locale et n'affectiez des commandes à des niveaux de privilège intermédiaires, les niveaux 0 et 15 sont les seuls niveaux utilisés.
Modes actuels	Les modes d'accès disponibles sont les suivants : • P_UNPR : mode EXEC de l'utilisateur (niveaux 0 et 1) • P_PRIV : mode d'exécution privilégié (niveaux 2 à 15) • P_CONF : mode de configuration

- **show quota management-session** [**ssh** | **telnet** | **http** | **username** *user*]

  Cette commande affiche les sessions actuelles en cours d'utilisation.

  Voici un exemple de sortie de la commande **show quota management-session** :

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                              SSH                      cisco
2                              TELNET                   cisco
1                              SSH                      cisco1
```

- **show aaa login-history** [**user** *name*]

  Cette commande affiche l'historique de connexion par utilisateur.

  Voici un exemple de sortie de la commande **show aaa login-history**.

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                   14
Privilege level changed from 11 to 14 at:          14:07:30 UTC Aug 21 2018
```

Historique de l'accès de gestion

Tableau 3 : Historique de l'accès de gestion

Nom de la caractéristique	Versions de plateforme	Description
Pile CiscoSSH maintenant par défaut	9.19(1)	La pile Cisco SSH est maintenant utilisée par défaut. Commandes nouvelles ou modifiées : **ssh stack ciscossh**
Prise en charge de l'interface de boucle avec retour pour SSH et Telnet	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour les fonctionnalités suivantes : • SSH • Telnet Commandes nouvelles/modifiées : **interface loopback**, **ssh**, **telnet**
Pile CiscoSSH	9.17(1)	L'ASA utilise une pile SSH propriétaire pour les connexions SSH. Vous pouvez maintenant choisir d'utiliser à la place la pile CiscoSSH, qui est basée sur OpenSSH. La pile par défaut continue d'être la pile ASA. Cisco SSH prend en charge : • Conformité FIPS • Mises à jour régulières, y compris les mises à jour de Cisco et de la communauté de code source libre. Notez que la pile CiscoSSH ne prend pas en charge : • SSH vers une interface différente sur VPN (accès de gestion) • Paire de clés EdDSA • Paire de clés RSA en mode FIPS Si vous avez besoin de ces fonctionnalités, vous devez continuer à utiliser la pile SSH ASA. Il y a une petite modification de la fonctionnalité SCP avec la pile CiscoSSH : pour utiliser la commande **copy** de l'ASA pour copier un fichier vers ou à partir d'un serveur SCP, vous devez activer l'accès SSH sur l'ASA pour le sous-réseau/hôte du serveur SCP à l'aide de la commande **ssh**. Commandes nouvelles ou modifiées : **ssh stack ciscossh**

