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

Contenu

Introduction

L'authentification de RAYON et TACACS+ peut être faite pour le FTP, le telnet, et les connexions HTTP. L'autorisation TACACS+ est prise en charge ; L'autorisation RADIUS n'est pas.

La syntaxe pour l'authentification a changé légèrement en logiciel PIX 4.2.2. Ce document utilise

la syntaxe pour les versions de logiciel 4.2.2.

Conditions préalables

Conditions requises

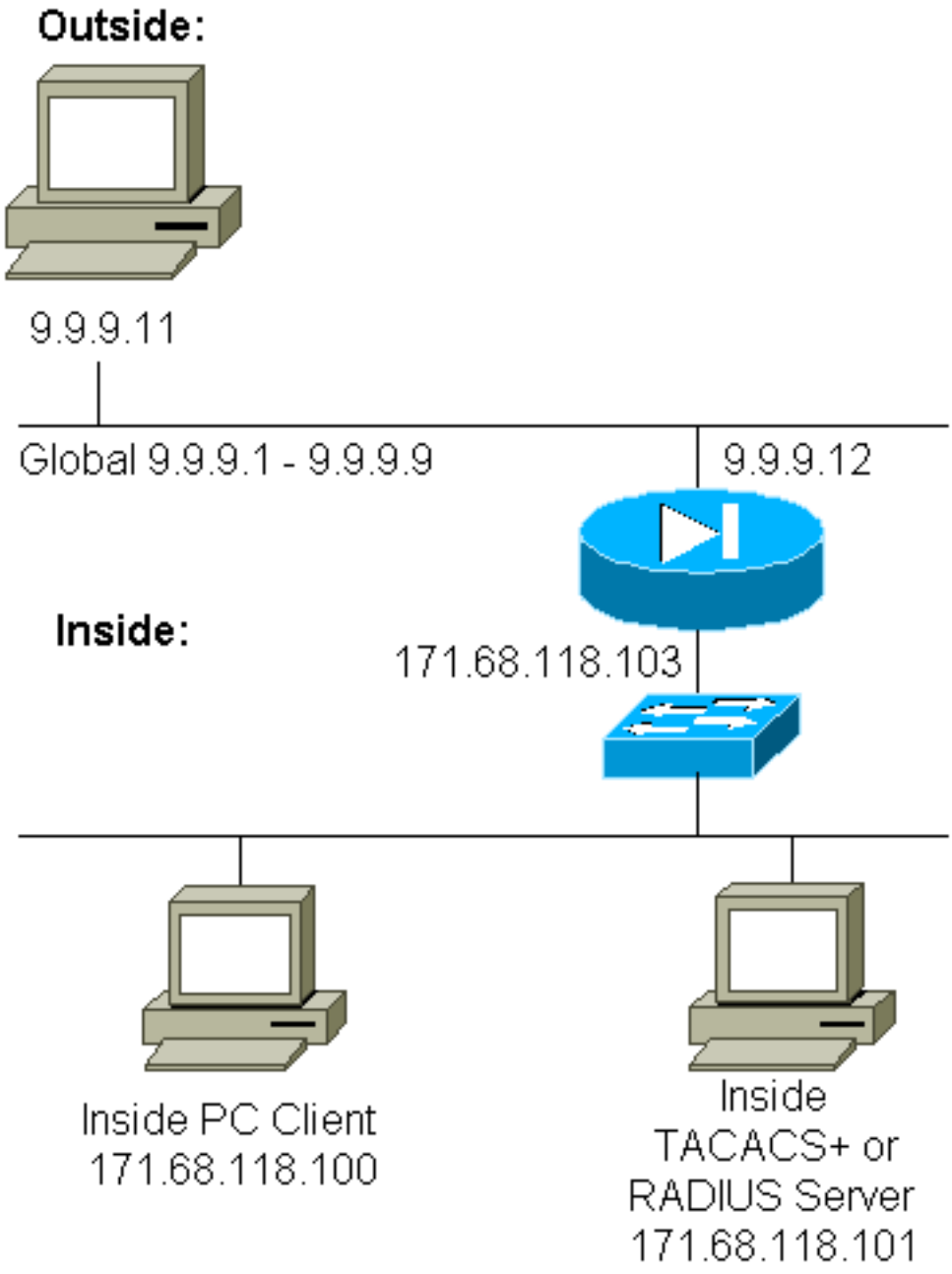
Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration PIX

```
pix2# write terminal Building configuration : Saved :
PIX Version 4.2(2) nameif ethernet0 outside security0
nameif ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr
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 with: 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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

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.

Comme comme exemple, supposez vous faites vouloir cent utilisateurs intérieurs et à vous seulement que six de ces utilisateurs puisse faire le FTP, le telnet, ou le HTTP en dehors du réseau. Dites le PIX d'authentifier le trafic sortant et de donner à chacun des six utilisateurs des id sur le serveur sécurisé TACACS+/RADIUS. Avec l'authentification simple, ces six utilisateurs peuvent être authentifiés avec le nom d'utilisateur et mot de passe, puis sortent. Les quatre-vingt-quatorze autres utilisateurs ne peuvent 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. En outre, selon la réponse, il ouvre ou refuse la connexion. Ces six utilisateurs pourraient faire le FTP, le telnet, ou le HTTP.

Cependant, assumez un de ces trois utilisateurs, « Terry », n'est pas à sont de confiance. Vous voudriez permettre à Terry pour faire le FTP, mais pas le HTTP ou le telnet à l'extérieur. Ceci vous signifie le besoin d'ajouter l'autorisation. C'est-à-dire, autorisant ce que les utilisateurs peuvent faire en plus d'authentifier qui ils sont. Quand vous ajoutez l'autorisation au PIX, le PIX d'abord envoie le nom d'utilisateur et mot de passe de Terry au serveur sécurisé, alors envoie une demande d'autorisation qui indique au serveur sécurisé ce que la « commande » Terry essaye de faire. Avec la configuration du serveur correctement, Terry peut être permis au « FTP 1.2.3.4 » mais est refusé la capacité au « HTTP » ou au « telnet » n'importe où.

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

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

- **Telnet** - L'utilisateur voit un affichage de l'invite nom d'utilisateur, suivi d'une demande pour le mot de passe. Si l'authentification (et l'autorisation) est réussie au PIX/server, l'utilisateur est incité pour le nom d'utilisateur et mot de passe par la destination host au-delà.
- **FTP** - L'utilisateur voit une invite de nom d'utilisateur être soulevé. Les besoins de l'utilisateur d'écrire « local_username@remote_username » pour le nom d'utilisateur et le « local_password@remote_password » pour le mot de passe. Le PIX envoie le « local_username » et le « local_password » au serveur de sécurité local, et si l'authentification (et l'autorisation) est réussie au PIX/server, le « remote_username » et le « remote_password » sont passés au serveur FTP de destination au-delà.
