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

Contenu

Introduction

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

L'autorisation TACACS+ est prise en charge ; L'autorisation RADIUS n'est pas valide. Les modifications apportées à l'authentification, à l'autorisation et à la comptabilité (AAA) PIX 4.4.1 par rapport à la version précédente sont les suivantes : Groupes de serveurs AAA et basculement, authentification pour l'accès à la console active et série, et acceptation et rejet des messages d'invite.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Conventions

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

Authentification et autorisation

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

Supposons que vous ayez 100 utilisateurs à l'intérieur et que vous voulez que seulement 6 de ces utilisateurs puissent faire FTP, Telnet ou HTTP en dehors du réseau. Vous demanderiez au PIX d'authentifier le trafic sortant et de donner les ID des 6 utilisateurs sur le serveur de sécurité TACACS+/RADIUS. Avec une authentification simple, ces 6 utilisateurs peuvent être authentifiés avec un nom d'utilisateur et un mot de passe, puis sortez. Les 94 autres utilisateurs n'ont pas pu sortir. Le PIX invite les utilisateurs à saisir leur nom d'utilisateur/mot de passe, puis transmet leur nom d'utilisateur et leur mot de passe au serveur de sécurité TACACS+/RADIUS et, selon la réponse, ouvre ou refuse la connexion. Ces 6 utilisateurs peuvent effectuer des protocoles FTP, Telnet ou HTTP.

Mais supposons qu'un de ces trois utilisateurs, « Terry », ne soit pas digne de confiance. Vous souhaitez autoriser Terry à faire FTP, mais pas HTTP ou Telnet vers l'extérieur. Cela signifie qu'il faut ajouter une autorisation, c'est-à-dire autoriser ce que les utilisateurs peuvent faire en plus d'authentifier qui ils sont. Lorsque nous ajoutons une autorisation au PIX, le PIX envoyait d'abord le nom d'utilisateur et le mot de passe de Terry au serveur de sécurité, puis envoyait une demande d'autorisation indiquant au serveur de sécurité quelle « commande » Terry essaie de faire. Une fois le serveur configuré correctement, Terry pourrait être autorisé à « FTP 1.2.3.4 »

mais refuserait la possibilité de HTTP ou Telnet n'importe où.

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

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

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

Configurations de serveur de sécurité utilisées pour tous les scénarios

Configuration du serveur TACACS 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 RADIUS UNIX CiscoSecure

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

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

CiscoSecure NT 2.x RADIUS

Procédez comme suit :

1. Obtenez un mot de passe dans la section GUI du programme d'installation de l'utilisateur.
2. Dans la section GUI de la configuration du groupe, définissez l'attribut 6 (Service-Type) sur Login ou Administrative.
3. Ajoutez l'adresse IP PIX dans l'interface graphique de configuration NAS.

EasyACS TACACS+

La documentation EasyACS décrit la configuration.

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

6. Exécutez les étapes 1 à 5 pour chacune des commandes autorisées (par exemple, Telnet, HTTP et/ou FTP).
7. Ajoutez l'adresse IP PIX dans la section Interface graphique utilisateur de la configuration NAS.

CiscoSecure 2.x TACACS+

L'utilisateur obtient un mot de passe dans la section Configuration utilisateur de l'interface utilisateur graphique.

