Configuration de PIX 5.1.x : TACACS+ et RADIUS

Table des matières

Introduction

L'authentification RADIUS et TACACS+ peut être effectuée pour les connexions FTP, Telnet et HTTP. L'authentification d'autres protocoles moins courants peut généralement être mise en oeuvre. L'autorisation TACACS+ est prise en charge, contrairement à l'autorisation RADIUS. Les changements dans l'authentification, l'autorisation et la comptabilité (AAA) PIX 5.1 par rapport à la version précédente incluent l'authentification étendue (xauth) - l'authentification des tunnels IPSec à partir du client VPN sécurisé Cisco 1.1.

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.

Conventions

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

Informations générales

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.
- La comptabilité est ce que l'utilisateur a fait.

Supposons que vous ayez une centaine d'utilisateurs à l'intérieur et que vous souhaitiez que seulement six de ces utilisateurs puissent effectuer des opérations FTP, Telnet ou HTTP en dehors du réseau. Vous demanderiez au PIX d'authentifier le trafic sortant et de donner les six ID des utilisateurs sur le serveur de sécurité TACACS+/RADIUS. Avec une authentification simple, ces six utilisateurs pouvaient être authentifiés avec un nom d'utilisateur et un mot de passe, puis sortir. Les quatre-vingt-quatorze autres utilisateurs n'ont pas pu 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, et selon la réponse, ouvre ou refuse la connexion. Ces six utilisateurs peuvent utiliser FTP, Telnet ou HTTP.

Mais supposons qu'un de ces six utilisateurs, « Festus », ne soit pas digne de confiance. Vous souhaitez autoriser Festus à effectuer des opérations FTP, mais pas HTTP ni Telnet vers l'extérieur. Cela implique d'ajouter une autorisation, c'est-à-dire d'autoriser ce que les utilisateurs peuvent faire en plus d'authentifier qui ils sont. Ceci est uniquement valide avec TACACS+. Quand nous ajoutons l'autorisation au PIX, le PIX envoie d'abord le nom d'utilisateur et le mot de passe de Festus au serveur de sécurité, puis envoie une demande d'autorisation indiquant au serveur de sécurité quelle "commande" Festus essaie de faire. Avec le serveur correctement configuré, Festus pourrait être autorisé à « ftp 1.2.3.4 » mais se verrait refuser 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 apparaître une invite de nom d'utilisateur, puis 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 pour le nom d'utilisateur et local_password@remote_password pour le mot de passe. Le PIX envoie le nom d'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 d'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 qui envoie le nom d'utilisateur et le mot de passe mis en cache au PIX, qui transfère ensuite ceci au serveur d'authentification. Le débogage de serveur et/ou syslog PIX montre ce phénomène. Si les protocoles Telnet et FTP semblent fonctionner normalement, mais pas les connexions HTTP, c'est la raison pour laquelle.

- Tunnel : lorsque vous tentez de tunnelliser le trafic IPSec sur le réseau avec le client VPN et xauth activé, une zone grise « Authentification utilisateur pour une nouvelle connexion » s'affiche pour le nom d'utilisateur/mot de passe.

  Remarque : cette authentification est prise en charge à partir de Cisco Secure VPN Client 1.1. Si le menu Aide > À propos n'affiche pas la version 2.1.x ou ultérieure, cela ne fonctionne pas.

Configurations du serveur de sécurité utilisées pour tous les scénarios

Configuration du serveur Cisco Secure UNIX TACACS

Cette section vous présente les informations nécessaires à la configuration de votre serveur de sécurité.

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 Cisco Secure UNIX RADIUS

Utilisez l'interface utilisateur graphique pour ajouter l'adresse IP PIX et la clé à la liste Network Access Server (NAS).

```
user=adminuser {
radius=Cisco {
```

```
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
}
```

Cisco Secure ACS pour Windows 2.x RADIUS

Suivez ces étapes pour configurer Cisco Secure ACS pour Windows 2.x RADIUS.

1. Obtenez un mot de passe dans la section User Setup GUI.
2. Dans la section Group Setup GUI, définissez l'attribut 6 (Service-Type) sur Login ou Administrative.
3. Ajoutez l'adresse IP PIX dans l'interface utilisateur graphique de la section Configuration NAS.