- **HTTP** - Une fenêtre est affichée dans le navigateur qui demande 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 « tir » le nom d'utilisateur en cache et le mot de passe au PIX. Il puis en avant ceci au serveur d'authentification. Le Syslog et/ou le serveur PIX met au point l'exposition ce phénomène. Si le telnet et le FTP semblent fonctionner normalement, mais les connexions HTTP ne font pas, c'est la raison.

Configurations du serveur utilisées pour tous les scénarios

Dans les exemples de configuration du serveur TACACS+, si seulement l'authentification est allumée, les utilisateurs « tous », « telnetonly », « httponly », et « ftponly » tous travaillent. Dans les exemples de configuration du serveur RADIUS, l'utilisateur « tout » travaille.

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

Dans un exemple postérieur, l'utilisateur chez 171.68.118.100 émet le **telnet 9.9.9.11 de** commande. Quand ceci est reçu au PIX, le PIX passe le nom d'utilisateur, mot de passe, et commande au serveur TACACS+ pour le traitement.

Ainsi avec l'autorisation en fonction en plus de l'authentification, l'utilisateur « telnetonly » peut exécuter des exécutions de telnet par le PIX. Cependant, les utilisateurs « httponly » et « ftponly » ne peuvent pas exécuter des exécutions de telnet par le PIX.

(De nouveau, l'autorisation n'est pas prise en charge avec le RAYON dû à la nature de la spécification de protocole).

Configuration du serveur de Cisco Secure UNIX TACACS+

2.x Cisco Secure

- Des strophes d'utilisateur sont affichées 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 RADIUS de Cisco Secure UNIX

Employez l'interface utilisateur graphique avancée (GUI) pour ajouter l'IP PIX et la clé à la liste de serveur d'accès à distance (NAS). La strophe d'utilisateur apparaît comme vu ici :

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

RAYON du NT Cisco Secure 2.x

La section de configurations d'échantillon du CiscoSecure 2.1 en ligne et documentation de Web décrit l'installation ; l'attribut 6 (type de service) serait procédure de connexion ou administratif.

Ajoutez l'IP du PIX dans la section de configuration de NAS utilisant le GUI.

EasyACS TACACS+

La documentation d'EasyACS fournit l'information de configuration.

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

NT Cisco Secure 2.x TACACS+

La documentation 2.x Cisco Secure fournit l'information de configuration.

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

Configuration du serveur Livingston RADIUS

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

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

Configuration du serveur Merit RADIUS

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

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

Exemples de debug d'authentification de PIX

Debug PIX - Bonne authentification - RAYON

C'est un exemple d'un PIX mettent au point avec la 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)
```

