Exemples de configurations PIX, TACACS+ et RADIUS : 4.2.x

Table des matières

Introduction

L'authentification RADIUS et TACACS+ peut être effectuée pour les connexions FTP, Telnet et HTTP. L'autorisation TACACS+ est prise en charge, contrairement à l'autorisation RADIUS.

La syntaxe pour l'authentification a légèrement changé dans le logiciel PIX 4.2.2. Ce document utilise la syntaxe pour les versions logicielles 4.2.2.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configuration PIX

```
<#root>

pix2#

write terminal

Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1TpOedmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
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  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
```

```
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
!--- The next entry depends on whether TACACS+ or RADIUS is used.

!
tacacs-server (inside) host 171.68.118.101 cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout 10

!
!--- The focus of concern is with hosts on the inside network !--- accessing a particular outside host

!
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius

!
!--- It is possible to be less granular and authenticate !--- all outbound FTP, HTTP, Telnet traffic w

aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
aaa authentication http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
aaa authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   tacacs+|radius
!
!--- Accounting records are sent for !--- successful authentications to the TACACS+ or RADIUS server.

!
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
!
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
telnet 171.68.118.100 255.255.255.255
mtu outside 1500
mtu inside 1500
mtu  1500
Smallest mtu: 1500
floodguard 0
tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0
: end
[OK]
```

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Authentification et autorisation

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

Par exemple, supposons que vous ayez une centaine d'utilisateurs à l'intérieur et que vous souhaitiez seulement que six de ces utilisateurs puissent effectuer des opérations FTP, Telnet ou HTTP en dehors du réseau. Demandez au PIX d'authentifier le trafic sortant et de donner les six ID d'utilisateurs sur le serveur de sécurité TACACS+/RADIUS. Avec une authentification simple, ces six utilisateurs peuvent être authentifiés avec un nom d'utilisateur et un mot de passe, puis sortir. Les quatre-vingt-quatorze autres utilisateurs ne peuvent pas sortir. Le PIX invite les utilisateurs à entrer leur nom d'utilisateur/mot de passe, puis transmet leur nom d'utilisateur et leur mot de passe au serveur de sécurité TACACS+/RADIUS. En outre, selon la réponse, il ouvre ou refuse la connexion. Ces six utilisateurs peuvent utiliser FTP, Telnet ou HTTP.

Cependant, supposons que l'un de ces trois utilisateurs, « Terry », n'est pas digne de confiance. Vous souhaitez autoriser Terry à effectuer des opérations FTP, mais pas HTTP ni Telnet vers l'extérieur. Cela signifie que vous devez ajouter une autorisation. Autrement dit, autoriser ce que les utilisateurs peuvent faire en plus d'authentifier qui ils sont. Lorsque vous ajoutez une autorisation au PIX, le PIX envoie d'abord le nom d'utilisateur et le mot de passe de Terry au serveur de sécurité, puis envoie une demande d'autorisation qui indique au serveur de sécurité ce que Terry essaie de faire. Une fois le serveur correctement configuré, Terry peut être autorisé à « FTP 1.2.3.4 », mais n'a pas 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 l'authentification/autorisation sur :

- Telnet - L'utilisateur voit s'afficher une invite de nom d'utilisateur, suivie d'une demande de mot de passe. Si l'authentification (et l'autorisation) est réussie sur le PIX/serveur, l'utilisateur est invité à entrer son nom d'utilisateur et son 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 » comme nom d'utilisateur et « local_password@remote_password » comme mot de passe. Le PIX envoie le "nom_utilisateur_local" et le "mot_de_passe_local" au serveur de sécurité local, et si l'authentification (et l'autorisation) est réussie au niveau du PIX/serveur, le "nom_utilisateur_distant" et le "mot_de_passe_distant" sont passés au serveur FTP de destination au-delà.

- HTTP : une fenêtre s'affiche dans le navigateur pour demander un nom d'utilisateur et un mot de passe. Si l'authentification (et l'autorisation) aboutissent, l'utilisateur accède au site Web de destination au-delà de cette étape. Gardez à l'esprit que les navigateurs mettent en cache les noms d'utilisateur et les mots de passe. S'il apparaît que le PIX devrait expirer une connexion HTTP mais ne le fait pas, il est probable que la ré-authentification a lieu en fait avec le navigateur "filmant" le nom d'utilisateur et le mot de passe mis en cache au PIX. Il transfère ensuite ce message au serveur d'authentification. Les débogages de serveur et/ou syslog PIX montrent ce phénomène. Si Telnet et FTP semblent fonctionner normalement, mais pas les connexions HTTP, c'est la raison.

