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

Contenu

Introduction

L'authentification RADIUS et TACACS+ peut être effectuée pour les connexions FTP, Telnet et HTTP via le pare-feu Cisco Secure PIX Firewall. L'authentification pour d'autres protocoles moins courants est généralement faite pour fonctionner. L'autorisation TACACS+ est prise en charge. L'autorisation RADIUS n'est pas prise en charge. Les modifications dans l'authentification, l'autorisation et la comptabilité (AAA) PIX 5.2 par rapport à la version précédente incluent la prise en charge de la liste d'accès AAA pour contrôler qui est authentifié et quelles ressources l'utilisateur accède. Dans PIX 5.3 et versions ultérieures, l'authentification, l'autorisation et la comptabilité (AAA) changent par rapport aux versions antérieures du code, car les ports RADIUS sont configurables.

Remarque : PIX 6.x peut comptabiliser le trafic de transit mais pas le trafic destiné au PIX.

Conditions préalables

Conditions requises

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

Components Used

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

- Logiciel Cisco Secure PIX Firewall versions 5.2.0.205 et 5.2.0.207

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

Remarque : Si vous exécutez le logiciel PIX/ASA version 7.x et ultérieure, reportez-vous à Configuration des serveurs AAA et de 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 administration (AAA)

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

- L'authentification est l'utilisateur.
- L'autorisation est ce que fait l'utilisateur.
- L'authentification est valide sans autorisation.
- L'autorisation n'est pas valide sans authentification.
- La comptabilité est ce que l'utilisateur a fait.

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

Lorsque l'utilisateur tente de passer de l'intérieur à l'extérieur (ou vice versa) avec authentification/autorisation sur :

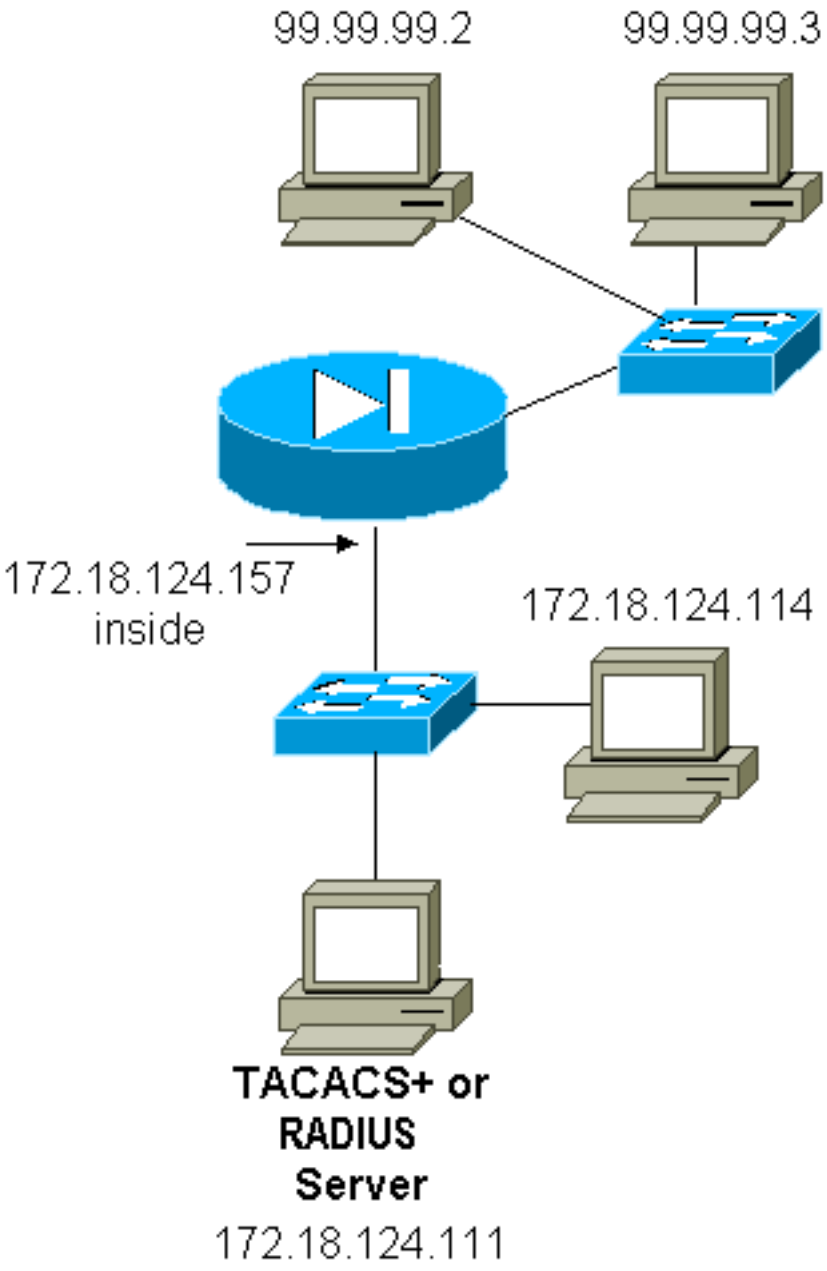
- **Telnet** : l'utilisateur voit apparaître une invite de nom d'utilisateur, puis une demande de mot de passe. Si l'authentification (et l'autorisation) réussit au niveau du PIX/serveur, l'utilisateur est invité à saisir le nom d'utilisateur et le mot de passe par l'hôte de destination au-delà.
- **FTP** : l'utilisateur voit apparaître une invite de nom d'utilisateur. L'utilisateur doit entrer "local_username@remote_username" pour le nom d'utilisateur et "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) réussit au niveau du PIX/serveur, les « remote_username » et « remote_password » sont transmis au serveur FTP de destination au-delà.
- **HTTP** : une fenêtre s'affiche dans le navigateur demandant le nom d'utilisateur et le mot de passe. Si l'authentification (et l'autorisation) aboutissent, l'utilisateur arrive sur le site Web de destination au-delà. Gardez à l'esprit que *les navigateurs mettent en cache les noms d'utilisateur et les mots de passe.* S'il apparaît que le PIX devrait expirer une connexion HTTP mais ne le fait pas, il est probable que la réauthentification a effectivement lieu avec le navigateur « filmer » le nom d'utilisateur et le mot de passe mis en cache au PIX. Le PIX le transfère au serveur d'authentification. PIX syslog et/ou debug serveur montre ce phénomène. Si Telnet et FTP semblent fonctionner « normalement », mais que les connexions HTTP ne fonctionnent pas, c'est la raison.

Étapes de débogage

- Assurez-vous que la configuration PIX fonctionne avant d'ajouter l'authentification et l'autorisation AAA. Si vous ne parvenez pas à transmettre le trafic avant d'instituer l'authentification et l'autorisation, vous ne pourrez pas le faire par la suite.
- Activez une sorte de connexion dans le PIX.Exécutez la commande **logging console debug** pour activer le débogage de la console de journalisation.**Remarque :** N'utilisez pas le débogage de la console de journalisation sur un système lourdement chargé.Utilisez la commande **logging monitor debug** pour enregistrer une session Telnet.La journalisation du débogage mis en mémoire tampon peut être utilisée, puis exécutez la commande **show logging**.La journalisation peut également être envoyée à un serveur syslog et examinée dans ce dernier.
- Activez le débogage sur les serveurs TACACS+ ou RADIUS.

