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 locale de commande est faite en assignant des commandes et des utilisateurs aux niveaux de privilège.

L'autorisation de remote command est faite par un serveur d'Authentification, autorisation et comptabilité (AAA) TACACS+. De plusieurs serveurs d'AAA peuvent être définis au cas où on serait inaccessible.

L'authentification fonctionne également avec IPSec précédemment configuré et connexions SSH. L'authentification de SSH exige que vous émettez cette commande :

aaa authentication ssh console <*LOCAL* | *server_tag*>
Remarque: Si vous utilisez un groupe de serveurs TACACS+ ou de RAYON pour l'authentification, vous pouvez configurer le PIX pour utiliser la base de données locale comme méthode de **RETOUR** si le serveur d'AAA est indisponible.

Par exemple

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```
Vous pouvez alternativement utiliser la base de données locale en tant que votre méthode d'authentification principale (sans le retour) si vous entrez dans seuls des GENS DU PAYS.

Par exemple, émettez cette commande afin de définir un compte utilisateur dans la base de données locale et 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 (5.2 à 6.2) pour plus d'informations sur la façon créer l'accès AAA-authentifié à un Pare-feu PIX qui exécute la version du logiciel PIX 5.2 à 6.2 et pour plus d'informations sur l'authentification d'enable, syslogging, et accédant quand le serveur d'AAA est en panne.

Reportez-vous à la section PIX/ASA : Le proxy de cut-through pour l'accès de réseau utilisant l'exemple de configuration de serveur TACACS+ et RADIUS pour plus d'informations sur la façon créer AAA-a authentifié l'accès (de proxy de cut-through) à un Pare-feu PIX qui exécute les versions du logiciel PIX 6.3 et plus tard.

Si la configuration est faite correctement, vous ne devriez pas être verrouillé hors du PIX. Si la configuration n'est pas enregistrée, la réinitialisation du PIX devrait le renvoyer à son état de pré-configuration. Si le PIX n'est pas dû accessible à la mauvaise configuration, référez-vous à la procédure de récupération de reprise de mot de passe et de configuration d'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.

Composants utilisés

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

- Version du logiciel PIX 6.2
- Cisco Secure ACS pour la version 3.0 (ACS) de Windows
- Cisco Secure ACS pour la version 2.3.6 d'UNIX (CSUnix)

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Test avant d'ajouter l'authentification/autorisation

Avant de mettre en application les nouvelles 6.2 caractéristiques d'authentification/autorisation, assurez-vous que vous pouvez actuellement accéder au PIX utilisant ces commandes :

```
!--- 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>
```

Compréhension des configurations de privilège

La plupart des commandes dans le PIX sont au niveau 15, bien que quelques uns soient au niveau 0. Pour visualiser des configurations actuelles pour toutes les commandes, utilisez cette commande :

```
show privilege all
```

La plupart des commandes sont au niveau 15 par défaut, suivant les indications de cet exemple :

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

Quelques commandes sont au niveau 0, suivant les indications de cet exemple :

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

Le PIX peut fonctionner dans l'enable et configurer des modes. Quelques commandes, telles que le **show logging**, sont disponibles dans les deux modes. Pour placer des privilèges sur ces commandes, vous devez spécifier le mode que la commande existe dedans, suivant les indications de l'exemple. L'autre option de mode est **enable**. Vous obtenez `se connecter est une commande disponible dans le` message d'erreur de `modes "MULTIPLE"`. Si vous ne configurez pas le mode, utilisez le **mode [enable|configurez] la** commande :

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

Ces exemples adressent la commande d'**horloge**. Utilisez cette commande de déterminer les configurations actuelles pour la commande d'**horloge** :

```
show privilege command clock
```