Configurations de serveur utilisées pour tous les scénarios

Dans les exemples de configuration du serveur TACACS+, si seule l'authentification est activée, les utilisateurs « all », « telnetonly », « httponly » et « ftponly » fonctionnent tous. Dans les exemples de configuration du serveur RADIUS, l'utilisateur « all » fonctionne.

Lorsque l'autorisation est ajoutée au PIX, en plus d'envoyer le nom d'utilisateur et le mot de passe au serveur d'authentification TACACS+, le PIX envoie des commandes (Telnet, HTTP ou FTP) au serveur TACACS+. Le serveur TACACS+ vérifie ensuite si cet utilisateur est autorisé pour cette commande.

Dans un exemple ultérieur, l'utilisateur à l'adresse 171.68.118.100 émet la commande telnet 9.9.9.11. Lorsque ce message est reçu au niveau du PIX, le PIX transmet le nom d'utilisateur, le mot de passe et la commande au serveur TACACS+ pour traitement.

Ainsi, avec l'autorisation activée en plus de l'authentification, l'utilisateur « telnetonly » peut effectuer des opérations Telnet via le PIX. Cependant, les utilisateurs « httponly » et « ftponly » ne peuvent pas effectuer d'opérations Telnet via le PIX.

(Là encore, l'autorisation n'est pas prise en charge avec RADIUS en raison de la nature de la spécification de protocole).

Configuration du serveur Cisco Secure UNIX TACACS+

Cisco Secure 2.x

- Les strophes utilisateur s'affichent ici.
- Ajoutez l'adresse IP PIX ou le nom de domaine complet et la clé à CSU.cfg.

```
user = all {
password = clear "all"
default service = permit
}

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

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

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

Configuration du serveur Cisco Secure UNIX RADIUS

Utilisez l'interface utilisateur graphique avancée (GUI) pour ajouter l'adresse IP et la clé PIX à la liste des serveurs d'accès réseau (NAS). L'utilisateur stanza apparaît comme on le voit ici :

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

Cisco Secure NT 2.x RADIUS

La section Exemples de configuration de la documentation en ligne et Web de CiscoSecure 2.1 décrit la configuration ; l'attribut 6 (Service-Type) serait Login ou Administrative.

Ajoutez l'adresse IP du PIX dans la section Configuration NAS à l'aide de l'interface utilisateur graphique.

EasyACS TACACS+

La documentation EasyACS fournit des informations de configuration.

1. Dans la section group, cliquez sur Shell exec (pour donner des privilèges d'exécution).
2. Pour ajouter une autorisation au PIX, cliquez sur Deny unmatch IOS commands au bas de la configuration du groupe.
3. Sélectionnez Add/Edit pour chaque commande que vous souhaitez autoriser (Telnet, par exemple).
4. Si vous souhaitez autoriser Telnet à des sites spécifiques, saisissez les adresses IP dans la section des arguments. Pour autoriser Telnet vers tous les sites, cliquez sur Allow all unlists arguments.
5. Cliquez sur Terminer la commande d'édition.
6. Exécutez les étapes 1 à 5 pour chacune des commandes autorisées (Telnet, HTTP et/ou FTP, par exemple).
7. Ajoutez l'adresse IP du PIX dans la section Configuration NAS à l'aide de l'interface utilisateur graphique.

Cisco Secure NT 2.x TACACS+

La documentation Cisco Secure 2.x fournit des informations sur la configuration.

1. Dans la section group, cliquez sur Shell exec (pour donner des privilèges d'exécution).
2. Pour ajouter une autorisation au PIX, cliquez sur Deny unmatch IOS commands au bas de la configuration du groupe.
3. Activez la case à cocher command en bas et entrez la commande que vous souhaitez autoriser (Telnet, par exemple).
4. Si vous souhaitez autoriser Telnet à des sites spécifiques, saisissez l'adresse IP dans la section des arguments (par exemple, « permit 1.2.3.4 »). Pour autoriser Telnet vers tous les sites, cliquez sur Autoriser les arguments non répertoriés.
5. Cliquez sur Submit.
6. Exécutez les étapes 1 à 5 pour chacune des commandes autorisées (Telnet, FTP et/ou HTTP, par exemple).
7. Ajoutez l'adresse IP du PIX dans la section Configuration NAS à l'aide de l'interface utilisateur graphique.

Configuration du serveur RADIUS Livingston

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

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

Configuration du serveur RADIUS Merit

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

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

Configuration du serveur de logiciel gratuit TACACS+

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

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

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

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

user = ftponly {
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 passer le trafic avant d'établir AAA, vous ne pourrez pas le faire

par la suite.

- Activez la journalisation dans le 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 ensuite 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.

Exemples de débogage d'authentification de PIX

Débogage PIX - Authentification correcte - RADIUS

Voici un exemple de débogage PIX avec une bonne authentification :

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

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

Ceci est un exemple de débogage PIX avec une mauvaise authentification (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre ensembles nom d'utilisateur/mot de passe. Le message « Erreur : nombre maximal de tentatives dépassé » s'affiche.

Remarque : s'il s'agit d'une tentative FTP, une tentative est autorisée. Pour HTTP, les tentatives infinies sont autorisées.

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

Débogage PIX - Serveur arrêté - RADIUS

Ceci est un exemple de débogage PIX avec le serveur hors service. L'utilisateur voit le nom d'utilisateur une fois. Le serveur « se bloque » et demande un mot de passe (trois fois).

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

Débogage PIX - Authentification correcte - TACACS+

Voici un exemple de débogage PIX avec une bonne authentification :

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

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

Ceci est un exemple de débogage PIX avec une mauvaise authentification (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre ensembles nom d'utilisateur/mot de passe. Le message « Erreur : nombre maximal de tentatives dépassé » s'affiche.

Remarque : s'il s'agit d'une tentative FTP, une tentative est autorisée. Pour HTTP, les tentatives infinies sont autorisées.

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

Débogage PIX - Serveur arrêté - TACACS+

Ceci est un exemple de débogage PIX avec le serveur hors service. L'utilisateur voit le nom d'utilisateur une fois. Immédiatement, le message « Erreur : nombre maximal de tentatives dépassé » s'affiche.

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