Authentification uniquement

Diagramme du réseau



Configuration du serveur - Authentification uniquement

Configuration du serveur TACACS Cisco Secure UNIX

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

Configuration du serveur RADIUS Cisco Secure UNIX

Remarque : ajoutez l'adresse IP PIX et la clé à la liste Network Access Server (NAS) à l'aide de

l'interface utilisateur graphique avancée.

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

Cisco Secure Windows RADIUS

Suivez ces étapes pour configurer un serveur Cisco Secure Windows RADIUS.

1. Obtenez un mot de passe dans la section **Configuration utilisateur**.
2. Dans la section **Configuration du groupe**, définissez l'attribut 6 (Service-Type) sur **Connexion** ou **Administration**.
3. Ajoutez l'adresse IP PIX dans la section **Configuration NAS** de l'interface graphique utilisateur.

Cisco Secure Windows TACACS+

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

Configuration du serveur RADIUS de Livingston

Remarque : ajoutez l'adresse IP PIX et la clé au fichier *clients*.

- bill Password=« foo » User-Service-Type = Shell-User

Mériter la configuration du serveur RADIUS

Remarque : ajoutez l'adresse IP PIX et la clé au fichier *clients*.

- bill Password=« foo » Type de service = Shell-User

Configuration du serveur de logiciel gratuit TACACS+

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

Configuration initiale de PIX - Authentification uniquement

Configuration initiale de PIX - Authentification uniquement

```
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
```

Ports RADIUS configurables (5.3 et versions ultérieures)

Certains serveurs RADIUS utilisent des ports RADIUS autres que 1645/1646 (généralement 1812/1813). Dans PIX 5.3 et versions ultérieures, les ports d'authentification et de comptabilité RADIUS peuvent être changés en autre chose que le 1645/1646 par défaut avec les commandes suivantes :

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

Exemples de débogage d'authentification PIX

Reportez-vous à Étapes de débogage pour plus d'informations sur l'activation du débogage. Voici des exemples d'un utilisateur sur 99.99.99.2 qui initie le trafic vers l'intérieur de 172.18.124.114 (99.99.99.99) et vice versa. Le trafic entrant est authentifié TACACS et le trafic sortant est authentifié RADIUS.

Authentification réussie - TACACS+ (entrée)

```
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 échouée en raison d'un nom d'utilisateur/mot de passe incorrect - TACACS+ (entrant). L'utilisateur voit « Erreur : Nombre maximal de tentatives dépassé. »

```
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+ (entrant). L'utilisateur voit un nom d'utilisateur une fois et le PIX ne demande jamais de mot de passe (il s'agit de Telnet). L'utilisateur voit « Erreur : Nombre maximal de tentatives dépassé. »

```
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
```

Authentification correcte - RADIUS (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 incorrecte (nom d'utilisateur ou mot de passe) - RADIUS (sortant). L'utilisateur voit une demande de nom d'utilisateur, puis de mot de passe, a trois opportunités d'entrer ces informations, et si cela échoue, voir « Erreur : Nombre maximal de tentatives dépassé. »

```
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
```

Le serveur peut envoyer une requête ping mais le démon est désactivé, le serveur ne peut pas envoyer de requête ping ou la clé/le client ne correspond pas - ne communiquera pas avec PIX - RADIUS (sortant). L'utilisateur voit le nom d'utilisateur, puis le mot de passe, puis « Échec du serveur RADIUS », puis enfin « Erreur : Nombre maximal de tentatives dépassé. »

```
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 Autorisation

Si vous voulez autoriser tous les utilisateurs authentifiés à effectuer toutes les opérations (HTTP, FTP et Telnet) via le PIX, alors l'authentification est suffisante et l'autorisation n'est pas nécessaire. Cependant, si vous voulez autoriser certains sous-ensembles de services à certains utilisateurs ou limiter l'accès à certains sites, une autorisation est nécessaire. L'autorisation RADIUS n'est pas valide pour le trafic via le PIX. L'autorisation TACACS+ est valide dans ce cas.

Si l'authentification réussit et que l'autorisation est activée, le PIX envoie la commande que l'utilisateur fait au serveur. Par exemple, « http 1.2.3.4 ». Dans la version 5.2 de PIX, l'autorisation TACACS+ est utilisée en conjonction avec les listes d'accès pour contrôler où vont les utilisateurs.

Si vous souhaitez implémenter l'autorisation pour HTTP (sites Web visités), utilisez des logiciels tels que Websense, car un seul site Web peut avoir un grand nombre d'adresses IP associées.

Configuration du serveur - Authentification et autorisation

Configuration du serveur TACACS 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 .*
  }
  }
  }
```

Cisco Secure Windows TACACS+

Complétez ces étapes pour configurer un serveur Cisco Secure Windows TACACS+.

1. Cliquez sur **Refuser les commandes IOS sans correspondance** au bas de la configuration du groupe.
2. Cliquez sur **Add/Edit New Command (FTP, HTTP, Telnet)**.Par exemple, si vous voulez autoriser Telnet à un site spécifique (« telnet 1.2.3.4 »), la commande est **telnet**. L'argument est *1.2.3.4*. Après avoir rempli « command=**telnet**, » entrez la ou les adresses IP « permit » dans le rectangle de l'argument (par exemple, « permit 1.2.3.4 »). Si tous les Telnet doivent être autorisés, la commande est toujours **telnet**, mais cliquez sur **Autoriser tous les arguments non répertoriés**. Cliquez ensuite sur **Terminer la commande de modification**.
3. Exécutez l'étape 2 pour chacune des commandes autorisées (par exemple, Telnet, HTTP et FTP).
4. Ajoutez l'adresse IP PIX dans la section Configuration du NAS à l'aide de l'interface utilisateur graphique.

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 - Ajout d'autorisation

Ajouter des commandes pour demander une 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 fonctionnalité 5.2 permet à cette instruction, associée à la liste d'accès 101 précédemment définie, de remplacer les trois instructions précédentes. Le verbiage ancien et nouveau ne doit pas être mélangé.