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

Configuration du serveur RADIUS de Livingston

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

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

Mériter la configuration du serveur RADIUS

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

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

Configuration du serveur de logiciel gratuit TACACS+

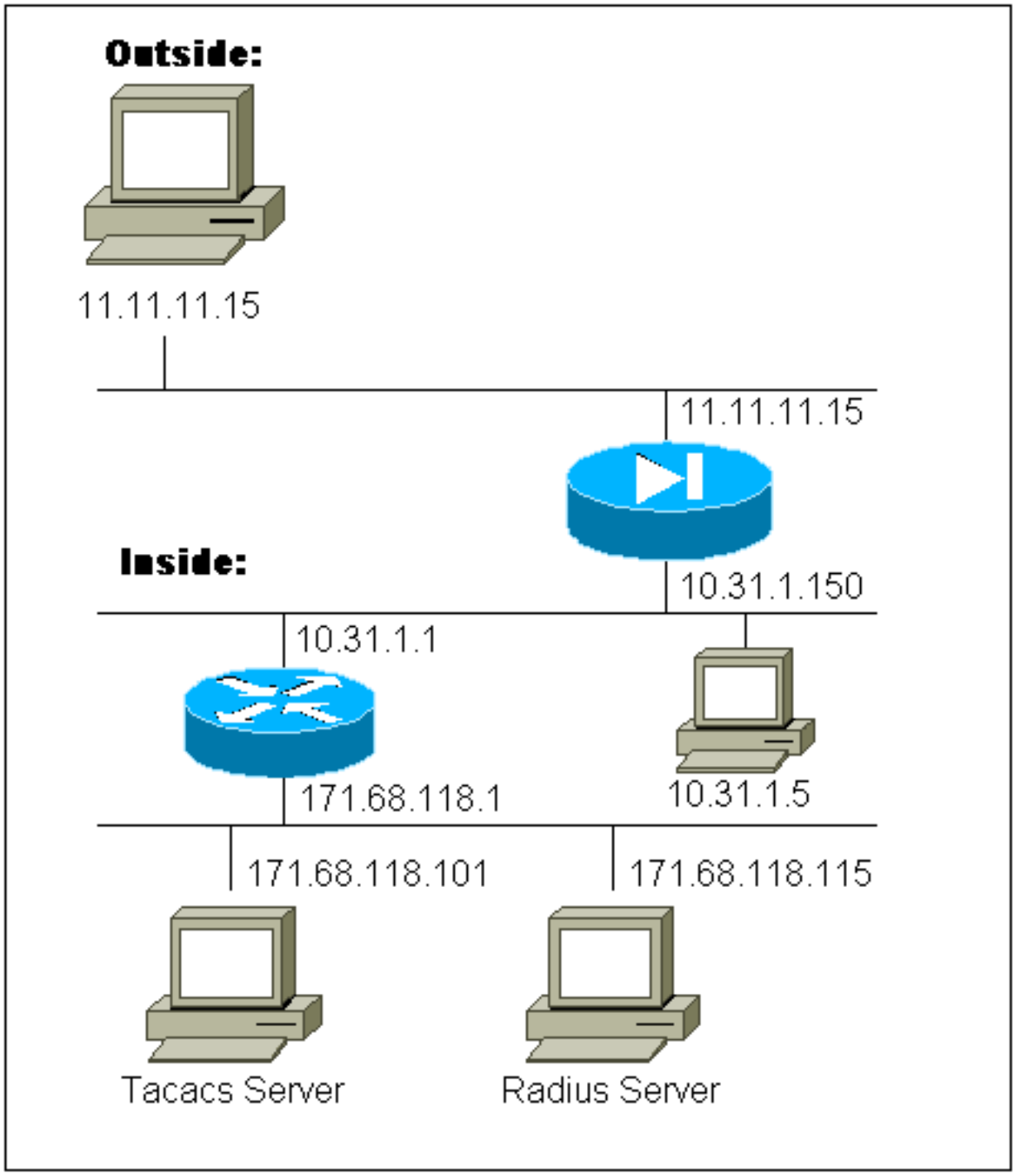
```
key = "cisco"

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

Diagramme du réseau



Configuration PIX

```
pix-5# write terminal
 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 débogage d'authentification à partir de PIX

Dans ces exemples de débogage :

Sortant

L'utilisateur interne 10.31.1.5 initie le trafic vers l'extérieur 11.11.11.15 et est authentifié via TACACS+ (le trafic sortant utilise la liste de serveurs « Sortant » qui inclut le serveur TACACS 171.68.118.101).

Entrant

L'utilisateur externe à l'adresse 11.11.15 initie le trafic vers l'adresse 10.31.1.5 interne (11.11.11.22) et est authentifié via RADIUS (le trafic entrant utilise la liste de serveurs « Entrant » qui inclut le serveur RADIUS 171.68.118.115).

Débogage PIX - Bonne authentification - TACACS+

L'exemple ci-dessous montre le débogage PIX avec une bonne authentification :

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

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

L'exemple ci-dessous montre le débogage PIX avec une authentification incorrecte (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre jeux de nom d'utilisateur/mot de passe. Le message suivant s'affiche : « Error : nombre maximal de tentatives dépassé ».

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

Débogage PIX - Ping possible, mais pas de réponse - TACACS+

L'exemple ci-dessous montre le débogage PIX pour un serveur ping qui ne parle pas au PIX. L'utilisateur voit le nom d'utilisateur une fois et PIX ne demande jamais de mot de passe (il s'agit de Telnet).

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

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

L'exemple ci-dessous montre le débogage PIX d'un serveur qui n'est pas capable d'envoyer une requête ping. L'utilisateur voit le nom d'utilisateur une fois. PIX ne demande jamais de mot de passe (il s'agit de Telnet). Le message suivant s'affiche : « Délai d'attente pour le serveur TACACS+" et « Erreur : Nombre maximal d'essais dépassé » (la configuration de cet exemple reflète un faux serveur).