La sortie de la commande d'**horloge de commande de show privilege** prouve que la commande d'**horloge** existe dans ces trois formats :

```
!--- 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'utilisateur locaux

Avant de changer le niveau de privilège de la commande d'**horloge**, vous devriez aller au port de console pour configurer un utilisateur administratif et pour activer l'authentification de procédure de connexion locale, suivant les indications de 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, suivant les indications de cet exemple :

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

L'utilisateur « poweruser » devrait pouvoir au telnet dans le PIX et à l'enable avec le mot de passe existant d'enable des gens du pays PIX (celui du **<password > de la** commande de **mot de passe d'enable**).

Vous pouvez ajouter plus de Sécurité en ajoutant l'authentification pour activer, suivant les indications de cet exemple :

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

Ceci exige de l'utilisateur d'entrer le mot de passe les deux pour la procédure de connexion et l'enable. Dans cet exemple, le mot de passe « poweruser » est utilisé pour la procédure de connexion et l'enable. L'utilisateur « poweruser » devrait pouvoir au telnet dans le PIX et également activer avec le mot de passe PIX local.

Si vous voulez que quelques utilisateurs puissent utiliser seulement certaines commandes, vous devez installer un utilisateur avec des privilèges inférieurs, suivant les indications de cet exemple :

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

Puisque pratiquement toutes vos commandes sont au niveau 15 par défaut, vous devez abaisser quelques commandes au niveau 9 de sorte que les utilisateurs « ordinaires » puissent les émettre. Dans ce cas, vous voulez que votre utilisateur du niveau 9 puisse utiliser la commande de **show clock**, mais ne pas modifier l'horloge, suivant les indications de cet exemple :

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

Vous avez besoin également de votre utilisateur pour pouvoir se déconnecter de le PIX (l'utilisateur pourrait être dans le niveau 1 ou 9 en voulant faire ceci), suivant les indications de cet exemple :

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

Vous avez besoin de l'utilisateur pour pouvoir utiliser la commande d'**enable** (l'utilisateur est à dans le niveau 1 en tentant ceci), suivant les indications de cet exemple :

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

En déplaçant la commande de **débronchement au** niveau 1, n'importe quel utilisateur entre les niveaux 2-15 peut sortir du mode enable, suivant les indications de cet exemple :

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

Si vous telnet dedans en tant qu'utilisateur « ordinaire » et enable en tant que même utilisateur (le mot de passe est également « ordinaire »), vous utilisez le **privilège configurez le débronchement de commande du niveau 1**, suivant les indications de cet exemple :

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

Si vous avez toujours la session initiale ouverte (celle avant d'ajouter toute authentification), le PIX peut ne pas savoir qui vous êtes parce que vous n'avez pas au commencement ouvert une session avec un nom d'utilisateur. Si c'est le cas, utilisez la commande de **débogage** de visualiser des messages au sujet de l'utilisateur "enable_15" ou "enable_1" s'il n'y a aucun nom d'utilisateur associé. Par conséquent, le telnet dans le PIX en tant qu'utilisateur « poweruser » (le « utilisateur de niveau 15") avant de configurer l'autorisation de commande, parce que vous devez être sûr le PIX peut associer un nom d'utilisateur avec les commandes étant 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 » devrait pouvoir au telnet dedans, activer, et exécuter toutes les commandes. L'utilisateur « ordinaire » devrait pouvoir utiliser le **show clock**, **n'activer**, **désactiver**, et **se déconnecter des** commandes mais pas autres, suivant les indications de cet exemple :

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

Authentification/autorisation avec un serveur d'AAA

Vous pouvez également authentifier et autoriser des utilisateurs à l'aide d'un serveur d'AAA. TACACS+ fonctionne meilleur parce que l'autorisation de commande est possible, mais le RAYON peut également être utilisé. Vérifiez pour voir s'il y a des commandes précédentes de telnet/console d'AAA sur le PIX (au cas où la commande **LOCALE d'AAA** était précédemment utilisée), suivant les indications de cet exemple :

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

S'il y a des commandes précédentes de telnet/console d'AAA, retirez-les à l'aide de ces commandes :

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

Comme avec configurer l'authentification locale, le test pour s'assurer des utilisateurs mettent en boîte le telnet dans 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.
```

Selon quel serveur vous utilisez, configurez le PIX pour l'authentification/autorisation avec un serveur d'AAA.

ACS - TACACS+

Configurez ACS pour communiquer avec le PIX en définissant le PIX en configuration réseau avec « authentifient utilisant » TACACS+ (pour le logiciel de Cisco IOS®). La configuration de l'utilisateur ACS dépend de la configuration du PIX. Au minimum, l'utilisateur ACS devrait être installé avec un nom d'utilisateur et mot de passe.