Nom de la caractéristique	Versions de plateforme	Description
Modifications du verrouillage de l'utilisateur local	9.17(1)	L'ASA peut verrouiller les utilisateurs locaux après un nombre configurable de tentatives de connexion échouées. Cette fonctionnalité ne s'applique pas aux utilisateurs ayant le niveau de privilège 15. De plus, un utilisateur serait verrouillé indéfiniment jusqu'à ce qu'un administrateur déverrouille son compte. Désormais, les utilisateurs seront déverrouillés après 10 minutes, à moins qu'un administrateur n'utilise la commande **clear aaa local user lockout** avant. Les utilisateurs ayant le niveau de privilège 15 sont également concernés par le paramètre de verrouillage. Commandes nouvelles ou modifiées : **aaa local authentication attempts max-fail** , **show aaa local user**
Invite de modification du mot de passe SSH et Telnet	9.17(1)	La première fois qu'un utilisateur local se connecte à l'ASA à l'aide de SSH ou de Telnet, il est invité à changer de mot de passe. Il sera également invité à se connecter pour la première fois après qu'un administrateur aura modifié son mot de passe. Si l'ASA se recharge, les utilisateurs ne seront pas invités, même s'il s'agit de leur première connexion. Notez que tout service qui utilise la base de données des utilisateurs locale, comme VPN, devra également utiliser le nouveau mot de passe s'il a été modifié lors d'une connexion SSH ou Telnet. Commandes nouvelles ou modifiées : **show aaa local user**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de la sécurité SSH	9.16(1)	SSH prend désormais en charge les améliorations de sécurité suivantes : • Format de clé d'hôte : **crypto key generate** {**eddsa** | **ecdsa**}. En plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EdDSA et ECDSA. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EdDSA, ECDSAA, puis RSA. Si vous configurez explicitement l'ASA pour utiliser la clé RSA avec la commande **ssh key-exchange hostkey rsa**, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge de RSA sera supprimée dans une version ultérieure. • Algorithmes d'échange de clés : **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • Algorithmes de chiffrement : **ssh cipher encryption chacha20-poly1305@openssh.com** • La version 1 de SSH n'est plus prise en charge. La commande **ssh version** est supprimée. Commandes nouvelles ou modifiées : **crypto key generate eddsa**, **crypto key zeroize eddsa**, **show crypto key mypubkey**, **ssh cipher encryption chacha20-poly1305@openssh.com**, **ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}, **ssh key-exchange hostkey**, **ssh version**
Accès de gestion pour SNMP	9.14(2)	Lors de la configuration de l'accès de gestion sur un tunnel VPN, incluez l'adresse IP de l'interface externe dans la liste d'accès de la carte cryptographique dans le cadre de la configuration du VPN pour sécuriser l'interrogation SNMP sur un VPN de site à site.
Paramètre de délai d'inactivité HTTPS	9.14(1)	Vous pouvez maintenant définir le délai d'inactivité pour toutes les connexions HTTPS à l'ASA, y compris ASDM, WebVPN et d'autres clients. Auparavant, avec la commande **http server idle-timeout**, vous pouviez uniquement définir le délai d'inactivité d'ASDM. Si vous définissez les deux délais, la nouvelle commande prévaut. Commandes nouvelles ou modifiées : **http connection idle-timeout**
Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la plus basse) pour les listes prédéfinies	9.13(1)	Le chiffrement SSH est désormais répertorié (de la sécurité la plus haute à la sécurité la plus basse) pour les listes prédéfinies (comme moyen ou élevé). Dans les versions précédentes, il était répertorié du niveau le plus bas au plus élevé, ce qui signifie qu'un chiffrement à faible sécurité serait proposé avant un chiffrement à sécurité élevée. Commandes nouvelles ou modifiées : **ssh cipher encryption**

Nom de la caractéristique	Versions de plateforme	Description
La définition du mode d'échange de clés SSH est limitée au contexte d'administration	9.12(2)	Vous devez définir l'échange de clés SSH dans le contexte d'administration; ce paramètre est hérité par tous les autres contextes. Commandes nouvelles ou modifiées : **ssh key-exchange**
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 caractères ou plus. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Commandes nouvelles ou modifiées : **enable password**
Limitation configurable des sessions d'administration	9.12(1)	Vous pouvez configurer le nombre maximum de sessions administratives agrégées, par utilisateur et par protocole. Auparavant, vous pouviez configurer uniquement le nombre agrégé de sessions. Cette fonctionnalité n'influe pas sur les sessions de console. Notez qu'en mode de contexte multiple, vous ne pouvez pas configurer le nombre de sessions HTTPS, où le maximum est fixé à 5 sessions. La commande **quota management-session** n'est également plus acceptée dans la configuration système et est plutôt disponible dans la configuration du contexte. Le nombre maximum de sessions agrégées est désormais de 15; si vous avez configuré 0 (illimité) ou 16+, lors de la mise à niveau, la valeur passe à 15. Commandes nouvelles/modifiées : **quota management-session**, **show quota management-session**
Notifications pour les modifications du niveau de privilège d'administration	9.12(1)	Lorsque vous vous authentifiez pour activer l'accès (**aaa authentication enable console**) ou autorisez directement l'accès EXEC privilégié (**aaa authorization exec auto-enable**), l'ASA informe désormais les utilisateurs si le niveau d'accès qui leur a été attribué a changé depuis leur dernière connexion. Commandes nouvelles ou modifiées : **show aaa login-history**

