# Exemples de configuration de PIX, TACACS+ et RADIUS : 4.4.x

## Contenu


Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Authentification contre l'autorisation
Sur ce que l'utilisateur voit avec l'Authentification/Autorisation activée
Configurations de serveur sécurisé utilisées pour tous les scénarios
Configuration de serveur TACACS de CiscoSecure UNIX
Configuration du serveur d'UNIX RADIUS de CiscoSecure
NT 2.x RADIUS de CiscoSecure
EasyACS TACACS+
CiscoSecure 2.x TACACS+
Configuration du serveur Livingston RADIUS
Configuration du serveur Merit RADIUS
Configuration du serveur de logiciel gratuit TACACS+
Étapes de débogage
Diagramme du réseau
Exemples de debug d'authentification de PIX
Ajout d'autorisation
Exemples de debug d'authentification et d'autorisation de PIX
Ajout de la comptabilité
TACACS+
RADIUS
Utilisation de excepté commande
Maximum-sessions et utilisateurs connectés de visionnement
Authentification et activation sur le PIX lui-même
Authentification sur la console série
Changeant les invites utilisateur voient
Personnalisant les utilisateurs de message voient sur le succès/panne
inactif et temporisations absolues de Par-utilisateur
HTTP virtuel
Telnet virtuel
Déconnexion virtuelle de Telnet
Autorisation sur le port
**Informations connexes**

# Introduction

L'authentification de RADIUS et TACACS+ peut être faite pour le FTP, le telnet, et les connexions HTTP. L'authentification pour d'autres protocoles TCP moins communs peut habituellement être faite fonctionner.

L'autorisation TACACS+ est prise en charge ; L'autorisation RADIUS n'est pas. Les changements de l'Authentification, autorisation et comptabilité (AAA) PIX 4.4.1 au-dessus de la version préalable incluent : Les Groupes de serveurs AAA et le Basculement, authentification pour l'accès d'enable et de console série, et reçoivent et rejettent les messages prompts.

# Conditions préalables

## Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

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 contre l'autorisation

- L'authentification est qui l'utilisateur est.
- Est l'autorisation ce que l'utilisateur peut faire.
- L'authentification est valide sans autorisation.
- L'autorisation est non valide sans authentification.

Supposez vous avez 100 utilisateurs intérieurs et vous vouloir voulez seulement que 6 de ces utilisateurs puissent faire le FTP, le telnet, ou le HTTP en dehors du réseau. Vous diriez le PIX d'authentifier le trafic sortant et de donner à chacun des 6 utilisateurs des id sur le serveur sécurisé TACACS+/RADIUS. Avec l'authentification simple, ces 6 utilisateurs pourraient être authentifiés avec le nom d'utilisateur et mot de passe, puis sortent. Les 94 autres utilisateurs ne pourraient pas sortir. Le PIX incite des utilisateurs pour le nom d'utilisateur/mot de passe, puis passe leur nom d'utilisateur et mot de passe au serveur sécurisé TACACS+/RADIUS, et selon la réponse, ouvre ou refuse la connexion. Ces 6 utilisateurs pourraient faire le FTP, le telnet, ou le HTTP.

Mais supposez un de ces trois utilisateurs, « Terry, » n'est pas à sont de confiance. Vous voudriez permettre à Terry pour faire le FTP, mais pas le HTTP ou le telnet à l'extérieur. Ceci signifie devoir ajouter l'autorisation, c.-à-d., autorisant ce que les utilisateurs peuvent faire en plus d'authentifier qui ils sont. Quand nous ajoutons l'autorisation au PIX, le PIX enverrait le nom d'utilisateur et mot de passe de Terry au serveur sécurisé, alors envoie la première fois à une demande d'autorisation indiquant au serveur sécurisé ce que la « commande » Terry essaye de faire. Avec la configuration du serveur correctement, Terry pourrait être permis au « FTP 1.2.3.4 » mais a refusé

la capacité au HTTP ou au telnet n'importe où.

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

En essayant d'aller de l'intérieur à l'extérieur (ou vice versa) avec l'authentification/autorisation en fonction :

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

## Configurations de serveur sécurisé utilisées pour tous les scénarios

### Configuration de serveur TACACS de CiscoSecure 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 d'UNIX RADIUS de CiscoSecure

Employez l'interface utilisateur graphique avancée (GUI) pour ajouter l'IP PIX et la clé à la liste de serveur d'accès à distance (NAS).