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

Débogage PIX - Bonne authentification - RADIUS

L'exemple ci-dessous montre le débogage PIX avec une bonne authentification :

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

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

L'exemple ci-dessous montre le débogage PIX avec une authentification incorrecte (nom d'utilisateur ou mot de passe). L'utilisateur voit une demande de nom d'utilisateur et de mot de passe. Si l'un des deux est incorrect, le message « Mot de passe incorrect » s'affiche quatre fois. Ensuite, l'utilisateur est déconnecté. Ce problème a reçu l'ID de bogue #CSCdm46934.

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

Débogage PIX - Démon désactivé, ne communiquera pas avec PIX - RADIUS

L'exemple ci-dessous montre le débogage PIX avec un serveur ping, mais le démon est

désactivé. Le serveur ne communiquera pas avec PIX. L'utilisateur voit Username, suivi d'un mot de passe. Les messages suivants s'affichent : « Échec du serveur RADIUS » et « Erreur : Nombre maximal de tentatives dépassé ».

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

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

L'exemple ci-dessous montre le débogage PIX d'un serveur qui n'est pas capable d'envoyer une requête ping ou où il y a une incompatibilité clé/client. L'utilisateur voit le nom d'utilisateur et le mot de passe. Les messages suivants s'affichent : « Délai d'attente du serveur RADIUS » et « Erreur : Nombre maximal d'essais dépassé » (le serveur de la configuration n'est utilisé qu'à titre d'exemple).

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

Ajout d'autorisation

Comme l'autorisation n'est pas valide sans authentification, nous aurons besoin d'une autorisation pour la même plage 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 d'autorisation pour le trafic « entrant » car le trafic entrant est authentifié avec RADIUS et l'autorisation RADIUS n'est pas valide

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

Débogage PIX avec bonne authentification et autorisation réussie - TACACS+

L'exemple ci-dessous montre le débogage PIX avec une authentification correcte et une autorisation réussie :

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

Débogage PIX - Authentification correcte, autorisation échouée - TACACS+

L'exemple ci-dessous montre le débogage PIX avec une bonne authentification, mais l'autorisation a échoué :

Ici, l'utilisateur voit également le message « Erreur : Autorisation refusée »

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

Ajout de comptabilité

TACACS+

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

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

Les enregistrements comptables TACACS+ ressemblent aux suivants (ceux-ci proviennent de CiscoSecure UNIX ; ceux de CiscoSecure NT peuvent être délimités par des virgules) :

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

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

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

Les enregistrements comptables RADIUS ressemblent aux suivants : (ceux-ci proviennent de CiscoSecure UNIX ; ceux de CiscoSecure NT peuvent être délimités par des virgules) :

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

Utilisation de la commande Exception

Dans notre réseau, si nous décidons qu'une source et/ou une destination particulière n'a pas besoin d'authentification, d'autorisation ou de comptabilité, nous pouvons effectuer les opérations suivantes :

```
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 « exceptez » les adresses ip de l'authentification et que vous avez l'autorisation, vous devez également les excepter de l'autorisation!

Nombre maximal de sessions et affichage des utilisateurs connectés

Certains serveurs TACACS+ et RADIUS ont des fonctionnalités « max-session » ou « view logging users ». La possibilité d'effectuer des sessions max ou d'enregistrer des utilisateurs connectés dépend des enregistrements comptables. Lorsqu'un enregistrement de début de

compte est généré mais qu'aucun enregistrement de fin de compte n'est généré, le serveur TACACS+ ou RADIUS suppose que la personne est toujours connectée (c'est-à-dire qu'elle a une session via PIX).

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

L'utilisateur établit une connexion Telnet via le PIX, en s'authentifiant sur le chemin :

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
 to 9.9.9.25 /23
 (pix) 109011: Authen Session Start: user 'cse', sid 3
 (pix) 109005: Authentication succeeded for user 'cse' from
 171.68.118.100/12 00 to 9.9.9.25/23
 (pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23
 gaddr 9.9.9.10/12 00 laddr 171.68.118.100/1200 (cse)
 (server start account) Sun Nov 8 16:31:10 1998 rtp-pinecone.rtp.cisco.com cse
 PIX 171.68.118.100 start task_id=0x3 foreign_ip=9.9.9.25
 local_ip=171.68.118.100 cmd=telnet
```

Comme le serveur a vu un enregistrement « start » mais pas d'enregistrement « stop » (à ce stade), le serveur indique que l'utilisateur « Telnet » est connecté. Si l'utilisateur tente une autre connexion qui nécessite une authentification (peut-être depuis un autre PC) et si max-sessions est défini sur « 1 » sur le serveur pour cet utilisateur (en supposant que le serveur prend en charge max-sessions), la connexion sera refusée par le serveur.