Sur le PIX, utilisez ces commandes :

```
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
```

En ce moment, l'utilisateur ACS devrait pouvoir au telnet dans le PIX, l'activer avec le mot de passe existant d'enable sur le PIX, et exécuter toutes les commandes. Procédez comme suit :

1. S'il y a un besoin de faire l'authentification d'enable PIX avec ACS, choisissez la **configuration d'interface > les configurations avancées TACACS+**.
2. Cochez les **caractéristiques avancées TACACS+ dans la** case d'**options de configuration avancée**.
3. Cliquez sur **Submit**. Les configurations avancées TACACS+ sont maintenant visibles sous la configuration utilisateur.
4. Placez le privilège maximum pour n'importe quel client d'AAA au niveau 15.
5. Choisissez le schéma de mot de passe d'enable pour l'utilisateur (qui pourrait impliquer de configurer un mot de passe distinct d'enable).
6. Cliquez sur **Submit**.

Pour activer l'authentification d'enable par TACACS+ dans le PIX, utilisez cette commande :

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

En ce moment, l'utilisateur ACS devrait pouvoir au telnet dans le PIX et à l'enable avec le mot de passe configuré d'enable dans ACS.

Avant d'ajouter l'autorisation de commande PIX, ACS 3.0 doit être corrigé. Vous pouvez télécharger le correctif du centre de logiciel (clients enregistrés seulement). Vous pouvez également visualiser les informations complémentaires au sujet de ce correctif en accédant à l'ID de bogue Cisco CSCdw78255 (clients enregistrés seulement).

L'authentification doit fonctionner avant de faire l'autorisation de commande. S'il y a un besoin d'exécuter l'autorisation de commande avec ACS, choisissez la **configuration d'interface > le TACACS+ (Cisco) > shell (exécutif) pour l'utilisateur et/ou le groupe** et cliquez sur Submit. Les configurations d'autorisation de commande shell sont maintenant visibles sous la configuration d'utilisateur (ou groupe).

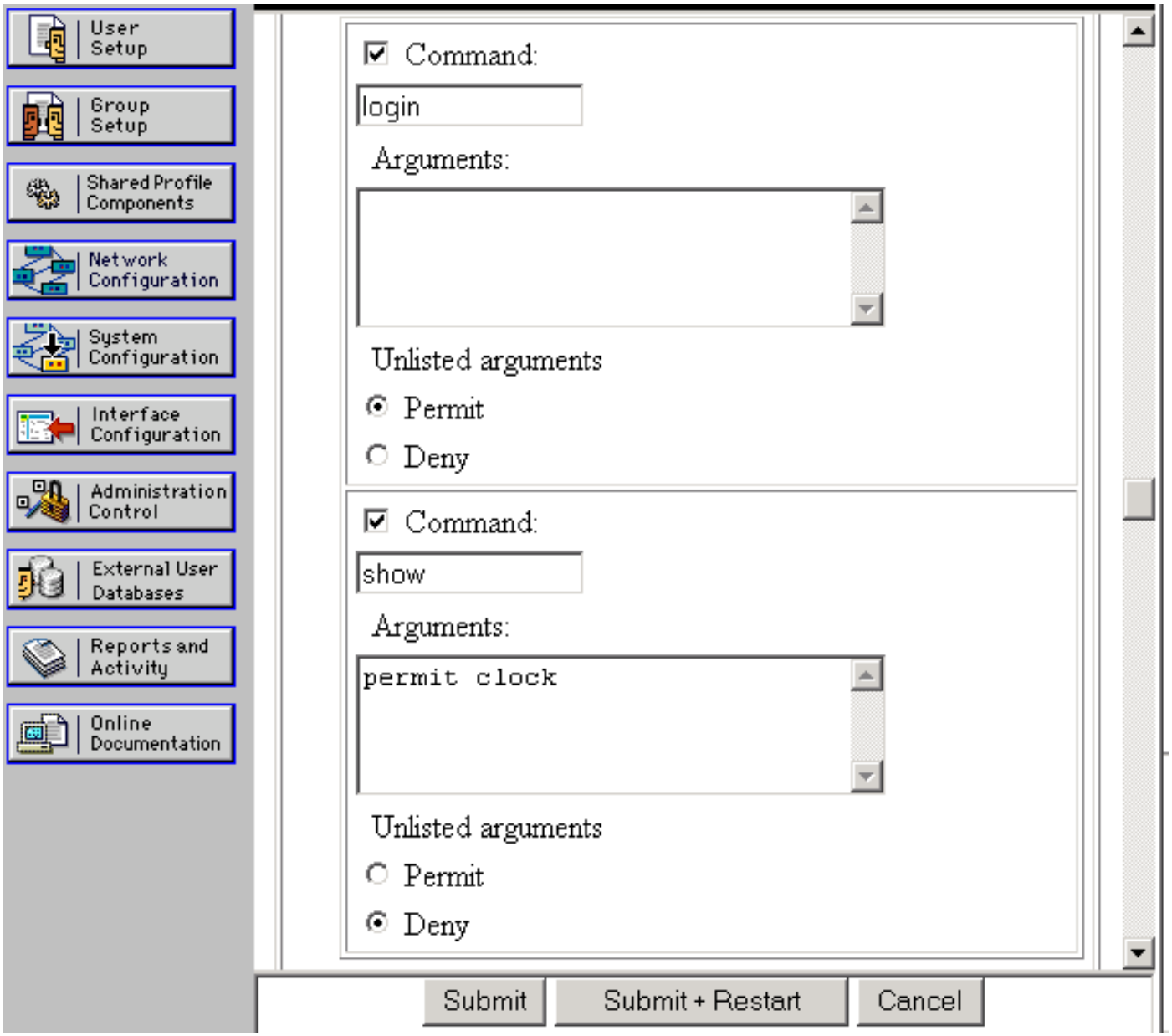
C'est une bonne idée d'installer au moins un utilisateur puissant ACS pour l'autorisation de commande et de permettre des commandes Cisco IOS inégalées.