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

Exemples de débogage d'authentification et d'autorisation PIX

Bonne authentification et autorisation réussie - 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)
```

Authentification correcte mais échec de l'autorisation - TACACS+. L'utilisateur voit également le message « Erreur : 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 fonction de liste d'accès

Dans le logiciel PIX version 5.2 et ultérieures, définissez les listes d'accès sur le PIX. Appliquez-les par utilisateur en fonction du profil utilisateur sur le serveur. TACACS+ nécessite une authentification et une autorisation. RADIUS nécessite une authentification uniquement. Dans cet exemple, l'authentification et l'autorisation sortantes vers TACACS+ sont modifiées . Une liste d'accès sur le PIX est configurée.

Remarque : dans PIX version 6.0.1 et ultérieure, si vous utilisez RADIUS, les listes d'accès sont implémentées en entrant la liste dans l'attribut RADIUS standard IETF 11 (Filter-Id) [CSCdt50422]. Dans cet exemple, l'attribut 11 est défini sur 115 au lieu de faire le verbiage « acl=115 » spécifique

au fournisseur.

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+ ne reconnaît pas le verbiage « acl ».

Configuration du serveur TACACS+ Cisco Secure UNIX

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

Cisco Secure Windows TACACS+

Afin d'ajouter l'autorisation au PIX pour contrôler où l'utilisateur va avec les listes d'accès, cochez **shell/exec**, cochez la case **Liste de contrôle d'accès** et indiquez le numéro (correspond au numéro de la liste d'accès sur le PIX).

Cisco Secure UNIX RADIUS

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

Cisco Secure Windows RADIUS

RADIUS/Cisco est le type de périphérique. L'utilisateur « pixa » a besoin d'un nom d'utilisateur, d'un mot de passe, d'une coche et d'une « acl=115 » dans la zone rectangulaire Cisco/RADIUS où il est indiqué 009\001 AV-Pair (spécifique au fournisseur).

Sortie

L'utilisateur sortant « pixa » avec « acl=115 » dans le profil authentifie et autorise. Le serveur

transmet 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
```

Lorsque l'utilisateur « pixa » tente d'accéder à 99.99.99.3 (ou toute adresse IP sauf 99.99.99.2, car il existe un refus implicite), l'utilisateur voit ceci :

```
Error: acl authorization denied
```

Nouvelle Liste D'Accès Téléchargeable Par Utilisateur Avec La Version 6.2

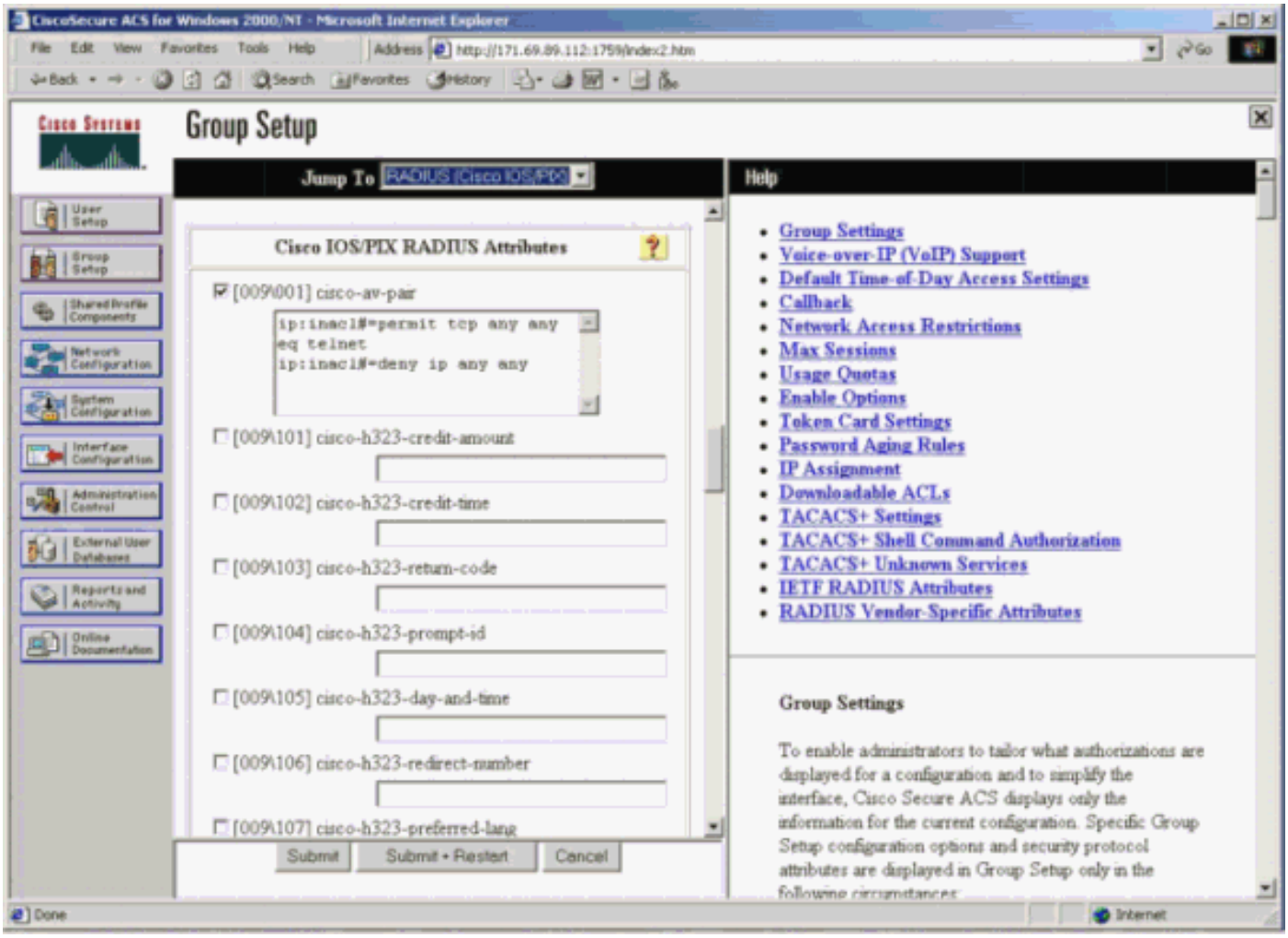
Dans les versions 6.2 et ultérieures du pare-feu PIX, les listes d'accès sont définies sur un serveur de contrôle d'accès (ACS) à télécharger sur le PIX après authentification. Cela fonctionne uniquement avec le protocole RADIUS. Il n'est pas nécessaire de configurer la liste d'accès sur le PIX lui-même. Un modèle de groupe est appliqué à plusieurs utilisateurs.

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

Remarque : si le basculement se produit, la table uauth n'est pas copiée Les utilisateurs sont réauthentifiés. La liste d'accès est téléchargée à nouveau.

Configuration ACS

Cliquez sur **Group Setup** et sélectionnez le type de périphérique **RADIUS (Cisco IOS/PIX)** pour configurer un compte d'utilisateur. Attribuez un nom d'utilisateur (« cse », dans cet exemple) et un mot de passe à l'utilisateur. Dans la liste Attributs, sélectionnez l'option à configurer **[009\001]** ***fournisseur-av*-pair**. Définissez la liste de contrôle d'accès comme illustré dans cet exemple :



Débogues PIX : Authentification valide et liste d'accès téléchargée

- Autorise uniquement Telnet et refuse tout 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 **show uauth**.

```
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 **show access-list**.

```
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)
```

- Refuser uniquement Telnet et autoriser d’autres trafics.

```
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 **show uauth**.

```
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 **show access-list**.

