Authentification, autorisation et traçabilité des utilisateurs par le biais du logiciel PIX version 5.2 et ultérieure

Contenu

Introduction

L'authentification de RAYON et TACACS+ peut être faite pour le FTP, le telnet, et les connexions HTTP par le pare-feu Cisco Secure PIX. L'authentification pour d'autres protocoles moins communs sont habituellement faites fonctionner. L'autorisation TACACS+ est prise en charge. L'autorisation RADIUS n'est pas prise en charge. Les changements de l'Authentification, autorisation et comptabilité (AAA) PIX 5.2 au-dessus de la version antérieure incluent la prise en charge de liste d'accès AAA pour contrôler qui est authentifié et les quels ressources les accès client. Dans PIX 5.3 et plus tard, la modification d'Authentification, autorisation et comptabilité (AAA) au-dessus des versions antérieures de code est que les ports de RAYON sont configurables.

Remarque: PIX 6.x peut faire l'explication traverse le trafic mais pas pour le trafic destinated au PIX.

Conditions préalables

Conditions requises

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

Composants utilisés

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

- Versions de logiciel 5.2.0.205 et 5.2.0.207 de pare-feu Cisco Secure PIX

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

Remarque: Si vous exécutez la version de logiciel 7.x PIX/ASA et plus tard, référez-vous aux serveurs de configuration d'AAA et à la base de données locale.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Authentification, autorisation, et comptabilité

Voici une explication de l'authentification, de l'autorisation et de la comptabilité :

- L'authentification est qui l'utilisateur est.
- Est l'autorisation ce que l'utilisateur fait.
- L'authentification est valide sans autorisation.
- L'autorisation est non valide sans authentification.
- Est la comptabilité ce que l'utilisateur a fait.

Sur ce que l'utilisateur voit avec l'Authentification/Autorisation activée

Quand les essais d'utilisateur à aller de l'intérieur à l'extérieur (ou vice versa) avec l'authentification/autorisation en fonction :

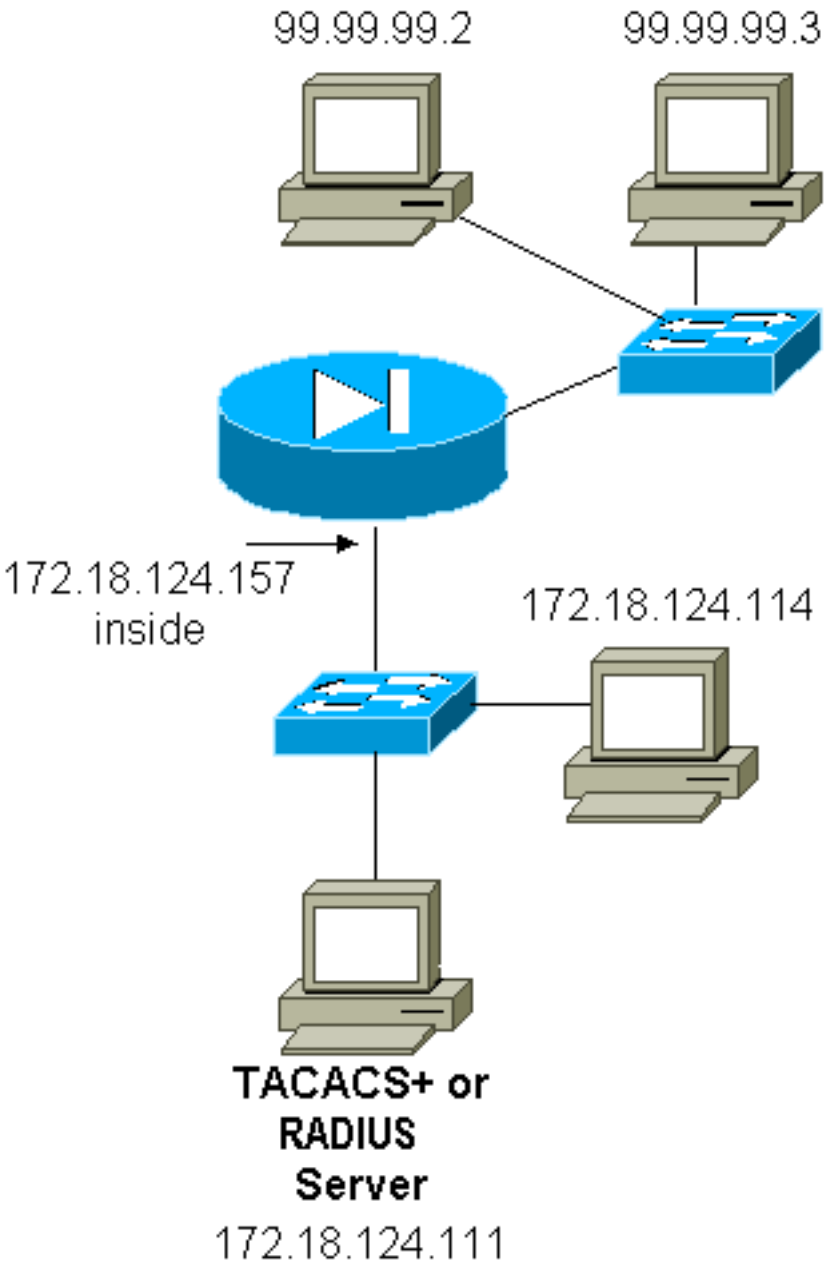
- **Telnet** — L'utilisateur voit une invite de nom d'utilisateur être soulevé, puis une demande pour le mot de passe. Si l'authentification (et l'autorisation) est réussie au PIX/server, l'utilisateur est incité pour le nom d'utilisateur et mot de passe par la destination host au-delà.
- **FTP** — L'utilisateur voit une invite de nom d'utilisateur être soulevé. Les besoins de l'utilisateur d'écrire « local_username@remote_username » pour le nom d'utilisateur et le « local_password@remote_password » pour le mot de passe. Le PIX envoie le « local_username » et le « local_password » au serveur de sécurité local. Si l'authentification (et l'autorisation) est réussie au PIX/server, le « remote_username » et le « remote_password » sont passés au serveur FTP de destination au-delà.
- **HTTP** — Une fenêtre est affichée dans le navigateur demandant le nom d'utilisateur et mot de passe. Si l'authentification (et l'autorisation) est réussie, l'utilisateur arrive au site Web de destination au-delà. Maintenez dans l'esprit que les *navigateurs cachent des noms d'utilisateur et mot de passe.* S'il s'avère que le PIX devrait chronométrer une connexion HTTP mais ne fait pas ainsi, il est probable que la ré-authentification ait lieu réellement avec le navigateur « tir » le nom d'utilisateur en cache et le mot de passe au PIX. Le PIX en avant ceci au serveur d'authentification. Le Syslog et/ou le serveur PIX mettent au point des expositions ce phénomène. Si le telnet et le FTP semblent fonctionner « normalement », mais les connexions HTTP ne font pas, c'est la raison.

Étapes de débogage

- Assurez-vous les travaux de configuration PIX avant que vous ajoutiez l'authentification et l'autorisation d'AAA. Si vous ne pouvez pas passer le trafic avant que vous instituiez l'authentification et l'autorisation, vous ne pouvez pas faire tellement après.
- Activez un certain genre d'ouvrir une session le PIX.Émettez la commande de **débogage de logging console** d'activer le logging console debugging.**Remarque:** N'utilisez pas le logging console debugging sur un système fortement chargé.Utilisez la commande de **débogage se connectante de moniteur** de se connecter une session de telnet.Le logging buffered debugging peut être utilisé, puis exécute la commande de **show logging**.Se connecter peut également être envoyé à un serveur de Syslog et être examiné là.
- Activez l'élimination des imperfections sur les serveurs TACACS+ ou de RAYON.

Authentification seulement

Diagramme du réseau



Configuration du serveur - Authentification seulement

Configuration de serveur TACACS de Cisco Secure UNIX

```
User = cse {
password = clear "cse"
default service = permit
}
```

Configuration du serveur RADIUS de Cisco Secure UNIX

Remarque: Ajoutez l'adresse IP et la clé PIX à la liste de serveur d'accès à distance (NAS) avec l'aide de l'interface graphique utilisateur avancée.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

RAYON Cisco Secure de Windows

Employez ces étapes pour installer un RAYON Cisco Secure de Windows divisent.

1. Obtenez un mot de passe dans la **section User Setup**.
2. **De la section Installation de groupe**, placez l'attribut 6 (type de service) **pour ouvrir une session** ou **administratif**.
3. Ajoutez l'adresse IP PIX dans la section de **configuration de NAS du** GUI.

Windows Cisco Secure TACACS+

L'utilisateur obtient un mot de passe dans la **section User Setup**.

Configuration du serveur Livingston RADIUS

Remarque: Ajoutez l'adresse IP PIX et la clé aux *clients* classent.

- affichez l'Utilisateur-Service-type = l'utilisateur de coque de " foo » de Password=

Configuration du serveur Merit RADIUS

Remarque: Ajoutez l'adresse IP PIX et la clé aux *clients* classent.

