Configuration de PIX 5.1.x : TACACS+ et RADIUS

Contenu

Introduction

L'authentification de RAYON et TACACS+ peut être faite pour le FTP, le telnet, et les connexions HTTP. L'authentification pour d'autres protocoles 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 5.1 au-dessus de la version préalable incluent l'authentification étendue (le Xauth)-- l'authentification d'IPSec perce un tunnel du Cisco Secure VPN Client 1.1.

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

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Informations générales

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.
- Est la comptabilité ce que l'utilisateur a fait.

Supposez vous avez cent utilisateurs intérieurs et vous vouloir voulez seulement que six de ces utilisateurs puisse faire le FTP, le telnet, ou le HTTP en dehors du réseau. Vous diriez le PIX d'authentifier le trafic sortant et de donner chacun des six à des utilisateurs id sur le serveur sécurisé TACACS+/RADIUS. Avec l'authentification simple, ces six utilisateurs pourraient être authentifiés avec le nom d'utilisateur et mot de passe, puis sortent. Les quatre-vingt-quatorze 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 six utilisateurs pourraient faire le FTP, le telnet, ou le HTTP.

Mais supposez *un de* ces six utilisateurs, « Festus, » n'est pas à sont de confiance. Vous voudriez permettre à Festus 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. C'est seulement valide avec TACACS+. Quand nous ajoutons l'*autorisation au* PIX, le PIX d'abord envoie le nom d'utilisateur et mot de passe de Festus au serveur sécurisé, alors envoie à une demande d'autorisation indiquant au serveur sécurisé ce que la « *commande* » Festus essaye de faire. Avec la configuration du serveur correctement, Festus a pu être permis au « FTP 1.2.3.4 » mais serait 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 une invite de nom d'utilisateur être soulevé, puis une demande pour le mot de passe. Si l'authentification (et l'autorisation) est réussie au PIX/server, l'utilisateur est incité pour le nom d'utilisateur et mot de passe par la destination host au-delà.
- **FTP** - L'utilisateur voit une invite de nom d'utilisateur être soulevé. Les besoins de l'utilisateur d'entrer dans **local_username@remote_username** pour le nom d'utilisateur et **local_password@remote_password** pour le mot de passe. Le PIX envoie le local_username et le local_password au serveur de sécurité local, 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 un 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 tirant 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 des expositions ce phénomène. Si le telnet et le FTP semblent fonctionner normalement, mais les connexions HTTP ne font pas, c'est pourquoi.
- **Tunnel** - En tentant de percer un tunnel le trafic d'IPSec dans le réseau avec le client vpn et le Xauth en fonction, une case grise pour la « authentification de l'utilisateur pour la nouvelle connexion » est affichée pour le nom d'utilisateur/mot de passe.**Remarque:** Cette authentification est début pris en charge avec le Cisco Secure VPN Client 1.1. Si l'**aide > au sujet du** menu ne fait pas le show version 2.1.x ou plus tard, ceci ne fonctionne pas.

Configurations de serveur sécurisé utilisées pour tous les scénarios

Configuration de serveur TACACS de Cisco Secure UNIX

Dans cette section, vous êtes présenté avec les informations pour configurer votre serveur sécurisé.

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 de Cisco Secure UNIX

Utilisez le GUI pour ajouter l'adresse IP et la clé PIX à la liste de serveur d'accès à distance (NAS).

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

Cisco Secure ACS pour le RAYON de Windows 2.x

Employez ces étapes pour configurer le Cisco Secure ACS pour le RAYON de Windows 2.x.

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'adresse IP PIX dans le GUI de section de configuration de NAS.

EasyACS TACACS+

La documentation d'EasyACS décrit l'installation.

1. Dans la section de groupe, **exécutif de shell de** clic pour donner des privilèges EXEC.
2. Pour ajouter l'autorisation au PIX, cliquez sur en fonction les **commandes IOS inégalées Deny au** bas de l'installation de groupe.
3. **Nouvelle commande d'Add/Edit** choisi pour chaque commande que vous souhaitez permettre, par exemple, le **telnet**.
4. Si on permet Telnetting aux sites spécifiques, complétez l'adresse IP dans l'argument section sous la forme la « autorisation #.#.#.# ». Autrement, pour permettre Telnetting, le clic **permettent à 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.

2.x Cisco Secure TACACS+

L'utilisateur obtient un mot de passe dans le partie Interface graphique d'installation des utilisateurs.

1. Dans la section de groupe, cliquez sur en fonction l'**exécutif de shell** pour donner des privilèges EXEC.
2. Pour ajouter l'autorisation au PIX, au bas de l'installation de groupe, le clic **refusent des commandes IOS inégalées**.
3. **Nouvelle commande d'Add/Edit** choisi pour chaque commande que vous souhaitez permettre (par exemple, **telnet**).
4. Pour permettre Telnetting aux sites spécifiques, écrivez l'adresse IP dans l'argument section sous la forme la « autorisation #.#.#.# ». Pour permettre Telnetting à n'importe quel site, 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. Assurez que l'adresse IP PIX est ajoutée dans la section GUI de configuration de NAS.

Configuration du serveur Livingston RADIUS

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

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

Configuration du serveur Merit RADIUS

Ajoutez l'adresse 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"
```

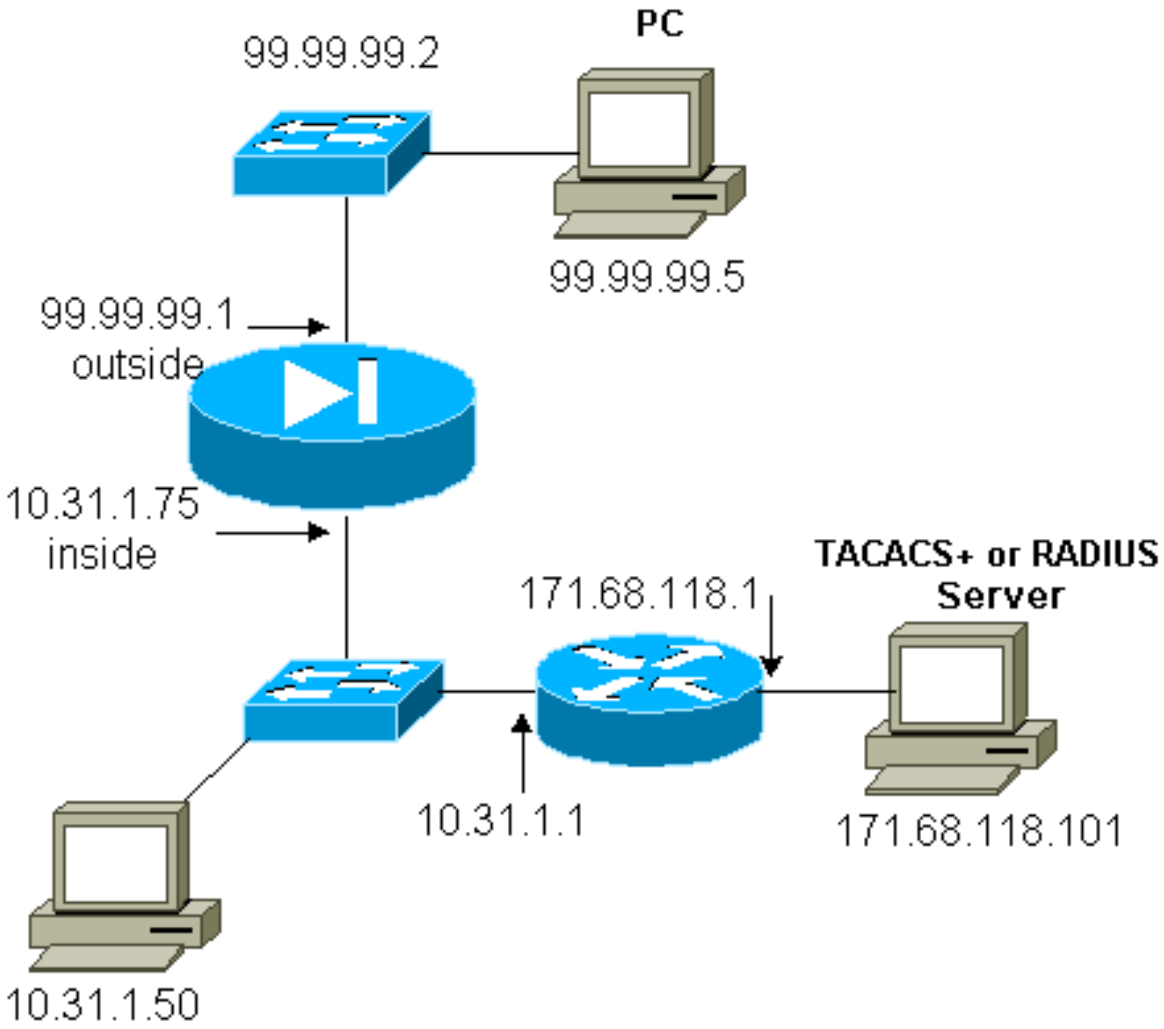
```
default service = permit
}

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

Remarque: Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- Assurez-vous que la configuration PIX fonctionne avant d'ajouter l'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.Le logging console debugging ne devrait pas être utilisé sur un système fortement chargé.Le logging buffered debugging peut être utilisé, puis exécute la commande de **show logging**.Se connecter peut également être envoyé à un serveur de Syslog et être examiné là.
- Activez l'élimination des imperfections sur les serveurs TACACS+ ou de RAYON (tous les serveurs ont cette option).