L’utilisateur poursuit son activité Telnet ou FTP sur l’hôte cible, puis quitte (y passe 10 minutes) :

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr
9.9.9.10/128 1 laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

(server stop account) Sun Nov 8 16:41:17 1998 rtp-pinecone.rtp.cisco.com cse

 PIX 171.68.118.100 stop task_id=0x3 foreign_ip=9.9.9.25 local_ip=171.68.118.100
 cmd=telnet elapsed_time=5 bytes_in=98 bytes_out=36
```

Que uauth soit 0 (authentification à chaque fois) ou plus (authentification une fois et non à nouveau pendant la période uauth), un enregistrement comptable est coupé pour chaque site auquel on accède.

Cependant, HTTP fonctionne différemment en raison de la nature du protocole. Voici un exemple de HTTP.

L'utilisateur navigue de 171.68.118.100 à 9.9.9.25 via le PIX :

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1281
 to 9.9.9.25 /80
 (pix) 109011: Authen Session Start: user 'cse', sid 5
 (pix) 109005: Authentication succeeded for user 'cse' from
 171.68.118.100/12 81 to 9.9.9.25/80
 (pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr
 9.9.9.10/12 81 laddr 171.68.118.100/1281 (cse)
 (server start account) Sun Nov 8 16:35:34 1998 rtp-pinecone.rtp.cisco.com cse
 PIX 171.68.118.100 start task_id=0x9 foreign_ip=9.9.9.25
 local_ip=171.68.118.100 cmd=http
```

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr
9.9.9.10/128 1 laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35.35 1998 rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9 foreign_ip =9.9.9.25
local_ip=171.68.118.100 cmd=http elapsed_time=0 bytes_ in=1907 bytes_out=223
```

L'utilisateur lit la page Web téléchargée.

L'enregistrement de début affiché à 16:35:34 et l'enregistrement de fin affiché à 16:35:35. Ce téléchargement a pris une seconde (c'est-à-dire il y a eu moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur est-il toujours connecté au site Web et la connexion est-elle toujours ouverte lorsqu'il lit la page Web ? Non. Le nombre maximal de sessions ou l'affichage des utilisateurs connectés fonctionnera-t-il ici ? Non, parce que le temps de connexion (le temps entre « Construite » et « Teardown ») dans HTTP est trop court. Les enregistrements « start » et « stop » sont en moins d'une seconde. Il n'y aura pas d'enregistrement « de début » sans enregistrement « d'arrêt », puisque les enregistrements ont lieu pratiquement au même moment. Il y aura toujours un enregistrement « start » et « stop » envoyé au serveur pour chaque transaction, que uauth soit défini sur 0 ou quelque chose de plus grand. Cependant, les utilisateurs connectés à max-sessions et à view ne fonctionneront pas en raison de la nature des connexions HTTP.

Authentification et activation sur le PIX lui-même

La discussion précédente portait sur l'authentification du trafic Telnet (et HTTP, FTP) via le PIX. Dans l'exemple ci-dessous, nous nous assurons que Telnet vers le pix fonctionne sans authentification sur :

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

Ensuite, nous ajoutons la commande pour authentifier les utilisateurs Telnet vers PIX :

```
aaa authentication telnet console Outgoing
```

Lorsque les utilisateurs établissent une connexion Telnet avec le PIX, ils sont invités à entrer le mot de passe Telnet (« ww »). Le PIX demande également le TACACS+ dans ce cas (puisque la liste de serveurs sortants est utilisée) ou le nom d'utilisateur et le mot de passe RADIUS.

```
aaa authentication enable console Outgoing
```

Avec cette commande, l'utilisateur est invité à saisir un nom d'utilisateur et un mot de passe qui sont envoyés au serveur TACACS ou RADIUS. Dans ce cas, puisque la liste des serveurs sortants est utilisée, la requête est envoyée au serveur TACACS. Puisque le paquet d'authentification pour enable est identique au paquet d'authentification pour la connexion, l'utilisateur peut activer via TACACS ou RADIUS avec le même nom d'utilisateur/mot de passe, en supposant que l'utilisateur peut se connecter au PIX avec TACACS ou RADIUS. Ce problème a reçu l'ID de bogue #CSCdm47044.

En cas de panne du serveur, l'utilisateur peut accéder au mode d'activation PIX en entrant « PIX » pour le nom d'utilisateur et le mot de passe d'activation normal à partir du PIX (« enable password

any »). Si « enable password any » ne figure pas dans la configuration PIX, l'utilisateur doit entrer « PIX » pour le nom d'utilisateur et appuyer sur la touche Entrée. Si le mot de passe actif est défini mais n'est pas connu, un disque de récupération de mot de passe est nécessaire pour la réinitialisation.

Authentification sur la console série

La commande **aaa authentication serial console** nécessite une vérification d'authentification afin d'accéder à la console série du PIX. Lorsque l'utilisateur exécute des commandes de configuration à partir de la console, les messages syslog sont coupés (si le PIX est configuré pour envoyer syslog au niveau de débogage à un hôte syslog). Voici un exemple tiré du serveur syslog :

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

Modification de l'invite Utilisateurs Voir

Si nous avons la commande :

```
auth-prompt THIS_IS_PIX_5
```

les utilisateurs passant par PIX voient la séquence :

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

puis, à l'arrivée dans la case de destination finale, les champs « Nom d'utilisateur : » et « Mot de passe : » indiquent la case de destination.

Cette invite n'affecte que les utilisateurs passant par le PIX, et non le PIX.

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

Personnalisation du message que les utilisateurs voient en cas de réussite ou d'échec

Si nous avons les commandes :

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

Les utilisateurs verront ce qui suit lors d'une connexion échouée/réussie via PIX :

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
```

```
"You blew it"
"THIS_IS_PIX_5"
Username: cse
Password:
"You're allowed through the pix"
```

Délais d'inactivité et d'abandon par utilisateur

Les délais d'attente uauth inactifs et absolus peuvent être envoyés par utilisateur à partir du serveur TACACS+. Si tous les utilisateurs de votre réseau doivent avoir le même délai d'attente, alors n'implémentez pas ceci ! Mais si vous avez besoin de différents uauths par utilisateur, lisez la suite.

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

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

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

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

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

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

L'utilisateur doit se réauthentifier lors du retour vers le même hôte cible ou vers un autre hôte.

HTTP virtuel

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

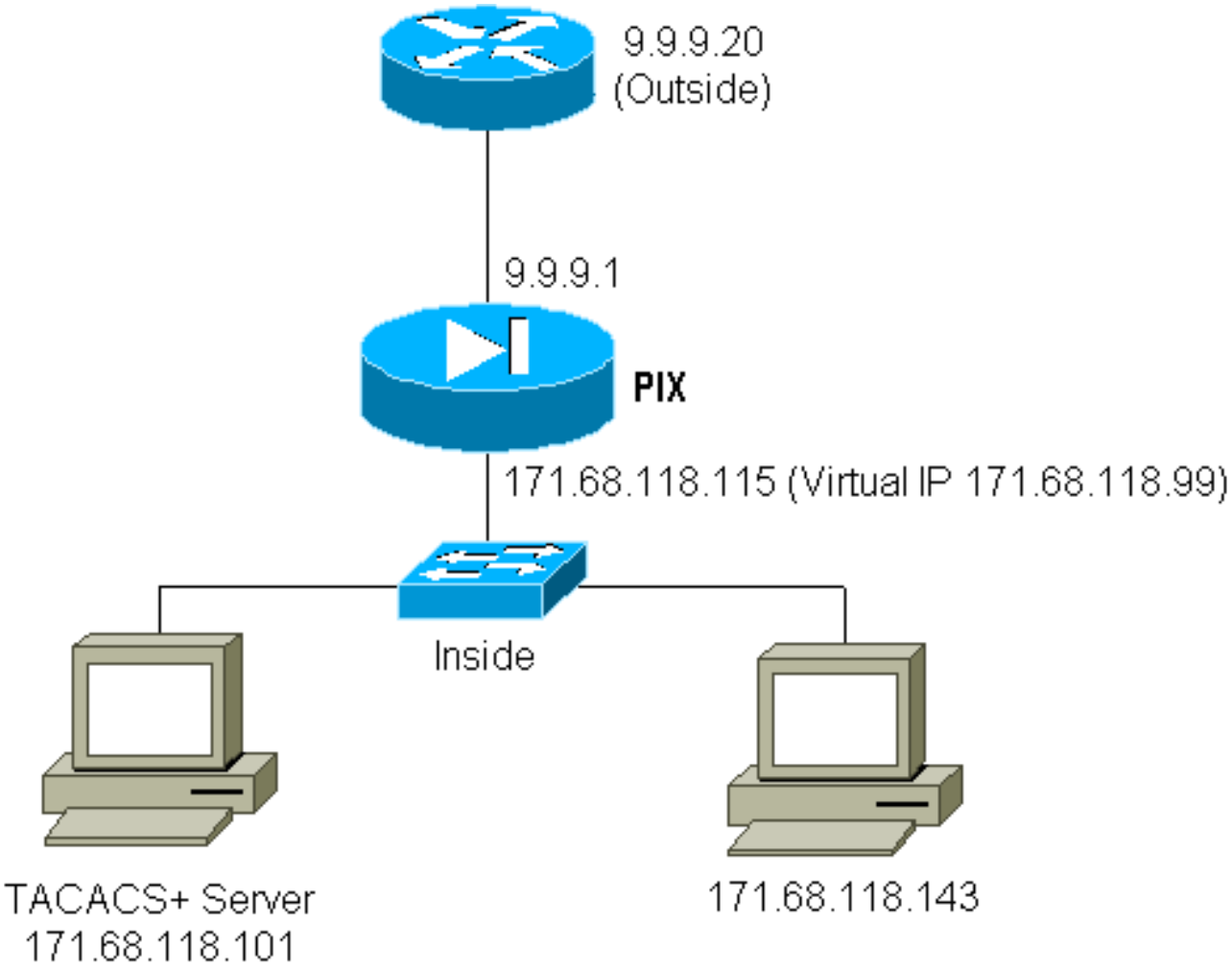
Pour éviter cela, vous pouvez mettre en oeuvre le protocole HTTP virtuel en ajoutant une adresse RFC 1918 (c'est-à-dire une adresse qui est non routable sur Internet, mais valide et unique pour le

