PIX 6.2 : Exemple de configuration des commandes d'authentification et d'autorisation

Contenu

Introduction

Les fonctions d'autorisation de commande et d'extension de l'authentification locale de PIX ont été introduites dans la version 6.2. Ce document montre comment les configurer sur PIX. Les fonctions d'authentification offertes précédemment sont toujours disponibles, mais ne sont pas mentionnées dans ce document (par exemple, Secure Shell (SSH), la connexion d'un client IPsec depuis un PC et ainsi de suite). Les commandes peuvent être contrôlées localement sur PIX ou à distance par TACACS+. L'autorisation de commande RADIUS n'est pas prise en charge; il s'agit d'une limite du protocole RADIUS.

L'autorisation de commande locale est effectuée en attribuant des niveaux de privilège aux commandes et aux utilisateurs.

L'autorisation des commandes à distance est effectuée via un serveur d'authentification, d'autorisation et de comptabilité TACACS+ (AAA). Plusieurs serveurs AAA peuvent être définis en cas d'inaccessibilité.

L'authentification fonctionne également avec les connexions IPSec et SSH précédemment configurées. L'authentification SSH nécessite que vous émettiez cette commande :

```
aaa authentication ssh console <LOCAL | server_tag>
```

Remarque : Si vous utilisez un groupe de serveurs TACACS+ ou RADIUS pour l'authentification, vous pouvez configurer le PIX pour qu'il utilise la base de données locale comme **méthode FALLBACK** si le serveur AAA n'est pas disponible.

Exemple

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```

Vous pouvez également utiliser la base de données locale comme principale méthode d'authentification (sans secours) si vous entrez LOCAL seul.

Par exemple, émettez cette commande afin de définir un compte d'utilisateur dans la base de données locale et d'exécuter l'authentification locale pour une connexion SSH :

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

Référez-vous à Comment exécuter l'authentification et l'activation sur le pare-feu Cisco Secure PIX Firewall (5.2 à 6.2) pour plus d'informations sur la création d'un accès authentifié AAA à un pare-feu PIX qui exécute le logiciel PIX version 5.2 à 6.2 et pour plus d'informations sur l'activation de l'authentification, de la syslogging et de l'accès lorsque le serveur AAA est arrêté.

Reportez-vous à la section PIX/ASA : Exemple de configuration du serveur Cut-through Proxy pour l'accès au réseau à l'aide de TACACS+ et RADIUS pour plus d'informations sur la création d'un accès AAA authentifié (Cut-through Proxy) à un pare-feu PIX qui exécute le logiciel PIX versions 6.3 et ultérieures.

Si la configuration est effectuée correctement, vous ne devez pas être verrouillé hors du PIX. Si la configuration n'est pas enregistrée, le redémarrage du PIX devrait revenir à son état de préconfiguration. Si le PIX n'est pas accessible en raison d'une mauvaise configuration, référez-vous à Procédure de récupération de mot de passe et de configuration AAA pour PIX.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Logiciel PIX version 6.2
- Cisco Secure ACS pour Windows version 3.0 (ACS)
- Cisco Secure ACS pour UNIX (CSUnix) version 2.3.6

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Test avant l'ajout de l'authentification/autorisation

Avant de mettre en oeuvre les nouvelles fonctionnalités d'authentification/autorisation 6.2, assurez-vous que vous êtes actuellement en mesure d'accéder au PIX à l'aide des commandes suivantes :

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0
!--- Telnet password. passwd <password>
!--- Enable password. enable password <password>
```

Présentation des paramètres de privilège

La plupart des commandes du PIX sont au niveau 15, mais quelques-unes sont au niveau 0. Pour afficher les paramètres actuels de toutes les commandes, utilisez cette commande :

```
show privilege all
```

La plupart des commandes sont au niveau 15 par défaut, comme illustré dans cet exemple :

```
privilege configure level 15 command route
```

Quelques commandes se trouvent au niveau 0, comme illustré dans cet exemple :

```
privilege show level 0 command curpriv
```

Le PIX peut fonctionner en mode enable et configure. Certaines commandes, telles que **show logging**, sont disponibles dans les deux modes. Pour définir des privilèges sur ces commandes, vous devez spécifier le mode dans lequel la commande existe, comme illustré dans l'exemple. L'autre option de mode est **enable**. Vous obtenez le `message d'`erreur `logging is a command available in multiple modes`. Si vous ne configurez pas le mode, utilisez la commande **mode [enable|configure]** :

```
privilege show level 5 mode configure command logging
```

Ces exemples traitent de la commande **clock**. Utilisez cette commande pour déterminer les paramètres actuels de la commande **clock** :

```
show privilege command clock
```

La sortie de la commande **show privilege clock** montre que la commande **clock** existe dans les trois formats suivants :

```
!--- Users at level 15 can use the show clock command.

privilege show level 15 command clock
!--- Users at level 15 can use the clear clock command.