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
```

## NT 2.x RADIUS de CiscoSecure

Procédez comme suit :

1. Obtenez un mot de passe dans le partie Interface graphique d'installation des utilisateurs.
2. De la section GUI de Group Setup, placez l'attribut 6 (type de service) pour ouvrir une session ou administratif.
3. Ajoutez l'IP PIX dans le GUI de configuration de NAS.

## EasyACS TACACS+

La documentation d'EasyACS décrit l'installation.

1. Dans la section de groupe, cliquez sur en fonction l'**exécutif de shell** (pour donner des privilèges EXEC).
2. Àpour ajouter l'autorisation au PIX, le clic **refusent des commandes IOS inégalées au** bas de l'installation de groupe.
3. Sélectionnez la nouvelle commande d'**Add/Edit** pour chaque commande que vous voulez permettre (par exemple, telnet).
4. Si vous voulez permettre le telnet aux sites spécifiques, écrivez l'IP dans l'argument section sous la forme la « autorisation #.#.#.# ». Pour permettre le telnet à tous les sites, le clic **permettent tous les arguments non listés**.

5. Cliquez sur Finish la **commande de retouche**.
6. Exécutez les étapes 1 à 5 pour chacune des commandes permises (par exemple, telnet, HTTP et/ou FTP).
7. Ajoutez l'IP PIX dans la section GUI de configuration de NAS.

## CiscoSecure 2.x TACACS+

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

1. Dans la section de groupe, **exécutif de shell de** clic (pour donner des privilèges EXEC).
2. Pour ajouter l'autorisation au PIX, le clic **refusent des commandes IOS inégalées au** bas de l'installation de groupe.
3. **Add/Edit** choisi pour chaque commande que vous voulez permettre (par exemple, telnet).
4. Si vous voulez permettre le telnet aux sites spécifiques, écrivez l'IP d'autorisation dans l'argument rectangle (par exemple, « autorisation 1.2.3.4"). Pour permettre le telnet à tous les sites, le clic **permettent tous les arguments non listés**.
5. Cliquez sur Finish la **commande de retouche**.
6. Exécutez les étapes 1 à 5 pour chacune des commandes permises (par exemple, telnet, HTTP ou FTP).
7. Ajoutez l'IP PIX dans la section GUI de configuration de NAS.

## Configuration du serveur Livingston RADIUS

Ajoutez l'IP PIX et la clé aux clients classent.

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

## Configuration du serveur Merit RADIUS

Ajoutez l'IP PIX et la clé aux clients classent.

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

## Configuration du serveur de logiciel gratuit TACACS+

```
key = "cisco"

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

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

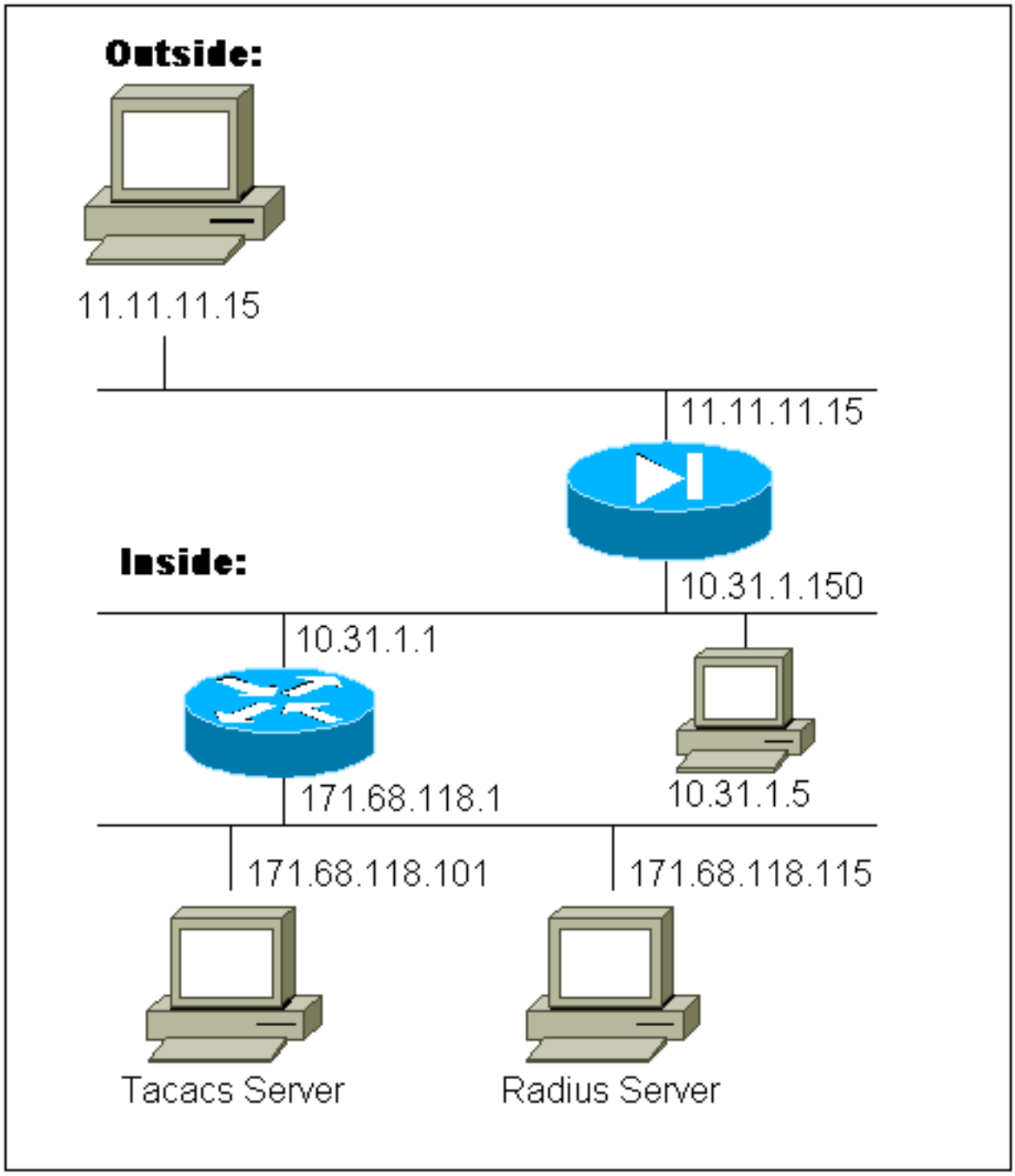
```
user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

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

## Étapes de débogage

- Assurez-vous que les configurations PIX fonctionnent avant d'ajouter l'Authentification, autorisation et comptabilité (AAA).Si vous ne pouvez pas passer le trafic avant d'instituer l'authentification et l'autorisation, vous ne pourrez pas faire tellement après.
- Enable ouvrant une session le PIX :La commande de **logging console debugging** ne devrait pas être utilisée sur un système fortement chargé.La commande de **logging buffered debugging** peut être utilisée. La sortie du **show logging** ou des commandes de **se connecter** peut être envoyée à un serveur de Syslog et être examinée.
- Assurez-vous que le débogage est allumé pour les serveurs TACACS+ ou de RADIUS. Tous les serveurs ont cette option.

## Diagramme du réseau




## Configuration PIX

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

# Exemples de debug d'authentification de PIX

Dans ces derniers mettez au point les exemples :

### Sortant

L'utilisateur intérieur aux initiés de 10.31.1.5 trafiquent à 11.11.11.15 extérieur et sont authentifiés par TACACS+ (la liste de serveur d'utilisations du trafic sortant « sortante » qui inclut le serveur TACACS 171.68.118.101).

### D'arrivée

L'utilisateur externe aux initiés de 11.11.11.15 trafiquent à 10.31.1.5 intérieur (11.11.11.22) et sont authentifiés par RADIUS (la liste d'arrivée de serveur d'utilisations du trafic « entrante » qui inclut le serveur 171.68.118.115 de RADIUS).

## Debug PIX - Bonne authentification - TACACS+

L'exemple au-dessous des expositions PIX mettent au point avec la bonne authentification :

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
```

```
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## PIX mettent au point - Authentification erronée (nom d'utilisateur ou mot de passe) - TACACS+

L'exemple au-dessous des expositions PIX mettent au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre positionnements de nom d'utilisateur/mot de passe. Les affichages de message de suivanux : « Error : nombre maximum d'essais dépassés ».