```
109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

Ajout d'autorisation

L'autorisation n'étant pas valide sans authentification, elle est requise pour la même source et la même destination :

<#root>

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius
```

Ou, si les trois services sortants ont été authentifiés à l'origine :

<#root>

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
```

Exemples de débogage d'authentification et d'autorisation depuis PIX

Débogage PIX - Authentification et autorisation correctes - TACACS+

Voici un exemple de débogage PIX avec une bonne authentification et autorisation :

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

Débogage PIX - Authentification correcte, mais échec d'autorisation - TACACS+

Voici un exemple de débogage PIX avec une bonne authentification mais un échec dans l'autorisation :

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

Débogage PIX - Authentification incorrecte, autorisation non tentée - TACACS+

Ceci est un exemple de débogage PIX avec authentification et autorisation, mais l'autorisation n'a pas été tentée en raison d'une mauvaise authentification (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre ensembles nom d'utilisateur/mot de passe. Le message « Erreur : nombre maximal de tentatives dépassé » s'affiche

Remarque : s'il s'agit d'une tentative FTP, une tentative est autorisée. Pour HTTP, les tentatives infinies sont autorisées.

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

Débogage PIX - Authentification/Autorisation, serveur arrêté - TACACS+

Ceci est un exemple de débogage PIX avec authentification et autorisation. Le serveur est en panne. L'utilisateur voit le nom d'utilisateur une fois. Immédiatement, le message « Erreur : nombre maximal d'essais dépassé » s'affiche.

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

Ajoutez la gestion des comptes

TACACS+

<#root>

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+

Le débogage est identique, que la gestion des comptes soit activée ou désactivée. Cependant, au moment de la création, un enregistrement de début de comptabilité est envoyé. De plus, au moment de la « Démontage », un enregistrement de comptabilité « stop » est envoyé :

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

Les enregistrements de comptabilité TACACS+ ressemblent à ce résultat (ceux-ci proviennent de CiscoSecure UNIX ; les enregistrements dans Cisco Secure Windows peuvent être délimités par des virgules à la place) :

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

Les champs se décomposent comme indiqué ici :