```
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)
```

Nouvelle liste d'accès téléchargeable par utilisateur utilisant ACS 3.0

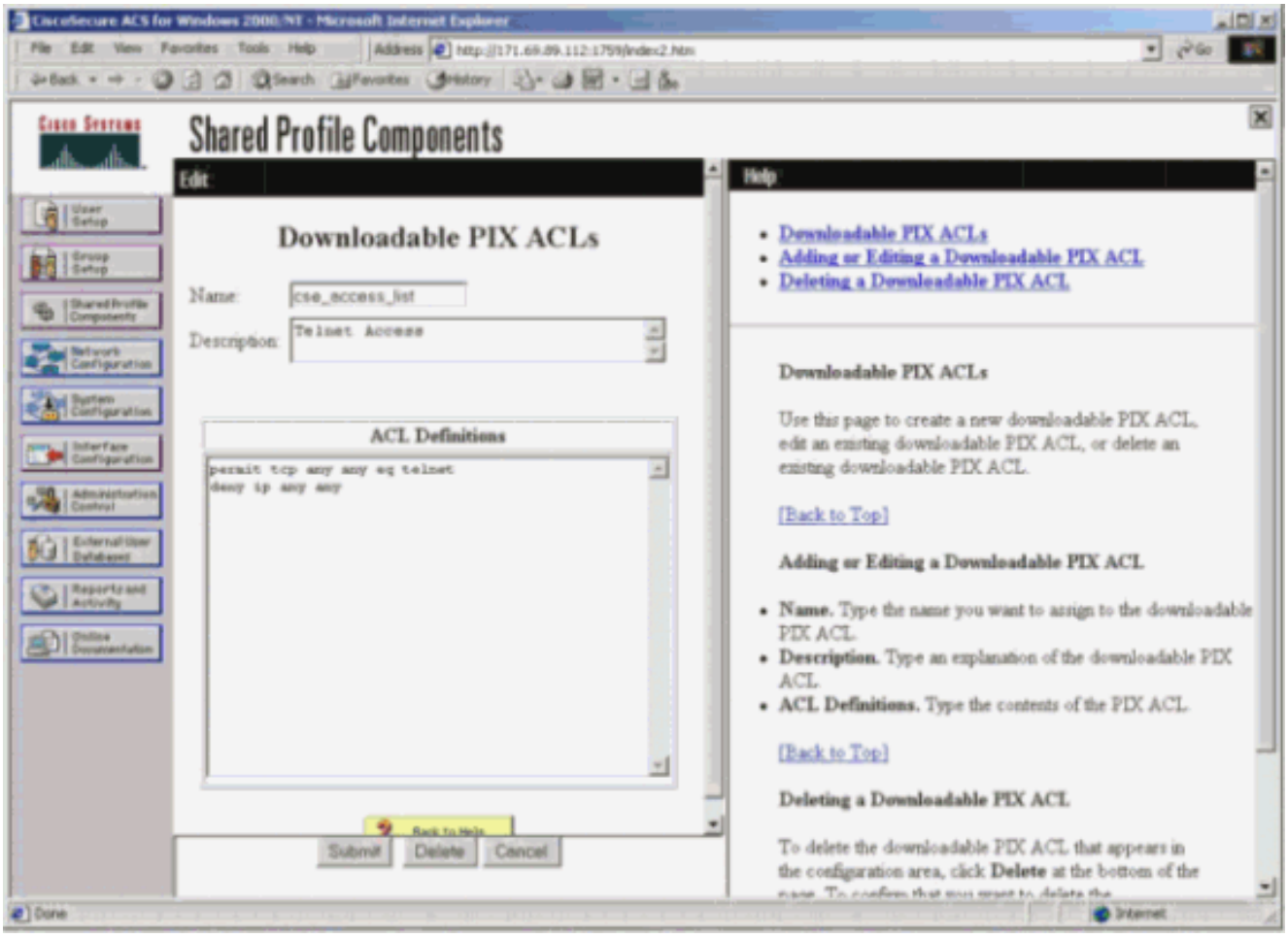
Dans ACS version 3.0, le composant de profil partagé permet à l'utilisateur de créer un modèle de liste d'accès et de définir le nom du modèle pour des utilisateurs ou des groupes spécifiques. Le nom du modèle peut être utilisé avec autant d'utilisateurs ou de groupes que nécessaire. Cela élimine la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

Remarque : si le basculement se produit, uauth n'est pas copié dans le PIX secondaire. Dans le basculement dynamique, la session est maintenue. Cependant, la nouvelle connexion doit être réauthentifiée et la liste d’accès doit être téléchargée à nouveau.

Utilisation de profils partagés

Complétez ces étapes lorsque vous utilisez des profils partagés.

1. Cliquez sur **Configuration de l'interface**.
2. Vérifiez les **listes de contrôle d'accès téléchargeables au niveau de l'utilisateur** et/ou les **listes de contrôle d'accès téléchargeables au niveau du groupe**.
3. Cliquez sur **Composants de profil partagé**. Cliquez sur **ACL téléchargeables au niveau de l'utilisateur**.
4. Définissez les listes de contrôle d’accès téléchargeables.
5. Cliquez sur **Configuration du groupe**. Sous Listes de contrôle d'accès téléchargeables, affectez la liste d'accès PIX à la liste d'accès créée précédemment.



[Débogues PIX : Authentification valide et liste d'accès téléchargée à l'aide de profils partagés]

- Autorise uniquement Telnet et refuse tout 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 **show uauth**.

```
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 **show access-list**.

```
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
```

- Refuser uniquement Telnet et autoriser d'autres trafics.

```
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 **show uauth**.

```
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 **show access-list**.

```
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 - Ajouter une 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 utilisez la nouvelle fonctionnalité de la version 5.2 pour définir ce qui doit être pris en compte par les listes de contrôle d'accès.

```
aaa accounting match 101 outside AuthInbound
```

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

RADIUS (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 utilisez la nouvelle fonctionnalité de la version 5.2 pour définir ce qui doit être pris en compte par les listes de contrôle d'accès.

```
aaa accounting match 101 outside AuthOutbound
```

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

Note : Les enregistrements comptables peuvent être générés pour les sessions administratives sur PIX à partir du code PIX 7.0.

Exemples de comptabilité

- Exemple de comptabilisation TACACS pour Telnet de 99.99.99.2 en dehors à 172.18.124.114 en 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 vers 99.99.99.2 à l'extérieur (Telnet) et 99.99.99.3 à l'extérieur (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'exclusion

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 disposez déjà des commandes **include**.

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

Ou, avec la nouvelle fonctionnalité de la version 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 que vous avez l'autorisation, vous devez également exclure cette case de l'autorisation.

Nombre maximal de sessions et affichage des utilisateurs connectés

Certains serveurs TACACS+ et RADIUS ont des fonctionnalités « max-session » ou « view logging users ». La possibilité d'effectuer des sessions max ou d'enregistrer des utilisateurs connectés dépend des enregistrements comptables. Lorsqu'un enregistrement de début de compte est généré mais qu'aucun enregistrement de fin de compte n'est généré, le serveur TACACS+ ou RADIUS suppose que la personne est toujours connectée (c'est-à-dire que l'utilisateur a une session via PIX). Cela fonctionne bien pour les connexions Telnet et FTP en raison de la nature des connexions. Cependant, cela ne fonctionne pas bien pour HTTP. Dans cet exemple, une configuration réseau différente est utilisée, mais les concepts sont identiques.

L'utilisateur établit une connexion Telnet via le PIX, en s'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
```

Comme le serveur a vu un enregistrement « start » mais pas « stop », à ce stade, le serveur indique que l'utilisateur « Telnet » est connecté. Si l'utilisateur tente une autre connexion qui nécessite une authentification (peut-être depuis un autre PC), et si max-sessions est défini sur « 1 » sur le serveur pour cet utilisateur (en supposant que le serveur prend en charge max-sessions), la connexion est refusée par le serveur. L'utilisateur effectue son activité Telnet ou FTP sur l'hôte cible, puis quitte (y passe dix minutes).

```
    (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
```

Que uauth soit 0 (c'est-à-dire, authentifier à chaque fois) ou plus (authentifier une fois et pas à nouveau au cours de la période uauth), un enregistrement comptable est coupé pour chaque site accessible.

HTTP fonctionne différemment en raison de la nature du protocole. Voici un exemple de HTTP où l'utilisateur navigue de 171.68.118.100 à 9.9.9.25 via 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 affiché à 16:35:34 et l'enregistrement d'arrêt à 16:35:35. Ce téléchargement a pris une seconde (c'est-à-dire qu'il y avait moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur n'est pas connecté au site Web. La connexion n'est pas ouverte lorsque l'utilisateur lit la page Web. Le nombre maximal de sessions ou l'affichage des utilisateurs connectés ne fonctionne pas ici. Ceci est dû au fait que le temps de connexion (le temps entre le « Conçu » et le « Teardown ») dans HTTP est trop court. Les enregistrements « start » et « stop » sont en moins d'une seconde. Il n'y a pas d'enregistrement « de début » sans enregistrement « d'arrêt » puisque les enregistrements ont lieu pratiquement au même moment. Il reste un enregistrement « start » et « stop » envoyé au serveur pour chaque transaction, que uauth soit défini sur 0 ou quelque chose de plus grand. Cependant, les utilisateurs connectés à max-sessions et à view ne fonctionnent pas en raison de la nature des connexions HTTP.

Interface utilisateur

Modifier l'invite Utilisateurs Voir

Si vous avez la commande :

```
auth-prompt prompt PIX515B
```

ensuite, les utilisateurs passant par le PIX voient cette invite.

```
PIX515B
```

Personnaliser le message Utilisateurs Voir

Si vous disposez des commandes suivantes :

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

les utilisateurs voient ensuite un message sur l'état de l'authentification lors d'une connexion échouée/réussie.

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

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

Délais d'inactivité et d'abandon par utilisateur

La commande **timeout uauth** PIX contrôle la fréquence à laquelle une réauthentification est requise. Si l'authentification/autorisation TACACS+ est activée, elle est contrôlée par utilisateur. Ce profil utilisateur est configuré pour contrôler le délai d'attente (il se trouve sur le serveur gratuit TACACS+ et les délais d'attente sont en 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
```

Au bout de deux minutes :

Délai d'attente absolu : la session est désactivée :

```
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

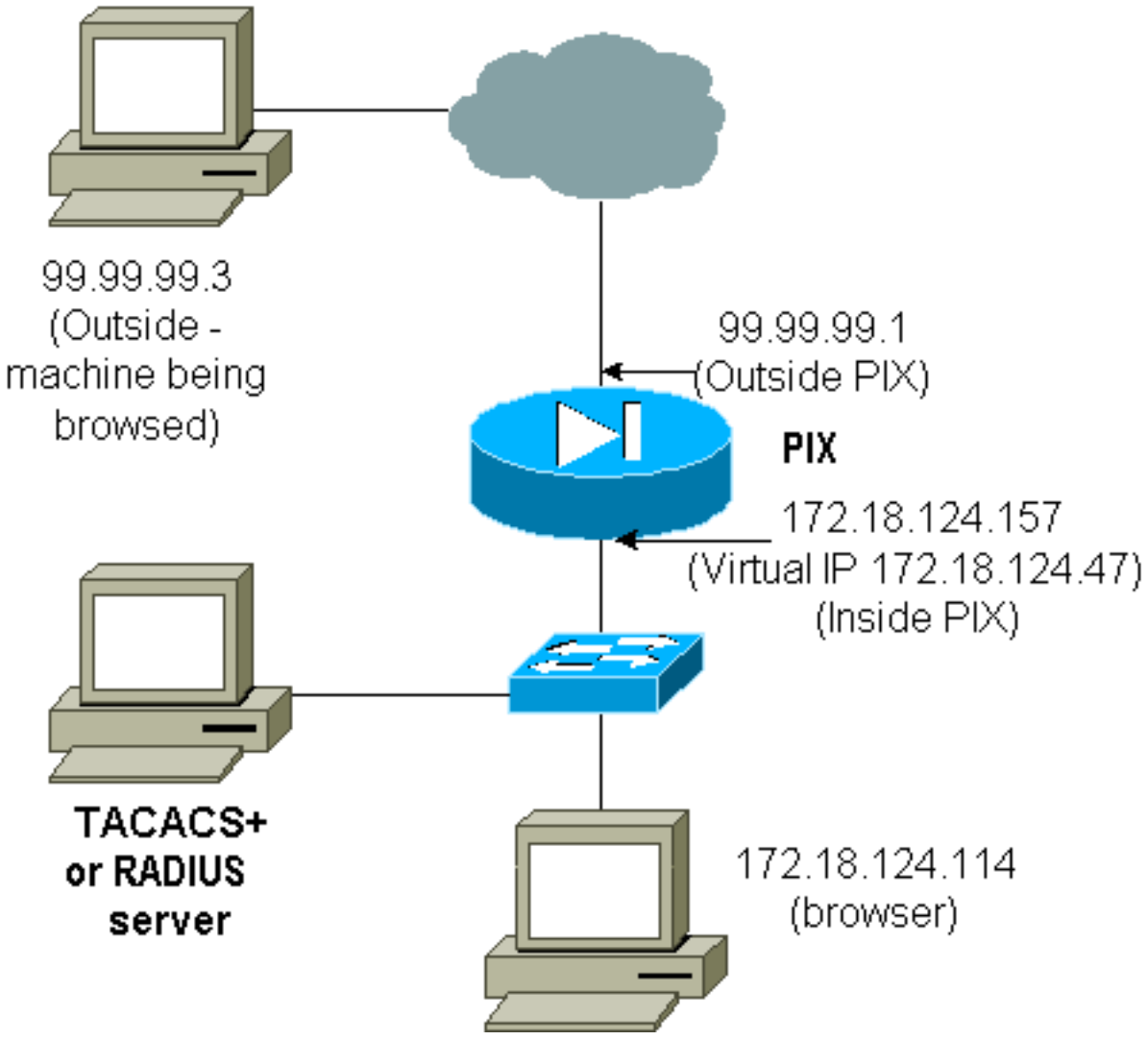
Si l'authentification est requise sur les sites en dehors du PIX ainsi que sur le PIX lui-même, le comportement inhabituel du navigateur est parfois observé, puisque les navigateurs mettent en cache le nom d'utilisateur et le mot de passe.

Afin d'éviter cela, mettez en oeuvre le protocole HTTP virtuel en ajoutant une adresse RFC 1918 (une adresse non routable sur Internet, mais valide et unique pour le réseau interne PIX) à la configuration PIX au format.

```
virtual http #.#.#.#
```

Lorsque l'utilisateur tente d'aller en dehors du PIX, l'authentification est requise. Si le paramètre d'avertissement est présent, l'utilisateur reçoit un message de redirection. L'authentification est correcte pour la durée de la requête. Comme indiqué dans la documentation, ne définissez pas la durée de la commande **timeout uauth** sur 0 seconde avec HTTP virtuel. Cela empêche les connexions HTTP au serveur Web réel.

Remarque : Les adresses IP HTTP et Telnet virtuelles doivent être incluses dans les instructions **d'authentification aaa**. Dans cet exemple, la spécification 0.0.0.0 inclut ces adresses.



Dans la configuration PIX, ajoutez cette commande.

```
virtual http 172.18.124.47
```

L'utilisateur pointe le navigateur sur 99.99.99.3. Ce message s'affiche.

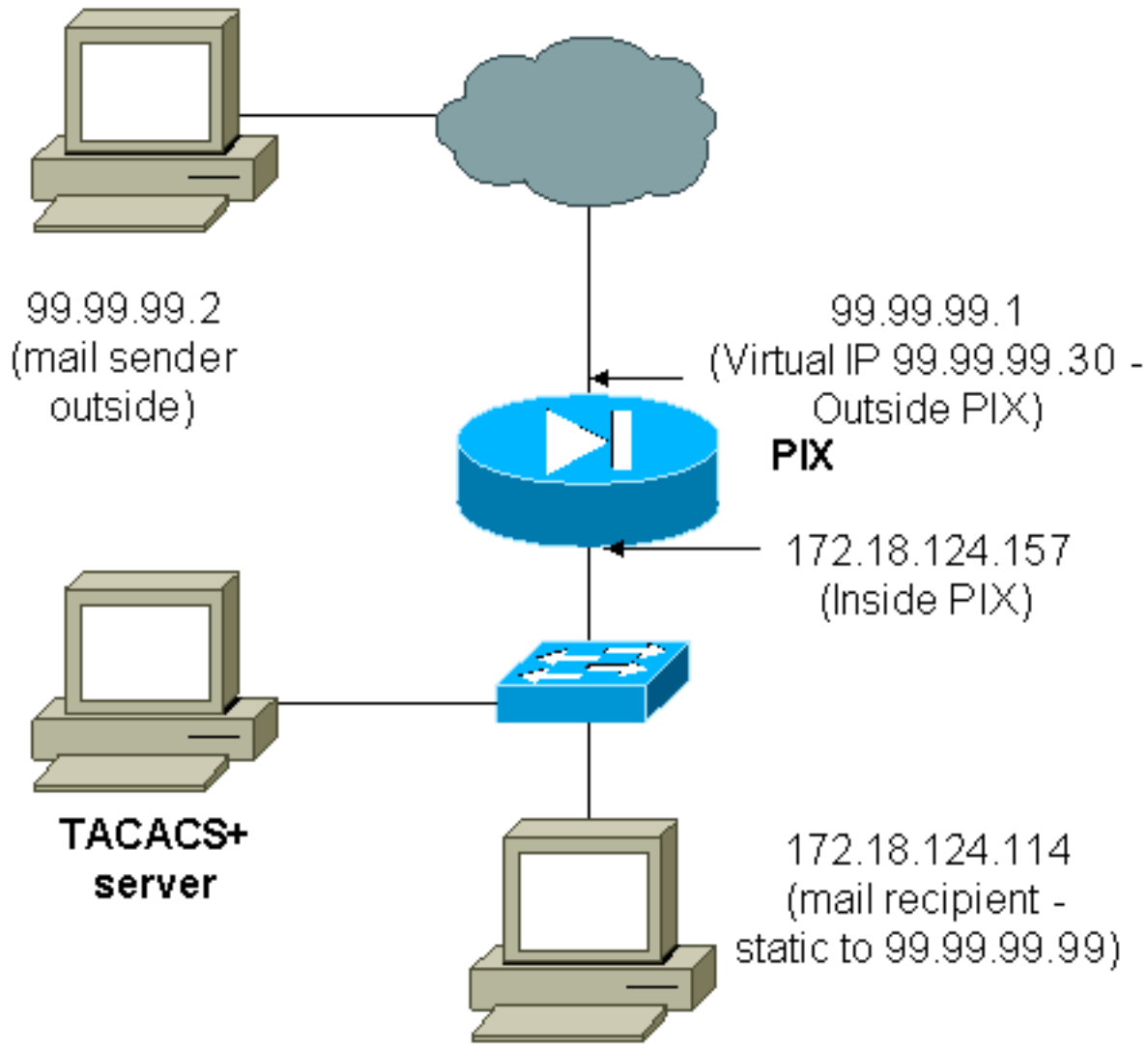
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

Après authentification, le trafic est redirigé vers 99.99.99.3.

Telnet virtuel

Remarque : Les adresses IP HTTP et Telnet virtuelles doivent être incluses dans les instructions **d'authentification aaa**. Dans cet exemple, la spécification 0.0.0.0 inclut ces adresses.

Entrant Virtual Telnet



Il n'est pas recommandé d'authentifier le courrier entrant car une fenêtre ne s'affiche pas pour que le courrier entrant soit envoyé. Utilisez la commande **exclure** à la place. Mais à titre d'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
```

Utilisateurs (il s'agit du logiciel gratuit TACACS+) :

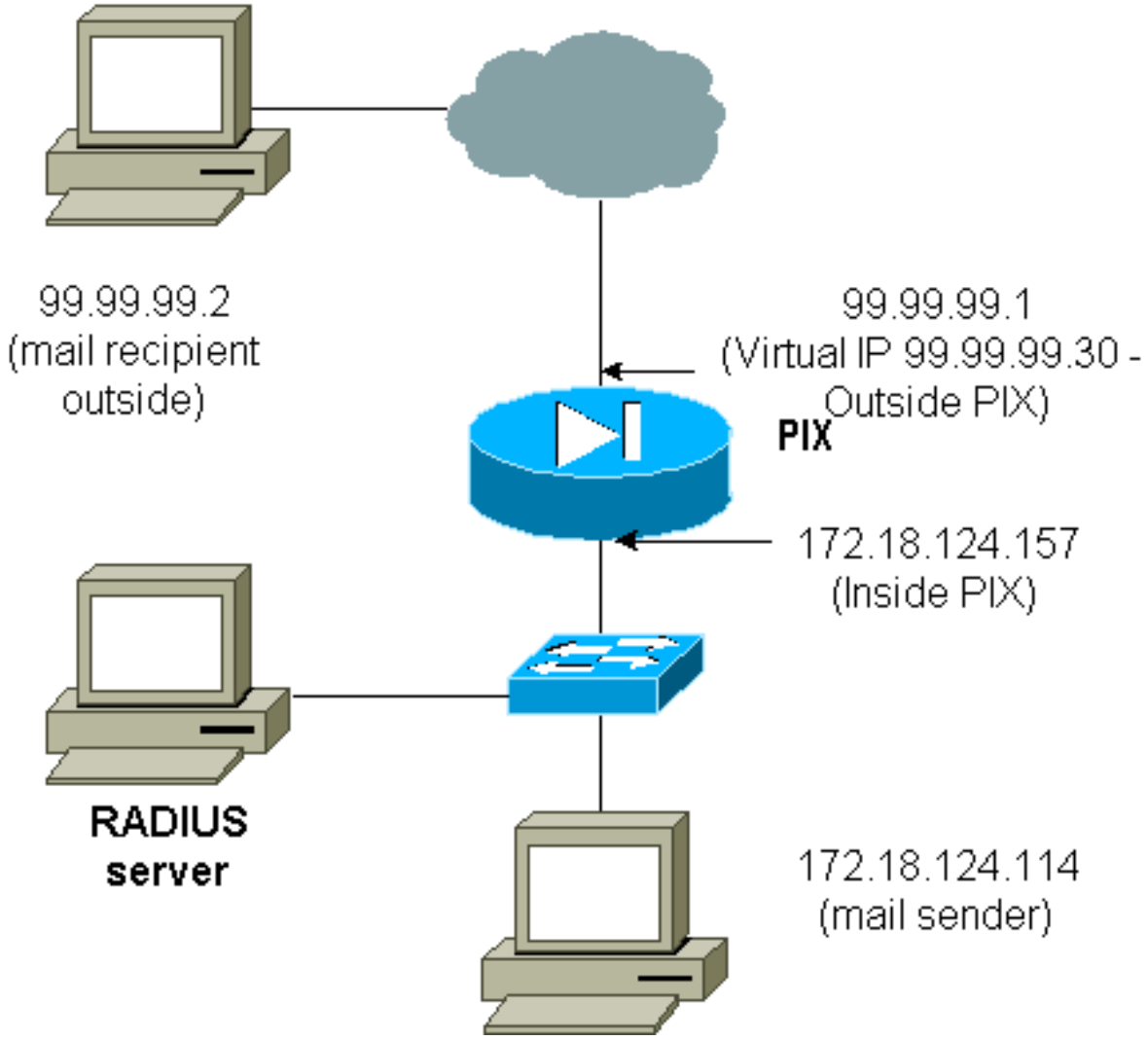
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


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

Si seule l'authentification est activée, les deux utilisateurs envoient du courrier entrant après l'authentification sur une adresse Telnet vers IP 99.99.99.30. Si l'autorisation est activée, l'utilisateur « cse » envoie une requête Telnet vers 99.99.99.30 et entre le nom d'utilisateur/mot de passe TACACS+. La connexion Telnet est interrompue. L'utilisateur « cse » envoie ensuite un message à 99.99.99.99 (172.18.124.114). L'authentification réussit pour l'utilisateur « pixuser ». Cependant, lorsque le PIX envoie la demande d'autorisation pour cmd=tcp/25 et cmd-arg=172.18.124.114, la demande échoue, comme indiqué dans 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



Il n'est pas recommandé d'authentifier le courrier entrant car une fenêtre ne s'affiche pas pour que le courrier entrant soit envoyé. Utilisez la commande **exclure** à la place. Mais à titre d'illustration, ces commandes sont ajoutées.

Il n'est pas recommandé d'authentifier les messages sortants car une fenêtre ne s'affiche pas pour que les messages sortants soient envoyés. Utilisez la commande **exclure** à la place. Mais à titre d'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 du courrier de l'intérieur vers l'extérieur, affichez une invite de commande sur l'hôte de messagerie et Telnet vers 99.99.99.30. Cela ouvre le trou que doit traverser le courrier. Le courrier est envoyé 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

Lorsque les utilisateurs établissent une connexion Telnet avec l'adresse IP Telnet virtuelle, la commande **show uauth** affiche l'heure à laquelle le trou est ouvert. Si les utilisateurs veulent empêcher le trafic de passer après la fin de leurs sessions (lorsque le temps reste dans la file d'attente), ils doivent à nouveau établir une connexion Telnet avec l'adresse IP Telnet virtuelle. Cette opération annule la session. Ceci est illustré par cet exemple.

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
```

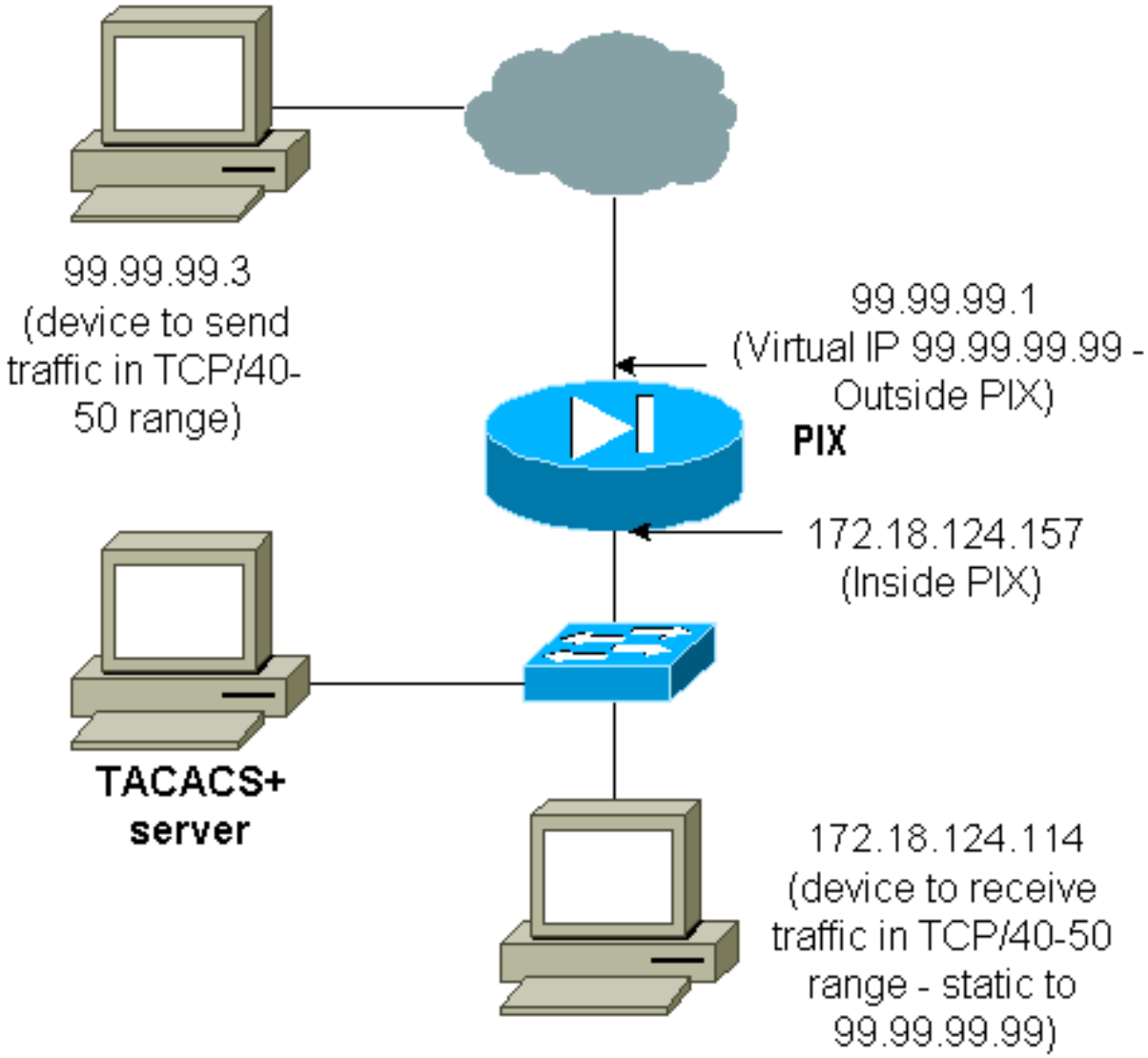
Après la deuxième authentification

```
pixfirewall#show uauth
```

```
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

Autorisation de port

Diagramme du réseau



L'autorisation est autorisée pour les plages de ports. Si Virtual Telnet est configuré sur le PIX et que l'autorisation est configurée pour une plage de ports, l'utilisateur ouvre le trou avec Virtual Telnet. Ensuite, si l'autorisation d'une plage de ports est activée et que le trafic de cette plage touche le PIX, le PIX envoie la commande au serveur TACACS+ pour autorisation. Cet exemple montre l'autorisation entrante sur une plage de ports.

```
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 de serveur TACACS+ (logiciel gratuit) :

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

L'utilisateur doit d'abord établir une connexion Telnet avec l'adresse IP virtuelle 99.99.99.99. Après l'authentification, lorsqu'un utilisateur tente de transmettre le trafic TCP dans la plage du port 40-50 via le PIX à 99.99.99.99 (172.18.124.114), cmd=tcp/40-50 est envoyé au serveur TACACS+ avec cmd-arg=17 2.18.124.114 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 Comptabilisation du trafic autre que HTTP, FTP et Telnet

Une fois que vous vous êtes assuré que Virtual Telnet fonctionne pour autoriser le trafic TCP/40-50 vers l'hôte à l'intérieur du réseau, ajoutez la comptabilisation de 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 d'enregistrements comptables TACACS+

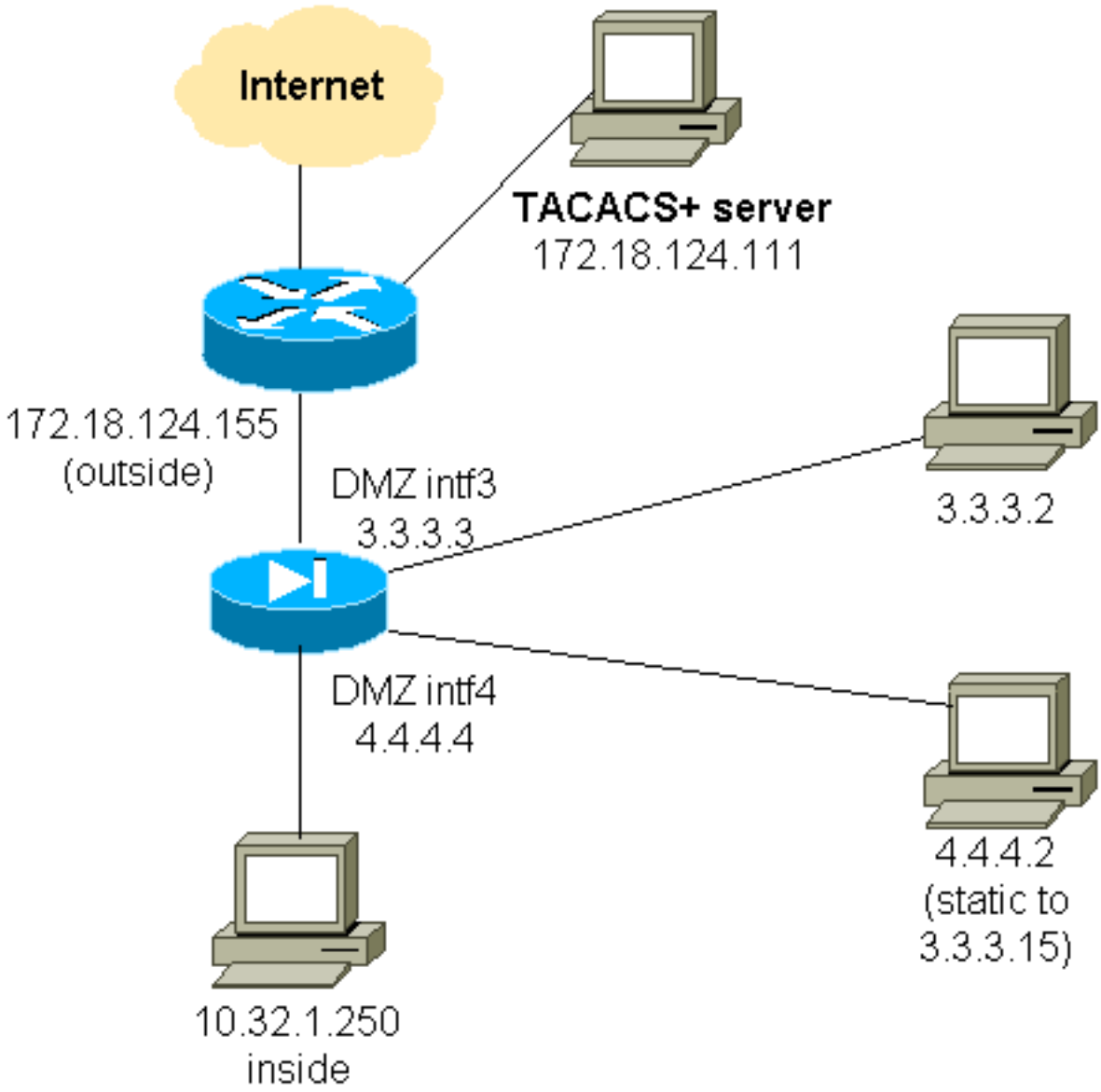
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8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

Authentification sur la DMZ

Afin d'authentifier les utilisateurs qui vont d'une interface DMZ à une autre, dites au PIX d'authentifier le trafic pour les interfaces nommées. Sur le PIX, l'arrangement est le suivant :

```
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 PIX partielle

Authentifiez le trafic Telnet entre pix/intf3 et pix/intf4, comme illustré ici.

Configuration PIX partielle

```
  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 toujours besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et que vous souhaitez ouvrir un dossier auprès du centre d'assistance technique Cisco, veillez à 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 de la commande **show log** après l'exécution de la commande **logging buffered debugging**, ou captures de console qui montrent le problème (si disponible)

Attachez les données rassemblées à votre dossier dans un format de texte brut (.txt) non compressé. Joignez les informations à votre dossier en les téléchargeant à l'aide

de l'outil de requête de dossier (clients enregistrés uniquement). Si vous ne parvenez pas à accéder à l'outil de requête de dossier, envoyez les informations dans une pièce jointe à un e-mail à attach@cisco.com avec votre numéro de dossier dans la ligne d'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
- RADIUS (Remote Authentication Dial-In User Service)
- Support et documentation techniques - Cisco Systems