réseau interne PIX) à la configuration PIX à l'aide de la commande suivante :

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

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

Exemple de trafic sortant HTTP virtuel :



Configuration PIX HTTP virtuel sortant :

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

Telnet virtuel

La configuration du PIX pour authentifier tout le trafic entrant et sortant n'est pas une bonne idée car certains protocoles, tels que « mail », ne sont pas facilement authentifiés. Lorsqu'un serveur de messagerie et un client essaient de communiquer via PIX lorsque tout le trafic via PIX est authentifié, le syslog PIX pour les protocoles non authentifiables affiche des messages tels que :

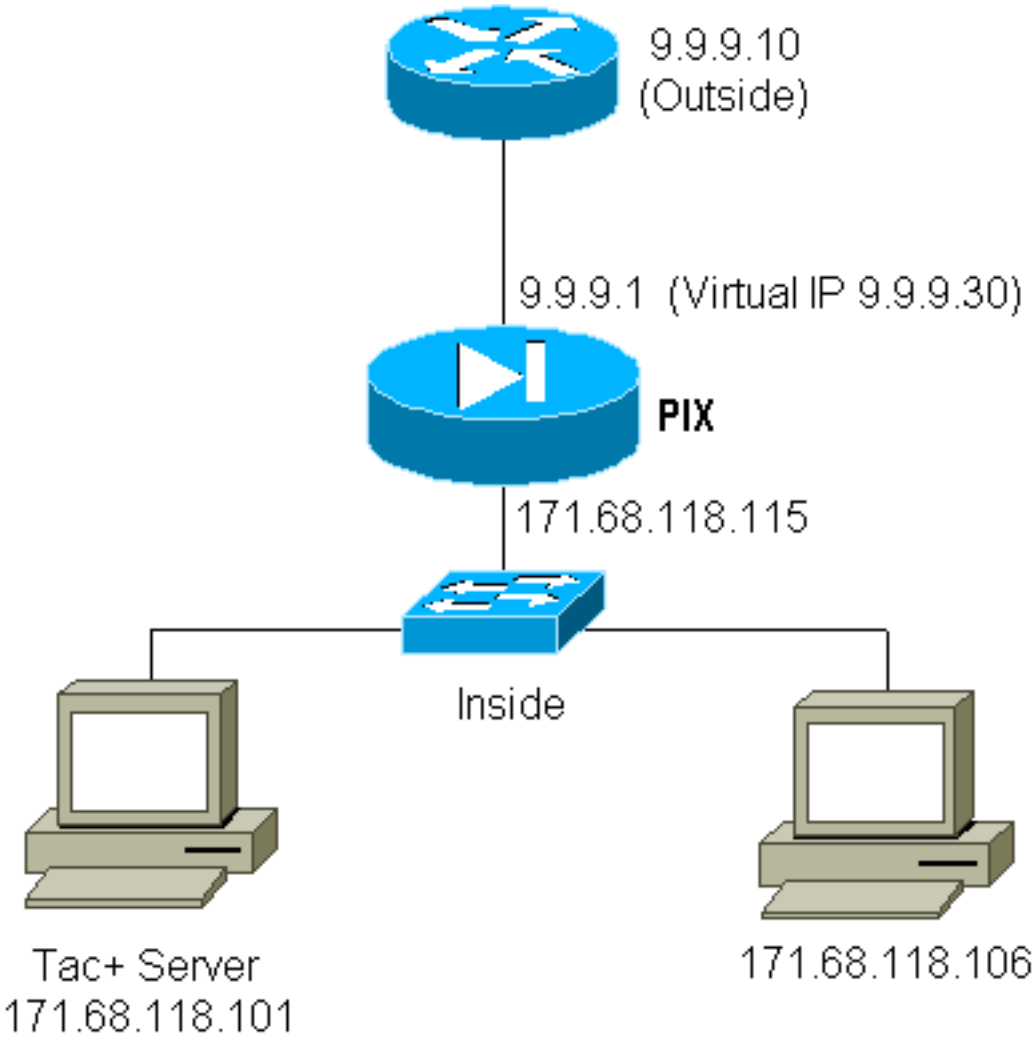
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

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

Mais s'il est vraiment nécessaire d'authentifier un service inhabituel, cela peut être fait à l'aide de la commande **Virtual Telnet**. Cette commande permet l'authentification sur l'adresse IP Telnet virtuelle. Après cette authentification, le trafic pour le service inhabituel peut aller au serveur réel qui est lié à l'IP virtuelle.

Dans notre exemple, nous voulons autoriser le trafic du port TCP 49 à circuler de l'hôte externe 9.9.9.10 vers l'hôte interne 171.68.118.106. Comme ce trafic n'est pas vraiment authentifiable, nous configurons Virtual Telnet.

Entrant Virtual Telnet :



Configuration PIX Virtual Telnet Inbound :

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
 aaa authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
 virtual telnet 9.9.9.30
```

Configuration utilisateur du serveur TACACS+ Virtual Telnet entrant :

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

Débogage de PIX Virtual Telnet entrant :

L'utilisateur à l'adresse 9.9.9.10 doit d'abord s'authentifier en établissant une connexion Telnet avec l'adresse 9.9.9.30 sur le PIX :

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

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

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

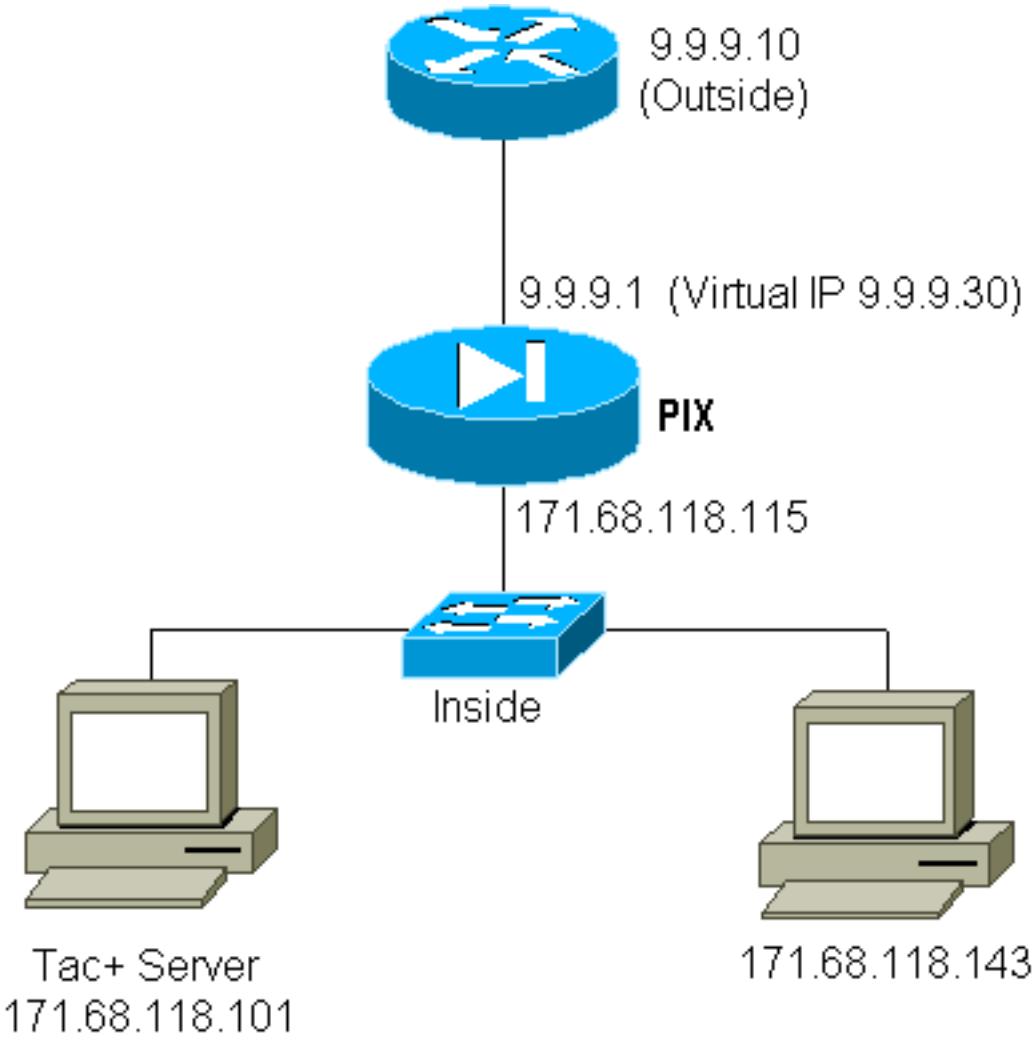
Et lorsque le périphérique 9.9.9.10 veut envoyer le trafic TCP/49 au périphérique 171.68.118.106 :

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr
 9.9.9.30/49 laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

Virtual Telnet sortant :

Puisque le trafic sortant est autorisé par défaut, aucune valeur statique n'est requise pour l'utilisation de trafic sortant Telnet virtuel. Dans l'exemple suivant, l'utilisateur interne à l'adresse 171.68.118.143 établit une connexion Telnet avec le réseau virtuel 9.9.9.30 et s'authentifie. La connexion Telnet est immédiatement abandonnée.

Une fois authentifié, le trafic TCP est autorisé à partir de 171.68.118.143 vers le serveur à l'adresse 9.9.9.10 :



Configuration PIX Virtual Telnet Outbound :

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

Débogage de PIX Virtual Telnet sortant :