Nom de la caractéristique	Versions de plateforme	Description
Sécurité SSH renforcée	9.12(1)	Consultez les améliorations de sécurité SSH suivantes : • Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Ce paramètre est désormais la valeur par défaut. L'ancienne valeur par défaut était le groupe 1 SHA1. • Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha2-256 uniquement). L'ancienne valeur par défaut était l'ensemble moyen. Commandes nouvelles ou modifiées : **ssh cipher integrity** , **ssh key-exchange group dh-group14-sha256**
Autoriser les clients HTTPS non basés sur le navigateur à accéder à l'ASA	9.12(1)	Vous pouvez autoriser les clients HTTPS non basés sur le navigateur à accéder aux services HTTPS sur l'ASA. Par défaut, ASDM, CSM et l'API REST sont autorisés. Commandes nouvelles ou modifiées : **http server basic-auth-client**
La paire de clés RSA prend en charge les clés de 3 072 bits	9.9(2)	Vous pouvez maintenant définir la taille du module à 3 072. Commande nouvelle ou modifiée : **crypto key generate rsa modulus**
Accès de gestion du VPN sur les interfaces virtuelles pontées (BVI)	9.9(2)	Vous pouvez maintenant activer des services de gestion, tels que **telnet**, **http** et **ssh**, sur une BVI si le paramètre **management-access** du VPN a été activé sur cette BVI. Pour l'accès de gestion non VPN, vous devez continuer à configurer ces services sur les interfaces membres du groupe de ponts. Commandes nouvelles ou modifiées : **https**, **telnet**, **ssh**, **management-access**
La version 1 de SSH est obsolète	9.9(1)	La version 1 de SSH est obsolète et sera supprimée dans une version ultérieure. Le paramètre par défaut est passé de SSH v1 et v2 à SSH v2. Commandes nouvelles ou modifiées : **ssh version**

Nom de la caractéristique	Versions de plateforme	Description
Authentification distincte pour les utilisateurs disposant d'une authentification par clé publique SSH et les utilisateurs disposant de mots de passe	9.6(3)/9.8(1)	Dans les versions antérieures à 9.6(2), vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer explicitement l'authentification SSH AAA avec la base de données des utilisateurs locale (**aaa authentication ssh console LOCAL**). Dans 9.6(2), l'ASA vous a demandé d'activer explicitement l'authentification SSH AAA. Dans cette version, vous n'avez plus à activer explicitement l'authentification SSH AAA; lorsque vous configurez la commande **ssh authentication** pour un utilisateur, l'authentification locale est activée par défaut pour les utilisateurs avec ce type d'authentification. De plus, lorsque vous configurez explicitement l'authentification SSH AAA, cette configuration s'applique uniquement aux noms d'utilisateur avec *mots de passe*, et vous pouvez utiliser n'importe quel type de serveur AAA (**aaa authentication ssh console radius_1**, par exemple). Par exemple, certains utilisateurs peuvent utiliser l'authentification par clé publique à l'aide de la base de données locale et d'autres utilisateurs peuvent utiliser des mots de passe avec RADIUS. Nous n'avons pas modifié de commandes.
Historique de connexion	9.8(1)	Par défaut, l'historique de connexion est enregistré pendant 90 jours. Vous pouvez désactiver cette fonctionnalité ou modifier la durée, jusqu'à 365 jours. Cette fonctionnalité s'applique uniquement aux noms d'utilisateur dans la base de données locale lorsque vous activez l'authentification AAA locale pour une ou plusieurs des méthodes de gestion (SSH, ASDM, Telnet, etc.). Nous avons introduit les commandes suivantes : **aaa authentication login-history, show aaa login-history**
Application de la politique de mot de passe pour interdire la réutilisation des mots de passe et l'utilisation d'un mot de passe correspondant à un nom d'utilisateur	9.8(1)	Vous pouvez désormais interdire la réutilisation des mots de passe précédents pour un maximum de 7 générations, et vous pouvez également interdire l'utilisation d'un mot de passe correspondant à un nom d'utilisateur. Nous avons introduit les commandes suivantes : **password-history, password-policy reuse-interval, password-policy username-check**
Mode du serveur SSL ASA correspondant à ASDM	9.6(2)	Pour un utilisateur ASDM qui s'authentifie avec un certificat, vous pouvez désormais exiger que le certificat corresponde à une carte de certificat. Nous avons modifié la commande suivante : **http authentication-certificate match**

Nom de la caractéristique	Versions de plateforme	Description
Améliorations de l'authentification par clé publique SSH	9.6(2)	Dans les versions antérieures, vous pouviez activer l'authentification par clé publique SSH (**ssh authentication**) sans activer également l'authentification SSH AAA avec la base de données d'utilisateurs locale (**aaa authentication ssh console LOCAL**). La configuration est désormais modifiée de manière à ce que vous deviez explicitement activer l'authentification SSH AAA. Pour empêcher les utilisateurs d'utiliser un mot de passe au lieu de la clé privée, vous pouvez désormais créer un nom d'utilisateur sans mot de passe défini. Nous avons modifié les commandes suivantes : **ssh authentication, username**
Autorisation de gestion ASDM	9.4(1)	Vous pouvez désormais configurer l'autorisation de gestion séparément pour l'accès HTTP par rapport à l'accès Telnet et SSH. Nous avons introduit la commande suivante : **aaa authorization http console**
Nom d'utilisateur ASDM dans la configuration du certificat	9.4(1)	Lorsque vous activez l'authentification par certificat ASDM (**http authentication-certificate**), vous pouvez configurer la façon dont ASDM extrait le nom d'utilisateur du certificat; vous pouvez également activer le préremplissage du nom d'utilisateur à l'invite de connexion. Nous avons introduit la commande suivante : **http username-from-certificate**
Authentification par mot de passe à usage unique améliorée	9.2(1)	Les administrateurs qui disposent de privilèges d'autorisation suffisants peuvent passer en mode d'exécution privilégié en saisissant une seule fois leurs informations d'authentification. L'option **auto-enable** a été ajoutée à la commande **aaa authorization exec**. Nous avons modifié la commande suivante : **aaa authorization exec**.
Prise en charge de la redirection HTTP pour IPV6	9.1(7)/9.6(1)	Lorsque vous activez la redirection HTTP vers HTTPS pour l'accès ASDM ou le SSL VPN sans client, vous pouvez désormais rediriger le trafic envoyé par vers l'adresse IPv6. Nous avons ajouté des fonctionnalités à la commande suivante : **http redirect**