- affichez le type de service = l'utilisateur de coque de " foo » de Password=

Configuration du serveur de logiciel gratuit TACACS+

```
key = "cisco"
user = cse {
login = cleartext "cse"
default service = permit
}
```

Configuration initiale PIX - Authentification seulement

Configuration initiale PIX - Authentification seulement
PIX Version 5.2(0)205 nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pixfirewall fixup protocol ftp 21

```
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet access-list 101 permit tcp
any any eq ftp access-list 101 permit tcp any any eq www
! pager lines 24 logging on no logging timestamp no
logging standby logging console debugging no logging
monitor no logging buffered logging trap debugging no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 10baset mtu
outside 1500 mtu inside 1500 ip address outside
99.99.99.1 255.255.255.0 ip address inside
172.18.124.157 255.255.255.0 ip audit info action alarm
ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0 arp
timeout 14400 global (outside) 1 99.99.99.10-99.99.99.20
netmask 255.255.255.0 nat (inside) 1 172.18.124.0
255.255.255.0 0 0 static (inside,outside) 99.99.99.99
172.18.124.114 netmask 255.255.255.255 0 0 conduit
permit tcp any any conduit permit udp any any conduit
permit icmp any any route inside 172.18.0.0 255.255.0.0
172.18.124.1 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 si p 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute ! !--- For the purposes of
illustration, the TACACS+ process is used !--- to
authenticate inbound users and RADIUS is used to
authenticate outbound users. aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
AuthInbound protocol tacacs+ aaa-server AuthInbound
(inside) host 172.18.124.111 cisco timeout 5 aaa-server
AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 172.18.124.111 cisco timeout 5 ! !--- The
next six statements are used to authenticate all inbound
!--- and outbound FTP, Telnet, and HTTP traffic. aaa
authentication include ftp outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound aaa authentication include
telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound aaa authentication include http outside
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include ftp inside
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound ! !--- OR
the new 5.2 feature allows these two statements in !---
conjunction with access-list 101 to replace the previous
six statements. !--- Note: Do not mix the old and new
verbiage. aaa authentication match 101 outside
AuthInbound aaa authentication match 101 inside
AuthOutbound no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable no sysopt route dnat
isakmp identity hostname telnet timeout 5 ssh timeout 5
terminal width 80
```

```
Cryptochecksum:5882f514247589d784a0d74c800907b8 : end
```

Le RAYON configurable met en communication (5.3 et plus tard)

Quelques serveurs de RAYON utilisent des ports de RAYON autres que 1645/1646 (habituellement 1812/1813). Dans PIX 5.3 et plus tard, l'authentification et les ports de traçabilité de RAYON peuvent être changés à quelque chose autre que le 1645/1646 par défaut avec ces commandes :

aaa-server radius-authport # aaa-server radius-acctport #

Exemples de debug d'authentification PIX

Voir les étapes de débogage pour des informations sur la façon activer l'élimination des imperfections. Ce sont des exemples d'un utilisateur chez 99.99.99.2 qui initie le trafic à 172.18.124.114 intérieur (99.99.99.99) et vice versa. Le trafic d'arrivée est TACACS-authentifié et sortant Rayon-est authentifié.

Authentification réussie - TACACS+ (d'arrivée)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

Authentification infructueuse due au mauvais nom d'utilisateur/mot de passe - TACACS+ (d'arrivée). L'utilisateur voit la « erreur : Nombre maximum d'essais dépassés. »

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

Serveur ne parlant pas à PIX - TACACS+ (d'arrivée). L'utilisateur voit que le nom d'utilisateur une fois et le PIX ne demande jamais un mot de passe (c'est sur le telnet). L'utilisateur voit la « erreur : Nombre maximum d'essais dépassés. »

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

Bonne authentification - RAYON (sortant)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

Authentification erronée (nom d'utilisateur ou mot de passe) - RAYON (sortant). L'utilisateur voit la demande pour le nom d'utilisateur, puis le mot de passe, a trois occasions d'entrer dans ces derniers, et s'infructueux, voient la « erreur : Nombre maximum d'essais dépassés. »

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

Serveur pingable mais démon vers le bas, serveur non pingable, ou non-concordance de clé/client - ne communiquera pas avec PIX - RAYON (sortant). L'utilisateur voit le nom d'utilisateur, puis le mot de passe, puis le « serveur de RAYON a manqué, » et puis finalement « erreur : Nombre maximum d'essais dépassés. »

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

Authentification plus l'autorisation

Si vous voulez permettre à tous les utilisateurs authentifiés pour exécuter toutes les exécutions (HTTP, FTP, et telnet) par le PIX, alors l'authentification est suffisante et l'autorisation n'est pas nécessaire. Cependant, si vous voulez permettre un certain sous-ensemble de services à certains utilisateurs ou limiter des utilisateurs d'aller à certains sites, l'autorisation est nécessaire. L'autorisation RADIUS est non valide pour le trafic par le PIX. L'autorisation TACACS+ est valide dans ce cas.

Si l'authentification passe et l'autorisation est allumée, le PIX envoie la commande que l'utilisateur fait au serveur. Par exemple, le « HTTP 1.2.3.4." dans la version 5.2 de PIX, autorisation TACACS+ est utilisé en même temps que des Listes d'accès pour contrôler où les utilisateurs vont.

Si vous voulez implémenter l'autorisation pour le HTTP (sites Web visités), utilisez le logiciel tel que Websense puisqu'un site Web simple peut avoir un grand nombre d'adresses IP associées avec lui.

Configuration du serveur - Authentification plus l'autorisation

Configuration de serveur TACACS de Cisco Secure UNIX

```
  user = can_only_do_telnet {
  password = clear "**********"
  service = shell {
  cmd = telnet {
  permit .*
  }
  }
  }

  user = can_only_do_ftp {
  password = clear "*******"
  service = shell {
  cmd = ftp {
  permit .*
  }
```

```
  }
  }

  user = httponly {
  password = clear "********"
  service = shell {
  cmd = http {
  permit .*
  }
  }
  }
```

Windows Cisco Secure TACACS+

Terminez-vous ces étapes pour installer un serveur Cisco Secure de Windows TACACS+.

1. Le clic **refusent des commandes IOS inégalées au** bas du Group Setup.
2. Cliquez sur Add**/éditez la nouvelle commande (FTP, HTTP, telnet)**.Par exemple, si vous voulez permettre le telnet à un site spécifique (« telnet 1.2.3.4"), la commande est **telnet**. L'argument est *1.2.3.4*. Après avoir complété le « command=telnet, » complétez la « autorisation » adresse IP dans l'argument rectangle (par exemple, « autorisation 1.2.3.4"). Si tous les telnets doivent être laissés, la commande est toujours **telnet**, mais le clic **permettent tous les arguments non listés**. Cliquez sur Finish alors la **commande de retouche**.
3. Exécutez l'étape 2 pour chacune des commandes permises (par exemple, telnet, HTTP, et FTP).
4. Ajoutez l'adresse IP PIX dans la section de configuration de NAS à l'aide du GUI.

Configuration du serveur de logiciel gratuit TACACS+

```
user = can_only_do_telnet {
   login = cleartext "telnetonly"
   cmd = telnet {
   permit .*
   }
   }

 user = httponly {
   login = cleartext "httponly"
   cmd = http {
   permit .*
   }
   }

 user = can_only_do_ftp {
   login = cleartext "ftponly"
   cmd = ftp {
   permit .*
   }
   }
```

Configuration PIX - Ajouter l'autorisation

Ajoutez les commandes d'exiger l'autorisation :

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization
include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

La nouvelle caractéristique 5.2 permet à cette déclaration en même temps que la liste d'accès précédemment définie 101 pour remplacer les trois déclarations précédentes. Le vieux et nouveau verbiage ne devrait pas être mélangé.

```
aaa authorization match 101 outside AuthInbound
```

Exemples de debug d'authentification PIX et d'autorisation

La bonne authentification et l'autorisation réussit - TACACS+

```
109001: Auth start for user '???' from
   99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to 99.99.99.2/11010
   on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

La bonne authentification mais l'autorisation échoue - TACACS+. L'utilisateur erreur voit également message « : Autorisation refusée. »

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

Nouvelle caractéristique de liste d'accès

Dans la version du logiciel PIX 5.2 et plus tard, définissez les Listes d'accès sur le PIX. Appliquez-les sur une base par utilisateur basée sur le profil utilisateur sur le serveur. TACACS+ exige l'authentification et l'autorisation. Le RAYON exige l'authentification seulement. Dans cet exemple, l'authentification en sortie et l'autorisation à TACACS+ sont changées. Une liste d'accès sur le PIX est installée.

Remarque: Dans la version de PIX 6.0.1 et plus tard, si vous utilisez le RAYON, les Listes d'accès sont mises en application en écrivant la liste dans l'attribut RADIUS IETF standard 11 (Filtre-id) [CSCdt50422]. Dans cet exemple, l'attribut 11 est placé à 115 au lieu de faire le verbiage de la constructeur-particularité "acl=115".

Configuration PIX

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet access-list 115 permit tcp any host
99.99.99.2 eq www access-list 115 permit tcp any host 99.99.99.2 eq ftp access-list 115 deny tcp
any host 99.99.99.3 eq www access-list 115 deny tcp any host 99.99.99.3 eq ftp access-list 115
deny tcp any host 99.99.99.3 eq telnet
```

Profils de serveur

Remarque: La version 2.1 du logiciel gratuit TACACS+ n'identifie pas le verbiage de « acl ».

Configuration du serveur de Cisco Secure UNIX TACACS+

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Windows Cisco Secure TACACS+

Afin d'ajouter l'autorisation au PIX de contrôler où l'utilisateur va de pair avec des Listes d'accès, cochez le **shell/exec**, cochez la **zone de liste de contrôle d'accès**, et complétez le nombre (apparie le nombre de listes d'accès sur le PIX).

Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

RAYON Cisco Secure de Windows

RADIUS/Cisco est le type de périphérique. Les besoins de l'utilisateur de « pixa » un nom d'utilisateur, un mot de passe, et un contrôle et un "acl=115" dans la zone rectangulaire Cisco/RADIUS où il indique la paire AV 009\001 (constructeur-particularité).

Sortie

L'utilisateur sortant « pixa » avec "acl=115" dans le profil authentifie et autorise. Le serveur passe en bas de l'acl=115 au PIX, et le PIX affiche ceci :

```
pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 2 user
'pixa' at 172.18.124.114, authenticated access-list 115 absolute timeout: 0:05:00 inactivity
timeout: 0:00:00
```

Quand les essais de « pixa » d'utilisateur à aller à 99.99.99.3 (ou n'importe quelle adresse IP exceptez 99.99.99.2, parce qu'il y a un implicite refusent), l'utilisateur voit ceci :

```
Error: acl authorization denied
```

Liste d'accès téléchargeable de nouvel Par-utilisateur avec la version 6.2

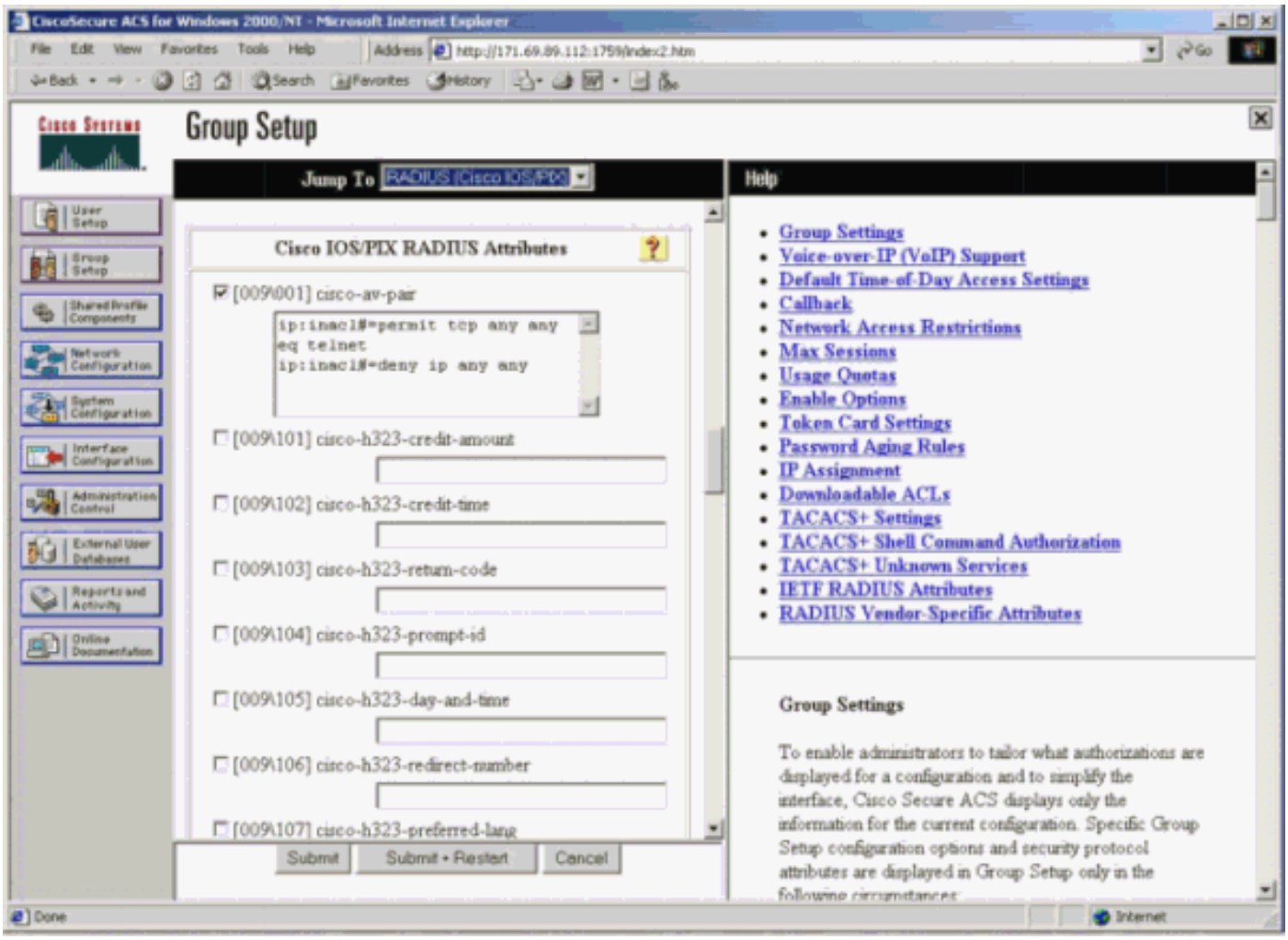
Dans la version de logiciel 6.2 et ultérieures du Pare-feu PIX, des Listes d'accès sont définies sur un serveur de contrôle d'accès (ACS) pour les télécharger au PIX après authentification. Ceci fonctionne seulement avec le protocole RADIUS. Il n'y a aucun besoin de configurer la liste d'accès sur le PIX elle-même. Un modèle de groupe est appliqué aux plusieurs utilisateurs.

Dans les versions antérieures, la liste d'accès est définie sur le PIX. Lors de l'authentification, l'ACS a poussé le nom de liste d'accès au PIX. La nouvelle version permet à l'ACS pour pousser la liste d'accès directement au PIX.

Remarque: Si le Basculement se produit, la table d'uauth n'est pas les utilisateurs copiés sont authentifiées à nouveau. La liste d'accès est téléchargée de nouveau.

Installation ACS

Cliquez sur le **Group Setup** et sélectionnez le type de périphérique de **RAYON (Cisco IOS/PIX)** pour installer un compte utilisateur. Générez un nom d'utilisateur (« cse », dans cet exemple) et le mot de passe pour l'utilisateur. De la liste d'attributs, sélectionnez l'option de configurer des constructeur-poids du commerce-**paires [009\001]**. Définissez la liste d'accès comme illustrée dans cet exemple :