```
109001: Auth start for user '???' from 171.68.118.143/1536 to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', sid 25
 109005: Authentication succeeded for user 'timeout_143' from
171.68.118.143/1536 to 9.9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
  laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
  laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
  laddr 171.68. 118.143/1537 duration 0:00:03 bytes 625 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
```

```
  laddr 171.68. 118.143/1538 duration 0:00:01 bytes 2281 (timeout_143)
 302009: 0 in use, 1 most used
```

Déconnexion virtuelle de Telnet

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

Autorisation de port

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

Configuration PIX :

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 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, lorsque nous envoyons une requête Telnet de 171.68.118.143 à 9.9.9.10, l'authentification et l'autorisation se sont produites parce que le port Telnet 23 se trouve dans la plage 23-49. Lorsque nous faisons une session HTTP de 171.68.118.143 à 9.9.9.10, nous devons toujours nous authentifier, mais le PIX ne demande pas au serveur TACACS+ d'autoriser HTTP car 80 n'est pas dans la plage 23-49.

Configuration du serveur de logiciel gratuit TACACS+

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

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

Déboguer sur PIX :

```
109001: Auth start for user '???' from 171.68.118.143/1051 to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', sid 0
 109005: Authentication succeeded for user 'telnetrange' from
 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', sid 0
 109007: Authorization permitted for user 'telnetrange' from
 171.68.118.143/1051 to 9.9 .9.10/23
 302001: Built TCP connection 0 for faddr 9.9.9.10/23 gaddr 9.9.9.5/1051
 laddr 171.68.1 18.143/1051 (telnetrange)
 109001: Auth start for user '???' from 171.68.118.143/1105 to 9.9.9.10/80
 109001: Auth start for user '???' from 171.68.118.143/1110 to 9.9.9.10/80
 109011: Authen Session Start: user 'telnetrange', sid 1
 109005: Authentication succeeded for user 'telnetrange' from
```

```
 171.68.118.143/1110 to 9. 9.9.10/80
 302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
 302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
 302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 laddr
171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

Informations connexes

- Assistance produit du logiciel Cisco PIX Firewall
- Références des commandes du pare-feu Cisco Secure PIX