D'autres utilisateurs ACS peuvent être installés avec l'autorisation de commande en permettant un sous-ensemble de commandes. Cet exemple utilise ces étapes :

1. Choisissez les configurations de groupe pour trouver le groupe désiré de la liste déroulante.
2. Cliquez sur Edit les **configurations**.
3. Choisissez le **positionnement d'autorisation de commande shell**.
4. Cliquez sur le bouton de **commande**.
5. Écrivez la **procédure de connexion**.
6. Choisissez l'autorisation sous des arguments non listés.
7. Répétez ce processus pour la **déconnexion**, **activez**, et **désactivez les** commandes.
8. Choisissez le positionnement d'autorisation de commande shell.
9. Cliquez sur le bouton de **commande**.
10. Entershow.
11. Sous des arguments, entrez dans l'**horloge d'autorisation**.
12. Choose refusent pour des arguments non listés.

13. Cliquez sur **Submit**.

Voici un exemple de ces étapes :



Si vous avez toujours votre session initiale ouverte (celle avant d'ajouter toute authentification), le PIX peut ne pas savoir qui vous êtes parce que vous n'avez pas au commencement ouvert une session avec un nom d'utilisateur ACS. Si c'est le cas, utilisez la commande de **débogage** de visualiser des messages au sujet d'utilisateur "enable_15" ou "enable_1" s'il n'y a aucun nom d'utilisateur associé. Vous devez être sûr que le PIX peut associer un nom d'utilisateur avec les commandes étant tentées. Vous pouvez faire ceci par Telnetting dans le PIX comme l'utilisateur du niveau 15 ACS 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
```

En ce moment, vous devriez avoir un utilisateur qui devrait pouvoir au telnet dedans, activer, et utiliser toutes les commandes, et un deuxième utilisateur qui peut seulement faire cinq commandes.

CSUnix - TACACS+

Configurez CSUnix pour communiquer avec le PIX comme vous avec n'importe quel autre périphérique de réseau. La configuration de l'utilisateur de CSUnix dépend de la configuration du PIX. Au minimum, l'utilisateur de CSUnix devrait être installé avec un nom d'utilisateur et mot de passe. Dans cet exemple, trois utilisateurs ont été installés :

```
!--- 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 le PIX, utilisez ces commandes :

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

En ce moment, les utilisateurs l'uns des de CSUnix devraient pouvoir au telnet dans le PIX, activer avec le mot de passe existant d'enable sur le PIX, et utiliser toutes les commandes.

Authentification d'enable par TACACS+ dans le PIX :

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

En ce moment, les utilisateurs de CSUnix qui ont des « mots de passe du privilège 15" devraient pouvoir au telnet dans le PIX et à l'enable avec ces « mots de passe d'enable ».

Si vous avez toujours votre session initiale ouverte (celle avant d'ajouter toute authentification), le PIX peut ne pas savoir qui vous êtes parce que vous n'avez pas au commencement ouvert une session avec un nom d'utilisateur. Si c'est le cas, émettre la commande de **débogage** peut afficher à des messages au sujet d'utilisateur "enable_15" ou "enable_1" s'il n'y a aucun nom d'utilisateur associé. Le telnet dans le PIX en tant qu'utilisateur « pixtest » (notre « utilisateur de niveau 15") avant de configurer l'autorisation de commande, parce que nous devons être sûrs le PIX peut associer un nom d'utilisateur avec les commandes étant tentées. L'authentification d'enable doit être en fonction avant de faire l'autorisation de commande. S'il y a un besoin d'exécuter l'autorisation de commande avec CSUnix, ajoutez cette commande :

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

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

ACS - RAYON

L'autorisation de commande de RAYON n'est pas prise en charge. Le telnet et l'authentification d'enable est possible avec ACS. ACS peut être configuré pour communiquer avec le PIX en définissant le PIX en configuration réseau avec « authentifie utilisant » le RAYON (toute variété). La configuration de l'utilisateur ACS dépend de la configuration du PIX. Au minimum, l'utilisateur ACS devrait être installé avec un nom d'utilisateur et mot de passe.

Sur le PIX, utilisez ces commandes :

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config) # aaa-server RADSERVER (inside) host <ip> <key> timeout 10 GOSS(config)# aaa
authentication telnet console RADSERVER
```

En ce moment, l'utilisateur ACS devrait pouvoir au telnet dans le PIX, activer avec le mot de passe existant d'enable sur le PIX, et utiliser toutes les commandes (le PIX n'envoie pas des commandes au serveur de RAYON ; L'autorisation de commande de RAYON n'est pas prise en charge).

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

```
aaa authentication enable console RADSERVER
```

Àla différence de avec TACACS+, le même mot de passe est utilisé pour le radius enable quant à la procédure de connexion de RAYON.

CSUnix - RAYON

Configurez CSUnix pour parler au PIX comme vous avec n'importe quel autre périphérique de réseau. La configuration de l'utilisateur de 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 le PIX, utilisez ces commandes :

```
GOSS(config)# enable password cisco123 GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host <ip> <key> timeout 10
```

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

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

Àla différence de avec TACACS+, le même mot de passe est utilisé pour le radius enable quant à la procédure de connexion de RAYON.

Restrictions d'accès au réseau

Des 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 région de restrictions d'accès au réseau des configurations de groupe. La configuration PIX est « appeler refusé/point des emplacements d'Access » ou « appeler permis/point des emplacements d'Access » (selon le plan de la sécurité).
- **CSUnix** — C'est un exemple d'un utilisateur qui est permis l'accès au PIX, mais de non 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
}
}
```

Debug

Pour s'activer mettez au point, utilisez cette commande :

logging on logging <console|monitor> debug

Ce sont des exemples de bon et mauvais met au point :

- **Bon mettez au point** — L'utilisateur peut utiliser la **procédure de connexion**, **activer**, et **exécuter des** commandes.`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`
- **Le mauvais mettent au point** — L'autorisation échoue pour l'utilisateur, suivant les indications de cet exemple :`610101: Authorization failed: Cmd: uauth Cmdtype: show`
- **Le serveur distant d'AAA est inaccessible :**`AAA server host machine not responding`

Comptabilité

Il n'y a aucune comptabilité des commandes réelle disponible, mais en ayant le Syslog lancé sur le PIX, vous pouvez voir quelles actions ont été exécutées, suivant les indications de 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
- Logiciels pare-feu Cisco PIX - Soutien technique et documentation
- Cisco Secure Access Control Server pour Windows - Soutien technique et documentation
- Cisco Secure Access Control Server pour Unix - Soutien technique et documentation
- Support et documentation techniques - Cisco Systems