```
pix-5# write terminal
 Building configuration...
 : Saved
```

```
:
PIX Version 4.4(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
nameif ethernet3 pix/intf3 security15
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix-5
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
pager lines 24
no logging timestamp
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500
mtu pix/intf3 1500
ip address outside 11.11.11.1 255.255.255.0
ip address inside 10.31.1.150 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
failover ip address pix/intf3 0.0.0.0
arp timeout 14400
global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
no rip pix/intf2 passive
no rip pix/intf2 default
no rip pix/intf3 passive
no rip pix/intf3 default
route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
```

```
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## PIX mettent au point - Ne peut cingler, mais aucune réponse - TACACS+

L'exemple au-dessous des expositions PIX mettent au point pour un serveur pingable qui ne parle pas au PIX. L'utilisateur voit le nom d'utilisateur une fois, et PIX ne demande jamais un mot de passe (c'est sur le telnet).

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
```

```
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## Debug PIX - Ne peut pas cingler le serveur - TACACS+

L'exemple au-dessous des expositions PIX mettent au point pour un serveur qui n'est pas pingable. L'utilisateur voit le nom d'utilisateur une fois. PIX ne demande jamais un mot de passe (c'est sur le telnet). Les affichages de message de suivanux : « Délai d'attente au serveur TACACS+ » et à la « erreur : Nombre maximum d'essais dépassés » (la configuration dans cet exemple reflète un serveur faux).

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
```

```
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## Debug PIX - Bonne authentification - RADIUS

L'exemple au-dessous de l'exposition PIX mettent au point avec la bonne authentification :

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## Debug PIX - Authentification erronée (nom d'utilisateur ou mot de passe) - RADIUS

L'exemple au-dessous des expositions PIX mettent au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit une demande pour le nom d'utilisateur et mot de passe. Si l'un ou l'autre est erroné, le message « mot de passe incorrect » affiche quatre fois. Puis, l'utilisateur est déconnecté. Ce problème a été assigné l'ID #CSCdm46934 de bogue.

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
```

```
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## Debug PIX - Deamon vers le bas, ne communiquera pas avec PIX - RADIUS

L'exemple au-dessous des expositions PIX mettent au point avec un serveur pingable, mais le démon est vers le bas. Le serveur ne communiquera pas avec PIX. L'utilisateur voit le nom d'utilisateur, suivi de mot de passe. L'affichage de messages de suivanux : Le « serveur de RADIUS a manqué » et « erreur : Nombre maximum d'essais dépassés ».