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

<#root>

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius
```

Le débogage est identique, que la gestion des comptes soit activée ou désactivée. Cependant, au moment de la création, un enregistrement de début de comptabilité est envoyé. De plus, au moment de la « Démontage », un enregistrement de comptabilité « stop » est envoyé :

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

Les enregistrements de comptabilité RADIUS ressemblent à ce résultat (ceux-ci proviennent de Cisco Secure UNIX ; ceux de Cisco Secure Windows sont délimités par des virgules) :

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

Les champs se décomposent comme indiqué ici :

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
```

```
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

Nombre maximal de sessions et affichage des utilisateurs connectés

Certains serveurs TACACS et RADIUS ont des fonctions « max-session » ou « afficher les utilisateurs connectés ». La possibilité d'effectuer un nombre maximal de sessions ou d'archiver les utilisateurs connectés dépend des enregistrements de comptabilité. Lorsqu'un enregistrement de début de compte est généré mais qu'aucun enregistrement d'arrêt 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. À titre d'exemple :

L'utilisateur établit une connexion Telnet de 171.68.118.100 à 9.9.9.25 via le PIX, en s'authentifiant en 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
```

Étant donné que le serveur a vu un enregistrement « start » mais aucun 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 à partir d'un autre PC) et si max-sessions est défini sur "1" sur le serveur pour cet utilisateur, la connexion est refusée par le serveur.

L'utilisateur se déplace sur l'hôte cible, puis se ferme (il 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 égal à 0 (c'est-à-dire authentifié à chaque fois) ou plus (authentifié une fois et pas à nouveau pendant la période uauth), il y aura une coupure d'enregistrement de comptabilité pour chaque site consulté.

Mais le protocole HTTP fonctionne différemment en raison de la nature du protocole. Voici un exemple :

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 une page Web téléchargée.

Notez l'heure. Ce téléchargement a pris une seconde (il y avait moins d'une seconde entre le début et l'enregistrement d'arrêt). L'utilisateur est-il toujours connecté au site Web et la connexion est-elle toujours ouverte ? No.

Max-sessions ou afficher les utilisateurs connectés fonctionneront-ils ici ? Non, car le temps de connexion dans HTTP est trop court. L'intervalle entre les enregistrements « Construit » et « Démontage » (les enregistrements « Début » et « Arrêt ») est inférieur à une seconde. Il n'y aura pas d'enregistrement "start" sans enregistrement "stop", puisque les enregistrements se produisent pratiquement au même instant. Il y aura toujours un enregistrement « start » et « stop » envoyé au serveur pour chaque transaction, que l'authentification uauth soit définie sur 0 ou sur une valeur supérieure. Cependant, les utilisateurs max-sessions et view connected-in ne fonctionneront pas en raison de la nature des connexions HTTP.

Utilisation de la commande Excepté

Dans notre réseau, si nous décidons qu'un utilisateur sortant (171.68.118.100) n'a pas besoin d'être authentifié, nous pouvons procéder comme suit :

<#root>

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
   255.255.255.255 tacacs+
```

Authentification au PIX lui-même

La discussion précédente porte sur l'authentification du trafic Telnet (et HTTP, FTP) via le PIX. Avec la version 4.2.2, les connexions Telnet au PIX peuvent également être authentifiées. Ici, nous définissons les IP des boîtes qui peuvent Telnet au PIX :

<#root>

```
telnet 171.68.118.100 255.255.255.255
```

Entrez ensuite le mot de passe Telnet : passwd ww.

Ajoutez la nouvelle commande permettant d'authentifier les utilisateurs qui utilisent Telnet sur le PIX :

<#root>

```
aaa authentication telnet console tacacs+|radius
```

Lorsque les utilisateurs établissent une connexion Telnet avec le PIX, ils sont invités à saisir le mot de passe Telnet (« ww »). Le PIX demande également le nom d'utilisateur et le mot de passe TACACS+ ou RADIUS.

Modification de l'invite affichée par les utilisateurs

Si vous ajoutez la commande : auth-prompt YOU_ARE_AT_THE_PIX, les utilisateurs passant par le PIX verront la séquence :

```
YOU_ARE_AT_THE_PIX [at which point you enter the username]
 Password:[at which point you enter the password]
```

À l'arrivée à la destination finale, les invites « Username: » et « Password: » s'affichent. Cette invite affecte uniquement les utilisateurs passant par le PIX, pas au PIX.

Remarque : il n'y a aucun enregistrement de comptabilité coupé pour l'accès au PIX.

Informations connexes

- Assistance produit pour le logiciel Cisco PIX Firewall
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.