Debugs PIX : Authentification valide et liste d'accès téléchargée

- Permet seulement le telnet et refuse l'autre trafic.

```
pix# 305011: Built dynamic TCP translation
from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside
```

```
302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```
Sortie de la commande d'**uauth d'exposition**.
```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated access-list AAA-user-cse absolute timeout:
0:05:00 inactivity timeout: 0:00:00
```
Sortie de la **commande access-list d'exposition**.
```
pix#show access-list access-list AAA-user-cse; 2 elements access-list AAA-user-cse permit tcp any any
eq telnet (hitcnt=1) access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Refuse seulement le telnet et permet l'autre trafic.
```
pix# 305011: Built dynamic TCP translation
from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```
Sortie de la commande d'**uauth d'exposition**.
```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In
Progress 0 1 user 'cse' at 172.16.171.33, authenticated access-list AAA-user-cse absolute
timeout: 0:05:00 inactivity timeout: 0:00:00
```
Sortie de la **commande access-list d'exposition**.
```
pix#show access-list access-list AAA-user-cse; 2 elements access-list AAA-user-
cse deny tcp any any eq telnet (hitcnt=1) access-list AAA-user-cse permit ip any any
(hitcnt=0)
```

Liste d'accès téléchargeable de nouvel Par-utilisateur utilisant ACS 3.0

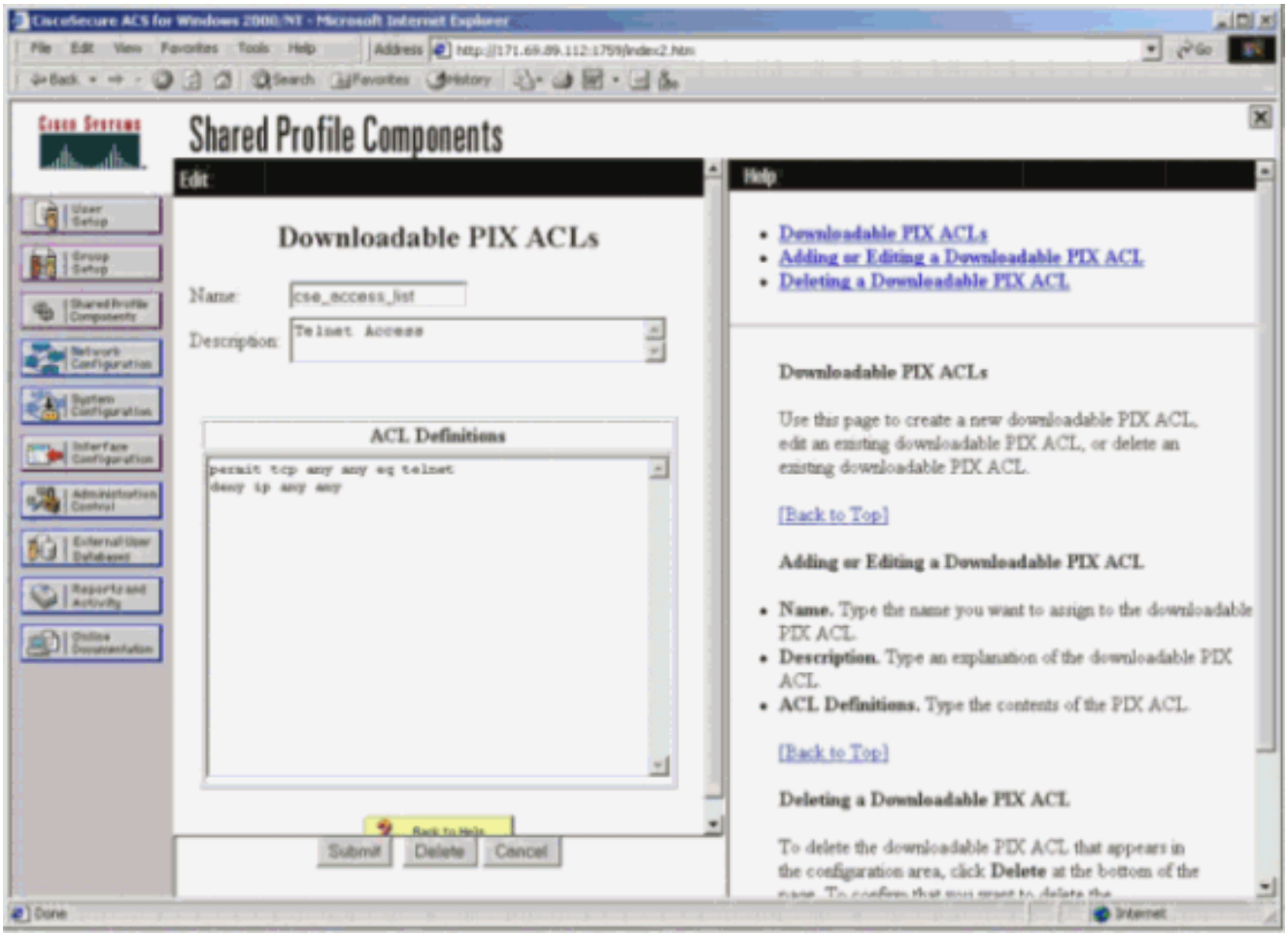
Dans la version 3.0 ACS, le composant partagé de profil permet à l'utilisateur pour créer un modèle de liste d'accès et pour définir le nom du modèle aux utilisateurs ou aux groupes spécifiques. Le nom du modèle peut être utilisé avec autant d'utilisateurs ou groupes comme nécessaire. Ceci élimine la nécessité de configurer les Listes d'accès identiques pour chaque utilisateur.

Remarque: Si le Basculement se produit, l'uauth n'est pas copié sur le PIX secondaire. Dans le basculement dynamique, la session est soutenue. Cependant, la nouvelle connexion doit être authentifiée à nouveau et la liste d'accès doit être téléchargée de nouveau.

Utilisant des profils partagés

Terminez-vous ces étapes quand vous utilisez des profils partagés.

1. **Configuration d'interface de** clic.
2. **Niveau utilisateur ACLs téléchargeable de** contrôle et/ou **niveau du groupe ACLs téléchargeable**.
3. Le clic **a partagé des composants de profil**. **Niveau utilisateur ACLs téléchargeable de** clic.
4. Définissez l'ACLs téléchargeable.
5. **Group Setup de** clic. Sous ACLs téléchargeable, assignez la liste d'accès PIX à la liste d'accès créée plus
   tôt.



[Debugs PIX : Authentification valide et liste d'accès téléchargée utilisant des profils partagés]

- Permet seulement le telnet et refuse l'autre trafic.`pix# 305011: Built dynamic TCP translation from inside:`
  `172.16.171.33/11065 to outside:172.16.171.201/1051`
  `109001: Auth start for user '???' from 172.16.171.33/11065 to`
  `172.16.171.202/23`
  `109011: Authen Session Start: user 'cse', sid 12`
  `109005: Authentication succeeded for user 'cse' from`
  `172.16.171.33/11065 to 172.16.171.202/23 on interface inside`
  `302013: Built outbound TCP connection 124 for outside:`
  `172.16.171.202/23 (172.16.171.202/23) to inside:`
  `172.16.171.33/11065 (172.16.171.201/1051) (cse)`Sortie de la commande d'**uauth d'exposition**.`pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user 'cse' at 172.16.171.33, authenticated access-list #ACSACL#-PIX-cse_access_list-3cff1bb3 absolute timeout: 0:05:00 inactivity timeout: 0:00:00 pix# 111009: User 'enable_15' executed cmd: show uauth pix#`Sortie de la **commande access-list d'exposition**.`pix#show access-list access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements access-list #ACSACL#-PIX-cse_access_list-3cff1bb3 permit tcp any any eq telnet (hitcnt=1) access-list #ACSACL#-PIX-cse_access_list-3cff1bb3 deny ip any any (hitcnt=0) pix# 111009: User 'enable_15' executed cmd: show access-list`
- Refuse seulement le telnet et permet l'autre trafic.`pix# 305011: Built dynamic TCP translation from inside:`
  `172.16.171.33/11066 to outside:172.16.171.201/1052`
  `109001: Auth start for user '???' from 172.16.171.33/11066 to`
  `172.16.171.202/23`
  `109011: Authen Session Start: user 'cse', sid 13`
  `109005: Authentication succeeded for user 'cse'`
  `from 172.16.171.33/11066`
  `to 172.16.171.202/23 on interface inside`

```
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```
Sortie de la commande d'**uauth d'exposition**.
```
pix#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00 inactivity timeout: 0:00:00 pix# 111009: User 'enable_15' executed
cmd: show uauth
```
Sortie de la **commande access-list d'exposition**.
```
pix#show access-list access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements access-list #ACSACL#-PIX-
cse_access_list-3cff1dd6 deny tcp any any eq telnet (hitcnt=1) access-list #ACSACL#-PIX-
cse_access_list-3cff1dd6 permit ip any any (hitcnt=0) pix# 111009: User 'enable_15' executed
cmd: show access-listpix#
```

Ajoutez la gestion des comptes

Configuration PIX - Ajoutez la comptabilité

TACACS (AuthInbound=tacacs)

Ajoutez cette commande.

aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

Ou employez la nouvelle caractéristique dans 5.2 pour définir ce qui doit être rendu compte par des Listes d'accès.

aaa accounting match 101 outside AuthInbound

Remarque: La liste d'accès 101 est définie séparément.

RAYON (AuthOutbound=radius)

Ajoutez cette commande.

aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

Ou employez la nouvelle caractéristique dans 5.2 pour définir ce qui doit être rendu compte par des Listes d'accès.

aaa accounting match 101 outside AuthOutbound

Remarque: La liste d'accès 101 est définie séparément.

Remarque: Des enregistrements des comptes peuvent être générés pour des sessions administratives sur le PIX à partir du code PIX 7.0.

Exemples de comptabilité

- Exemple de comptabilité TACACS pour le telnet de 99.99.99.2 dehors à 172.18.124.114 à l'intérieur (99.99.99.99).
```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
```

```
local_ip=172.18.124.114
cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- Exemple de comptabilisation RADIUS pour la connexion de 172.18.124.114 à l'intérieur à 99.99.99.2 en dehors de (telnet) et à 99.99.99.3 dehors (HTTP).

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Username = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
        Acct-Session-Id = 0x0000000a
        Username = cse
        Acct-Session-Time = 0
        Acct-Input-Octets = 1277
        Acct-Output-Octets = 310
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35949
        Vendor-Specific = Destination-IP=99.99.99.3
        Vendor-Specific = Destination-Port=80
```

Utilisation de la commande d'exclure

Dans ce réseau, si vous décidez qu'une source ou une destination particulière n'a pas besoin d'authentification, d'autorisation, ou de comptabilité, émettez ces commandes.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255 99.99.99.3
255.255.255.255 AuthInbound aaa authorization exclude telnet outside 172.18.124.114
255.255.255.255 99.99.99.3 255.255.255.255 AuthInbound aaa accounting exclude telnet outside
172.18.124.114 255.255.255.255 99.99.99.3 255.255.255.255 AuthInbound
```

Remarque: Vous avez déjà les commandes d'**inclusion**.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

Ou, avec la nouvelle configuration dans 5.2, définissez ce que vous voulez exclure.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet access-list 101 deny tcp
host 99.99.99.3 host 172.18.124.114 eq ftp access-list 101 deny tcp host 99.99.99.3 host
172.18.124.114 eq www access-list 101 permit tcp any any eq telnet access-list 101 permit tcp
any any eq www access-list 101 permit tcp any any eq ftp aaa authentication match 101 outside
AuthInbound aaa authorization match 101 outside AuthInbound aaa accounting match 101 outside
AuthInbound
```

Remarque: Si vous excluez une case de l'authentification et vous avez l'autorisation en fonction, vous devez également exclure la case de l'autorisation.

Maximum-sessions et affichage des utilisateurs connectés

Quelques serveurs TACACS+ et RADIUS ont des caractéristiques de « maximum-session » ou de « affichage des utilisateurs connectés ». La capacité de faire des maximum-sessions ou des utilisateurs connectés de contrôle dépend des enregistrements des comptes. Quand il y a un enregistrement de « début » de comptabilité généré mais aucun enregistrement de « arrêt », le serveur TACACS+ ou de RAYON suppose que la personne est encore ouverte une session (c'est-à-dire, l'utilisateur a une session par le PIX). Ceci fonctionne bien pour le telnet et les connexions FTP en raison de la nature des connexions. Cependant, ceci ne fonctionne pas bien pour le HTTP. Dans cet exemple, une configuration réseau différente est utilisée, mais les concepts sont identiques.