EasyACS TACACS+

La documentation EasyACS décrit 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. Sélectionnez Add/Edit new command pour chaque commande que vous souhaitez autoriser, par exemple, Telnet.
4. Si la connexion Telnet à des sites spécifiques est autorisée, indiquez la ou les adresses IP dans la section des arguments sous la forme « permit #.#.#.# ». Sinon, pour autoriser la connexion Telnet, 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 (par exemple, Telnet, HTTP ou FTP).
7. Ajoutez l'adresse IP PIX dans la section de l'interface utilisateur graphique de configuration NAS.

Cisco Secure 2.x TACACS+

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

1. Dans la section group, cliquez sur Shell exec pour donner des privilèges d'exécution.

2. Pour ajouter une autorisation au PIX, au bas de la configuration du groupe, cliquez sur Deny unmatch IOS commands.
3. Sélectionnez Add/Edit new command pour chaque commande que vous souhaitez autoriser (par exemple, Telnet).
4. Pour autoriser la connexion Telnet à des sites spécifiques, saisissez l'adresse IP dans la section des arguments sous la forme « permit #.#.#.# ». Pour autoriser la connexion Telnet à n'importe quel site, cliquez sur Autoriser tous les arguments non répertoriés.
5. Cliquez sur Terminer la commande d'édition.
6. Exécutez les étapes 1 à 5 pour chacune des commandes autorisées (par exemple, Telnet, HTTP ou FTP).
7. Assurez-vous que l'adresse IP PIX est ajoutée dans la section de l'interface graphique de configuration NAS.

Configuration du serveur RADIUS Livingston

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

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

Configuration du serveur RADIUS Merit

Ajoutez l'adresse IP et la clé PIX 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

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

- Assurez-vous que la configuration PIX fonctionne avant d'ajouter AAA. Si vous ne parvenez pas à transmettre le trafic avant d'instaurer l'authentification et l'autorisation, vous ne pourrez pas le faire par la suite.
- Activez la journalisation dans le PIX.
    - Le débogage de la console de journalisation ne doit pas être utilisé sur un système lourdement chargé.
    - Le débogage en mémoire tampon de journalisation peut être utilisé, puis exécutez la commande show logging.
    - La journalisation peut également être envoyée à un serveur syslog et examinée à cet endroit.
- Activez le débogage sur les serveurs TACACS+ ou RADIUS (tous les serveurs ont cette option).

Diagramme du réseau

Configuration PIX
<#root> PIX Version 5.1(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted

```
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging timestamp
no logging standby

logging console debugging

no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu pix/intf2 1500

ip address outside 99.99.99.1 255.255.255.0
ip address inside 10.31.1.75 255.255.255.0

ip address pix/intf2 127.0.0.1 255.255.255.255
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address pix/intf2 0.0.0.0
arp timeout 14400

global (outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0
nat (inside) 1 10.31.1.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 10.31.1.50 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp any any
conduit permit udp any any


route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
route inside 171.68.120.0 255.255.255.0 10.31.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute

aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 5
aaa authentication include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

```
aaa authentication include http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
aaa authentication include ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca
: end
[OK]
```

Exemples de débogage d'authentification de PIX

Cette section présente des exemples de débogages d'authentification pour différents scénarios.

Entrant

L'utilisateur externe à l'adresse 99.99.99.2 initie le trafic vers l'adresse interne 10.31.1.50 (99.99.99.99) et est authentifié via TACACS (c'est-à-dire que le trafic entrant utilise la liste de serveurs « AuthInbound » qui inclut le serveur TACACS 171.68.118.101).

Débogage PIX - Authentification correcte - TACACS+

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

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

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

L'exemple ci-dessous montre un débogage PIX avec une mauvaise authentification (nom d'utilisateur ou mot de passe). L'utilisateur voit trois ensembles nom d'utilisateur/mot de passe, suivis de ce message : `Erreur : nombre maximal de tentatives dépassé.`

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

```
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

Débogage PIX - Serveur Can Ping, pas de réponse - TACACS+

L'exemple ci-dessous montre un débogage PIX où le serveur peut envoyer une requête ping, mais ne parle pas au PIX. L'utilisateur voit le nom d'utilisateur une fois, mais le PIX ne demande jamais de mot de passe (c'est sur Telnet). L'utilisateur voit `Erreur : le nombre maximal d'essais a été dépassé`.