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

C'est un exemple d'un PIX mettent au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre positionnements de nom d'utilisateur/mot de passe. La « erreur : le nombre maximum du » message dépassé par relances est affiché.

Remarque: Si c'est une tentative de FTP, on permet un essai. Pour le HTTP, on permet des relances infinies.

```
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
```

Debug PIX - Serveur vers le bas - RAYON

C'est un exemple d'un PIX mettent au point avec le serveur vers le bas. L'utilisateur voit le nom d'utilisateur une fois. Le serveur alors « s'arrête » 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)
```

Debug PIX - Bonne authentification - TACACS+

C'est un exemple d'un PIX mettent au point avec la 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)
```

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

C'est un exemple d'un PIX mettent au point avec l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre positionnements de nom d'utilisateur/mot de passe. La « erreur : le nombre maximum du » message dépassé par relances est affiché.

Remarque: Si c'est une tentative de FTP, on permet un essai. Pour le HTTP, on permet des relances infinies.

```
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
```

Debug PIX - Serveur vers le bas - TACACS+

C'est un exemple d'un PIX mettent au point avec le serveur vers le bas. L'utilisateur voit le nom d'utilisateur une fois. Immédiatement, la « erreur : Le nombre maximum du » message dépassé par essais est affiché.

```
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

Puisque l'autorisation est non valide sans authentification, l'autorisation est exigée pour la mêmes source et destination :

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

Ou, si chacun des trois services sortants était initialement authentifié :

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

Debug PIX - Bonne authentification et autorisation - TACACS+

C'est un exemple d'un PIX mettent au point avec la bonne authentification et l'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)
```

Debug PIX - Bonne authentification, mais panne dans l'autorisation - TACACS+

C'est un exemple d'un PIX mettent au point avec la bonne authentification mais la panne 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
```

Debug PIX - Authentification erronée, autorisation non tentée - TACACS+

C'est un exemple d'un PIX mettent au point avec l'authentification et l'autorisation, mais en raison

non tenté d'autorisation de l'authentification erronée (nom d'utilisateur ou mot de passe). L'utilisateur voit quatre positionnements de nom d'utilisateur/mot de passe. La « erreur : nombre maximum de relances dépassées. » le message est affiché

Remarque: Si c'est une tentative de FTP, on permet un essai. Pour le HTTP, on permet des relances infinies.