Telnets d'utilisateur par le PIX, authentifiant sur le chemin.

```
(pix) 109001: Auth start for user '???' from
        171.68.118.100/1200 to 9.9.9.25 /23
    (pix) 109011: Authen Session Start: user 'cse', Sid 3
    (pix) 109005: Authentication succeeded for user
        'cse' from 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 laddr
        171.68.118.100/1200 (cse)
    (server start account) Sun Nov 8 16:31:10 1998
        rtp-pinecone.rtp.cisco.com cse
        PIX 171.68.118.100 start task_id=0x3
        foreign_ip=9.9.9.25
        local_ip=171.68.118.100 cmd=telnet
```

Puisque le serveur n'a vu un enregistrement de « début » mais aucun enregistrement de « arrêt », en ce moment, le serveur prouve que l'utilisateur de « telnet » est ouvert une session. Si l'utilisateur tente une autre connexion qui exige l'authentification (peut-être d'un autre PC), et si des maximum-sessions est placées à "1" sur le serveur pour cet utilisateur (supposant le serveur prend en charge des maximum-sessions), la connexion est refusée par le serveur. L'utilisateur va environ leur telnet ou activités en FTP sur l'hôte de cible, puis les sorties (passe dix minutes là).

```
    (pix) 302002: Teardown TCP connection 5 faddr
```

```
     9.9.9.25/80 gaddr 9.9.9.10/128 1 laddr
     171.68.118.100/1281 duration 0:00:00 bytes
     1907 (cse)
(server stop account) Sun Nov 8 16:41:17 1998
     rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 stop task_id=0x3
     foreign_ip=9.9.9.25 local_ip=171.68.118.100
     cmd=telnet elapsed_time=5 bytes_in=98
     bytes_out=36
```

Si l'uauth est 0 (c'est-à-dire, authentifiez chaque fois) ou plus (authentifiez une fois et pas de nouveau au cours de la période uauth), un enregistrement des comptes est coupé pour chaque site accédé à.

Le HTTP fonctionne différemment en raison de la nature du protocole. Voici un exemple de HTTP où l'utilisateur parcourt de 171.68.118.100 à 9.9.9.25 par le PIX.

```
(pix) 109001: Auth start for user '???' from
    171.68.118.100/1281 to 9.9.9.25 /80
(pix) 109011: Authen Session Start: user 'cse', Sid 5
(pix) 109005: Authentication succeeded for user
    'cse' from 171.68.118.100/12 81 to 9.9.9.25/80
(pix) 302001: Built TCP connection 5 for faddr
    9.9.9.25/80 gaddr 9.9.9.10/12 81 laddr
    171.68.118.100/1281 (cse)
(server start account) Sun Nov 8 16:35:34 1998
    rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 start task_id=0x9
    foreign_ip=9.9.9.25 local_ip=171.68.118.100 cmd=http
(pix) 302002: Teardown TCP connection 5 faddr
    9.9.9.25/80 gaddr 9.9.9.10/128 1
laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35.35 1998
    rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9
    foreign_ip =9.9.9.25 local_ip=171.68.118.100
    cmd=http elapsed_time=0 bytes_ in=1907 bytes_out=223
```

L'utilisateur lit la page Web téléchargée. L'enregistrement de début est signalé à 16:35:34 et à l'enregistrement d'arrêt à 16:35:35. Ce téléchargement a pris une seconde (c'est-à-dire, il y avait moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur n'est pas ouvert une session au site Web. La connexion n'est pas ouverte quand l'utilisateur lit la page Web. les Maximum-sessions ou l'affichage des utilisateurs connectés ne fonctionnent pas ici. C'est parce que le temps de connexion (le temps entre « construit » et la « désinstallation ») dans le HTTP est trop court. L'enregistrement de « début » et de « arrêt » est fraction de seconde. Il n'y a aucun enregistrement de « début » sans enregistrement de « arrêt » puisque les enregistrements se produisent pratiquement au même instant. Il y a toujours un enregistrement de « début » et de « arrêt » envoyé au serveur pour chaque transaction si l'uauth est placé pour 0 ou quelque chose plus grande. Cependant, les maximum-sessions et l'affichage des utilisateurs connectés ne fonctionnent pas en raison de la nature de la connexion HTTP.

Interface utilisateur

Changez les invites utilisateur voient

Si vous avez la commande :

auth-prompt prompt PIX515B

alors les utilisateurs allant par le PIX voient cette demande.

```
PIX515B
```

Personnalisez les utilisateurs de message voient

Si vous avez les commandes :

```
auth-prompt accept "GOOD_AUTHENTICATION" auth-prompt reject "BAD_AUTHENTICATION"
```

alors les utilisateurs voient un message au sujet d'état d'authentification sur procédure de connexion défectueuse/réussie.

```
  PIX515B
  Username: junk Password: "BAD_AUTHENTICATION" PIX515B Username: cse Password:
"GOOD_AUTHENTICATION"
```

Inactif et temporisations absolues de Par-utilisateur

Les contrôles de commande d'**uauth de délai d'attente** PIX combien de fois la réauthentification est exigée. Si l'authentification/autorisation TACACS+ est allumée, ceci est contrôlé sur une base par utilisateur. Ce profil utilisateur est installé pour contrôler le délai d'attente (c'est sur le serveur de logiciel gratuit TACACS+ et les délais d'attente ont lieu en quelques minutes).

```
user = cse {
default service = permit
login = cleartext "csecse"
service = exec {
timeout = 2
idletime = 1
}
}
```

Après authentification/autorisation :

```
show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user 'cse' at
99.99.99.3, authorized to: port 172.18.124.114/telnet absolute timeout: 0:02:00 inactivity
timeout: 0:01:00
```

Àla fin de deux minutes :

Temporisation absolue - la session obtient démoli :

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

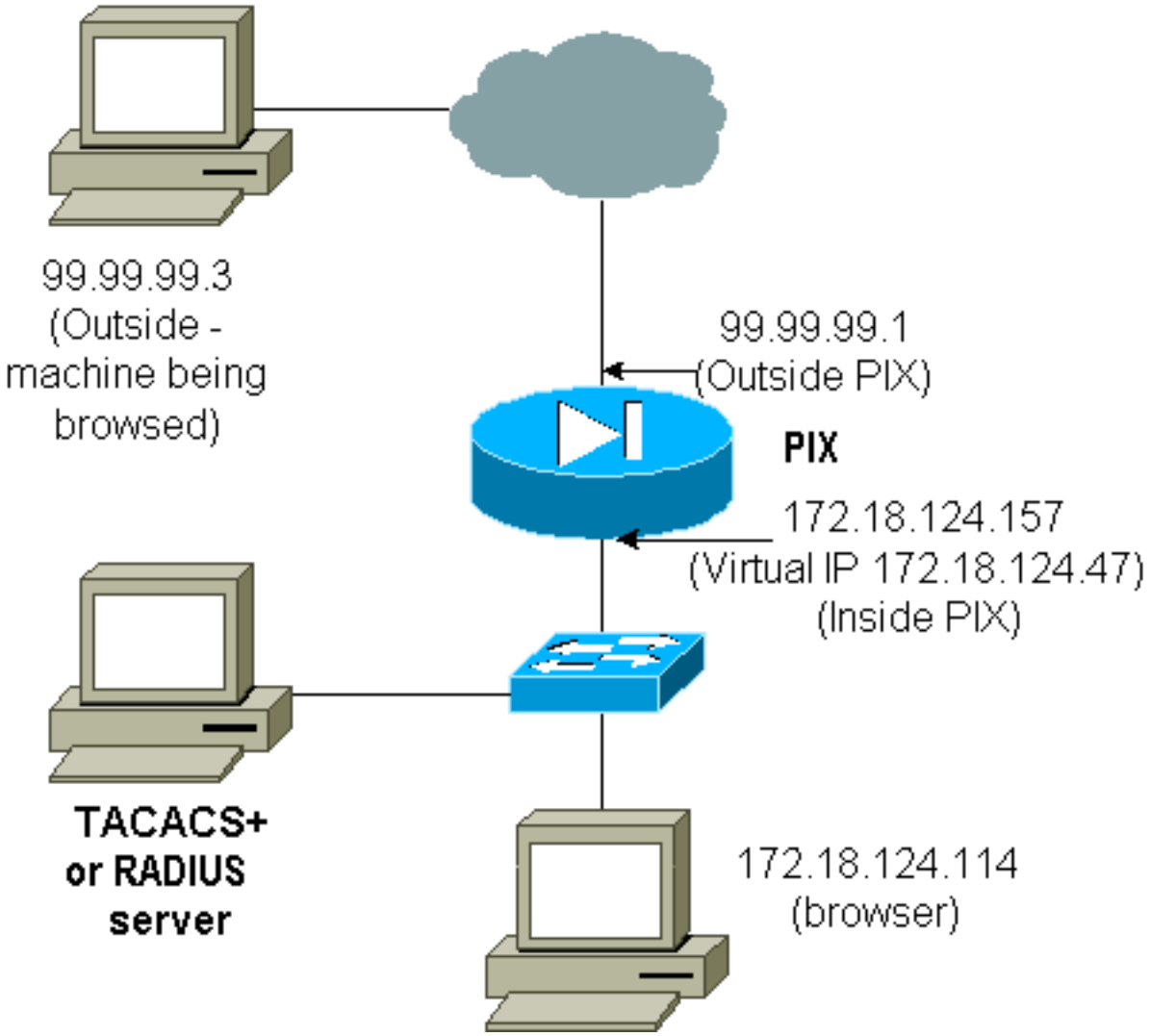
HTTP virtuel sortant

Si l'authentification est exigée sur des sites en dehors du PIX aussi bien que sur le PIX lui-même, on observe parfois le comportement du navigateur peu commun, puisque les navigateurs cachent le nom d'utilisateur et mot de passe.

Afin d'éviter ceci, implémentez le HTTP virtuel en ajoutant une adresse RFC 1918 (une adresse non-routable sur l'Internet, mais valide et seul pour le PIX à l'intérieur du réseau) à la configuration PIX dans le format.

virtual http #.#.#.# <warn>
Quand l'utilisateur essaye d'aller en dehors du PIX, l'authentification est exigée. Si le paramètre d'avertissement est présent, l'utilisateur reçoit un message de réorientation. L'authentification est bonne pour la durée dans l'uauth. Comme indiqué dans la documentation, ne placez pas la durée de commande d'**uauth de délai d'attente aux** secondes 0 avec le HTTP virtuel. Ceci empêche des connexions HTTP au vrai web server.

Remarque: Le HTTP virtuel et les adresses IP virtuelles de telnet doivent être inclus dans les **instuctions d'authentification d'AAA**. Dans cet exemple, spécifiant 0.0.0.0 inclut ces adresses.



Dans la configuration PIX ajoutez cette commande.

virtual http 172.18.124.47
L'utilisateur dirige le navigateur chez 99.99.99.3. Ce message est affiché.

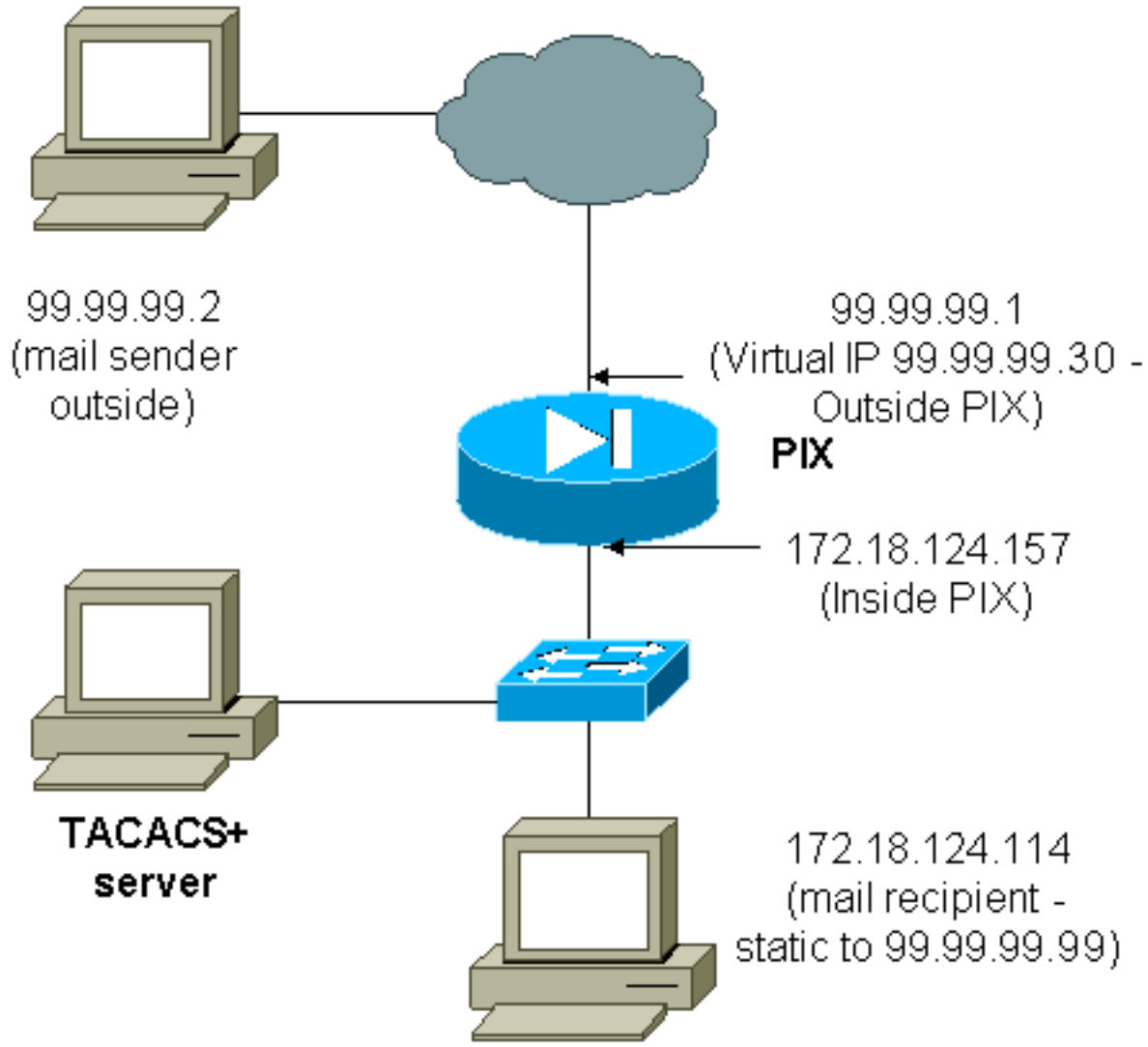
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Après authentification, le trafic est réorienté à 99.99.99.3.

Telnet virtuel

Remarque: Le HTTP virtuel et les adresses IP virtuelles de telnet doivent être inclus dans les **instuctions d'authentification d'AAA**. Dans cet exemple, spécifiant 0.0.0.0 inclut ces adresses.

Telnet virtuel d'arrivée



Ce n'est pas une excellente idée d'authentifier la messagerie d'arrivée puisqu'une fenêtre n'est pas affichée pour que la messagerie soit envoyée à d'arrivée. Utilisez la commande d'**exclure** à la place. Mais pour le but de l'illustration, ces commandes sont ajoutées.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the new
5.2 feature allows these !--- four statements to perform the same function. !--- Note: The old
and new verbiage should not be mixed. access-list 101 permit tcp any any eq smtp !--- The "mail"
was a Telnet to port 25. access-list 101 permit tcp any any eq telnet aaa authentication match
101 outside AuthInbound aaa authorization match 101 outside AuthInbound ! !--- plus ! virtual
telnet 99.99.99.30 static (inside,outside) 99.99.99.30 172.18.124.30 netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114 netmask 255.255.255.255 0 0 conduit permit
tcp host 99.99.99.30 eq telnet any conduit permit tcp host 99.99.99.99 eq telnet any conduit
permit tcp host 99.99.99.99 eq smtp any
```

Les utilisateurs (c'est logiciel gratuit TACACS+) :

```
user = cse {
default service = permit
login = cleartext "csecse"
}
```

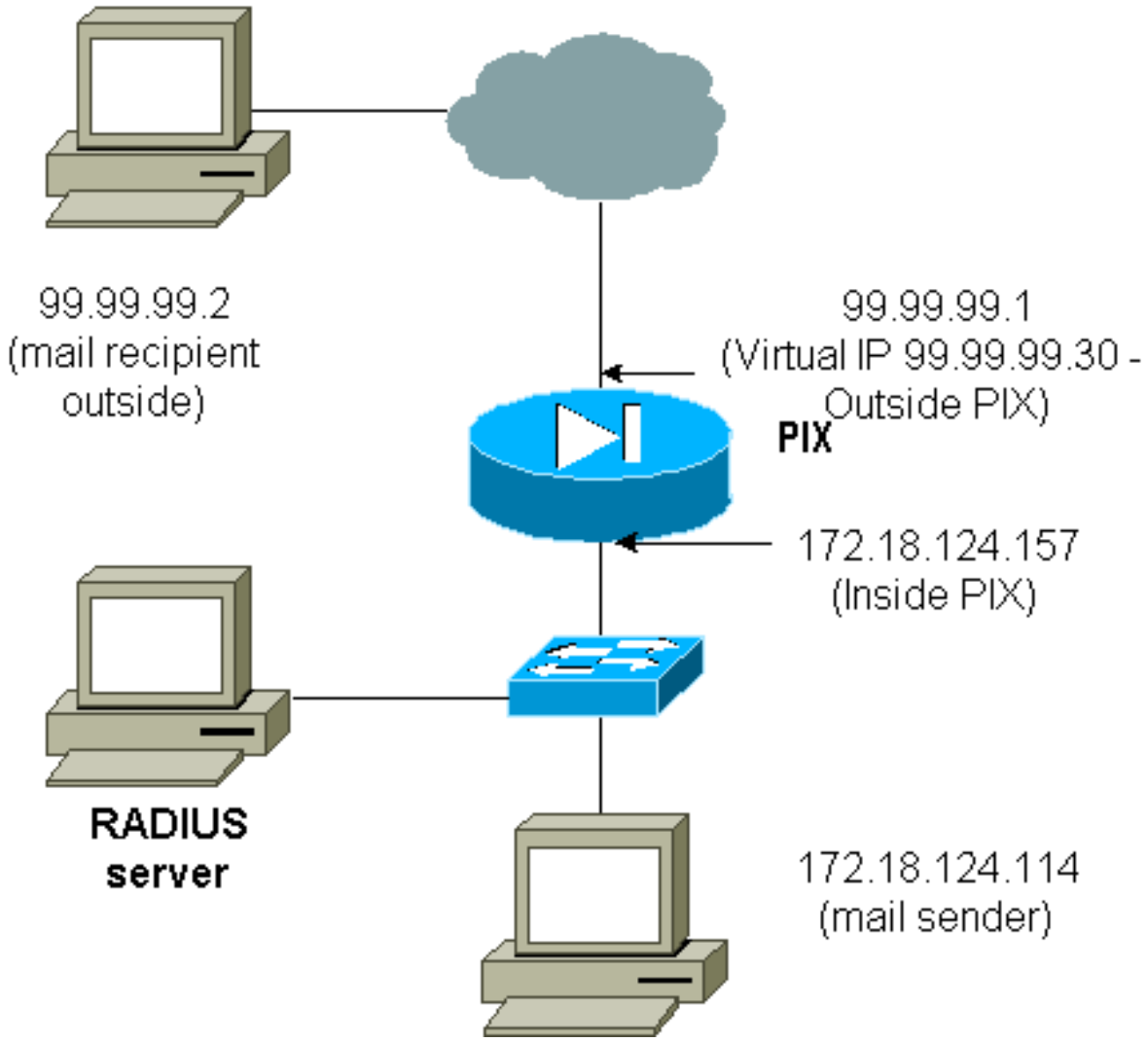
```
  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

Si seulement l'authentification est allumée, les deux utilisateurs envoient la messagerie d'arrivée après avoir authentifié sur un telnet à l'adresse IP 99.99.99.30. Si l'autorisation est activée, les telnets de « cse » d'utilisateur à 99.99.99.30, et entre dans le nom d'utilisateur/mot de passe TACACS+. Les baisses de connexion de telnet. L'utilisateur « cse » envoie alors la messagerie à 99.99.99.99 (172.18.124.114). L'authentification réussit pour l'utilisateur « pixuser ». Cependant, quand le PIX envoie la demande d'autorisation pour cmd=tcp/25 et cmd-arg=172.18.124.114, la demande échoue, suivant les indications de cette sortie.

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

pixfirewall#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11173 to 172.18.124.30/23 109011:
Authen Session Start: user 'cse', sid 10 109005: Authentication succeeded for user 'cse' from
99.99.99.2/23 to 172.18.124.30/11173 on interface outside 109011: Authen Session Start: user
'cse', sid 10 109007: Authorization permitted for user 'cse' from 99.99.99.2/11173 to
172.18.124.30/23 on interface outside 109001: Auth start for user 'cse' from 99.99.99.2/11174 to
172.18.124.114/25 109011: Authen Session Start: user 'cse', sid 10 109007: Authorization
permitted for user 'cse' from 99.99.99.2/11174 to 172.18.124.114/25 on interface outside 302001:
Built inbound TCP connection 5 for faddr 99.99.99.2/11174 gaddr 99.99.99.99/25 laddr
172.18.124.114/25 (cse) pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175 to
172.18.124.30/23 109011: Authen Session Start: user 'pixuser', sid 11 109005: Authentication
succeeded for user 'pixuser' from 99.99.99.2/23 to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11 109007: Authorization permitted for user
'pixuser' from 99.99.99.2/11175 to 172.18.124.30/23 on interface outside 109001: Auth start for
user 'pixuser' from 99.99.99.2/11176 to 172.18.124.114/25 109008: Authorization denied for user
'pixuser' from 99.99.99.2/25 to 172.18.124.114/11176 on interface outside
```

Telnet virtuel sortant



Ce n'est pas une excellente idée d'authentifier la messagerie d'arrivée puisqu'une fenêtre n'est pas affichée pour que la messagerie soit envoyée à d'arrivée. Utilisez la commande d'**exclure** à la place. Mais pour le but de l'illustration, ces commandes sont ajoutées.

Ce n'est pas une excellente idée d'authentifier la messagerie sortante puisqu'une fenêtre n'est pas affichée pour que la messagerie soit envoyée à sortant. Utilisez la commande d'**exclure** à la place. Mais aux fins de l'illustration, ces commandes sont ajoutées.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound !--- OR
the new 5.2 feature allows these three statements !--- to replace the previous statements. !---
Note: Do not mix the old and new verbiage. access-list 101 permit tcp any any eq smtp access-
list 101 permit tcp any any eq telnet aaa authentication match 101 inside AuthOutbound ! !---
plus ! virtual telnet 99.99.99.30 !--- The IP address on the outside of PIX is not used for
anything else.
```

Afin d'envoyer la messagerie de l'intérieur à dehors, apportez une invite de commande sur l'hôte de messagerie et le telnet à 99.99.99.30. Ceci ouvre le trou pour que la messagerie intervienne. La messagerie est envoyée de 172.18.124.114 à 99.99.99.2 :

```
305002: Translation built for gaddr 99.99.99.99
   to laddr 172.18.124.114
109001: Auth start for user '???' from
   172.18.124.114/32860 to 99.99.99.30/23
109011: Authen Session Start: user 'cse', Sid 14
109005: Authentication succeeded for user 'cse'
   from 172.18.124.114/32860 to    99.99.99.30/23
   on interface inside
```

```
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 172.18.124.114, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

Déconnexion virtuelle de Telnet

Quand le telnet d'utilisateurs à l'adresse IP virtuelle de telnet, la commande d'**uauth d'exposition** affiche le temps le trou est ouvert. Si les utilisateurs veulent empêcher le trafic d'aller après que leurs sessions soient de finition (quand le temps demeure dans l'uauth), elles ont besoin de telnet à l'adresse IP virtuelle de telnet de nouveau. Ceci bascule la session hors fonction. Ceci est montré par cet exemple.

La première authentification

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

Après la première authentification

```
pixfirewall#show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'cse' at 172.18.124.114, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

La deuxième authentification

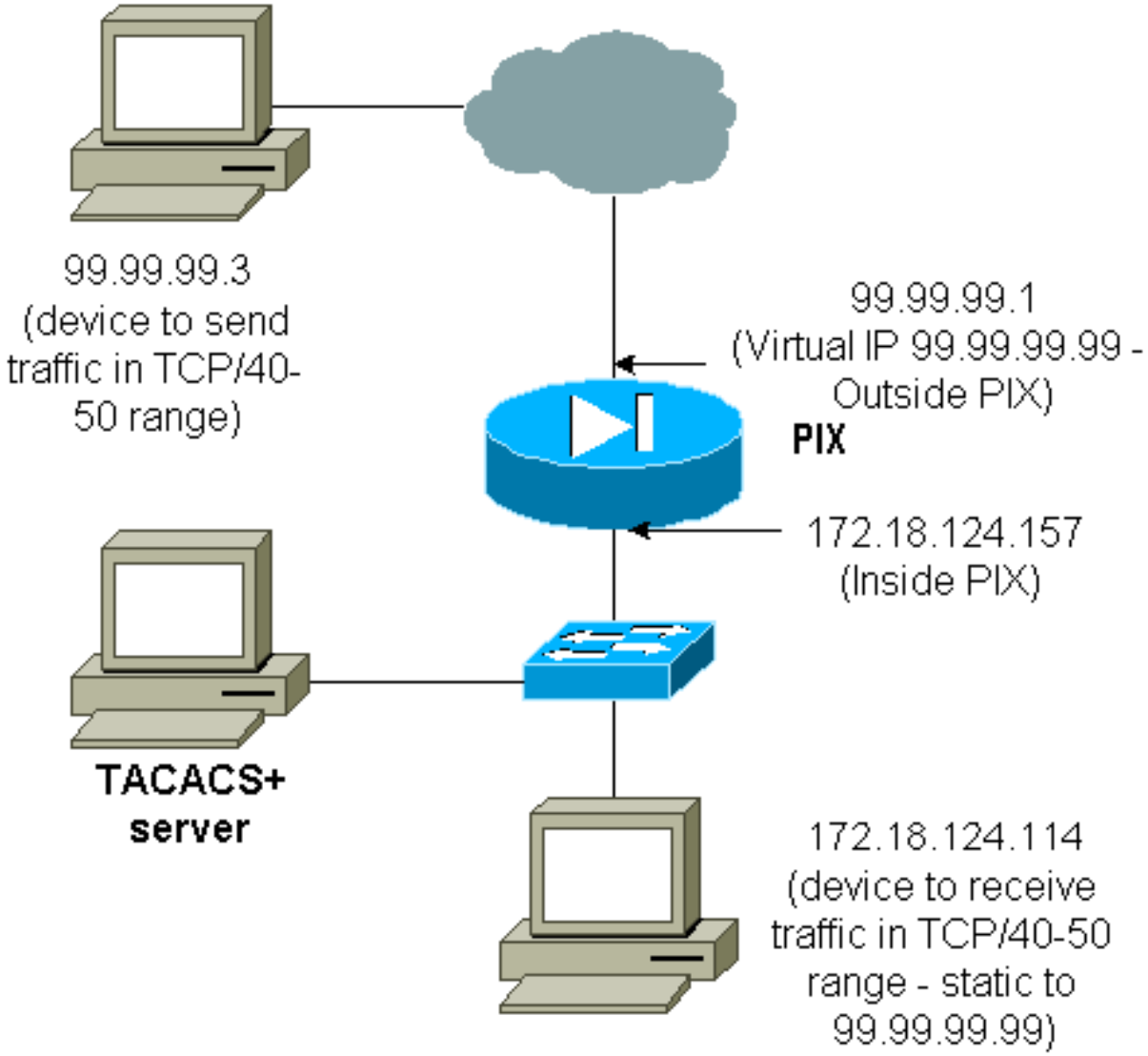
```
   pixfirewall#109001: Auth start for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse' from 172.18.124.114/32863 to 99.99.99.30/23 on
interface inside
```