Nom de la caractéristique	Versions de plateforme	Description
Chiffrement SSH et d'intégrité configurables	9.1(7.4), 9.5(3), 9.6(1)	Les utilisateurs peuvent sélectionner des modes de chiffrement lors de la gestion du chiffrement SSH et peuvent configurer le HMAC et le chiffrement pour divers algorithmes d'échange de clés. Vous souhaiterez peut-être modifier les chiffres pour qu'ils soient plus ou moins stricts, selon votre application. Notez que la performance de la copie sécurisée dépend en partie du chiffrement utilisé. Par défaut, l'ASA négocie l'un des algorithmes suivants dans l'ordre : 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. Si le premier algorithme proposé (3des-cbc) est choisi, la performance est beaucoup plus lente qu'un algorithme plus efficace tel que aes128-cbc. Pour modifier les chiffres proposés, utilisez **ssh cipher encryption custom aes128-cbc**, par exemple. Nous avons introduit les commandes suivantes : **ssh cipher encryption, ssh cipher integrity**.
Chiffrement AES-CTR pour SSH	9.1(2)	La mise en œuvre du serveur SSH dans l'ASA prend désormais en charge le chiffrement en mode AES-CTR.
Intervalle de renouvellement SSH amélioré	9.1(2)	Une connexion SSH est renouvelée après 60 minutes de connexion ou 1 Go de trafic de données. Nous avons introduit la commande suivante : **show ssh sessions detail**.
Pour l'ASASM en mode de contexte multiple, prenez en charge l'authentification Telnet et de la console virtuelle à partir du commutateur.	8.5(1)	Bien que la connexion à l'ASASM à partir du commutateur en mode de contexte multiple se connecte à l'espace d'exécution du système, vous pouvez configurer l'authentification dans le contexte d'administration pour régir ces connexions.
Prise en charge de la politique de mot de passe administrateur lors de l'utilisation de la base de données locale	8.4(4.1), 9.1(2)	Lorsque vous configurez l'authentification pour l'accès à l'interface de ligne de commande ou à ASDM à l'aide de la base de données locale, vous pouvez configurer une politique de mot de passe qui oblige un utilisateur à changer de mot de passe après une durée spécifiée et qui exige également des normes de mot de passe telles qu'une longueur minimum et le nombre minimum de modifications de caractères. Nous avons introduit les commandes suivantes : **change-password**, **password-policy lifetime**, **password-policy minimum changes**, **password-policy minimum-length**, **password-policy minimum-lowercase**, **password-policy minimum-uppercase**, **password-policy minimum-numeric**, **password-policy minimum-special**, **password-policy authenticate enable**, **clear configure password-policy**, **show running-config password-policy**.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de l'authentification par clé publique SSH	8.4(4.1), 9.1(2)	Vous pouvez activer l'authentification par clé publique pour les connexions SSH à l'ASA par utilisateur. Vous pouvez spécifier une clé formatée de fichier de clé publique (PKF) ou une clé Base64. La clé PKF peut comporter jusqu'à 4 096 bits. Utilisez le format PKF pour les clés qui sont trop grandes pour la prise en charge ASA du format Base64 (jusqu'à 2 048 bits). Nous avons introduit les commandes suivantes : **ssh authentication**. *Le format de clé PKF est uniquement pris en charge dans la version 9.1(2) et les versions ultérieures.*
Prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH	8.4(4.1), 9.1(2)	La prise en charge du groupe Diffie-Hellman 14 pour l'échange de clés SSH a été ajoutée. Auparavant, seul le groupe 1 était pris en charge. Nous avons introduit la commande suivante : **ssh key-exchange**.
Prise en charge d'un nombre maximum de sessions de gestion	8.4(4.1), 9.1(2)	Vous pouvez définir le nombre maximum de sessions ASDM, SSH et Telnet simultanées. Nous avons ajouté les commandes suivantes : **quota management-session**, **show running-config quota management-session**, **show quota management-session**.
Sécurité SSH améliorée; le nom d'utilisateur SSH par défaut n'est plus pris en charge.	8.4(2)	À partir de la version 8.4(2), vous ne pouvez plus vous connecter à l'ASA à l'aide de SSH avec le nom d'utilisateur pix ou asa et le mot de passe de connexion. Pour utiliser SSH, vous devez configurer l'authentification AAA à l'aide de la commande **aaa authentication ssh console LOCAL** (interface de ligne de commande) ou Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > AAA Access (Accès AAA) > Authentication (ASDM) (Authentification (ASDM)); puis définissez un utilisateur local en saisissant la commande **username** (interface de ligne de commande) ou en sélectionnant Configuration > Device Management (Gestion des périphériques) > Users/AAA (Utilisateurs/AAA) > User Accounts (ASDM) (Comptes d'utilisateurs (ASDM)). Si vous souhaitez utiliser un serveur AAA pour l'authentification au lieu de la base de données locale, nous vous conseillons de configurer également l'authentification locale comme méthode de sauvegarde.

Nom de la caractéristique	Versions de plateforme	Description
Accès de gestion	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **show running-config all privilege all**, **show running-config privilege level**, **show running-config privilege command**, **telnet**, **telnet timeout**, **ssh**, **ssh timeout**, **http**, **http server enable**, **asdm image disk, banner**, **console timeout**, **icmp**, **ipv6 icmp**, **management access**, **aaa authentication console**, **aaa authentication enable console**, **aaa authentication telnet | ssh console**, **service-type**, **login**, **privilege**, **aaa authentication exec authentication-server**, **aaa authentication command LOCAL**, **aaa accounting serial | telnet | ssh | enable console**, **show curpriv**, **aaa accounting command privilege**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.