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

## Debug PIX - Ne peut pas cingler le serveur ou les introduire/non-concordance de client - RADIUS

L'exemple au-dessous des expositions PIX mettent au point pour un serveur qui n'est pas pingable ou où il y a une clé/non-concordance de client. L'utilisateur voit le nom d'utilisateur et mot de passe. L'affichage de messages de suivanux : « Délai d'attente au serveur de RADIUS » et à la « erreur : Nombre maximum d'essais dépassés » (le serveur dans la configuration est par exemple des buts seulement).

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 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
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 failover ip address pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask 255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101 netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask 255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
```

```
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 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
!
!--- For any given list, multiple AAA servers can !--- be configured. They will be !--- tried
sequentially if any one of them is down. ! aaa-server Outgoing protocol tacacs+ aaa-server
Outgoing (inside) host 171.68.118.101 cisco timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco timeout 10 aaa authentication ftp outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 Outgoing aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Outgoing aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication telnet
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming no snmp-server location no snmp-server contact
snmp-server community public no snmp-server enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

# Ajout d'autorisation

Car l'autorisation est non valide sans authentification, nous aurons besoin de l'autorisation pour le même intervalle source et de destination :

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

### Sortant

Notez que nous n'ajoutons pas l'autorisation pour « entrant » parce que le trafic entrant est authentifié avec RADIUS, et l'autorisation RADIUS est non valide

# Exemples de debug d'authentification et d'autorisation de PIX

## Debug PIX avec la bonne authentification et l'autorisation réussie - TACACS+

L'exemple au-dessous de l'exposition PIX mettent au point avec la bonne authentification et l'autorisation réussie :

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

## Debug PIX - Bonne authentification, autorisation défaillante - TACACS+

L'exemple au-dessous des expositions PIX mettent au point avec la bonne authentification, mais l'autorisation défaillante :

Ici l'utilisateur erreur voit également message « : Autorisation refusée »

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

# Ajout de la comptabilité

## TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Le debug regardera la même chose si la comptabilité est "Marche/Arrêt". Cependant, au moment « construit », il y aura de l'enregistrement des comptes de « début » envoyé. Au moment « désinstallation », il y aura de l'enregistrement des comptes de « arrêt » envoyé.

Les enregistrements des comptes TACACS+ ressemblent au suivant (ceux-ci sont de CiscoSecure UNIX ; ceux dans le NT de CiscoSecure peuvent être délimités par une virgule à la place) :

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

## RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

Le debug regardera la même chose si la comptabilité est "Marche/Arrêt". Cependant, au moment « a construit », de l'enregistrement des comptes de « début » est envoyé. Au moment la « désinstallation », de l'enregistrement des comptes de « arrêt » est envoyée :

Les enregistrements des comptes de RADIUS ressemblent à ce qui suit : (ceux-ci sont de CiscoSecure UNIX ; ceux dans le NT de CiscoSecure peuvent être délimités par une virgule à la place) :

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

# Utilisation de excepté commande

Dans notre réseau, si nous décidons qu'une source et/ou une destination particulières n'a pas besoin d'authentification, d'autorisation, ou de comptabilité, nous pouvons faire quelque chose comme ce qui suit :

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

Si vous êtes « sauf » des IP address de l'authentification et avez l'autorisation en fonction, vous devez également les excepter de l'autorisation !

## Maximum-sessions et utilisateurs connectés de visionnement

Quelques serveurs TACACS+ et RADIUS ont des caractéristiques de « maximum-session » ou de « affichage des utilisateurs connectés ». La capacité de faire des maximum-sessions ou des utilisateurs connectés de contrôle dépend des enregistrements des comptes. Quand il y a un enregistrement de « début » de comptabilité généré mais aucun enregistrement de « arrêt », le serveur TACACS+ ou de RADIUS suppose que la personne est encore ouverte une session (c'est-à-dire, a une session par le PIX).

Ceci fonctionne bien pour le telnet et les connexions FTP en raison de la nature des connexions. Ceci ne fonctionne pas bien pour le HTTP en raison de la nature de la connexion. Dans l'exemple suivant, une configuration réseau différente est utilisée mais les concepts sont identiques.

Les telnets d'utilisateur par le PIX, authentifiant sur le chemin :

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

Puisque le serveur n'a vu un enregistrement de « début » mais aucun enregistrement de « arrêt » (en ce moment), le serveur prouvera que l'utilisateur de « telnet » est ouvert une session. Si l'utilisateur tente une autre connexion qui exige l'authentification (peut-être d'un autre PC) et si des maximum-sessions est placées à "1" sur le serveur pour cet utilisateur (assumant le serveur prend en charge des maximum-sessions), la connexion sera refusée par le serveur.

L'utilisateur va en fonction de pair avec son telnet ou activités en FTP sur l'hôte de cible, puis les sorties (passe 10 minutes là) :

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

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

Cependant, le HTTP fonctionne différemment en raison de la nature du protocole. Est ci-dessous un exemple de HTTP.

L'utilisateur parcourt de 171.68.118.100 à 9.9.9.25 par le PIX :

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

L'utilisateur lit la page Web téléchargée.

L'enregistrement de début signalé à 16:35:34, et l'enregistrement d'arrêt signalé à 16:35:35. Ce téléchargement a pris une seconde (qu'est à dire ; il y avait moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur est-il encore ouvert une session au site Web et à la connexion encore ouverts quand ils lisent la page Web ? No. Les maximum-sessions ou l'affichage des utilisateurs connectés fonctionneront-ils ici ? Non, parce que le temps de connexion (le temps entre « construit » et la « désinstallation ») dans le HTTP est trop court. L'enregistrement de « début » et de « arrêt » est fraction de seconde. Il n'y aura pas un enregistrement de « début » sans enregistrement de « arrêt », puisque les enregistrements se produisent pratiquement au même instant. Il y aura toujours « début » et « arrêtez » l'enregistrement envoyé au serveur pour chaque transaction, si l'uauth est placé pour 0 ou quelque chose plus grande. Cependant, les maximum-sessions et l'affichage des utilisateurs connectés ne fonctionneront pas en raison de la nature de la connexion HTTP.

## Authentification et activation sur le PIX lui-même

La discussion précédente était d'authentifier le trafic de telnet (et HTTP, FTP) par le PIX. Dans l'exemple ci-dessous, nous nous assurons que le telnet au pix fonctionne sans authentification en fonction :

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Puis, nous ajoutons la commande d'authentifier des utilisateurs Telnetting au PIX :

```
aaa authentication telnet console Outgoing
```

Quand le telnet d'utilisateurs au PIX, ils sont incités pour le mot de passe de telnet (« ww »). Le PIX demande également le TACACS+ dans ce cas (puisque la liste « sortante » de serveur est utilisée) ou nom d'utilisateur RADIUS et mot de passe.

```
aaa authentication enable console Outgoing
```

Avec cette commande, l'utilisateur est incité pour un nom d'utilisateur et mot de passe qui est envoyé au serveur TACACS ou de RADIUS. Dans ce cas, puisque la liste « sortante » de serveur

est utilisée, la demande va au serveur TACACS. Puisque le paquet d'authentification pour l'enable est identique que le paquet d'authentification pour la procédure de connexion, l'utilisateur peut activer par TACACS ou RADIUS avec le même nom d'utilisateur/mot de passe, assumer l'utilisateur peut ouvrir une session au PIX avec TACACS ou RADIUS. Ce problème a été assigné l'ID #CSCdm47044 de bogue.

Au cas où le serveur serait en panne, l'utilisateur peut accéder au mode enable PIX en écrivant « PIX » pour le nom d'utilisateur et le mot de passe normal d'enable du PIX (« mot de passe d'enable quoi que »). Si le « mot de passe d'enable celui qui » ne soit pas dans la configuration PIX, l'utilisateur écrit « PIX » pour le nom d'utilisateur et appuie sur la touche Enter. Si le mot de passe d'enable est placé mais pas connu, une disquette de récupération de mot de passe sera exigée afin de remettre à l'état initial.

## Authentification sur la console série

La commande de **console série d'authentification d'AAA** exige de la vérification d'authentification afin d'accéder à la console série du PIX. Quand l'utilisateur exécute des commandes de configuration de la console, des messages de Syslog seront coupés (si le PIX est configuré pour envoyer le Syslog au niveau de débogage à un hôte de Syslog). Est ci-dessous un exemple du serveur de Syslog :

```
aaa authentication enable console Outgoing
```

## Changeant les invites utilisateur voient

Si nous avons la commande :

```
auth-prompt THIS_IS_PIX_5
```

les utilisateurs allant par le PIX voient l'ordre :

```
auth-prompt THIS_IS_PIX_5
```

et puis, dès l'arrivée à la zone de destination finale, le « nom d'utilisateur :  » et « mot de passe :  » incitez la case de destination est présenté.

Cette demande affecte seulement des utilisateurs allant par le PIX, pas au PIX.

**Remarque:** Il n'y a aucun enregistrement des comptes coupé pour l'accès au PIX.

## Personnalisant les utilisateurs de message voient sur le succès/panne

Si nous avons les commandes :

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

Les utilisateurs verront le suivant sur procédure de connexion défectueuse/réussie par le PIX :


```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```


## inactif et temporisations absolues de Par-utilisateur

L'inactif et les limites absolues d'UAUTH peuvent être envoyés vers le bas du serveur TACACS+ sur une base par utilisateur. Si tous les utilisateurs dans votre réseau doivent avoir le même « uauth de délai d'attente, » alors n'implémentez pas ceci ! Mais, si vous avez besoin du par-utilisateur différent d'uauths, lisez en fonction.

Dans notre exemple sur le PIX, nous utilisons la commande de l'**uauth 3:00:00 de délai d'attente**. Ceci signifie qu'une fois qu'une personne authentifie, ils ne devront pas authentifier à nouveau pendant 3 heures. Mais si nous installons un utilisateur avec le profil suivant et avons l'autorisation d'AAA TACACS en fonction dans le PIX, l'inactif et les temporisations absolues dans le profil utilisateur ignorent l'uauth de délai d'attente dans le PIX pour cet utilisateur. Ceci ne signifie pas que la session de telnet par le PIX obtient déconnecté après l'inactif/temporisation absolue. Il contrôle juste si la ré-authentification a lieu.


```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```


Après authentification, émettez une commande d'**uauth d'exposition** 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
```

Après que l'utilisateur repose l'inactif pour une minute, le débogage sur le PIX affiche :

```
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
```

L'utilisateur devra authentifier à nouveau quand retournant au même hôte de cible ou à un

différent hôte.

## HTTP virtuel

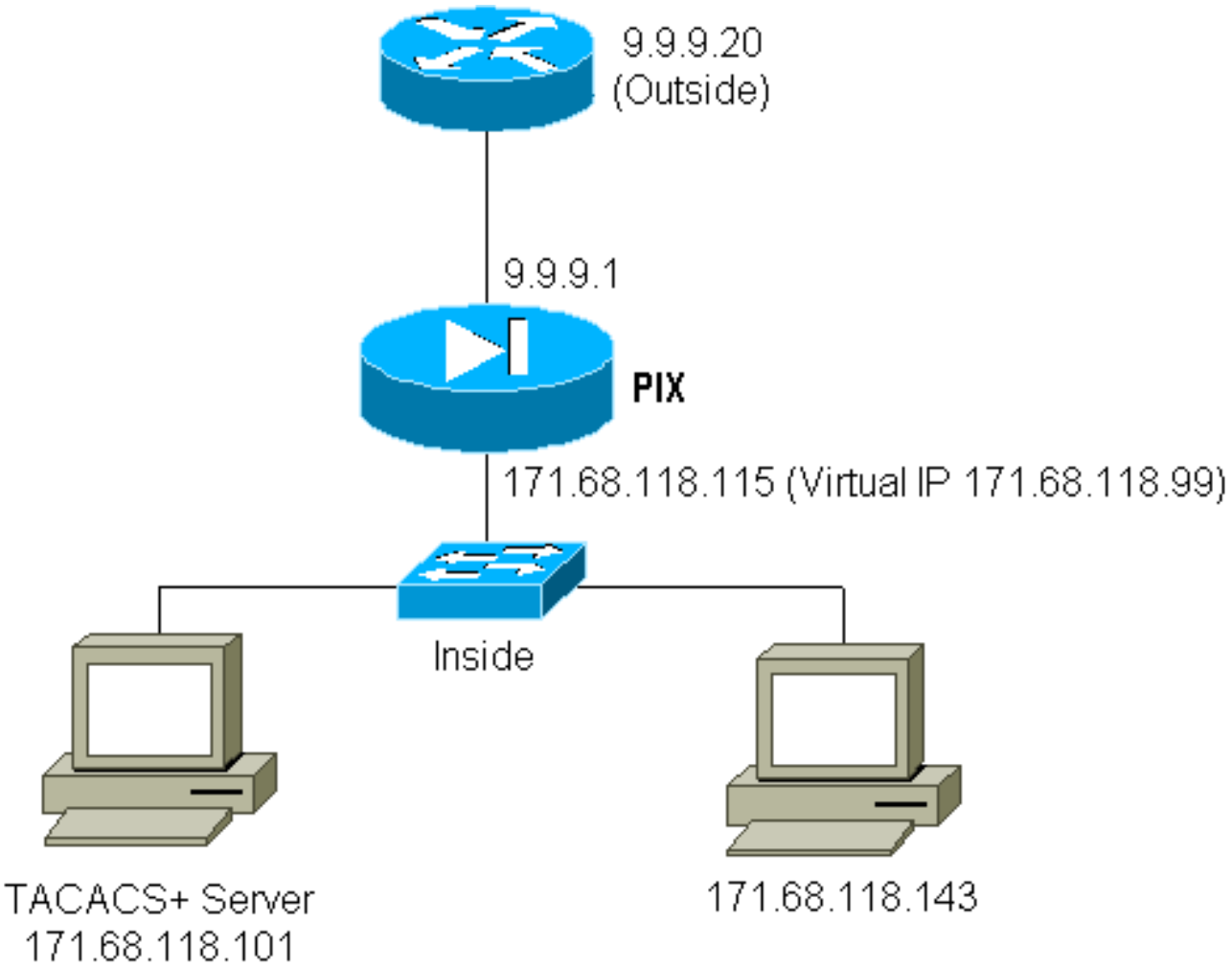
Si l'authentification est exigée sur des sites en dehors du PIX, aussi bien que sur le PIX lui-même, on peut parfois observer le comportement du navigateur peu commun puisque les navigateurs cachent le nom d'utilisateur et mot de passe.

Pour éviter ceci, vous pouvez implémenter le HTTP virtuel en ajoutant une adresse RFC 1918 (c'est-à-dire, une adresse qui est unroutable sur l'Internet, mais valide et seul pour le PIX à l'intérieur du réseau) à la configuration PIX utilisant la commande suivante :

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

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

**Exemple de sortie HTTP virtuelle :**




**HTTP virtuel de configuration PIX sortant :**

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

## Telnet virtuel

Configurer le PIX pour authentifier tout le trafic en entrée et en sortie n'est pas une bonne idée parce que quelques protocoles, tels que la « messagerie, » ne sont pas facilement authentifiés. Quand un essai de serveur de messagerie et de client à communiquer par le PIX quand tout le trafic par le PIX est authentifié, le Syslog PIX pour des protocoles non authentifiable affichera des messages comme :

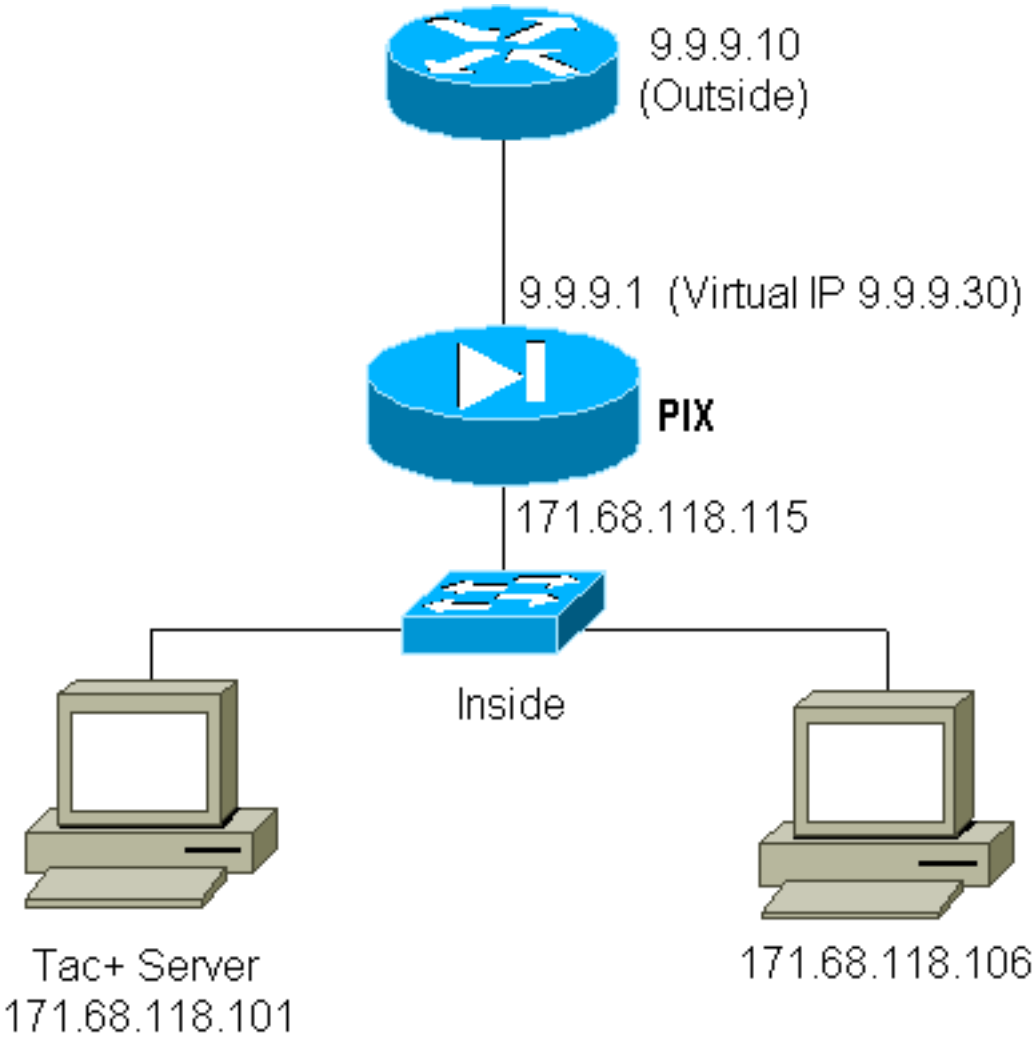
```
virtual http #.#.#.# [warn]
```

Puisque la messagerie et quelques autres services ne sont pas assez interactifs pour authentifier, une solution est d'utiliser **à moins que** commande pour l'authentification/autorisation (authentifiez tous excepté la source/destination du serveur de messagerie/du client).

Mais s'il y a vraiment un besoin d'authentifier un certain type service peu commun, ceci peut être fait au moyen de la **commande telnet virtuelle**. Cette commande permet à l'authentification pour se produire à l'IP virtuel de telnet. Après cette authentification, le trafic pour le service peu commun peut aller au vrai serveur qui est attaché à l'IP virtuel.

Dans notre exemple, nous voulons permettre au trafic du port TCP 49 pour découler de l'hôte 9.9.9.10 d'extérieur à l'hôte interne 171.68.118.106. Car ce trafic n'est pas vraiment authenticatable, nous installons le telnet virtuel.

**Telnet virtuel d'arrivée :**




**Configuration Virtual Telnet PIX d'arrivée :**

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

**Telnet virtuel de configuration utilisateur de serveur TACACS+ d'arrivée :**

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

**Telnet virtuel de debug PIX d'arrivée :**

L'utilisateur chez 9.9.9.10 doit d'abord authentifier par telnetting à l'adresse de 9.9.9.30 sur le PIX :

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

Après l'authentification réussie, la commande d'**uauth d'exposition** affiche que l'utilisateur a le « temps sur le mètre » :