```
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
```

Debug authentication/autorisation PIX, serveur vers le bas - TACACS+

C'est un exemple d'un PIX mettent au point avec l'authentification et l'autorisation. Le serveur est en panne. L'utilisateur voit le nom d'utilisateur une fois. Immédiatement, la « erreur : Nombre maximum d'essais dépassés. » est affiché.

```
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+

`aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+`

Débuggez les aspects les mêmes si la comptabilité est "Marche/Arrêt". Cependant, au moment du « a construit, » enregistrement des comptes de « début » a est envoyé. En outre, au moment de la « désinstallation, » l'enregistrement des comptes de « arrêt » a 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 des comptes TACACS+ ressemblent à cette sortie (ceux-ci sont de CiscoSecure UNIX ; les enregistrements dans Windows Cisco Secure peuvent être délimités par une virgule 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 décomposent comme vu 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>
```

RAYON

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

Débuggez les aspects les mêmes si la comptabilité est "Marche/Arrêt". Cependant, au moment du « a construit, » enregistrement des comptes de « début » a est envoyé. En outre, au moment de la « désinstallation, » l'enregistrement des comptes de « arrêt » a 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 des comptes de RAYON ressemblent à cette sortie (ceux-ci sont de Cisco Secure UNIX ; celui dans Windows Cisco Secure est délimité par une virgule) :

```
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 décomposent comme vu 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 = #>
```

Sessions maximum et utilisateurs connectés de visionnement

Quelques serveurs TACACS et de RAYON 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 (qu'est à dire ; a une session par le PIX). Ceci fonctionne bien pour le telnet et les connexions FTP en raison de la nature des connexions. Comme exemple :

Les telnets d'utilisateur de 171.68.118.100 à 9.9.9.25 par le PIX, 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
```

Puisque le serveur n'a vu un enregistrement de « début » mais aucun enregistrement de « 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, la connexion est refusée par le serveur.

L'utilisateur va environ l'entreprise sur l'hôte de cible, puis les sorties (passe 10 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 (qu'est à dire ; authentifiez chaque fois) ou plus (authentifiez une fois et pas de nouveau au cours de la période uauth), il y ayez une coupe d'enregistrement des comptes pour chaque site accédé à.

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

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 une page Web téléchargée.

Notez le temps. 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 encore ouvert une session au site Web et à la connexion encore ouverts ? Non.

Les maximum-sessions ou l'affichage des utilisateurs connectés fonctionneront-ils ici ? Non, parce que le temps de connexion dans le HTTP est trop court. Le temps entre « construit » et la « désinstallation » (l'enregistrement de « début » et de « arrêt ») est fraction de seconde. Il n'y aura pas un enregistrement de « début » sans enregistrement de « arrêt », puisque les enregistrements se produisent pratiquement au même instant. Il y aura toujours « début » et « arrêtez » l'enregistrement envoyé au serveur pour chaque transaction si l'uauth est placé pour 0 ou quelque chose plus grande. Cependant, les maximum-sessions et l'affichage des utilisateurs connectés ne fonctionneront pas en raison de la nature de la connexion HTTP.

Utilisation de excepté la commande

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

```
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 elle-même

La discussion précédente est d'authentifier le trafic de telnet (et HTTP, FTP) par le PIX. Avec 4.2.2, des connexions de telnet au PIX peuvent également être authentifiées. Ici, nous définissons l'IPS de cases qui peuvent telnet au PIX :

```
telnet 171.68.118.100 255.255.255.255
```

Fournissez alors le mot de passe de telnet : **ww de passwd**.

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

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

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.

Changeant la demande les utilisateurs voient

Si vous ajoutez la commande : **l'authentique-demande YOU_ARE_AT_THE_PIX**, des utilisateurs allant par le PIX verra l'ordre :

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

Sur l'arrivée à la destination finale, le « nom d'utilisateur : » et « mot de passe : des » demandes seront affichées. 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.

Informations connexes

- Support produit de Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems