# Configuration de PIX 5.0.x : TACACS+ et RADIUS

## Contenu

# Introduction

L'authentification RADIUS et TACACS+ peut être effectuée pour les connexions FTP, Telnet et HTTP. L'authentification d'autres protocoles TCP moins courants peut généralement fonctionner.

L'autorisation TACACS+ est prise en charge. L'autorisation RADIUS n'est pas valide. Les modifications apportées à l'authentification, à l'autorisation et à la comptabilité (AAA) PIX 5.0 par rapport à la version précédente incluent la comptabilisation AAA du trafic autre que HTTP, FTP et Telnet.

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

# Authentification et autorisation

- L'authentification est l'utilisateur.
- L'autorisation est ce que l'utilisateur peut faire.
- L'*authentification est* valide sans autorisation.
- L'autorisation *n*'est *pas* valide sans authentification.

Par exemple, supposons que vous avez cent utilisateurs à l'intérieur et que vous voulez que seulement six de ces utilisateurs puissent faire FTP, Telnet ou HTTP en dehors du réseau. Demandez au PIX d'authentifier le trafic sortant et de fournir les six ID d'utilisateurs sur le serveur de sécurité TACACS+/RADIUS. Avec une *authentification* simple, ces six utilisateurs peuvent être authentifiés avec nom d'utilisateur et mot de passe, puis sortir. Les quatre-vingt-quatorze autres utilisateurs ne peuvent pas sortir. Le PIX invite les utilisateurs à saisir leur nom d'utilisateur/mot de passe, puis transmet leur nom d'utilisateur et leur mot de passe au serveur de sécurité TACACS+/RADIUS. Selon la réponse, il ouvre ou refuse la connexion. Ces six utilisateurs peuvent effectuer des protocoles FTP, Telnet ou HTTP.

D'un autre côté, supposons que *l'un* de ces trois utilisateurs, « Terry », ne soit pas digne de confiance. Vous souhaitez autoriser Terry à faire FTP, mais pas HTTP ou Telnet vers l'extérieur. Cela signifie que vous devez ajouter une *autorisation*. C'est-à-dire autoriser *ce que* les utilisateurs peuvent faire en plus d'authentifier *qui* ils sont. Lorsque vous ajoutez *une autorisation* au PIX, le PIX envoie d'abord le nom d'utilisateur et le mot de passe de Terry au serveur de sécurité, puis envoie une demande d'autorisation indiquant au serveur de sécurité quelle *commande* Terry tente de faire. Une fois le serveur configuré correctement, Terry peut être autorisé à « FTP 1.2.3.4 » mais ne peut pas être autorisé à « HTTP » ou « Telnet » n'importe où.

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

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

- **Telnet** - L'utilisateur voit une invite de nom d'utilisateur, suivie d'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 les « local_username » et « local_password » au serveur de sécurité local, et 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** : fenêtre affichée dans le navigateur qui demande 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 doit temporiser une connexion

HTTP mais ne le fait pas, il est probable que la réauthentification a réellement lieu avec le navigateur « filmer » le nom d'utilisateur et le mot de passe mis en cache au PIX, qui le transfère ensuite au serveur d'authentification. PIX syslog et/ou le débogage du serveur montreront ce phénomène. Si Telnet et FTP semblent fonctionner normalement, mais que les connexions HTTP ne fonctionnent pas, c'est pourquoi.

## Configurations de serveur de sécurité utilisées pour tous les scénarios

### Configuration du serveur TACACS Cisco Secure UNIX

Assurez-vous que vous avez l'adresse IP PIX ou le nom de domaine complet et la clé dans le fichier CSU.cfg.

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

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

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

### Configuration du serveur RADIUS Cisco Secure UNIX

Utilisez l'interface utilisateur graphique (GUI) pour ajouter l'adresse IP PIX et la clé à la liste des serveurs d'accès au réseau (NAS).

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
```

```
}
reply_attributes= {
6=6
}
}
```

## Cisco Secure Windows 2.x RADIUS

Suivez ces étapes :

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

## EasyACS TACACS+

La documentation EasyACS décrit la configuration.

1. Dans la section group, cliquez sur **Shell exec** (pour accorder des privilèges d'exécution).
2. Pour ajouter une autorisation au PIX, cliquez sur **Refuser les commandes IOS sans correspondance** au bas de la configuration du groupe.
3. Sélectionnez **Add/Edit new command** pour chaque commande que vous souhaitez autoriser (par exemple, Telnet).
4. Si vous voulez autoriser Telnet à des sites spécifiques, entrez les adresses IP dans la section d'argument sous la forme « permit #.#.#.#« . Pour autoriser Telnet à tous les sites, cliquez sur **Autoriser tous les arguments non répertoriés**.
5. Cliquez sur **Terminer la commande de modification**.
6. Exécutez les étapes 1 à 5 pour chacune des commandes autorisées (par exemple, Telnet, HTTP ou FTP).
7. Ajoutez l'adresse IP PIX dans la section Interface graphique utilisateur de la configuration NAS.

## Cisco Secure 2.x TACACS+

L'utilisateur obtient un mot de passe dans la section User setup GUI.

1. Dans la section group, cliquez sur **Shell exec** (pour accorder des privilèges d'exécution).
2. Pour ajouter une autorisation au PIX, cliquez sur **Refuser les commandes IOS sans correspondance** au bas de la configuration du groupe.
3. Sélectionnez **Add/Edit new command** pour chaque commande que vous voulez autoriser (par exemple, Telnet).
4. Si vous souhaitez autoriser Telnet à des sites spécifiques, saisissez permit IP(s) dans le rectangle d'arguments (par exemple, « permit 1.2.3.4 »). Pour autoriser Telnet à tous les sites, cliquez sur **Autoriser tous les arguments non répertoriés**.
5. Cliquez sur **Terminer la commande de modification**.
6. Exécutez les étapes précédentes pour chacune des commandes autorisées (par exemple, Telnet, HTTP et/ou FTP).
7. Ajoutez l'adresse IP PIX dans la section Interface graphique utilisateur de la configuration NAS.

## Configuration du serveur RADIUS de Livingston

Ajoutez l'adresse IP PIX et la clé au fichier clients.

```
adminuser Password="all"
User-Service-Type = Shell-User
```

## Mériter la configuration du serveur RADIUS

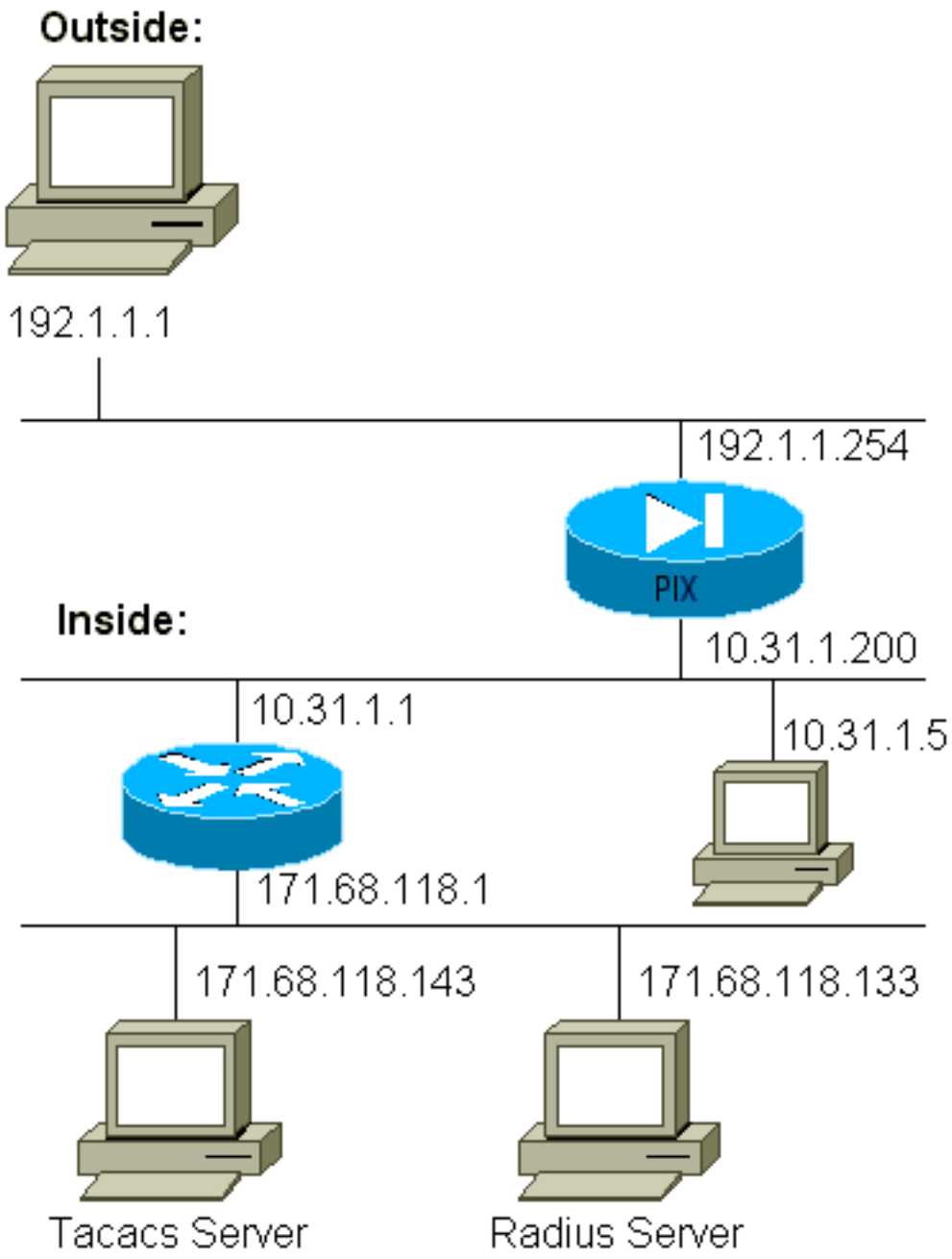
Ajoutez l'adresse IP PIX et la clé au fichier clients.