Privilege clear level 15 command clock
!--- Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01
2001).

privilege configure level 15 command clock
```

Authentification/Autorisation - Noms d'utilisateurs locaux

Avant de modifier le niveau de privilège de la commande **clock**, accédez au port de console pour configurer un utilisateur administratif et activez l'authentification de connexion LOCAL, comme indiqué dans cet exemple :

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

Le PIX confirme l'ajout de l'utilisateur, comme indiqué dans cet exemple :

```
GOSS(config)# 502101: New user added to local dbase:
      Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

L'utilisateur « poweruser » doit pouvoir établir une connexion Telnet avec le PIX et l'activer avec le mot de passe local PIX enable existant (celui de la commande **enable password <*password*>**).

Vous pouvez ajouter plus de sécurité en ajoutant l'authentification pour l'activation, comme illustré dans cet exemple :

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

Pour cela, l'utilisateur doit entrer le mot de passe pour la connexion et l'activation. Dans cet

exemple, le mot de passe « poweruser » est utilisé pour la connexion et l'activation. L'utilisateur « poweruser » doit pouvoir établir une connexion Telnet avec le PIX et également l'activer avec le mot de passe PIX local.

Si vous voulez que certains utilisateurs ne puissent utiliser que certaines commandes, vous devez configurer un utilisateur avec des privilèges inférieurs, comme illustré dans cet exemple :

```
GOSS(config)# username ordinary password ordinary privilege 9
```

Comme presque toutes vos commandes sont au niveau 15 par défaut, vous devez déplacer certaines commandes vers le niveau 9 pour que les utilisateurs « ordinaires » puissent les émettre. Dans ce cas, vous voulez que votre utilisateur de niveau 9 puisse utiliser la commande **show clock**, mais pas reconfigurer l'horloge, comme illustré dans cet exemple :

```
GOSS(config)# privilege show level 9 command clock
```

Vous avez également besoin que votre utilisateur puisse se déconnecter du PIX (l'utilisateur peut se trouver au niveau 1 ou 9 lorsque vous voulez faire ceci), comme indiqué dans cet exemple :

```
GOSS(config)# privilege configure level 1 command logout
```

Vous devez permettre à l'utilisateur d'utiliser la commande **enable** (l'utilisateur se trouve au niveau 1 lors de cette tentative), comme indiqué dans cet exemple :

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

En déplaçant la commande **disable** vers le niveau 1, tout utilisateur entre les niveaux 2 à 15 peut sortir du mode enable, comme illustré dans cet exemple :

```
GOSS(config)# privilege configure level 1 command disable
```

Si vous établissez une connexion Telnet en tant qu'utilisateur « ordinaire » et activez le même utilisateur (le mot de passe est également « ordinaire »), vous devez utiliser le **privilège configure level 1 command disable**, comme indiqué dans cet exemple :

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

Si vous avez toujours la session d'origine ouverte (celle avant d'ajouter une authentification), le PIX peut ne pas savoir qui vous êtes parce que vous ne vous êtes pas connecté initialement avec un nom d'utilisateur. Si tel est le cas, utilisez la commande **debug** pour afficher les messages relatifs à l'utilisateur « enable_15 » ou « enable_1 » s'il n'y a aucun nom d'utilisateur associé. Par conséquent, établissez une connexion Telnet avec le PIX en tant qu'utilisateur « poweruser » (l'utilisateur de niveau 15) avant de configurer l'autorisation de commande, car vous devez être sûr que le PIX peut associer un nom d'utilisateur aux commandes tentées. Vous êtes prêt à tester l'autorisation de commande à l'aide de cette commande :

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

L'utilisateur « poweruser » doit être en mesure d'établir une connexion Telnet, d'activer et d'exécuter toutes les commandes. L'utilisateur « normal » doit pouvoir utiliser les commandes **show clock**, **enable**, **disable** et **logout** mais pas d'autres, comme illustré dans cet exemple :

```
GOSS# show xlate
Command authorization failed
```