Après la deuxième authentification

```
pixfirewall#show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

Autorisation sur le port

Diagramme du réseau



On permet l'autorisation pour des plages de port. Si le telnet virtuel est configuré sur le PIX, et l'autorisation est configurée pour une plage de port, l'utilisateur ouvre le trou avec le telnet virtuel. Puis, si l'autorisation pour une plage de port est allumée et le trafic dans cette plage frappe le PIX, le PIX envoie la commande au serveur TACACS+ pour l'autorisation. Cet exemple affiche l'autorisation en entrée sur une plage de port.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the new 5.2 feature allows these three statements !--- to perform the same function as the previous two statements. !--- Note: The old and new verbiage should not be mixed. access-list 116 permit tcp any any range 40 50 aaa authentication match 116 outside AuthInbound aaa authorization match 116 outside AuthInbound ! !--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114 netmask 255.255.255.255 0 0 conduit permit tcp any any virtual telnet 99.99.99.99
```

Exemple de configuration du serveur TACACS+ (logiciel gratuit) :

```
user = cse {
login = cleartext "numeric"
cmd = tcp/40-50 {
permit 172.18.124.114
}
}
```

L'utilisateur doit d'abord telnet à l'adresse IP virtuelle 99.99.99.99. Après authentification, quand des essais d'un utilisateur pour pousser le trafic TCP dans la plage du port 40-50 par le PIX à 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 est envoyés au serveur TACACS+ avec cmd-

arg=172.18.124.114 comme illustré ici :

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

AAA expliquant le trafic autre que le HTTP, le FTP, et le telnet

Après que vous veilliez les travaux virtuels de telnet pour permettre le trafic TCP/40-50 à l'hôte à l'intérieur du réseau, ajoutez expliquer ce trafic avec ces commandes.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound !--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement. !--- Note: Do not mix the old and new verbiage. aaa accounting match 116 outside AuthInbound access-list 116 permit ip any any
```

Exemple des enregistrements des comptes TACACS+

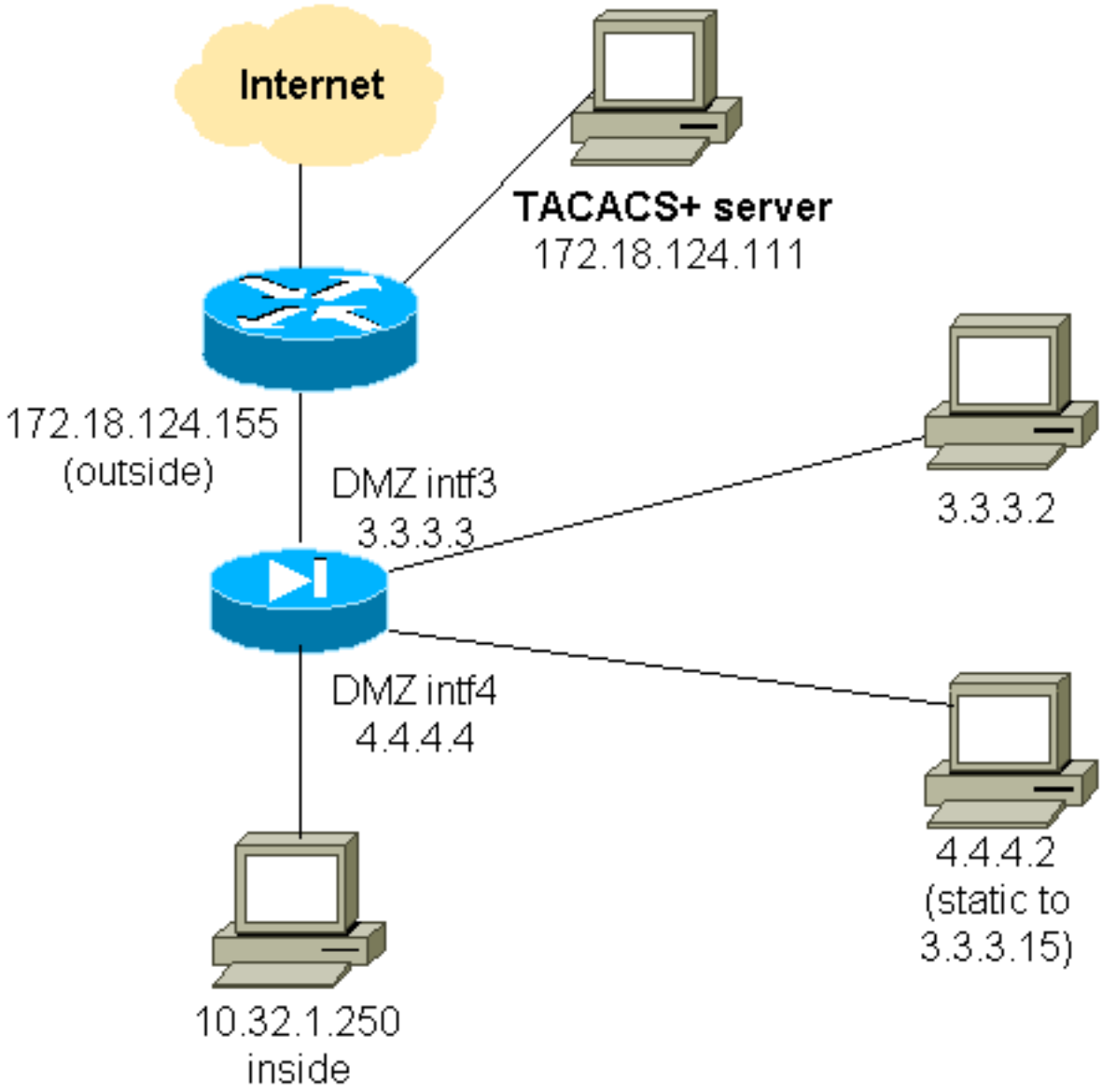
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

Authentification sur le DMZ

Afin d'authentifier les utilisateurs qui vont d'une interface DMZ à des autres, dites le PIX d'authentifier le trafic pour les interfaces Désignées. Sur le PIX, l'organisation est comme ceci :

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

Diagramme du réseau



Configuration partielle de PIX

Authentifiez le trafic de telnet entre pix/intf3 et pix/intf4, comme expliqué ici.

Configuration partielle de PIX
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2 pix/intf2 security10) nameif ethernet3 pix/intf3 security15 nameif ethernet4 pix/intf4 security20 (nameif ethernet5 pix/intf5 security25) interface ethernet0 auto interface ethernet1 auto (interface ethernet2 auto shutdown) interface ethernet3 auto interface ethernet4 auto (interface ethernet5 auto shutdown) ip address outside 172.18.124.155 255.255.255.0 ip address inside 10.32.1.250 255.255.255.0 **ip address pix/intf3 3.3.3.3 255.255.255.0 ip address pix/intf4 4.4.4.4 255.255.255.0 static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask 255.255.255.255 0 0 conduit permit tcp host 3.3.3.15 host 3.3.3.2 aaa-server xway protocol tacacs+ aaa-server**

```
xway (outside) host 172.18.124.111 timeout 5 aaa
authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0 255.255.255.0 3.3.3.0
255.255.255.0 xway aaa authentication include telnet
pix/intf3 4.4.4.0 255.255.255.0 3.3.3.0 255.255.255.0
3.3.3.0 255.255.255.0 xway !--- OR the new 5.2 feature
allows these four statements !--- to replace the
previous two statements. !--- Note: Do not mix the old
and new verbiage. access-list 103 permit tcp 3.3.3.0
255.255.255.0 4.4.4.0 255.255.255.0 eq telnet access-
list 104 permit tcp 4.4.4.0 255.255.255.0 3.3.3.0
255.255.255.0 eq telnet aaa authentication match 103
pix/intf3 xway aaa authentication match 104 pix/intf4
xway
```

Informations à collecter si vous ouvrez un dossier TAC

Si vous avez besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et voulez toujours ouvrir une valise avec Cisco TAC, soyez sûr d'inclure ces informations pour dépanner votre Pare-feu PIX.

- Description du problème et des détails topologiques pertinents
- Dépannage avant d'ouvrir le dossier
- Sortie de la commande **show tech-support**
- Sortie du **show log command** après que vous vous exécutiez avec la commande de **logging buffered debugging**, ou captures de console qui expliquent le problème (si disponible)

Attachez les données rassemblées à votre dossier dans un format de texte brut (.txt) non compressé. Reliez les informations dans votre cas en le téléchargeant à l'aide de la Case Query Tool (clients enregistrés seulement). Si vous ne pouvez pas accéder à la Case Query Tool, envoyez les informations dans une pièce jointe à un courriel à attach@cisco.com avec votre numéro de dossier dans le champ objet de votre message.

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Cisco Secure Access Control Server pour Windows
- Cisco Secure Access Control Server pour Unix
- Terminal Access Controller Access Control System
- Service RADIUS (Remote Authentication Dial-In User Service)
- Support et documentation techniques - Cisco Systems