```
adminuser Password="all"
Service-Type = Shell-User

key = "cisco"

user = adminuser {
login = cleartext "all"
default service = permit
}

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 .*
}
}
```

# Étapes de débogage

- Assurez-vous que les configurations PIX fonctionnent avant d'ajouter AAA.Si vous ne pouvez pas transmettre le trafic avant d'instituer l'authentification et l'autorisation, vous ne pourrez pas le faire ultérieurement.
- Activer la journalisation dans PIXLa commande **logging console debugging** *ne doit pas* être utilisée sur un système chargé.La commande **logging buffered debugging** peut être utilisée. Les résultats des commandes **show logging** ou **logging** peuvent être envoyés à un serveur syslog et examinés.
- Assurez-vous que le débogage est activé pour les serveurs TACACS+ ou RADIUS. Tous les serveurs disposent de cette option.

## Diagramme du réseau




**Configuration PIX**

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
 names
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
```

```
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
 timeout rpc 0:10:00 h323 0:05:00
 timeout uauth 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 no snmp-server location
 no snmp-server contact
 snmp-server community public
 no snmp-server enable traps
 telnet timeout 5
```

```
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

# Exemples de débogage d'authentification à partir de PIXAuthentication Exemples de débogage à partir de PIX

Dans ces exemples de débogage :

## Sortant

L'utilisateur interne à l'adresse 10.31.1.5 initie le trafic vers l'extérieur 192.1.1.1 et est authentifié via TACACS+. Le trafic sortant utilise la liste de serveurs « AuthOutbound » qui inclut le serveur RADIUS 171.68.118.133.

## Entrant

L'utilisateur externe à l'adresse 192.1.1.1 initie le trafic vers l'adresse 10.31.1.5 interne (192.1.1.30) et est authentifié via TACACS. Le trafic entrant utilise la liste de serveurs « AuthInbound » qui inclut le serveur TACACS 171.68.118.143).

## Débogage PIX - Bonne authentification - TACACS+

Cet exemple montre un débogage PIX avec une bonne authentification :

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

## Débogage PIX - Authentification incorrecte (nom d'utilisateur ou mot de passe) - TACACS+

Cet exemple montre le débogage PIX avec une authentification incorrecte (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre jeux de nom d'utilisateur/mot de passe et le message "`Erreur : nombre maximal de tentatives dépassé.` »

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

## Débogage PIX - Ping Server, pas de réponse - TACACS+

Cet exemple montre le débogage PIX où le serveur peut être envoyé par ping mais ne parle pas au PIX. L'utilisateur voit un nom d'utilisateur, mais PIX ne demande jamais de mot de passe (il s'agit de Telnet). L'utilisateur voit "`Erreur : Nombre maximal de tentatives dépassé.`"

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

## Débogage PIX - Impossible d'envoyer une requête ping au serveur - TACACS+

Cet exemple montre un débogage PIX où le serveur ne peut pas envoyer de requête ping. L'utilisateur voit un nom d'utilisateur, mais le PIX ne demande jamais de mot de passe (il s'agit de Telnet). Ces messages s'affichent : "`Délai d'attente pour le serveur TACACS+`" et "`Erreur : Nombre maximal d'essais dépassé`" (nous avons changé dans un faux serveur dans la configuration).

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

## Débogage PIX - Bonne authentification - RADIUS

Cet exemple montre un débogage PIX avec une bonne authentification :

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

## Débogage PIX - Authentification incorrecte (nom d'utilisateur ou mot de passe) - RADIUS

Cet exemple montre un débogage PIX avec une authentification incorrecte (nom d'utilisateur ou mot de passe). L'utilisateur voit une demande de nom d'utilisateur et de mot de passe. L'utilisateur dispose de trois possibilités d'entrée de nom d'utilisateur/mot de passe réussie.

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
```

```
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

## Débogage Ping - Ping Server, démon désactivé - RADIUS

Cet exemple montre un débogage PIX où le serveur peut envoyer une requête ping, mais le démon est arrêté et ne communiquera pas avec le PIX. L'utilisateur voit le nom d'utilisateur, le mot de passe et les messages "`Échec du serveur RADIUS`" et "`Erreur : Nombre maximal de tentatives dépassé.`"

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

## Débogage PIX - Impossible d'envoyer une requête ping au serveur ou à la clé/au client - RADIUS

Cet exemple montre comment envoyer un débogage PIX dans lequel le serveur ne peut pas envoyer de requête ping ou où il y a une incompatibilité clé/client. L'utilisateur voit le nom d'utilisateur, le mot de passe et les messages "`Timeout to RADIUS server`" et "`Error : Nombre maximal d'essais dépassé`" (un faux serveur a été remplacé dans la configuration).

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

# Ajoutez l'autorisation

Si vous décidez d'ajouter une autorisation, vous devrez obtenir une autorisation pour la même plage source et de destination (car l'autorisation n'est pas valide sans authentification) :

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization HTTP inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Notez que l'autorisation n'est pas ajoutée pour le trafic sortant, car le trafic sortant est authentifié avec RADIUS et l'autorisation RADIUS n'est pas valide.

# Exemples de débogage d'authentification et d'autorisation à partir de PIX

## Débogage PIX - Authentification correcte et autorisation réussie - TACACS+

Cet exemple montre un débogage PIX avec une authentification correcte et une autorisation réussie :

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

## Débogage PIX - Authentification correcte, autorisation échouée - TACACS+

Cet exemple montre un débogage PIX avec une bonne authentification mais avec une autorisation échouée. Ici, l'utilisateur voit également le message "`Erreur : Autorisation refusée.`"

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

# Ajoutez la gestion des comptes

## TACACS+

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Le débogage est identique, que la comptabilité soit activée ou désactivée. Cependant, au moment de la « Construite », un enregistrement comptable « de début » est envoyé. Au moment de l'arrêt, un enregistrement comptable d'arrêt est envoyé.

Les enregistrements comptables TACACS+ ressemblent à ce résultat (ceux-ci proviennent de Cisco Secure NT, d'où le format délimité par des virgules) :

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
```

```
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,
```

## RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

Le débogage est identique, que la comptabilité soit activée ou désactivée. Cependant, au moment de la « Construite », un enregistrement comptable « de début » est envoyé. Au moment de l'arrêt, un enregistrement comptable d'arrêt est envoyé.

Les enregistrements comptables RADIUS ressemblent à ce résultat (ceux-ci proviennent de Cisco Secure UNIX ; les uns de Cisco Secure NT peuvent être délimités par des virgules) :

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

# Utilisation de la commande Exception

Dans notre réseau, si nous décidons qu'une source et/ou une destination particulière n'a pas besoin d'authentification, d'autorisation ou de comptabilité, nous pouvons effectuer une opération comme celle-ci :

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

Si vous « exceptez » une case de l'authentification et que vous avez l'autorisation, vous devez également excepter la 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 (a une session via PIX).

Cela fonctionne bien pour les connexions Telnet et FTP en raison de la nature des connexions. Cela ne fonctionne pas bien pour HTTP en raison de la nature de la connexion. Dans cet exemple de sortie, 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 171.68.118.100/12 00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23
    gaddr 9.9.9.10/12 00 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 d'enregistrement « 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 poursuit l'activité Telnet ou FTP sur l'hôte cible, puis quitte (y passe 10 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 (authentification à chaque fois) ou plus (authentification une fois et non à nouveau pendant la période uauth), un enregistrement comptable est coupé pour chaque site auquel on accède.

HTTP fonctionne différemment en raison de la nature du protocole. Cette sortie montre un exemple de HTTP :

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 affiché à 16:35:34 et l'enregistrement de fin affiché 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 est-il toujours connecté au site Web et la connexion est-elle toujours ouverte lorsqu'il lit la page Web ? Non. Le nombre maximal de sessions ou l'affichage des utilisateurs connectés fonctionnera-t-il ici ? Non, parce que le temps de connexion (le temps entre « Construite » et « Teardown ») dans HTTP est trop court. Les enregistrements « start » et « stop » sont en moins d'une seconde. Il n'y aura pas d'enregistrement « de début » sans enregistrement « d'arrêt », puisque les enregistrements ont lieu pratiquement au même moment. Il y aura toujours 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.

## Authentification et activation sur le PIX lui-même

La discussion précédente a décrit l'authentification du trafic Telnet (et HTTP, FTP) *par* le PIX. Nous nous assurons que Telnet *vers* PIX fonctionne *sans* authentification sur :

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

Lorsque les utilisateurs établissent une connexion Telnet avec le PIX, ils sont invités à saisir le mot de passe Telnet (**ww**). Ensuite, le PIX demande aussi TACACS+ (dans ce cas, puisque la liste de serveurs « AuthInbound » est utilisée) ou le nom d'utilisateur et le mot de passe RADIUS. Si le serveur est en panne, vous pouvez accéder au PIX en entrant **pix** pour le nom d'utilisateur, puis le mot de passe enable (**enable password** ***any any*** ) pour y accéder.

Avec cette commande :

```
aaa authentication enable console AuthInbound
```

l'utilisateur est invité à saisir un nom d'utilisateur et un mot de passe, qui sont envoyés au TACACS (dans ce cas, puisque la liste de serveurs « AuthInbound » est utilisée, la demande est envoyée au serveur TACACS) ou au serveur RADIUS. Puisque le paquet d'authentification pour enable est identique au paquet d'authentification pour la connexion, si l'utilisateur peut se connecter au PIX avec TACACS ou RADIUS, il peut activer via TACACS ou RADIUS avec le même nom d'utilisateur/mot de passe. Ce problème a reçu l'ID de bogue Cisco CSCdm47044

(clients enregistrés uniquement).

## Authentification sur la console série

La commande **aaa authentication serial console AuthInbound** nécessite une vérification d'authentification afin d'accéder à la console série du PIX.

Lorsque l'utilisateur exécute des commandes de configuration à partir de la console, les messages syslog sont coupés (en supposant que le PIX est configuré pour envoyer syslog au niveau de débogage à un hôte syslog). Voici un exemple de ce qui est affiché sur le serveur Syslog :

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

## Modifier l'invite que les utilisateurs voient

Si vous avez la commande **auth-prompt PIX_PIX_PIX**, les utilisateurs qui passent par PIX voient cette séquence :

```
PIX_PIX_PIX [at which point one would enter the username]
Password:[at which point one would enter the password]
```

À l'arrivée dans la zone de destination finale, l'invite « Nom d'utilisateur : » et « Mot de passe : » s'affiche. Cette invite n'affecte que les utilisateurs qui passent *par* le PIX, et non *vers* le PIX.

**Remarque :** aucun enregistrement comptable n'est coupé pour l'accès au PIX.

## Personnaliser le message que les utilisateurs voient en cas de réussite ou d'échec

Si vous disposez des commandes suivantes :

```
auth-prompt accept "GOOD_AUTH"
auth-prompt reject "BAD_AUTH"
```

les utilisateurs voient cette séquence lors d'une connexion échouée/réussie via PIX :

```
PIX_PIX_PIX
 Username: asjdkl
 Password:
 "BAD_AUTH"
 "PIX_PIX_PIX"
 Username: cse
 Password:
 "GOOD_AUTH"
```

## Délais d'inactivité et d'abandon par utilisateur

Les délais d'attente uauth inactifs et absolus peuvent être envoyés par utilisateur à partir du serveur TACACS+. Si tous les utilisateurs de votre réseau doivent avoir le même délai d'attente, ne mettez pas en oeuvre ceci ! Mais si vous avez besoin de différents uauths par utilisateur, continuez à lire.

Dans cet exemple, la commande **timeout uauth 3:00:00** est utilisée. Une fois qu'une personne s'authentifie, elle n'a pas à se réauthentifier pendant trois heures. Cependant, si vous configurez un utilisateur avec ce profil et que l'*autorisation* TACACS AAA est activée dans le PIX, les délais d'inactivité et absolus dans le profil utilisateur remplacent le délai d'attente dans le PIX pour cet utilisateur. Cela ne signifie pas que la session Telnet via le PIX est déconnectée après le délai d'inactivité/absolu. Il contrôle simplement si la réauthentification a lieu.

Ce profil provient du logiciel gratuit TACACS+ :

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

Après authentification, exécutez une commande **show uauth** sur le PIX :

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

Une fois l'utilisateur inactif pendant une minute, le débogage sur le PIX affiche :

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

L'utilisateur doit se réauthentifier lorsqu'il retourne au même hôte cible ou à un autre hôte.

## HTTP virtuel

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

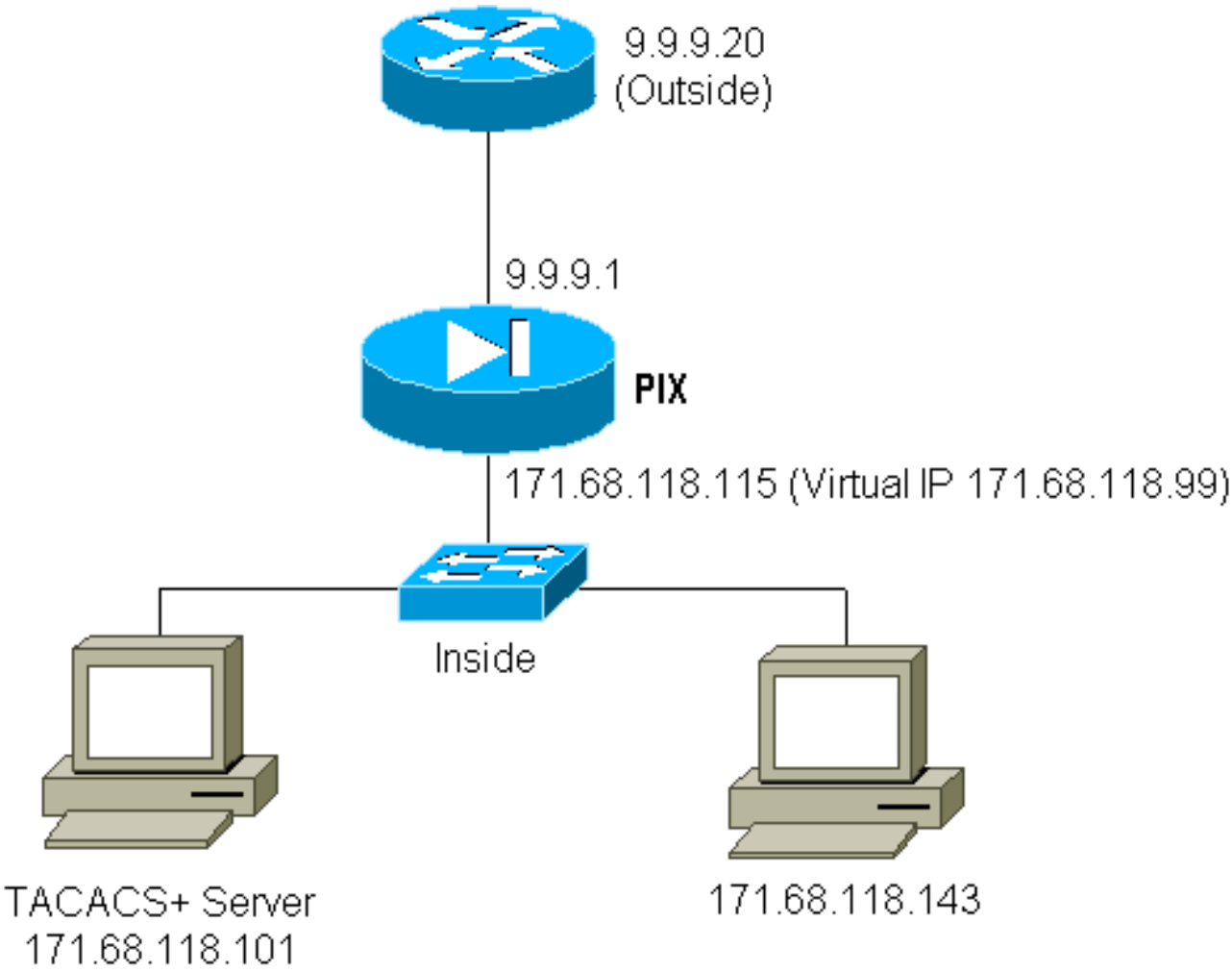
Pour éviter cela, vous pouvez mettre en oeuvre le protocole HTTP virtuel en ajoutant une adresse RFC 1918 (une adresse qui n'est pas routable sur Internet, mais valide et unique pour le réseau interne PIX) à la configuration PIX à l'aide de cette commande :

```
virtual http #.#.#.# [warn]
```

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.

## Diagramme sortant HTTP virtuel




## Configuration PIX HTTP virtuel sortant

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

# Telnet virtuel

Il est possible de configurer le PIX pour authentifier tout le trafic entrant et sortant, mais ce n'est pas une bonne idée de le faire. En effet, certains protocoles, tels que « mail », ne sont pas facilement authentifiés. Lorsqu'un serveur de messagerie et un client essaient de communiquer

via PIX lorsque tout le trafic via PIX est authentifié, le syslog PIX pour les protocoles non authentifiables affiche des messages tels que :

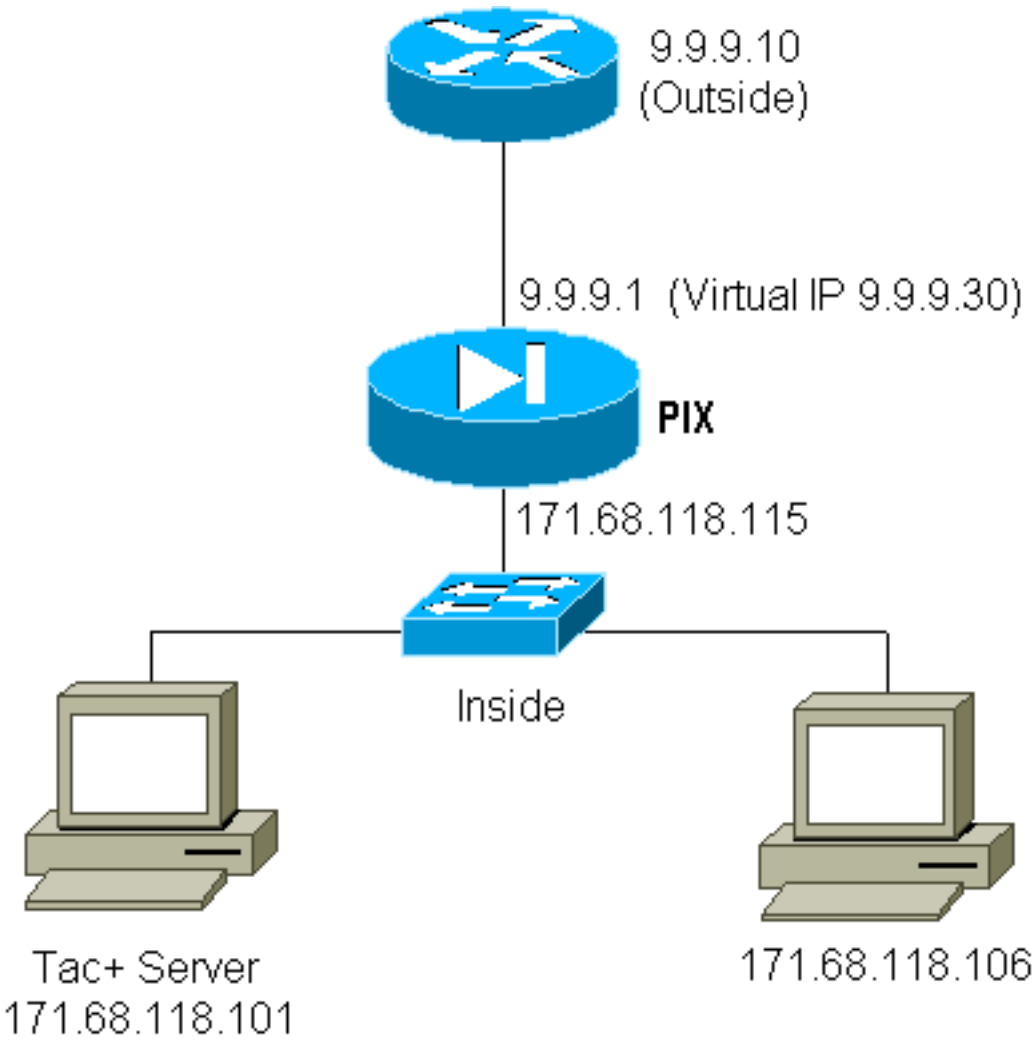
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

Comme le courrier et d'autres services ne sont pas suffisamment interactifs pour s'authentifier, une solution consiste à utiliser la commande **excepté** pour l'authentification/autorisation (authentifier tout sauf pour la source/destination du serveur de messagerie/client).

Si vous avez réellement besoin d'authentifier un service inhabituel, vous pouvez le faire à l'aide de la commande **Virtual Telnet**. Cette commande permet l'authentification sur l'adresse IP Telnet virtuelle. Après cette authentification, le trafic du service inhabituel peut aller au serveur réel.

Dans cet exemple, nous voulons que le trafic du port TCP 49 circule de l'hôte externe 9.9.9.10 vers l'hôte interne 171.68.118.106. Comme ce trafic n'est pas vraiment authentifiable, nous configurons un Telnet virtuel. Pour la connexion Telnet virtuelle entrante, il doit y avoir une connexion statique associée. Ici, les adresses virtuelles 9.9.9.20 et 171.68.118.20 sont toutes deux des adresses virtuelles.

## Diagramme entrant Telnet virtuel



## Configuration PIX Virtual Telnet Inbound

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

## Configuration utilisateur du serveur TACACS+ Virtual Telnet entrant

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

## PIX Debug Virtual Telnet Inbound

L'utilisateur à l'adresse 9.9.9.10 doit d'abord s'authentifier par Telnet à l'adresse 9.9.9.20 sur le PIX :

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

Après l'authentification réussie, la commande **show uauth** montre que l'utilisateur dispose de « temps sur le compteur » :

```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

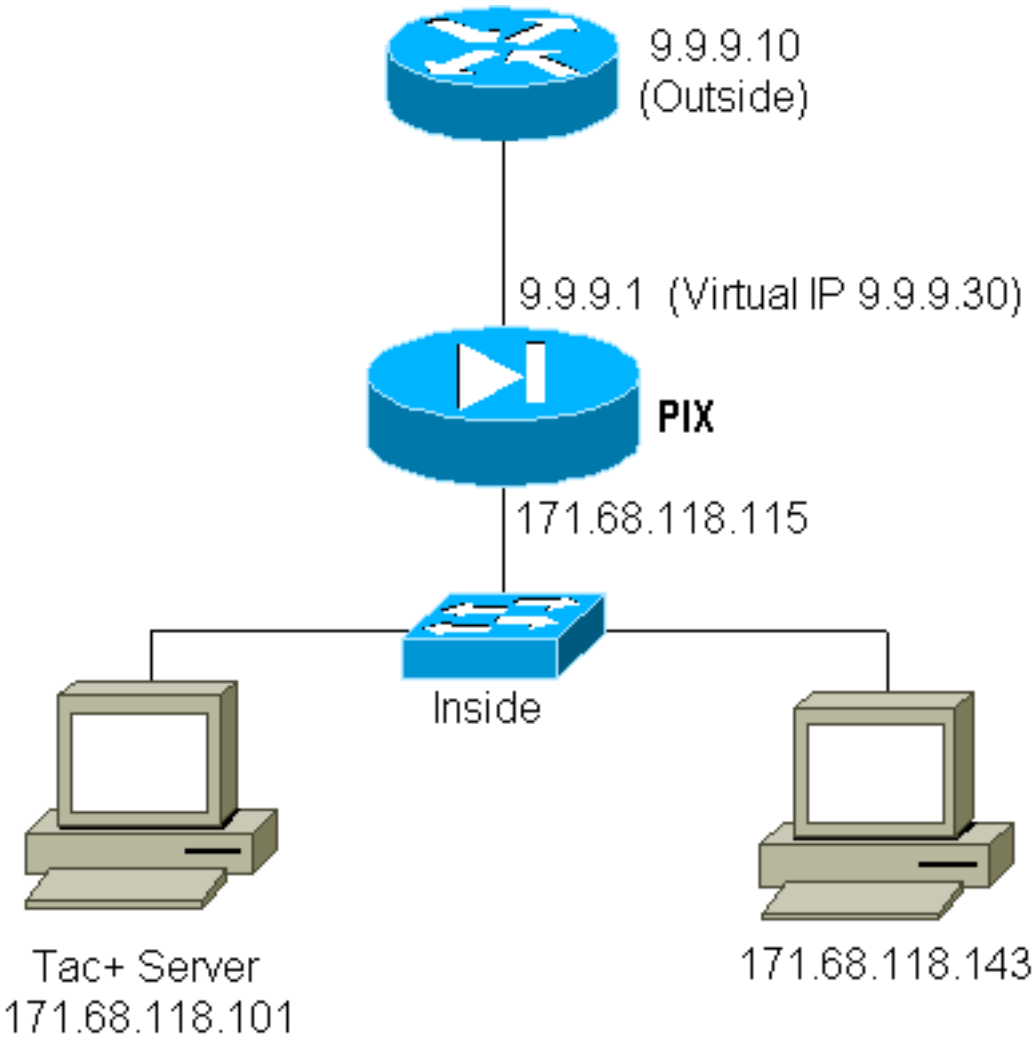
Ici, le périphérique à 9.9.9.10 veut envoyer le trafic TCP/49 au périphérique à 171.68.118.106 :

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
```

```
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

## Telnet virtuel sortant

Puisque le trafic sortant est autorisé par défaut, aucune valeur statique n'est requise pour l'utilisation de trafic sortant Telnet virtuel. Dans cet exemple, l'utilisateur interne 171.68.118.143 établit une connexion Telnet avec le réseau virtuel 9.9.9.30 et s'authentifie. La connexion Telnet est immédiatement abandonnée. Une fois authentifié, le trafic TCP est autorisé à partir de 171.68.118.143 vers le serveur à l'adresse 9.9.9.10 :




## Configuration PIX Virtual Telnet Outbound

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

## Débogage de PIX Virtual Telnet sortant

```
109001: Auth start for user '???' from 171.68.118.143/1536
```

```
    to 9.9.9.30/23
109011: Authen Session Start: user 'timeout_143', Sid 25
109005: Authentication succeeded for user 'timeout_143' from
   171.68.118.143/1536 to 9. 9.9.30/23
302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
   9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
   9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
   9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
   bytes 625 (timeout_143)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
   9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
   bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

## Déconnexion virtuelle de Telnet

Lorsque l'utilisateur établit une connexion Telnet avec l'adresse IP Telnet virtuelle, la commande **show uauth** affiche la valeur uauth.

Si l'utilisateur veut empêcher le trafic de passer après la fin de la session (lorsqu'il reste du temps dans la uauth), il doit à nouveau établir une connexion Telnet avec l'adresse IP Telnet virtuelle. Cette opération annule la session.

## Autorisation de port

Vous pouvez exiger une autorisation sur une plage de ports. Dans cet exemple, l'authentification était toujours requise pour tous les ports sortants, mais seule l'autorisation était requise pour les ports TCP 23-49.

### Configuration PIX

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

Lorsque Telnet a été effectué de 171.68.118.143 à 9.9.9.10, l'authentification et l'autorisation se sont produites car le port Telnet 23 se trouve dans la plage 23-49.

Lorsqu'une session HTTP est effectuée de 171.68.118.143 à 9.9.9.10, vous devez toujours vous authentifier, mais le PIX ne demande pas au serveur TACACS+ d'autoriser HTTP car 80 ne se trouve pas dans la plage 23-49.

### Configuration du serveur de logiciel gratuit TACACS+

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
```

```
        }
        }
```

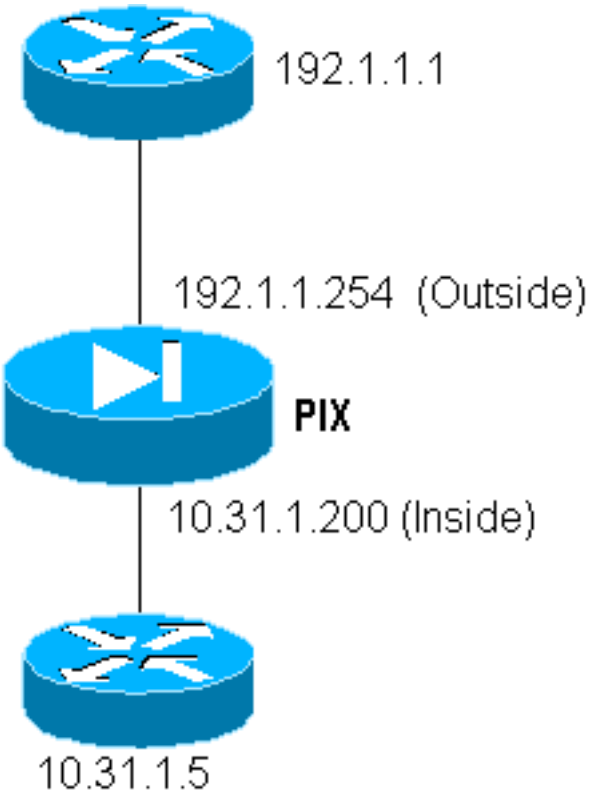
Notez que le PIX envoie "`cmd=tcp/23-49`" et "`cmd-arg=9.9.9.10`" au serveur TACACS+.

## Déboguer sur PIX

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109007: Authorization permitted for user 'telnetrange'
    from 171.68.118.143/1051 to 9.9 .9.10/23
 302001: Built TCP connection 0 for faddr 9.9.9.10/23
    gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
 109001: Auth start for user '???' from 171.68.118.143/1105
    to 9.9.9.10/80
 109001: Auth start for user '???' from 171.68.118.143/1110
    to 9.9.9.10/80
 109011: Authen Session Start: user 'telnetrange', Sid 1
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1110 to 9. 9.9.10/80
 302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
  laddr 171.68.1 18.143/1110 (telnetrange)
 302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
  laddr 171.68.1 18.143/1111 (telnetrange)
 302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
  laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
  laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

# AAA Comptabilisation du trafic autre que HTTP, FTP et Telnet

Le logiciel PIX version 5.0 modifie la fonctionnalité de comptabilité du trafic. Les enregistrements comptables peuvent maintenant être coupés pour le trafic autre que HTTP, FTP et Telnet, une fois l'authentification terminée.




Pour copier un fichier du routeur externe (192.1.1.1) sur le routeur interne (10.31.1.5) sur TFTP, ajoutez Virtual Telnet pour ouvrir un trou pour le processus TFTP :

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Ensuite, établissez une connexion Telnet à partir du routeur externe à l'adresse 192.1.1.1 vers l'adresse IP virtuelle 192.1.1.30 et authentifiez-vous à l'adresse virtuelle qui permet au protocole UDP de traverser le PIX. Dans cet exemple, le processus **copy tftp flash** a été démarré de l'extérieur vers l'intérieur :

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

Pour chaque **copie tftp flash** sur le PIX (il y en avait trois pendant cette copie IOS), un enregistrement de comptabilité est coupé et envoyé au serveur d'authentification. Voici un exemple d'enregistrement TACACS sur Cisco Secure Windows) :

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

## Informations connexes

- Référence des commandes PIX
- Page d'assistance produit PIX