Authentification/autorisation avec un serveur AAA

Vous pouvez également authentifier et autoriser des utilisateurs à l'aide d'un serveur AAA. TACACS+ fonctionne mieux car l'autorisation de commande est possible, mais RADIUS peut également être utilisé. Vérifiez s'il existe des commandes Telnet/console AAA précédentes sur le PIX (dans le cas où la commande **LOCAL AAA** était précédemment utilisée), comme indiqué dans cet exemple :

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

S'il existe des commandes Telnet/console AAA précédentes, supprimez-les à l'aide des commandes suivantes :

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

Comme pour la configuration de l'authentification locale, testez pour vous assurer que les utilisateurs peuvent établir une connexion Telnet avec le PIX à l'aide de ces commandes.

```
telnet 172.18.124.0 255.255.255.0
!--- IP range allowed to telnet to the PIX (values would depend on network). passwd <password>
!--- Telnet password. Enable password <password>
!--- Enable password.
```

En fonction du serveur que vous utilisez, configurez le PIX pour l'authentification/autorisation avec un serveur AAA.

ACS - TACACS+

Configurez ACS pour communiquer avec le PIX en définissant le PIX dans la configuration du réseau avec l'authentification TACACS+ (pour le logiciel Cisco IOS®). La configuration de l'utilisateur ACS dépend de la configuration du PIX. Au minimum, l'utilisateur ACS doit être configuré avec un nom d'utilisateur et un mot de passe.

Sur PIX, utilisez les commandes suivantes :

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

Àce stade, l'utilisateur ACS doit pouvoir établir une connexion Telnet avec le PIX, l'activer avec le mot de passe enable existant sur le PIX et exécuter toutes les commandes. Procédez comme suit :

1. S'il est nécessaire d'activer l'authentification PIX avec ACS, choisissez **Interface Configuration > Advanced TACACS+ Settings**.
2. Cochez la case **Advanced TACACS+ Features in Advanced Configuration Options**.
3. Cliquez sur Submit. Les paramètres TACACS+ avancés sont désormais visibles dans la configuration utilisateur.
4. Définissez Max Privilege pour n'importe quel client AAA au niveau 15.
5. Choisissez le modèle de mot de passe enable pour l'utilisateur (qui peut impliquer la configuration d'un mot de passe enable distinct).
6. Cliquez sur Submit.

Pour activer l'authentification via TACACS+ dans PIX, utilisez cette commande :

```
GOSS(config)# aaa authentication enable console TACSERVER
```

Àce stade, l'utilisateur ACS doit pouvoir établir une connexion Telnet avec le PIX et l'activer avec le mot de passe enable configuré dans ACS.

Avant d'ajouter une autorisation de commande PIX, ACS 3.0 doit être corrigé. Vous pouvez télécharger le patch à partir du Software Center (clients enregistrés uniquement). Vous pouvez également afficher des informations supplémentaires sur ce correctif en accédant à l'ID de bogue Cisco CSCdw78255 (clients enregistrés uniquement).

L'authentification doit fonctionner avant d'autoriser les commandes. S'il est nécessaire d'exécuter une autorisation de commande avec ACS, sélectionnez **Interface Configuration > TACACS+ (Cisco) > Shell (exec) pour l'utilisateur et/ou le groupe** et cliquez sur **Soumettre**. Les paramètres d'autorisation de la commande shell sont maintenant visibles dans la configuration de l'utilisateur (ou du groupe).

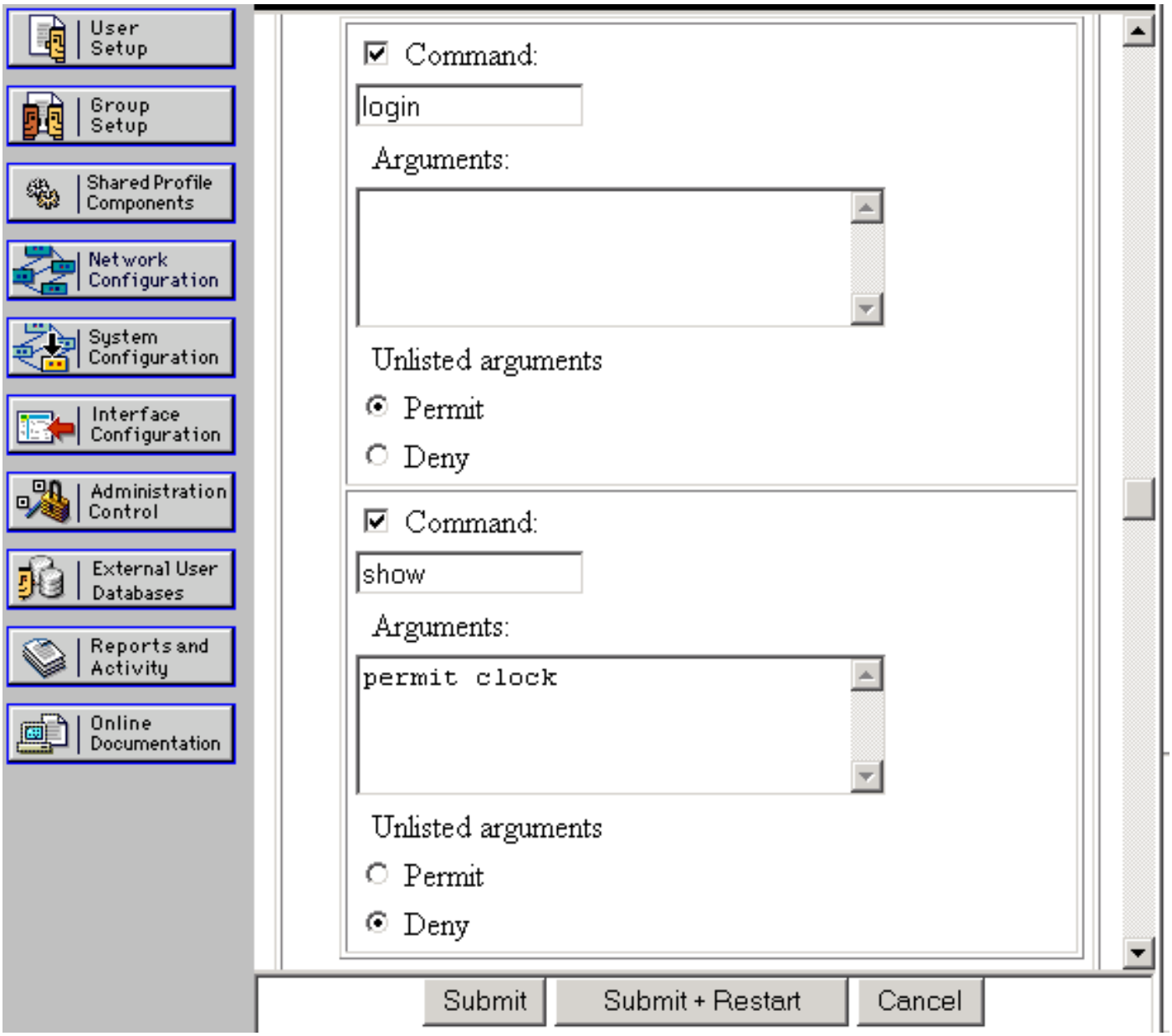
Il est recommandé de configurer au moins un utilisateur ACS puissant pour l'autorisation des commandes et d'autoriser des commandes Cisco IOS sans équivalent.

D'autres utilisateurs ACS peuvent être configurés avec l'autorisation de commande en autorisant un sous-ensemble de commandes. Cet exemple utilise les étapes suivantes :

1. Sélectionnez Paramètres de groupe pour rechercher le groupe souhaité dans la liste déroulante.
2. Cliquez sur **Modifier les paramètres**.
3. Choisissez **Jeu d'autorisations de commande Shell**.
4. Cliquez sur le bouton **Commande**.
5. Entrez **login**.
6. Sélectionnez Autoriser sous Arguments non répertoriés.

7. Répétez ce processus pour les commandes **logout**, **enable** et **disable**.
8. Sélectionnez Jeu d'autorisations de commande Shell.
9. Cliquez sur le bouton **Commande**.
10. **Spectacle**.
11. Sous Arguments, saisissez **permit clock**.
12. Sélectionnez Refuser pour les arguments non répertoriés.
13. Cliquez sur Submit.

Voici un exemple de ces étapes :



Si votre session d'origine est toujours ouverte (celle avant l'ajout d'une authentification), le PIX peut ne pas savoir qui vous êtes, car vous ne vous êtes pas d'abord connecté avec un nom d'utilisateur ACS. Si tel est le cas, utilisez la commande **debug** pour afficher les messages relatifs à l'utilisateur « enable_15 » ou « enable_1 » s'il n'y a aucun nom d'utilisateur associé. Vous devez vous assurer que le PIX peut associer un nom d'utilisateur aux commandes tentées. Pour ce faire, vous pouvez établir une connexion Telnet avec le PIX en tant qu'utilisateur ACS de niveau 15 avant de configurer l'autorisation de commande. Vous êtes prêt à tester l'autorisation de commande à l'aide de cette commande :

```
aaa authorization command TACSERVER
```

Àce stade, vous devez avoir un utilisateur qui doit être en mesure d'établir une connexion Telnet, d'activer et d'utiliser toutes les commandes, et un deuxième utilisateur qui ne peut exécuter que cinq commandes.

CSUnix - TACACS+

Configurez CSUnix pour communiquer avec le PIX comme avec tout autre périphérique réseau. La configuration de l'utilisateur CSUnix dépend de la configuration du PIX. Au minimum, l'utilisateur CSUnix doit être configuré avec un nom d'utilisateur et un mot de passe. Dans cet exemple, trois utilisateurs ont été configurés :

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login password is in the 'clear "********"' statement. !--- The enable password is in the 'clear "********" 15' statement. user = pixtest{ password = clear "********" privilege = clear "********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-- The login password is in the 'clear "********"' statement. !--- The enable password is in the 'clear "********" 15' statement.

user = limitpix{
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "clock"
}
cmd=logout {
permit ".*"
}
cmd=enable {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}

 !--- This user can Telnet in, but not enable. This user can use any !--- show commands in non-enable mode as well as logout, exit, and ?.

user = oneuser{
password = clear "********"
service=shell {
cmd=show {
permit ".*"
}
cmd=logout {
permit ".*"
}
cmd="?" {
permit ".*"
}
cmd=exit {
permit ".*"
```

```
}
}
}
```

Sur PIX, utilisez les commandes suivantes :

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host
```

```
GOSS(config)# aaa authentication telnet console TACSERVER
```

Àce stade, tous les utilisateurs de CSUnix doivent pouvoir établir une connexion Telnet avec le PIX, activer avec le mot de passe enable existant sur le PIX et utiliser toutes les commandes.

Activez l'authentification via TACACS+ dans PIX :

```
GOSS(config)# aaa authentication enable console TACSERVER
```

Àce stade, les utilisateurs de CSUnix qui ont des mots de passe « privilège 15 » devraient pouvoir établir une connexion Telnet avec le PIX et activer avec ces mots de passe « enable ».

Si votre session d'origine est toujours ouverte (celle avant d'ajouter une authentification), le PIX peut ne pas savoir qui vous êtes, car vous ne vous êtes pas connecté avec un nom d'utilisateur. Si c'est le cas, l'exécution de la commande **debug** peut afficher des messages sur l'utilisateur « enable_15 » ou « enable_1 » s'il n'y a aucun nom d'utilisateur associé. Établissez une connexion Telnet avec le PIX en tant qu'utilisateur « pixtest » (notre utilisateur de niveau 15) avant de configurer l'autorisation de commande, car nous devons nous assurer que le PIX peut associer un nom d'utilisateur aux commandes tentées. L'authentification d'activation doit être activée avant d'effectuer l'autorisation de commande. Si vous devez exécuter une autorisation de commande avec CSUnix, ajoutez cette commande :

```
GOSS(config)# aaa authorization command TACSERVER
```

Sur les trois utilisateurs, « pixtest » peut tout faire, et les deux autres utilisateurs peuvent faire un sous-ensemble de commandes.

ACS - RADIUS

L'autorisation de commande RADIUS n'est pas prise en charge. L'authentification Telnet et enable est possible avec ACS. ACS peut être configuré pour communiquer avec le PIX en définissant le PIX dans la configuration du réseau à l'aide de RADIUS « Authenticate Using » (toute variété). La configuration de l'utilisateur ACS dépend de la configuration du PIX. Au minimum, l'utilisateur ACS doit être configuré avec un nom d'utilisateur et un mot de passe.

Sur PIX, utilisez les commandes suivantes :

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host
```

```
GOSS(config)# aaa authentication telnet console RADSERVER
```

Àce stade, l'utilisateur ACS doit pouvoir établir une connexion Telnet avec le PIX, activer avec le mot de passe enable existant sur le PIX et utiliser toutes les commandes (le PIX n'envoie pas de commandes au serveur RADIUS ; L'autorisation de commande RADIUS n'est pas prise en charge).

Si vous voulez activer avec ACS et RADIUS sur le PIX, ajoutez cette commande :

```
aaa authentication enable console RADSERVER
```

Contrairement à TACACS+, le même mot de passe est utilisé pour RADIUS enable que pour RADIUS login.

CSUnix - RADIUS

Configurez CSUnix pour parler au PIX comme vous le feriez avec tout autre périphérique réseau. La configuration de l'utilisateur CSUnix dépend de la configuration du PIX. Ce profil fonctionne pour l'authentification et l'activation :

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "********"' statement; !--- this is used for the login,
enable, and non-enable commands.

password = clear "********" < pixradius
}
```

Sur PIX, utilisez les commandes suivantes :

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host
```

Si vous voulez activer avec ACS et RADIUS sur le PIX, utilisez cette commande :

```
GOSS(config)# aaa authentication enable console RADSERVER
```

Contrairement à TACACS+, le même mot de passe est utilisé pour RADIUS enable que pour RADIUS login.

Restrictions d'accès au réseau

Les restrictions d'accès au réseau peuvent être utilisées dans ACS et CSUnix pour limiter qui peut se connecter au PIX à des fins administratives.

- **ACS** - Le PIX serait configuré dans la zone Restrictions d'accès au réseau des paramètres de groupe. La configuration PIX est soit « Emplacements d'appel/point d'accès refusés », soit « Emplacements d'appel/point d'accès autorisés » (selon le plan de sécurité).
- **CSUnix** : exemple d'utilisateur autorisé à accéder au PIX, mais pas aux autres périphériques :

```
user = naruser{
profile_id = 119
profile_cycle = 1
password = clear "********"
privilege = clear "********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

Déboguer

Pour activer le débogage, utilisez cette commande :

```
logging on
logging
```

Voici des exemples de débogages bons et mauvais :

- **Bon débogage** : l'utilisateur peut utiliser les commandes **de connexion**, **enable** et **exécuter**.
```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixpartial at console
502103: User priv level changed: Uname: pixpartial From: 1 To: 15
111009: User 'pixpartial' executed cmd: show clock
```
- **Débogage incorrect** - L'autorisation échoue pour l'utilisateur, comme illustré dans cet exemple :
```
610101: Authorization failed: Cmd: uauth Cmdtype: show
```
- **Le serveur AAA distant est inaccessible :**
```
AAA server host machine not responding
```

Gestion de comptes

Il n'y a pas de comptabilité de commande réelle disponible, mais en activant syslog sur le PIX, vous pouvez voir quelles actions ont été effectuées, comme indiqué dans cet exemple :

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
611103: User logged out: Uname: pixtest
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
502103: User priv level changed: Uname: pixtest From: 1 To: 15
111008: User 'pixtest' executed the 'enable' command.
111007: Begin configuration: 172.18.124.111 reading from terminal
111008: User 'pixtest' executed the 'configure t' command.
111008: User 'pixtest' executed the 'write t' command.
```

Informations à collecter si vous ouvrez un dossier TAC

Si vous avez encore besoin d'aide après avoir suivi les étapes de dépannage ci-dessus et que voulez ouvrir un dossier avec le TAC Cisco, n'oubliez pas d'inclure les informations suivantes pour le dépannage de votre pare-feu PIX.
• Description du problème et des détails topologiques pertinents • Dépannage exécuté avant d'ouvrir le cas • Sortie de la commande **show tech-support** • Sortie de la commande **show log après l'exécution avec la commande logging buffered debugging , ou les captures de console qui expliquent le problème (si disponible)** Veuillez attacher les données rassemblées à votre cas en format texte décompressé (.txt). Vous pouvez joindre des informations à votre dossier en les téléchargeant à l'aide du Case Query Tool (clients enregistrés uniquement). Si vous ne pouvez pas accéder au Case Query Tool, vous pouvez envoyer les informations en pièce-jointe dans un e-mail à attach@cisco.com avec votre numéro de dossier dans l'objet du message.

Informations connexes

- Référence des commandes PIX
- Logiciel Cisco PIX Firewall - Assistance technique et documentation
- Cisco Secure Access Control Server pour Windows - Support technique et documentation
- Cisco Secure Access Control Server pour Unix - Assistance technique et documentation