```
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
```

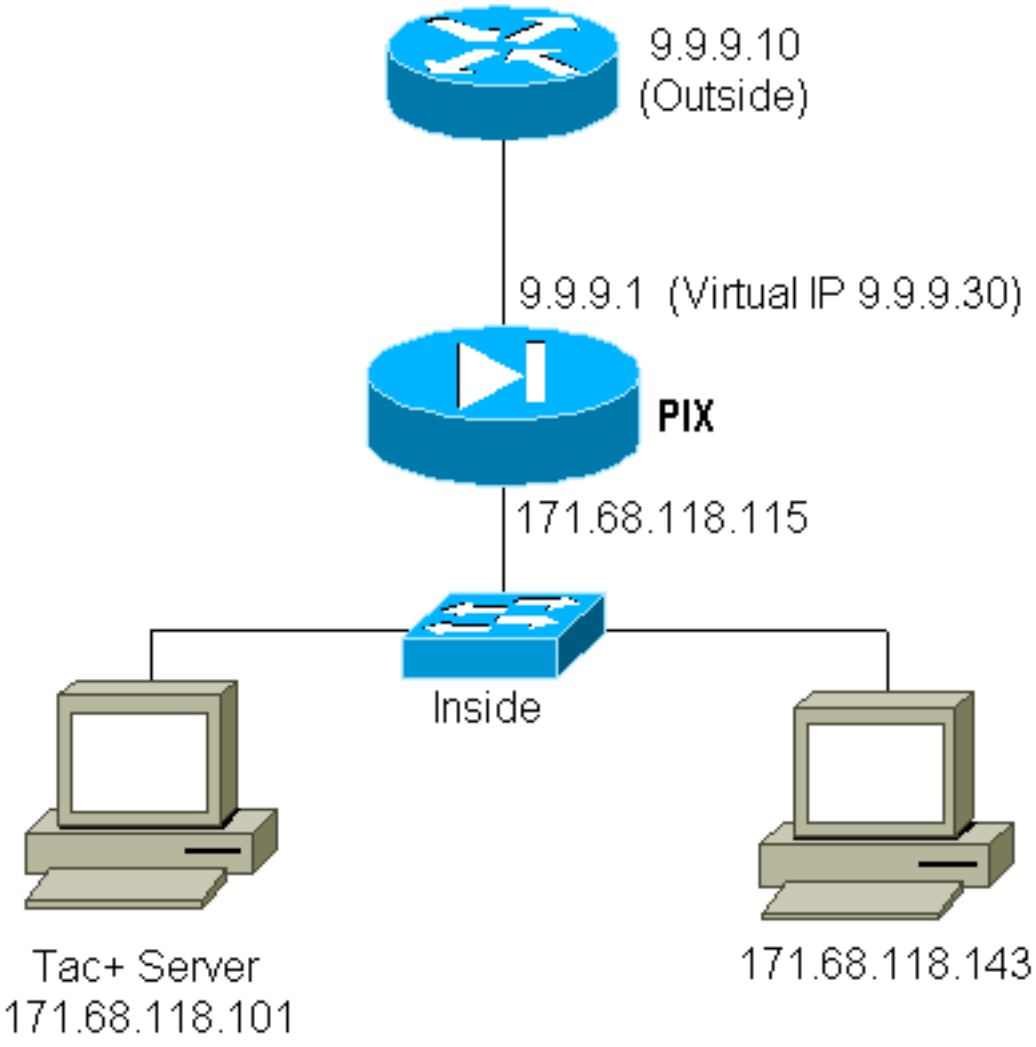
Et quand le périphérique chez 9.9.9.10 veut envoyer le trafic TCP/49 au périphérique chez 171.68.118.106 :