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

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

L'exemple ci-dessous montre un débogage PIX où le serveur n'est pas pingable. L'utilisateur voit le nom d'utilisateur une fois, mais le PIX ne demande jamais de mot de passe (c'est sur Telnet). Les messages suivants s'affichent : `Timeout to TACACS+ server` et `Error : Max number of tries beyond` (a bogus server was swap in the configuration).

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

Débogage PIX - Authentification correcte - RADIUS

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

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

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

L'exemple ci-dessous montre un débogage PIX avec une mauvaise authentification (nom d'utilisateur ou mot de passe). L'utilisateur voit la demande de nom d'utilisateur et de mot de passe et a trois possibilités de les saisir. Lorsque l'entrée échoue, le message suivant s'affiche : `Erreur : nombre maximal de tentatives dépassé.`

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

Débogage PIX - Peut envoyer une requête ping au serveur, démon arrêté - RADIUS

L'exemple ci-dessous montre un débogage PIX où le serveur peut envoyer une requête ping, mais le démon est arrêté et ne communiquera pas avec le PIX. L'utilisateur voit le nom d'utilisateur, puis le mot de passe, le message `RADIUS server failed` et le message d'erreur `Error : Max number of tries beyond.....`

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

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

L'exemple ci-dessous montre un débogage PIX où le serveur n'est pas pingable ou il y a une incompatibilité Client/clé. L'utilisateur voit un nom d'utilisateur, un mot de passe, le message `Délai d'attente du serveur RADIUS` et le message `Erreur : nombre maximal de tentatives dépassé (`un serveur factice a été échangé dans la configuration).

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

Ajout d'autorisation

Si vous décidez d'ajouter une autorisation, puisque l'autorisation n'est pas valide sans authentification, vous devez exiger une autorisation pour la même plage source et de destination.

<#root>

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

Notez que vous n'ajoutez pas d'autorisation pour le trafic sortant, car le trafic sortant est authentifié avec RADIUS et l'autorisation RADIUS n'est pas valide.

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

Débogage PIX - Authentification correcte et autorisation réussie - TACACS+

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

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

```
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

Débogage PIX - Authentification correcte, Échec de l'autorisation - TACACS+

L'exemple ci-dessous montre le débogage PIX avec une bonne authentification mais une autorisation échouée. L'utilisateur voit également le message `Erreur : autorisation refusée`.

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

Ajout de comptabilisation

TACACS+

<#root>

aaa accounting include any inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound

Sortie du logiciel gratuit TACACS+ :

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

RADIUS

<#root>

```
aaa accounting include any outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

Résultat RADIUS de mérite :

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

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

Utilisation de la commande Exclude

Si nous ajoutons un autre hôte externe (à l'adresse 99.99.99.100) à notre réseau et que cet hôte est approuvé, vous pouvez les exclure de l'authentification et de l'autorisation à l'aide des commandes suivantes :

<#root>

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

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

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 que l'utilisateur 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 en chemin :

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

Étant donné que le serveur a vu un enregistrement de début mais aucun enregistrement d'arrêt, 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 (en supposant que le serveur prend en charge max-sessions), la connexion est refusée par le serveur.

L'utilisateur poursuit ses activités Telnet ou FTP sur l'hôte cible, puis se ferme (il y passe dix 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 supérieur (authentifié une fois et pas à nouveau pendant la période uauth), un enregistrement de comptabilité est coupé pour chaque site consulté.

HTTP fonctionne différemment en raison de la nature du protocole. Voici un exemple de protocole 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 est publié à 16:35:34 et l'enregistrement d'arrêt à 16:35:35. Ce téléchargement a pris une seconde (c'est-à-dire qu'il y avait moins d'une seconde entre le début et l'arrêt de l'enregistrement). L'utilisateur est-il toujours connecté au site Web et la connexion est-elle toujours ouverte lorsque l'utilisateur lit la page Web ? Non. Est-ce que max-sessions ou afficher les utilisateurs connectés fonctionnera ici ? Non, parce que le temps de connexion (le temps entre le « Construit » et le « Démontage ») dans HTTP est trop court. L'enregistrement de début et de fin est inférieur à la seconde. Il n'y a pas d'enregistrement de début sans enregistrement d'arrêt car les enregistrements se produisent pratiquement au même moment. Un enregistrement de début et de fin est toujours 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.

Authentification et activation sur le PIX lui-même

La discussion précédente concerne l'authentification du trafic Telnet (et HTTP, FTP) via le PIX. Assurez-vous que Telnet vers le PIX fonctionne sans authentification sur :

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

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

<#root>

```
aaa authentication telnet console AuthInbound
```

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. Dans ce cas, puisque la liste de serveurs AuthInbound est utilisée, le PIX demande le nom d'utilisateur et le mot de passe TACACS+.

Si le serveur est en panne, vous pouvez accéder au PIX en entrant pix pour le nom d'utilisateur, puis le mot de passe enable (enable password quoiqu'il arrive). Avec la commande :

<#root>

```
aaa authentication enable console AuthInbound
```

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 de serveurs AuthInbound est utilisée, le PIX demande le nom d'utilisateur et le mot de passe TACACS+.

Puisque le paquet d'authentification pour activer est le même que le paquet d'authentification pour la connexion, si l'utilisateur peut se connecter au PIX avec TACACS ou RADIUS, il peut activer via TACACS ou RADIUS avec le même nom d'utilisateur/mot de passe. L'ID de bogue Cisco CSCdm47044 (clients enregistrés uniquement) a été attribué à ce problème.

Si le serveur est en panne, vous pouvez 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 quoiqu'il arrive). Si enable password quoi que ce soit n'est pas dans la configuration PIX, entrez pix pour le nom d'utilisateur et appuyez sur Entrée. Si le mot de passe actif est défini mais inconnu, un disque de récupération de mot de passe doit être créé pour réinitialiser le mot de passe.

Modification de l'invite des utilisateurs Voir

Si vous avez la commande :

<#root>

```
auth-prompt PIX_PIX_PIX
```

les utilisateurs qui passent par le PIX voient la séquence suivante :

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

À l'arrivée à la destination finale, les utilisateurs verront l'invite Nom d'utilisateur et Mot de passe s'afficher dans la zone de destination. Cette invite affecte uniquement les utilisateurs qui passent par le PIX, pas vers le PIX.

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

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

Si vous disposez des commandes suivantes :

<#root>

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

ensuite, les utilisateurs voient la séquence suivante sur une connexion échouée/réussie par le PIX :

<#root>

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

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

Délais d'inactivité et de dépassement de délai absolu par utilisateur

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

HTTP virtuel

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

Pour éviter cela, vous pouvez implémenter le HTTP virtuel en ajoutant une adresse RFC 1918 (c'est-à-dire, une adresse qui n'est pas routable sur Internet, mais valide et unique pour le réseau interne PIX) à la configuration PIX en utilisant la commande suivante :

<#root>

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

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

Exemple de trafic sortant HTTP virtuel

Configuration PIX HTTP virtuel sortant :

<#root>

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

Telnet virtuel

Il est possible de configurer le PIX pour authentifier tous les messages entrants et sortants, mais ce n'est pas une bonne idée parce que certains protocoles, tels que le courriel, ne sont pas facilement authentifiés. Lorsqu'un serveur de messagerie et un client essaient de communiquer via le PIX lorsque tout le trafic via le PIX est authentifié, le syslog PIX pour les protocoles non authentifiables affiche des messages tels que :

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

Cependant, s'il y a vraiment un besoin d'authentifier une sorte de service inhabituel, ceci peut être fait en utilisant la commande virtual telnet. Cette commande permet l'authentification de l'adresse IP Telnet virtuelle. Après cette authentification, le trafic pour le service inhabituel peut aller au vrai serveur.

Dans cet exemple, vous voulez que le trafic du port TCP 49 circule de l'hôte externe 99.99.99.2 vers l'hôte interne 171.68.118.106. Puisque ce trafic n'est pas vraiment authentifiable, configurez un Telnet virtuel. Pour un Telnet virtuel, un réseau statique doit être associé. Ici, 99.99.99.20 et 171.68.118.20 sont des adresses virtuelles.

Telnet virtuel entrant

Configuration PIX Virtual Telnet Inbound

<#root>

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

Débogage PIX Virtual Telnet Inbound

L'utilisateur à l'adresse 99.99.99.2 doit d'abord s'authentifier par Telnet à l'adresse 99.99.99.20 sur le PIX :

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

Une fois l'authentification réussie, la commande show uauth montre que l'utilisateur a « time on the meter » :

```
<#root>

pixfirewall#

show uauth

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

Et lorsque le périphérique situé à l'adresse 99.99.99.2 veut envoyer le trafic TCP/49 au périphérique situé à l'adresse 171.68.118.106 :

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

L'autorisation peut être ajoutée :

```
<#root>

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

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

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

Sur le serveur TACACS+, il s'agit des éléments suivants :

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

Telnet virtuel sortant

Puisque le trafic sortant est autorisé par défaut, aucun trafic statique n'est requis pour l'utilisation du trafic sortant Telnet virtuel. Dans l'exemple suivant, l'utilisateur interne à l'adresse 10.31.1.50 établit une connexion Telnet avec le réseau virtuel 99.99.99.30 et s'authentifie ; la connexion Telnet est immédiatement abandonnée. Une fois authentifié, le trafic TCP est autorisé de 10.31.1.50 vers le serveur à l'adresse 99.99.99.2 :

Configuration PIX Virtual Telnet Sortant :

<#root>

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

Remarque : il n'y a aucune autorisation car il s'agit de RADIUS.

Débogage PIX Virtual Telnet Sortant :

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

```
   10.31.1.50/11036 (pixuser)
302002: Teardown TCP connection 18 faddr 99.99.99.2/49
   gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
   duration 0:00:02 bytes 0 (pixuser)
```

Déconnexion virtuelle de Telnet

Lorsque les utilisateurs établissent une connexion Telnet avec l'adresse IP Telnet virtuelle, la commande show uauth affiche leur uauth. Si les utilisateurs veulent empêcher le trafic d'être acheminé après la fin de leurs sessions alors qu'il reste du temps dans l'authentification, ils doivent à nouveau établir une connexion Telnet avec l'adresse IP Telnet virtuelle. Cette opération désactive la session.

Après la première authentification :

<#root>

```
pix3#
```

show uauth

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

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

<#root>

```
pix3#
```

show uauth

```
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

Autorisation de port

L'autorisation est autorisée pour les plages de ports (comme TCP/30-100). Si le Telnet virtuel est configuré sur le PIX et l'autorisation pour une plage de ports, une fois que le trou est ouvert avec le Telnet virtuel, le PIX émet une commande tcp/30-100 au serveur TACACS+ pour l'autorisation :

<#root>

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

Configuration du serveur de logiciel gratuit TACACS+:

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

Comptabilisation AAA pour le trafic autre que HTTP, FTP et Telnet

Après avoir vérifié que le protocole Telnet virtuel permettait le trafic TCP/49 vers l'hôte à l'intérieur du réseau, nous avons décidé de tenir compte de ce problème. Nous avons donc ajouté :

<#root>

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

Ceci a pour conséquence d'avoir un enregistrement de comptabilité coupé quand le trafic tcp/49 passe (cet exemple est du freeware TACACS+) :

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

Authentification étendue (Xauth)

Exemples de configuration

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

Authentification sur la DMZ

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

```
least secure

PIX outside (security0) = 1.1.1.1

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

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

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

Diagramme du réseau

Configuration PIX

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

<#root>

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
(nameif ethernet2 pix/intf2 security10
nameif ethernet3 pix/intf3 security15)
nameif ethernet4 pix/intf4 security20
nameif ethernet5 pix/intf5 security25
ip address outside 1.1.1.1 255.255.255.0
ip address inside 10.31.1.47 255.255.255.0
(ip address pix/intf2 127.0.0.1 255.255.255.255
ip address pix/intf3 127.0.0.1 255.255.255.255)
ip address pix/intf4 4.4.4.4 255.255.255.0
ip address pix/intf5 5.5.5.5 255.255.255.0
static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask 255.255.255.255 0 0
```

```
aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0
4.4.4.0 255.255.255.0 AuthInbound
aaa-server TACACS+ protocol tacacs+
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Comptabilité Xauth

Si la commande sysopt connection permit-ipsec, et non la commande sysopt ipsec pl-compatible, est configurée dans le PIX avec xauth, la comptabilisation est valide pour les connexions TCP, mais pas ICMP ou UDP.

Informations connexes

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

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.