Diagramme du réseau



Configuration PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
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
no logging standby
logging console debugging no logging monitor no logging
buffered no logging trap no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu pix/intf2
1500 ip address outside 99.99.99.1 255.255.255.0 ip
address inside 10.31.1.75 255.255.255.0 ip address
pix/intf2 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 arp timeout 14400 global (outside) 1
```

```
99.99.99.7-99.99.99.10 netmask 255.255.255.0 nat
(inside) 1 10.31.1.0 255.255.255.0 0 0 static
(inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0 conduit permit icmp any any conduit
permit tcp any any conduit permit udp any any route
outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 route inside
171.68.120.0 255.255.255.0 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 0:05:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.101 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.101 cisco timeout 5 aaa authentication
include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include telnet inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
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
floodguard enable telnet timeout 5 terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca : end
[OK]
```

Exemples de debug d'authentification de PIX

Cette section affiche que les échantillons d'authentification met au point pour différents scénarios.

D'arrivée

L'utilisateur externe aux initiés de 99.99.99.2 trafiquent à 10.31.1.50 intérieur (99.99.99.99) et sont authentifiés par TACACS (c'est-à-dire, liste d'arrivée « AuthInbound » de serveur d'utilisations du trafic qui inclut le serveur TACACS 171.68.118.101).

Debug PIX - Bonne authentification - TACACS+

L'exemple ci-dessous affiche qu'un PIX met au point avec la bonne authentification :

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

Debug PIX - Authentification erronée (nom d'utilisateur ou mot de passe) - TACACS+

L'exemple ci-dessous affiche qu'un PIX met au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit trois positionnements de nom d'utilisateur/mot de

passe, suivis de ce message : `Erreur : nombre maximum d'essais dépassés.`

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

Debug PIX - Ne peut cingler le serveur, aucune réponse - TACACS+

L'exemple ci-dessous affiche qu'un PIX met au point où le serveur fait l'objet d'un ping, mais ne parlant pas au PIX. L'utilisateur voit le nom d'utilisateur une fois, mais le PIX ne demande jamais un mot de passe (c'est sur le telnet). L'utilisateur voit l'`erreur : Nombre maximum d'essais dépassés.`

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

Debug PIX - Incapable de cingler le serveur - TACACS+

L'exemple ci-dessous affiche qu'un PIX met au point où le serveur n'est pas pingable. L'utilisateur voit le nom d'utilisateur une fois, mais le PIX ne demande jamais un mot de passe (c'est sur le telnet). Les messages suivants sont affichés : `Délai d'attente au serveur` et à l'`erreur TACACS+ : Nombre maximum d'essais dépassés` (un serveur faux a été permuté dedans la configuration).

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

Debug PIX - Bonne authentification - RAYON

L'exemple ci-dessous affiche qu'un PIX met au point avec la bonne authentification :

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

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

L'exemple ci-dessous affiche qu'un PIX met au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit la demande pour un nom d'utilisateur et mot de passe, et a trois occasions d'entrer dans ces derniers. Quand l'entrée est infructueuse, le message suivant est affiché : `Erreur : nombre maximum d'essais dépassés.`

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

Debug PIX - Peut cingler le serveur, le démon vers le bas - RAYON

L'exemple ci-dessous affiche qu'un PIX met au point où le serveur fait l'objet d'un ping, mais le démon est vers le bas et ne communiquera pas avec le PIX. L'utilisateur voit le nom d'utilisateur, puis le mot de passe, le `serveur de RAYON a manqué` message, et l'`erreur : Nombre maximum d'essais dépassés.` .

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

Debug PIX - Incapable de cingler le serveur ou de les introduire/non-concordance de client - RAYON

L'exemple ci-dessous affiche qu'un PIX met au point où le serveur n'est pas pingable ou il y a un client/non-concordance principale. L'utilisateur voit un nom d'utilisateur, le mot de passe, le `délai d'attente aux messages serveur de RAYON`, et l'`erreur : Le nombre maximum du message de dépassement d'essais un` serveur faux a été permuté dedans la configuration).

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

Ajout d'autorisation

Si vous décidez d'ajouter l'autorisation, puisque l'autorisation est non valide sans authentification, vous devez avoir besoin de l'autorisation pour le même intervalle source et de destination.

```
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 vous n'ajoutez pas l'autorisation pour sortant parce que le trafic sortant est authentifié avec le RAYON, et l'autorisation RADIUS est non valide.

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

Debug PIX - Bonne authentification et autorisation réussie - TACACS+

L'exemple ci-dessous affiche qu'un PIX met au point avec la bonne authentification et l'autorisation réussie :

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

Debug PIX - Bonne authentification, autorisation défaillante - TACACS+

L'exemple ci-dessous affiche que les PIX mettent au point avec la bonne authentification mais l'autorisation défaillante. Ici l'utilisateur voit également l'`erreur de` message `: Autorisation refusée`.

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

Ajout de la comptabilité

TACACS+

aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

Logiciel gratuit TACACS+ sorti :

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RAYON

aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound

Merit RADIUS sorti :

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

L'utilisation de excluent la commande

Si nous ajoutons un autre extérieur d'hôte (chez 99.99.99.100) à notre réseau, et cet hôte est de confiance, vous pouvez les exclure de l'authentification et de l'autorisation avec les commandes suivantes :

aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255 AuthInbound

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 RAYON suppose que la personne est encore ouverte une session (c'est-à-dire, l'utilisateur a une session par le PIX).

Ceci fonctionne bien pour le telnet et les connexions FTP en raison de la nature des connexions. 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.

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

```
   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
```

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

L'utilisateur va environ leur telnet ou activités en FTP sur l'hôte de cible, puis les sorties (passe dix minutes là) :

```
pix) 302002: Teardown TCP connection 5 faddr
     9.9.9.25/80 gaddr 9.9.9.10/128
  1 laddr 171.68.118.100/1281 duration 0:00:00
     bytes 1907 (cse)
  (server stop account) Sun Nov 8 16:41:17 1998
     rtp-pinecone.rtp.cisco.com cse
  PIX 171.68.118.100 stop task_id=0x3 foreign_ip=9.9.9.25
     local_ip=171.68.118.100
  cmd=telnet elapsed_time=5 bytes_in=98 bytes_out=36
```

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

Le HTTP fonctionne différemment en raison de la nature du protocole. Est ci-dessous un exemple de HTTP :

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

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

L'utilisateur lit la page Web téléchargée.

L'enregistrement de début est signalé à 16:35:34 et à l'enregistrement d'arrêt à 16:35:35. Ce téléchargement a pris une seconde (c'est-à-dire, il y avait moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur est-il encore ouvert une session au site Web et à la connexion encore ouverts quand l'utilisateur lit la page Web ? Non. 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 d'arrêt est fraction de seconde. Il n'y a pas un enregistrement de début sans enregistrement d'arrêt puisque les enregistrements se produisent pratiquement au même instant. Il y aura toujours enregistrement de début et d'arrêt envoyé au serveur pour chaque transaction si l'uauth est placé pour 0 ou quelque chose plus grande. Cependant, les maximum-sessions et l'affichage des utilisateurs connectés ne fonctionneront pas en raison de la nature de la connexion HTTP.

Authentification et activation sur le PIX lui-même

Les soucis précédents de discussion authentifiant le telnet (et le HTTP, le FTP) trafiquent par le PIX. Assurez le telnet aux travaux PIX sans authentification en fonction :

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

Ajoutez alors la commande d'authentifier des utilisateurs Telnetting au PIX :

```
aaa authentication telnet console AuthInbound
```

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

Si le serveur est en panne, vous pouvez accéder au PIX en écrivant le **pix** pour le nom d'utilisateur, et puis le mot de passe d'enable (**mot de passe d'enable** *quoi que*). Avec la commande :

```
aaa authentication enable console AuthInbound
```

L'utilisateur est incité pour un nom d'utilisateur et mot de passe qui est envoyé au serveur TACACS ou de RAYON. Dans ce cas puisque la liste de serveur d'AuthInbound est utilisée, le PIX demande le nom d'utilisateur et mot de passe TACACS+.

Puisque le paquet d'authentification pour l'enable est identique que le paquet d'authentification pour la procédure de connexion, si l'utilisateur peut ouvrir une session au PIX avec TACACS ou RAYON, ils peuvent activer par TACACS ou RAYON avec le même nom d'utilisateur/mot de passe. Ce problème a été assigné l'ID de bogue Cisco CSCdm47044 (clients enregistrés seulement).

Si le serveur est en panne, vous pouvez accéder au mode enable PIX en entrant le **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, écrivent le **pix** pour le nom d'utilisateur et appuyez sur **entrent**. Si le mot de passe d'enable est placé mais pas connu, une disquette de récupération de mot de passe doit être construite pour remettre à l'état initial le mot de passe.

Changeant les invites utilisateur voient

Si vous avez la commande :

auth-prompt PIX_PIX_PIX

les utilisateurs allant par le PIX voient l'ordre suivant :

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

Dès l'arrivée à la destination finale, les utilisateurs verraient le nom d'utilisateur : et mot de passe : demande affichée par la case de destination. 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 le youh ont les commandes :

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

alors les utilisateurs voient l'ordre suivant sur procédure de connexion défectueuse/réussie par le PIX :

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

inactif et temporisations absolues de Par-utilisateur

Cette fonction ne fonctionne actuellement pas et le problème a été assigné l'ID de bogue Cisco CSCdp93492 (clients enregistrés seulement).

HTTP virtuel

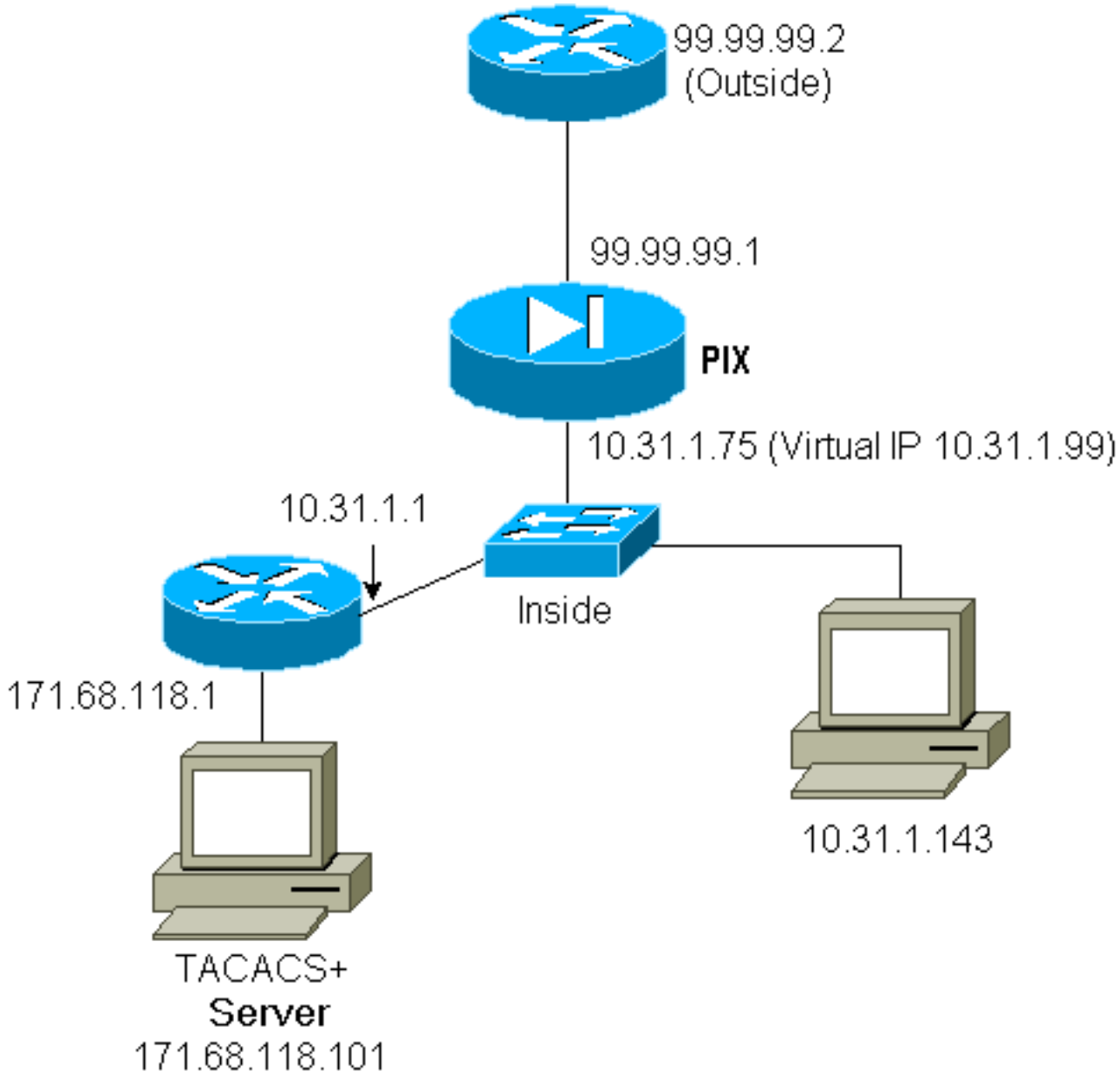
Si l'authentification est exigée sur des sites en dehors du PIX aussi bien que sur le PIX lui-même, on peut parfois observer le comportement du navigateur peu commun, puisque les navigateurs cachent le nom d'utilisateur et mot de passe.

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 :

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 01:00:00 aaa
authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa-server
RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound (inside)
host 171.68.118.101 cisco timeout 5 virtual http 10.31.1.99
```

Telnet virtuel

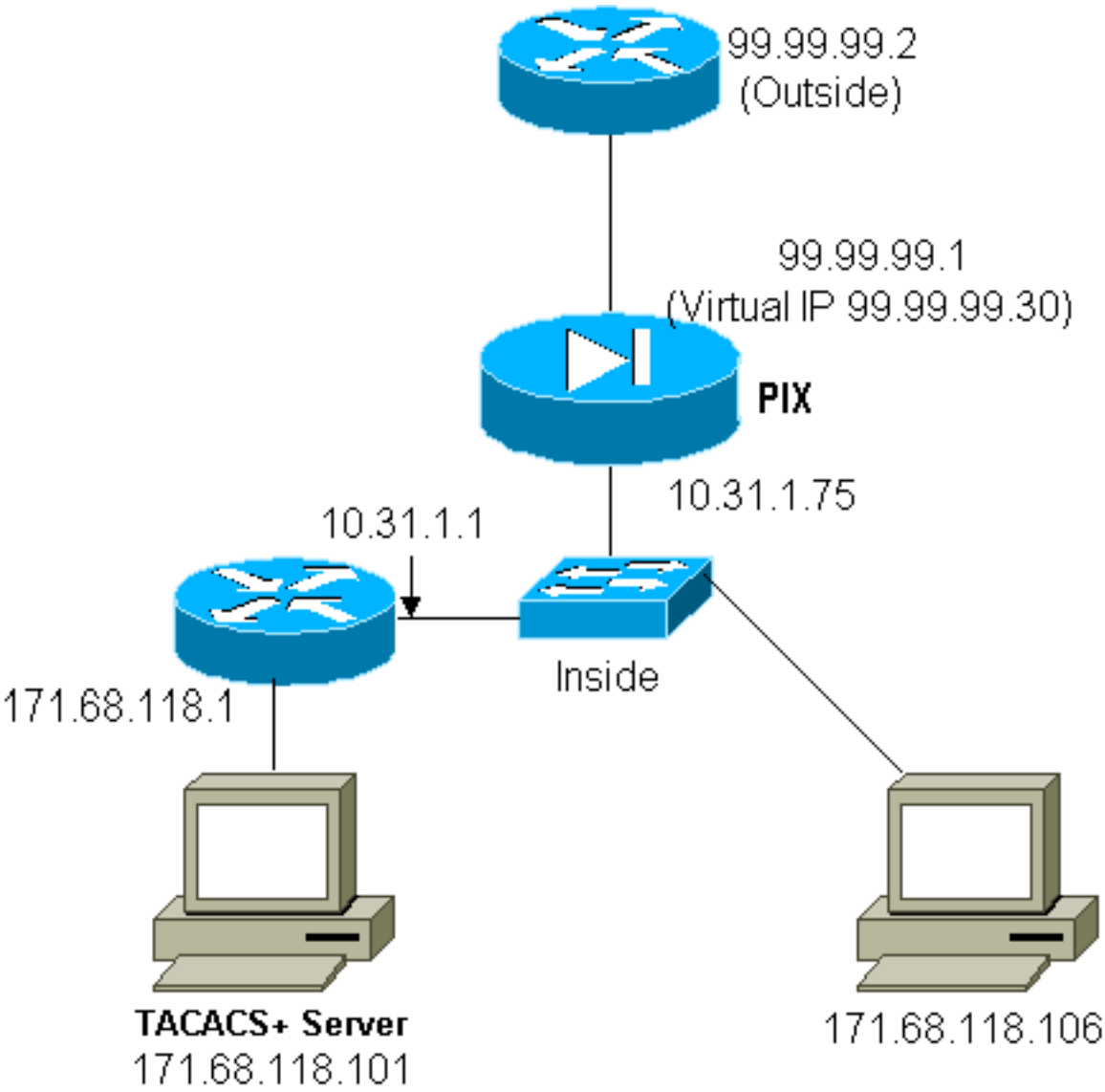
Il est possible de configurer le PIX pour authentifier tout d'arrivée et sortant, mais ce n'est pas une bonne idée parce que quelques protocoles, tels que la messagerie, ne sont pas facilement authentifiés. Quand un serveur de messagerie et un essai de client à communiquer par le PIX quand tout le trafic par le PIX est authentifié, Syslog PIX pour des protocoles non authentifiable affiche des messages comme :

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

Cependant, 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'adresse IP virtuelle de telnet. Après cette authentification, le trafic pour le service peu commun peut aller au vrai serveur.

Dans cet exemple, vous voulez que le trafic du port TCP 49 découle de l'hôte 99.99.99.2 d'extérieur à l'hôte interne 171.68.118.106. Puisque ce trafic n'est pas vraiment authenticatable, installez un telnet virtuel. Pour le telnet virtuel, il doit y a une charge statique associée. Ici, 99.99.99.20 et 171.68.118.20 sont des adresses virtuelles.

Telnet virtuel d'arrivée



Configuration Virtual Telnet PIX d'arrivée

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 static
(inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0 static (inside,outside)
99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.20 eq
telnet any conduit permit tcp host 99.99.99.30 eq tacacs any aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+ aaa-server Incoming (inside) host 171.68.118.101 cisco
timeout 5 aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming virtual telnet
```

99.99.99.20

Telnet virtuel de debug PIX d'arrivée

L'utilisateur chez 99.99.99.2 doit d'abord authentifier par Telnetting à l'adresse de 99.99.99.20 sur le PIX :

```
109001: Auth start for user '???' from
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

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 2 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

Et quand le périphérique chez 99.99.99.2 veut envoyer le trafic TCP/49 au périphérique chez 171.68.118.106 :

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

L'autorisation peut être ajoutée :

```
aaa authorization include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

de sorte que quand le trafic TCP/49 est tenté par le PIX, le PIX envoie également la requête d'autorisation au serveur :

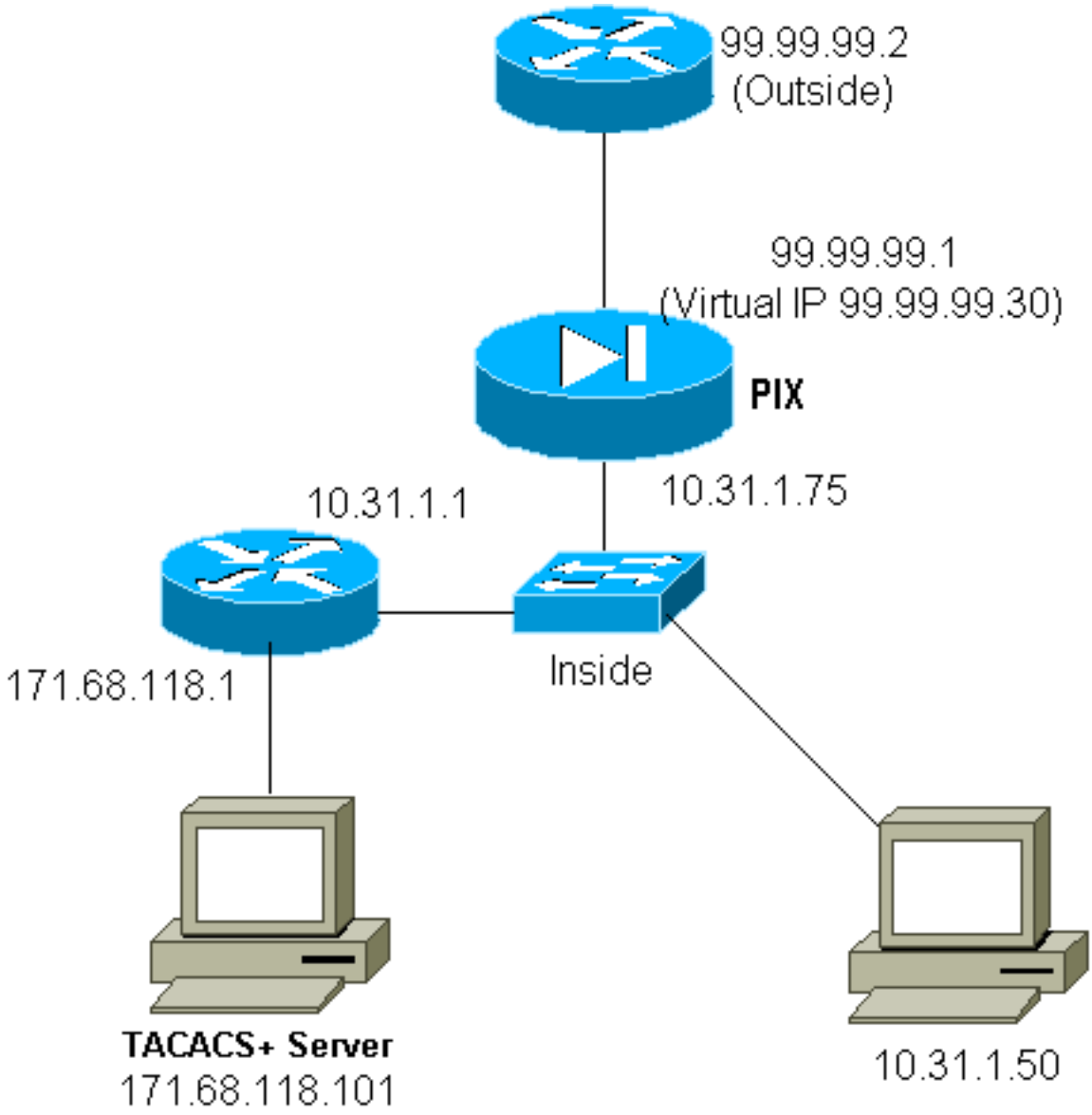
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

Sur le serveur TACACS+, ceci est vu en tant que :

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

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 aux telnets de 10.31.1.50 à 99.99.99.30 virtuel et authentifie ; la connexion de telnet est immédiatement abandonnée. Une fois qu'authentifié, on permet le trafic TCP de 10.31.1.50 au serveur chez 99.99.99.2 :



Configuration Virtual Telnet PIX sortante :

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 0:05:00 absolute aaa-
server RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 171.68.118.101 cisco timeout 5 aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound virtual telnet 99.99.99.30
```

Remarque: Il n'y a aucune autorisation puisque c'est RAYON.

Telnet virtuel de debug PIX sortant :

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
```

```
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

Déconnexion virtuelle de Telnet

Quand le telnet d'utilisateurs à l'adresse IP virtuelle de telnet, la commande d'**uauth d'exposition** affiche leur uauth. Si les utilisateurs veulent empêcher le trafic d'aller après que leurs sessions soient de finition quand il y a temps laissé dans l'uauth, elles ont besoin de telnet à l'adresse IP virtuelle de telnet de nouveau. Ceci bascule la session hors fonction.

Après la première authentification :

```
 pix3# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'pixuser' at 10.31.1.50, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 109005:
Authentication succeeded for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 on interface
inside
```

Après la deuxième authentification (c'est-à-dire, le trou est basculé fermé) :

```
 pix3# show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

Autorisation sur le port

On permet l'autorisation pour des plages de port (comme TCP/30-100). Si le telnet virtuel est configuré sur le PIX et l'autorisation pour une plage de port, une fois que le trou est ouvert avec le telnet virtuel, le PIX fournit une commande **tcp/30-100 au** serveur TACACS+ pour l'autorisation :

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0 conduit permit tcp
host 99.99.99.75 host 99.99.99.2 static (inside,outside) 99.99.99.75 10.31.1.50 netmask
255.255.255.255 0 0 virtual telnet 99.99.99.75 aaa authentication include any inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound virtual telnet 99.99.99.30
```

Configuration du serveur de logiciel gratuit TACACS+ :

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

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

Après vérification du telnet virtuel travaillé pour permettre le trafic TCP/49 à l'hôte à l'intérieur du réseau, nous avons décidé que nous avons voulu expliquer ceci, ainsi nous avons ajouté :

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

Ceci a en faisant couper un enregistrement des comptes quand le trafic tcp/49 intervient (cet exemple est du logiciel gratuit TACACS+) :

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

Authentification étendue (Xauth)

Exemples de configuration

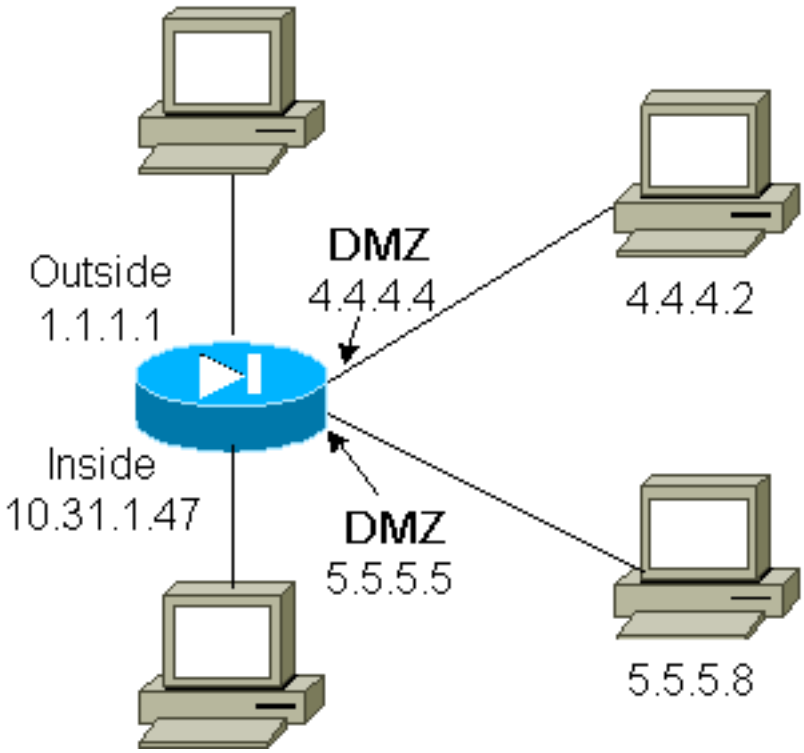
- Terminaison de tunnels IPSec sur des interfaces de pare-feu Cisco Secure PIX Firewall multiples avec Xauth
- IPSec entre le pare-feu Cisco Secure PIX et un client vpn avec l'authentification étendue

Authentification sur le DMZ

Pour authentifier des utilisateurs allant d'une interface DMZ à l'autre, dites le PIX d'authentifier le trafic pour les interfaces Désignées. Sur notre PIX l'organisation est :

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

Diagramme du réseau



Configuration PIX

Nous voulons authentifier le trafic de telnet entre pix/intf4 et pix/intf5 :

```
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3 security15) nameif ethernet4 pix/intf4
security20 nameif ethernet5 pix/intf5 security25 ip address outside 1.1.1.1 255.255.255.0 ip
address inside 10.31.1.47 255.255.255.0 (ip address pix/intf2 127.0.0.1 255.255.255.255 ip
address pix/intf3 127.0.0.1 255.255.255.255) ip address pix/intf4 4.4.4.4 255.255.255.0 ip
address pix/intf5 5.5.5.5 255.255.255.0 static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask
255.255.255.255 0 0 aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa-server TACACS+ protocol tacacs+ aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Comptabilité de Xauth

Si la commande d'**autorisation-ipsec de connexion de sysopt**, pas la commande pl-**compatible d'ipsec de sysopt**, n'est configurée dans le PIX avec le Xauth, la comptabilité est valide pour des connexions TCP, mais pas l'ICMP ou l'UDP.

Informations connexes

- Page de support produit PIX
- Référence des commandes PIX
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Page d'assistance Cisco Secure UNIX
- Cisco Secure ACS pour la page d'assistance de Windows
- Support technique - Cisco Systems