```
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
```

**Telnet virtuel sortant :**

Puisqu'on permet le trafic sortant par défaut, pas statique est exigé pour l'usage du telnet virtuel sortant. Dans l'exemple suivant, l'utilisateur intérieur chez 171.68.118.143 veulent le telnet à 9.9.9.30 virtuel et l'authentifient. La connexion de telnet est immédiatement abandonnée.

Une fois qu'authentifié, on permet le trafic TCP de 171.68.118.143 au serveur chez 9.9.9.10 :




**Configuration Virtual Telnet PIX sortante :**

```
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
```

**Telnet virtuel de debug PIX sortant :**

```
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
```

## Déconnexion virtuelle de Telnet

Quand les telnets d'utilisateur à l'IP virtuel de telnet, la commande d'**uauth d'exposition** affiche son uauth. Si l'utilisateur veut empêcher le trafic d'aller après que sa session soit de finition (quand il y a temps laissé dans l'uauth), il a besoin de telnet à l'IP virtuel de telnet de nouveau. Ceci bascule la session hors fonction.

## Autorisation sur le port

Vous pouvez avoir besoin de l'autorisation sur une plage de port. Dans l'exemple suivant, l'authentification était encore exigée pour tout le sortant, mais l'autorisation est seulement exigée pour des 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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Ainsi, quand nous telnet de 171.68.118.143 à 9.9.9.10, à l'authentification et à l'autorisation nous sommes produits parce que le port 23 de telnet est dans la plage 23-49. Quand nous faisons une session de HTTP de 171.68.118.143 à 9.9.9.10, nous devons encore authentifier, mais le PIX ne demande pas au serveur TACACS+ d'autoriser le HTTP parce que 80 n'est pas dans la plage 23-49.

**Configuration du serveur de logiciel gratuit TACACS+**

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

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

**Debug sur le PIX :**

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

## Informations connexes

- Support produit de Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX