Comment ajouter l'authentification AAA (Xauth) au logiciel IPSec PIX version 5.2 et ultérieure

Contenu

Introduction

Le RAYON et l'authentification et la comptabilité TACACS+, et dans une certaine mesure, autorisation, est fait pour le Cisco Secure VPN Client 1.1 et le Cisco VPN 3000 2.5 tunnels de client matériel qui se terminent au PIX. Les changements de PIX 5.2 et d'authentification étendue postérieure (Xauth) au-dessus de cela des versions préalables qui incluent la prise en charge de liste d'accès d'Authentification, autorisation et comptabilité (AAA) pour contrôler ce qui a authentifié des utilisateurs peuvent accéder à et les prendre en charge pour l'arrêt de Xauth du Cisco VPN 3000 Client 2.5. Les commandes enables de **Segmentation de tunnel de groupe de vpn le** client VPN 3000 à connecter au réseau à l'intérieur du PIX aussi bien que d'autres réseaux (par exemple, l'Internet) en même temps. Dans PIX 5.3 et plus tard, la modification d'AAA au-dessus des versions préalables de code est que les ports de RAYON sont configurables. Dans PIX 6.0, le soutien du client vpn 3.x est ajouté. Ceci exige le groupe 2. de Diffie-Hellman.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version du logiciel PIX 5.2.1
- Cisco Secure VPN Client 1.1
- Client ou client vpn 3.x du Cisco VPN 3000 2.5**Remarque:** La release de Client VPN Cisco 3.0.x ne fonctionne pas avec des versions de PIX plus tôt que 6.0. Référez-vous au matériel et aux clients vpn de Cisco prenant en charge le pour en savoir plus IPsec/PPTP/L2TP.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

La version 6.2 de logiciel pare-feu PIX prend en charge le téléchargement du Listes de contrôle d'accès (ACL) au Pare-feu PIX d'un serveur de contrôle d'accès (ACS). Ceci permet à la configuration du par-utilisateur ACLs sur un serveur d'AAA de fournir l'autorisation d'ACL de par-utilisateur. Il est alors téléchargeable par l'ACS au Pare-feu PIX. Cette caractéristique est prise en charge pour des serveurs de RAYON seulement. Il n'est pas pris en charge pour des serveurs TACACS+.

Étapes de debug

Terminez-vous ces derniers mettent au point des étapes :

1. Assurez-vous les travaux de configuration de Xauth PIX avant que vous ajoutiez l'authentification d'AAA.Si vous ne pouvez pas passer le trafic avant que vous implémentiez l'AAA, vous ne pouvez pas le faire après.
2. Activez un certain genre d'ouvrir une session le PIX :N'émettez pas la commande de **logging console debugging** sur un système chargé lourd.La commande de **logging buffered debugging** peut être émise. Émettez alors la commande de **show logging**.Se connecter peut également être envoyé à un serveur de journal des messages système (Syslog) et être examiné.
3. Activez l'élimination des imperfections sur les serveurs TACACS+ ou de RAYON. Tous les serveurs ont cette option.

Commandes de debug sur le PIX

- **debug crypto ipsec SA** — Cette commande de débogage affiche des événements d'IPsec.
- **debug crypto isakmp SA** — Cette commande de débogage affiche des messages au sujet des événements d'Échange de clés Internet (IKE).
- **engine de debug crypto isakmp** — Cette commande de débogage affiche des messages au sujet des événements d'IKE.

Debug de côté client

Permettez au visualiseur de log de voir que le côté client met au point dans 1.1 Cisco Secures ou VPN 3000 client 2.5.

Profils de serveur d'AAA

Cisco Secure UNIX TACACS+

```
user = noacl{
password = clear "********"
service=shell {
}
}
user = pixb{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
user = 3000full{
  password = clear "********"
  service=shell {
  }
  }
user = 3000partial{
  password = clear "********"
  service=shell {
```

```
  }
  }
```

Cisco Secure ACS pour Windows TACACS+

Le noacl, le besoin de l'utilisateur 3000full, et 3000partial seulement un nom d'utilisateur et un mot de passe dans le Cisco Secure ACS de Windows. Les besoins de l'utilisateur de pixb un nom d'utilisateur, un mot de passe, un groupe dedans coché par shell/exec, un ACL ont coché, et 115 dans la case.

Cisco Secure UNIX RADIUS

```
user = noacl{
password = clear "********"
}
user = pixb{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
user = 3000full{
  password = clear "********"
  }
user = 3000partial{
  password = clear "********"
  }
```

Cisco Secure ACS pour le RAYON de Windows

RADIUS/Cisco est le type de périphérique. Le noacl, le besoin de l'utilisateur 3000full, et 3000partial seulement un nom d'utilisateur et un mot de passe dans le Cisco Secure ACS de Windows. Les besoins de l'utilisateur de pixb un nom d'utilisateur, un mot de passe, et un contrôle et un acl=115 dans la zone rectangulaire Cisco/RADIUS où il indique la paire AV 009\001 (constructeur-particularité).

Remarque: Vous avez besoin de l'attribut du constructeur pour l'ACL. L'attribut 11, filtre-id, est non valide. Cette question est assignée l'ID de bogue Cisco CSCdt50422 (clients enregistrés seulement). Il est réparé dans la version du logiciel PIX 6.0.1.

Merit RADIUS (prenant en charge des paires AV de Cisco)

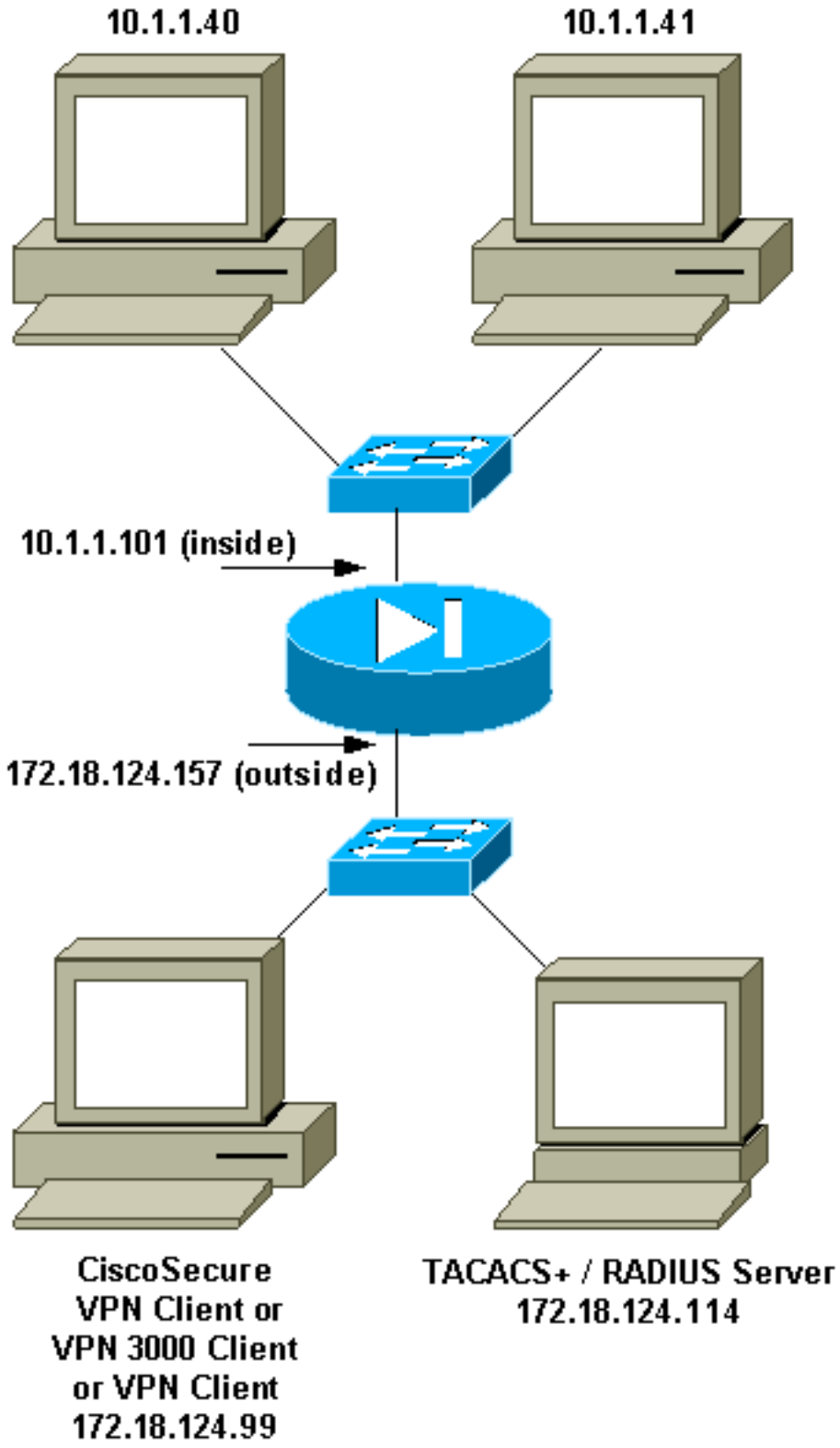
```
noacl Password= "noacl"

pixb Password= "pixb"
cisco-avpair = "acl=115"

3000full Password= "3000full"

3000partial Password= "3000partial"
```

Diagramme du réseau



Le RAYON configurable met en communication (5.3 et plus tard)

Quelques serveurs de RAYON utilisent des ports de RAYON autres que 1645/1646 (habituellement 1812/1813). Dans PIX 5.3 et plus tard, l'authentification et les ports de traçabilité de RAYON peuvent être changés aux ports autres que le 1645/1646 par défaut avec ces commandes :

- rayon-authport d'AAA-serveur #
- rayon-acctport d'AAA-serveur #

Comment authentifier avec le Xauth sans groupes VPN

Dans cet exemple, chacun des trois clients vpn est authentifié avec le Xauth. Cependant, les clients vpn peuvent accéder à seulement le réseau à l'intérieur du PIX, car la Segmentation de tunnel est non utilisable. Voyez comment authentifier le Xauth avec des groupes VPN pour plus d'informations sur la Segmentation de tunnel. ACLs a passé vers le bas du serveur d'AAA s'appliquent à tous les clients vpn. Dans cet exemple, le but est pour que le noacl d'utilisateur connecte et à obtient à toutes les ressources à l'intérieur du PIX. L'utilisateur que le pixb connecte, mais parce que l'ACL 115 est passé vers le bas du serveur d'AAA pendant le processus de Xauth, l'utilisateur peut seulement obtenir à 10.1.1.40. Access à 10.1.1.41 et à tout l'autre intérieur d'adresses IP est refusé.

Remarque: La version du logiciel PIX 6.0 est exigée pour le support du client 3.0 VPN.

Cisco Secure VPN Client 1.1 installé - Xauth sans groupes VPN

```
Name of connection:
Remote party address = IP_Subnet = 10.1.1.0, Mask 255.255.255.0
Connect using Secure Gateway Tunnel to 172.18.124.157
My Identity:
Select certificate = None
ID_Type = ip address, pre-shared key and fill in key
('cisco1234') - matches that of pix in 'isakmp key' command
Security policy = defaults
Proposal 1 (Authen) = DES, MD5
Proposal 2 (Key Exchange) = DES, MD5, Tunnel
```

Ouvrez une fenêtre du déni de service (DOS) et émettez le **ping -** commande **t** *#.#.#.#*. Quand la fenêtre d'authentification apparaît, tapez le nom d'utilisateur et mot de passe qui sont conforme à celui sur le serveur d'AAA.

VPN 3000 le client 2.5 ou le client vpn 3.x a installé - le Xauth sans groupes VPN

Procédez comme suit :

1. **Options** choisies **> Properties > nom d'authentification > de groupe**.
2. Le nom de groupe est ne font pas _care et le mot de passe est conforme à celui sur PIX dans la commande de **clé d'ISAKMP**. Le nom d'hôte est 172.18.124.157.
3. Cliquez sur **Connect**.
4. Quand la fenêtre d'authentification monte, tapez le nom d'utilisateur et mot de passe qui sont conforme à celui sur le serveur d'AAA.

Xauth sans groupes VPN - Configuration de PIX

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
```

```
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 access-list 115 deny
ip any host 10.1.1.41 access-list 115 permit ip any host 10.1.1.40 pager lines 24 logging on no
logging timestamp no logging standby logging console debugging no logging monitor no logging
buffered logging trap debugging no logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu outside 1500 mtu inside 1500 ip address
outside 172.18.124.157 255.255.255.0 ip address inside 10.1.1.101 255.255.255.0 ip audit info
action alarm ip audit attack action alarm ip local pool test 192.168.1.1-192.168.1.5 no failover
failover timeout 0:00:00 failover poll 15 failover ip address outside 0.0.0.0 failover ip
address inside 0.0.0.0 arp timeout 14400 global (outside) 1 172.18.124.154 nat (inside) 0
access-list 108 Nat (inside) 1 10.1.1.0 255.255.255.0 0 0 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute AAA-server TACACS+ protocol tacacs+ AAA-server RADIUS protocol
radius AAA-server AuthInbound protocol tacacs+ AAA-server AuthInbound (outside) host
172.18.124.114 cisco timeout 5 no snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec no
sysopt route dnat crypto ipsec transform-set myset esp-des esp-md5-hmac crypto dynamic-map
dynmap 10 set transform-set myset crypto map mymap 10 ipsec-isakmp dynamic dynmap crypto map
mymap client configuration address initiate crypto map mymap client configuration address
respond crypto map mymap client authentication AuthInbound crypto map mymap interface outside
isakmp enable outside isakmp key ******** address 0.0.0.0 netmask 0.0.0.0 isakmp identity
address isakmp client configuration address-pool local test outside !--- Internet Security
Association and Key Management Protocol (ISAKMP) !--- Policy for Cisco VPN Client 2.5 or !---
Cisco Secure VPN Client 1.1. isakmp policy 10 authentication pre-share isakmp policy 10
encryption des isakmp policy 10 hash md5 !--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-
H) !--- group 1 policy (PIX default). isakmp policy 10 group 1 isakmp policy 10 lifetime 86400 !
!--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20 authentication pre-share isakmp policy 20
encryption des isakmp policy 20 hash md5 !--- The VPN 3.0 Clients use D-H group 2 policy !---
and PIX 6.0 code. isakmp policy 20 group 2 isakmp policy 20 lifetime 86400 telnet timeout 5 ssh
timeout 5 terminal width 80 Cryptochecksum:05c6a2f3a7d187162c4408503b55affa : end [OK]
```

Comment authentifier avec le Xauth avec des groupes VPN

Dans cet exemple, VPN 3000 le client 2.5 ou le client vpn 3.0 peut être authentifié avec le Xauth, et la Segmentation de tunnel est en vigueur. En vertu de l'adhésion de groupe VPN, un ACL est passé du PIX au client VPN 3000. Il spécifie que seulement le réseau à l'intérieur du PIX a un tunnel chiffré. Autre trafiquent (peut-être à l'Internet) n'est pas chiffré.

Dans cet exemple, un client vpn, avec le nom d'utilisateur 3000full (sur le serveur d'AAA), dans le groupe vpn3000-all (sur le PIX) accède au réseau 10.1.1.X entier à l'intérieur du PIX en même temps que l'Internet. Le client vpn reçoit le wins-serveur, le dns-server, et les informations de domain-name. L'autre client vpn, avec le nom d'utilisateur 3000partial (sur l'AAA-serveur), dans le groupe vpn3000-41 (sur le PIX) accède à seulement une adresse IP à l'intérieur du réseau (10.1.1.40) en vertu du profil de groupe. Ce client vpn ne reçoit pas les informations de victoires et de dns-server, mais fait toujours la Segmentation de tunnel.

Remarque: La version du logiciel PIX 6.0 est exigée pour le support du client 3.0 VPN.

Client vpn 2.5 ou 3.0 installés - Xauth avec des groupes VPN

Procédez comme suit :

Remarque: L'installation de client VPN 2.5 ou 3.0 dépend de l'utilisateur impliqué.

1. **Options** choisies **> Properties > authentification**.

2. Le nom et le mot de passe de groupe de groupe apparient le nom de groupe sur le PIX comme dans : ******** de mot de passe du vpngroup vpn3000-all ou ******** de mot de passe du vpngroup vpn3000-41. Le nom d'hôte est 172.18.124.157.
3. Cliquez sur **Connect**.
4. Quand la fenêtre d'authentification monte, entrez le nom d'utilisateur et mot de passe qui sont conforme à celui sur le serveur d'AAA.

Dans cet exemple, une fois que l'utilisateur 3000full est authentifié, il prend les informations du groupe vpn3000-all. L'utilisateur 3000partial prend les informations du groupe vpn3000-41. La fenêtre affiche que **négociant la Sécurité les profils** et **votre lien est maintenant sécurisée**.

L'utilisateur 3000full utilise le mot de passe pour le groupe vpn3000-all. La liste d'accès 108 est associée avec ce groupe pour des buts de partitionner la mise en tunnel. Le tunnel est formé au réseau 10.1.1.x. La circulation décryptée aux périphériques pas dans la liste d'accès 108 (par exemple, l'Internet). C'est Segmentation de tunnel.

C'est la sortie pour la fenêtre d'état de connexion client VPN pour l'utilisateur 3000full :

```
        Network         Mask
key     10.1.1.0        255.255.255.0
key     172.18.124.157  255.255.255.255
```

L'utilisateur 3000partial utilise le mot de passe pour le groupe vpn3000-41. La liste d'accès 125 est associée avec ce groupe pour des buts de partitionner la mise en tunnel. Le tunnel est formé au périphérique de 10.1.1.41. La circulation décryptée aux périphériques pas dans la liste d'accès 125 (par exemple, l'Internet). Cependant, le trafic ne circule pas au périphérique de 10.1.1.40 parce que ce trafic est unroutable. Il n'est pas spécifié dans la liste de tunnels de chiffrement.

C'est la sortie pour la fenêtre d'état de connexion client VPN pour l'utilisateur 3000partial :

```
        Network         Mask
key     10.1.1.41       255.255.255.255
key     172.18.124.157  255.255.255.255
```

Xauth avec des groupes VPN - Configuration de PIX

Remarque: Le Cisco Secure VPN Client 1.1 ne travaille pas avec ceci parce qu'il n'y a aucune clé de Protocole ISAKMP (Internet Security Association and Key Management Protocol). Ajoutez la commande de **0.0.0.0 de netmask de 0.0.0.0 d'adresse de ******** de clé d'ISAKMP** de faire fonctionner tous les clients vpn.

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname goss-pixb
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 access-list 125
permit ip host 10.1.1.41 any pager lines 24 logging on no logging timestamp no logging standby
logging console debugging no logging monitor no logging buffered logging trap debugging no
```

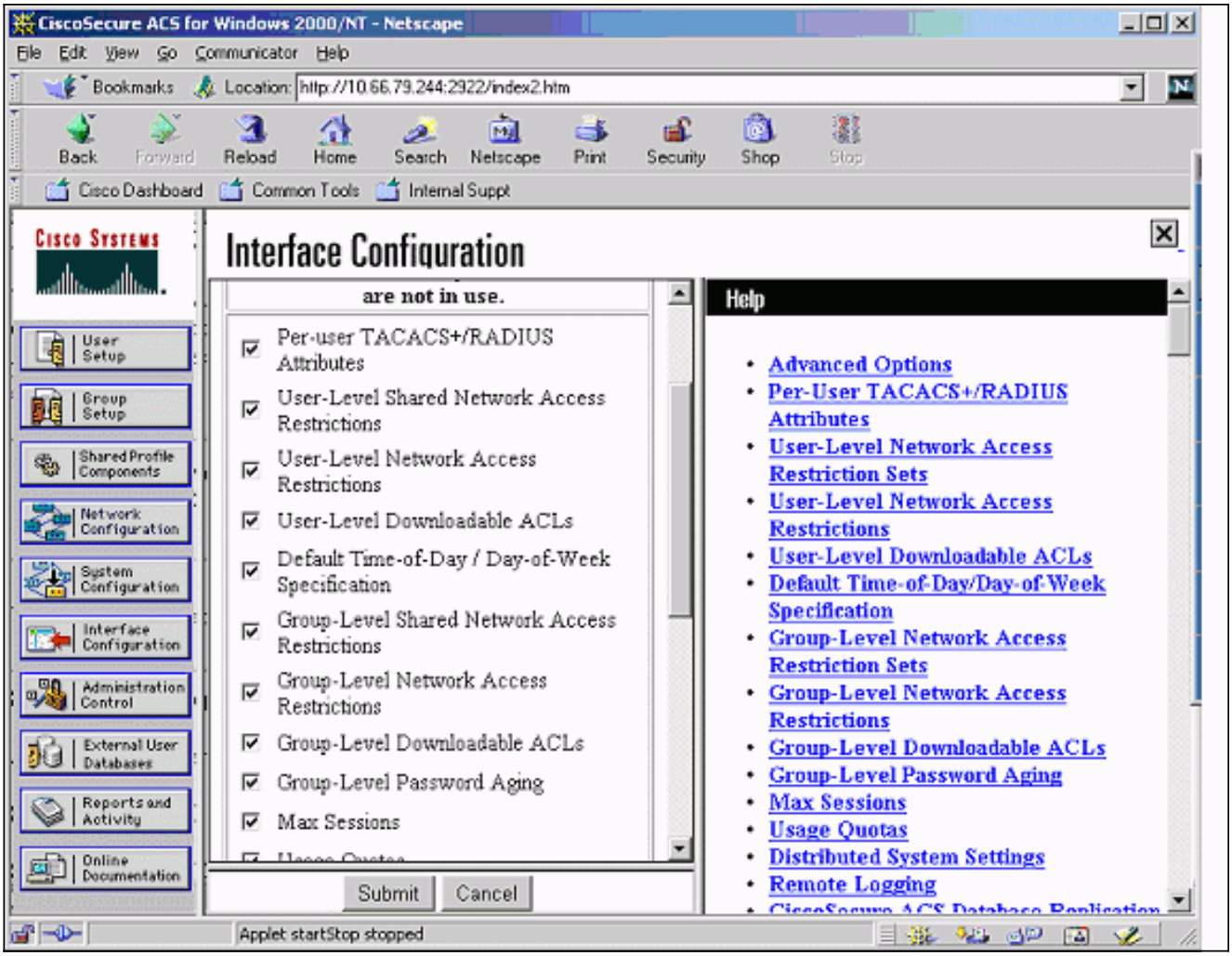
```
logging history logging facility 20 logging queue 512 interface ethernet0 auto interface
ethernet1 auto mtu outside 1500 mtu inside 1500 ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm
ip local pool test 192.168.1.1-192.168.1.5 no failover failover timeout 0:00:00 failover poll 15
failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0 arp timeout 14400 global
(outside) 1 172.18.124.154 Nat (inside) 0 access-list 108 Nat (inside) 1 10.1.1.0 255.255.255.0
0 0 route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
uauth 0:05:00 absolute AAA-server TACACS+ protocol tacacs+ AAA-server RADIUS protocol radius
AAA-server AuthInbound protocol tacacs+ AAA-server AuthInbound (outside) host 172.18.124.111
cisco timeout 5 no snmp-server location no snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset ESP-Des esp-md5-hmac crypto dynamic-map dynmap 10 set
transform-set myset crypto map mymap 10 ipsec-isakmp dynamic dynmap crypto map mymap client
configuration address initiate crypto map mymap client configuration address respond crypto map
mymap client authentication AuthInbound crypto map mymap interface outside isakmp enable outside
isakmp identity address isakmp client configuration address-pool local test outside !--- ISAKMP
Policy for Cisco VPN Client 2.5 or !--- Cisco Secure VPN Client 1.1. isakmp policy 10
authentication pre-share isakmp policy 10 encryption des isakmp policy 10 hash md5 !--- The 1.1
and 2.5 VPN Clients use Diffie-Hellman (D-H) !--- group 1 policy (PIX default). isakmp policy 10
group 1 isakmp policy 10 lifetime 86400 ! !--- ISAKMP Policy for VPN Client 3.0 isakmp policy 20
authentication pre-share isakmp policy 20 encryption des isakmp policy 20 hash md5 !--- The VPN
3.0 Clients use D-H group 2 policy !--- and PIX 6.0 code. isakmp policy 20 group 2 isakmp policy
20 lifetime 86400 vpngroup vpn3000-all address-pool test vpngroup vpn3000-all dns-server
10.1.1.40 vpngroup vpn3000-all wins-server 10.1.1.40 vpngroup vpn3000-all default-domain
rtp.cisco.com vpngroup vpn3000-all split-tunnel 108 vpngroup vpn3000-all idle-time 1800 vpngroup
vpn3000-all password ******** vpngroup vpn3000-41 address-pool test vpngroup vpn3000-41 split-
tunnel 125 vpngroup vpn3000-41 idle-time 1800 vpngroup vpn3000-41 password ******** telnet
timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:429db0e7d20451fc28074f4d6f990d25 : end
```

Xauth avec les groupes VPN et le Par-utilisateur ACLs téléchargeable - installation ACS

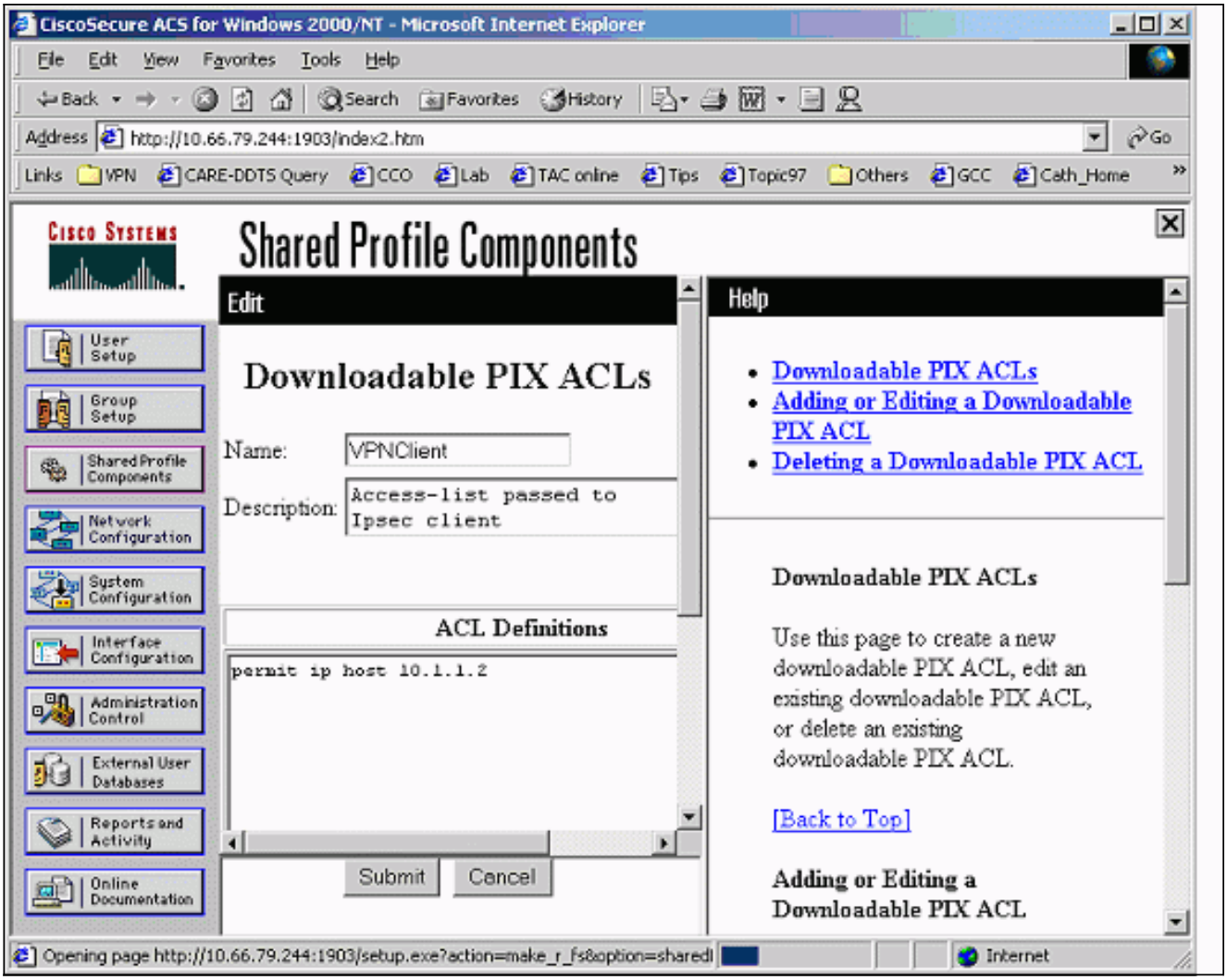
Installez le Cisco Secure ACS

Procédez comme suit :

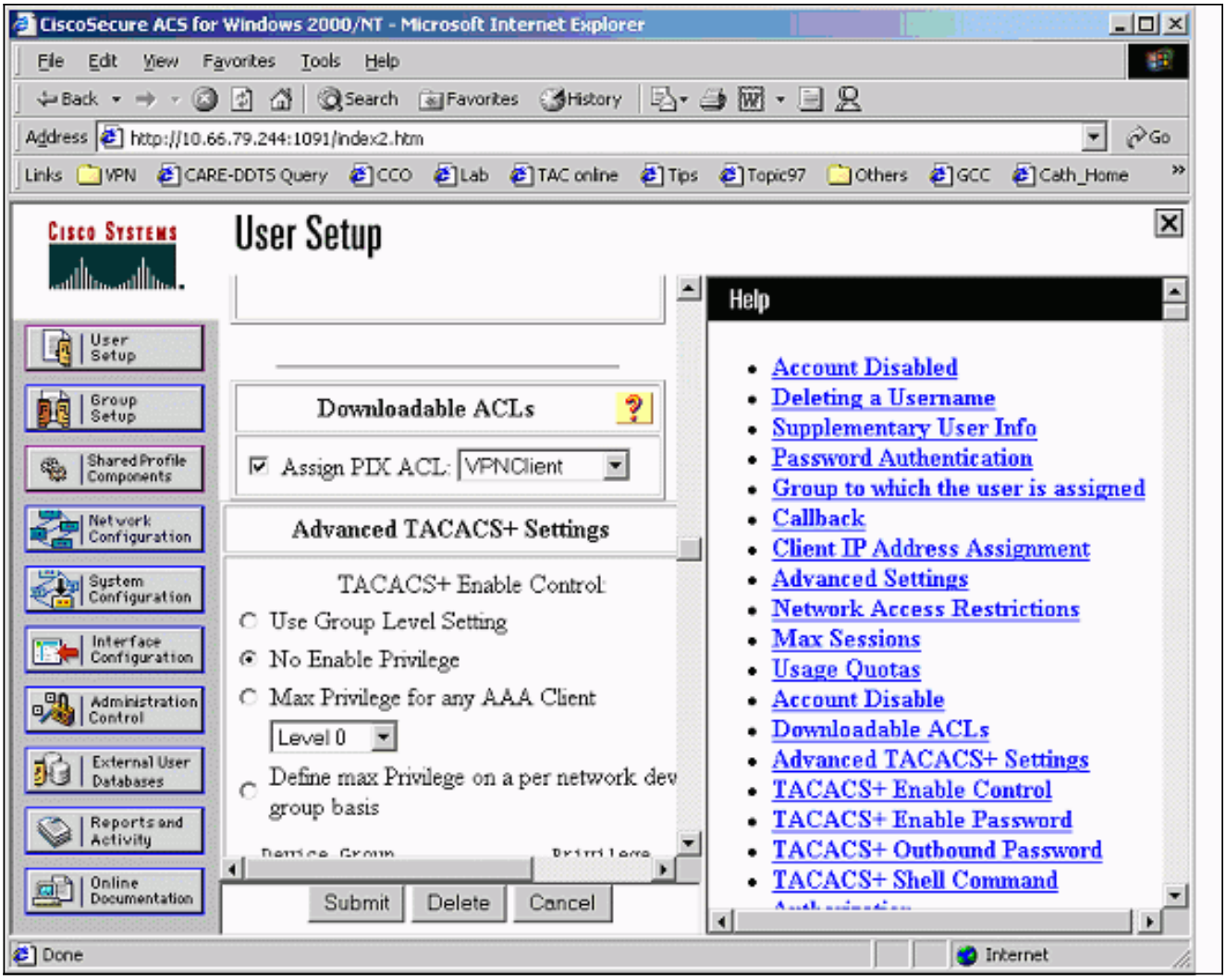
1. Cliquez sur la **configuration d'interface** et sélectionnez l'option pour le **niveau utilisateur ACLs téléchargeable**.



2. Cliquez sur les **composants partagés de profil** et définissez un ACL téléchargeable.



3. Cliquez sur User Setup. Sélectionnez l'option **d'assigner l'ACL PIX**. Choisissez l'ACL correct de la liste
déroulante.



Xauth avec les groupes VPN et le Par-utilisateur ACLs téléchargeable - installation PIX 6.x

Si vous voulez conduire un ACL téléchargeable de par-utilisateur d'utilisateur pour l'autorisation, utilisez la version 6.2(2) de logiciel pare-feu PIX. Référez-vous à l'ID de bogue Cisco CSCdx47975 (clients enregistrés seulement).

```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-4
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 pager lines 24
logging buffered debugging interface ethernet0 auto interface ethernet1 auto mtu outside 1500
mtu inside 1500 ip address outside 10.66.79.69 255.255.255.224 ip address inside 10.1.1.1
```

255.255.255.0 ip audit info action alarm ip audit attack action alarm ip local pool test 192.168.1.1-192.168.1.5 pdm history enable arp timeout 14400 **nat (inside) 0 access-list 108** conduit permit icmp any any route outside 0.0.0.0 0.0.0.0 10.66.79.65 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius aaa-server LOCAL protocol local **aaa-server AuthInbound protocol radius aaa-server AuthInbound (outside) host 10.66.79.244 cisco123 timeout 10** no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable **sysopt connection permit-ipsec** no sysopt route dnat **crypto ipsec transform-set myset esp-des esp-md5-hmac crypto dynamic-map dynmap 10 set transform-set myset crypto map mymap 10 ipsec-isakmp dynamic dynmap** *!--- This commands the router to respond to the VPN 3.x Client.* **crypto map mymap client configuration address respond** *!--- This tells the router to expect Xauth for the VPN 3.x Client.* **crypto map mymap client authentication AuthInbound crypto map mymap interface outside isakmp enable outside** isakmp policy 20 authentication pre-share isakmp policy 20 encryption des isakmp policy 20 hash md5 isakmp policy 20 group 2 isakmp policy 20 lifetime 86400 ! *!--- This is the VPN group configuration.* **vpngroup vpn3000-all address-pool test vpngroup vpn3000-all default-domain apt.cisco.com** *!--- The split-tunnel mode-config is not used, !--- which enforces authorization on a per-user basis.* **vpngroup vpn3000-all idle-time 1800 vpngroup vpn3000-all password ********** ! telnet timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:7c3d067232f427e7522f4a679e963c58 end:

Xauth avec les groupes VPN et le Par-utilisateur ACLs téléchargeable - installation asa PIX 7.x

```
PIX Version 7.1(1)
!
hostname PIX
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.66.79.69 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns domain-lookup inside
dns server-group DefaultDNS
 timeout 30
```

access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 pager lines 24 logging buffer-size 500000 logging console debugging logging monitor errors mtu outside 1500 mtu inside 1500 ip local pool test 192.168.1.1-192.168.1.5 no failover icmp permit any outside icmp permit any inside no asdm history enable arp timeout 14400 **nat (inside) 0 access-list 108** route outside 0.0.0.0 0.0.0.0 10.66.79.65 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute **aaa-server AuthInbound protocol radius aaa-server AuthInbound host 10.66.79.244 key cisco123 group-policy vpn3000 internal group-policy vpn3000 attributes dns-server value 172.16.1.1 default-domain value cisco.com username vpn3000 password nPtKy7KDCerzhKeX encrypted** no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart **crypto ipsec transform-set my-set esp-des esp-md5-hmac crypto dynamic-map dynmap 10 set transform-set my-set crypto dynamic-map dynmap 10 set reverse-route crypto map mymap 10 ipsec-isakmp dynamic dynmap crypto map mymap interface outside isakmp enable outside isakmp policy 10 authentication pre-share isakmp policy 10 encryption des isakmp policy 10 hash md5 isakmp policy 10 group 2 isakmp policy 10 lifetime 1000** isakmp policy 65535 authentication pre-share isakmp

```
policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp
policy 65535 lifetime 86400 tunnel-group DefaultRAGroup general-attributes authentication-
server-group (outside) vpn tunnel-group vpn3000 type ipsec-ra tunnel-group vpn3000 general-
attributes address-pool test authentication-server-group vpn tunnel-group vpn3000 ipsec-
attributes pre-shared-key * telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras
inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

Comment configurer le Xauth local pour la connexion client VPN

Ces commandes sont exigées pour configurer le Xauth local pour la connexion client VPN :

- *gens du pays de* **protocole de serveur-***balise d'AAA***-serveur**
- *AAA-serveur-nom d'***authentification client de** *map name de* **crypto map**

Émettez la commande de **nom d'utilisateur** de définir des utilisateurs locaux sur PIX.

Afin d'utiliser la base de données d'authentification de l'utilisateur du pare-feu PIX local, entrez dans les **GENS DU PAYS** pour le paramètre de serveur-*balise* pour l'ordre d'AAA-**serveur**. L'ordre d'AAA-**serveur** est émis avec la commande de **crypto map** d'établir une association d'authentification de sorte que des clients vpn soient authentifiés quand ils accèdent au Pare-feu PIX.

Comment ajouter la comptabilité

C'est la syntaxe de la commande d'ajouter la comptabilité :

- *acctg_service d'***aaa accounting|à moins que d'arrivée|sortant**/*foreign_mask* **tacacs+ de** *foreign_ip de local_mask de local_ip d'if_name***|rayon** ;

ou (nouveau dans 5.2) :

- **l'aaa accounting incluent l'***acctg_service* **d'arrivée|***server_tag* **sortant de correspondance**

Dans la configuration PIX, c'est la commande ajoutée :

- **l'aaa accounting incluent tout 0.0.0.0 d'arrivée 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound** ;

ou (nouveau dans 5.2) :

- **IP d'autorisation de la liste d'accès 150 toute toute correspondance 150 AuthInbound extérieur d'aaa accounting**

Remarque: La commande d'**autorisation-ipsec de connexion de sysopt**, pas la commande pl-**compatible d'ipsec de sysopt**, est nécessaire pour que la comptabilité de Xauth fonctionne. La comptabilité de Xauth ne fonctionne pas avec seulement la commande pl-**compatible d'ipsec de sysopt**. La comptabilité de Xauth est valide pour des connexions TCP. Il est non valide pour le Protocole ICMP (Internet Control Message Protocol) ou le Protocole UDP (User Datagram Protocol).

Exemple de comptabilité TACACS+

```
Fri Sep 8 03:48:40 2000 172.18.124.157
pixc PIX 192.168.1.1 start task_id=0x17 foreign_ip=192.168.1.1
```

```
    local_ip=10.1.1.40 cmd=telnet
Fri Sep 8 03:48:44 2000 172.18.124.157 pixc PIX 192.168.1.1
    stop task_id=0x17 foreign_ip=192.168.1.1 local_ip=10.1.1.40
    cmd=telnet elapsed_time=4 bytes_in=42 bytes_out=103
Fri Sep 8 03:49:31 2000 172.18.124.157 pixc PIX 192.168.1.1
    start task_id=0x18
foreign_ip=192.168.1.1 local_ip=10.1.1.40 cmd=http
Fri Sep 8 03:49:35 2000 172.18.124.157 pixc PIX 192.168.1.1
    stop task_id=0x18 foreign_ip=192.168.1.1 local_ip=10.1.1.40
    cmd=http elapsed_time=4 bytes_in=242 bytes_out=338
```

Exemple de comptabilisation RADIUS

```
Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000003
User-Name = noacl
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1141
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23

Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 80
Acct-Session-Id = 0x00000004
User-Name = noacl
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1168
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=80

Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.41
Login-TCP-Port = 80
Acct-Session-Id = 0x00000008
User-Name = noacl
Acct-Session-Time = 4
Acct-Input-Octets = 242
Acct-Output-Octets = 338
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1182
Vendor-Specific = Destination-IP=10.1.1.41
Vendor-Specific = Destination-Port=80

Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 10.1.1.40
Login-TCP-Port = 23
Acct-Session-Id = 0x00000015
User-Name = noacl
Acct-Session-Time = 33
Acct-Input-Octets = 43
Acct-Output-Octets = 103
Vendor-Specific = Source-IP=192.168.1.1
Vendor-Specific = Source-Port=1257
Vendor-Specific = Destination-IP=10.1.1.40
Vendor-Specific = Destination-Port=23
```

Debug et exposition - Xauth sans groupes VPN

goss-pixb#**show debug** debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get Off put Off verify Off switch Off fail Off fmsg Off goss-pixb#**terminal monitor** goss-pixb# crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_MM exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5 ISAKMP: default group 1 ISAKMP: auth pre-share ISAKMP (0): atts are acceptable. Next payload is 0 ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_MM exchange ISAKMP (0): processing KE payload. Message ID = 0 ISAKMP (0): processing NONCE payload. Message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): processing vendor id payload return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_MM exchange ISAKMP (0): processing ID payload. Message ID = 0 ISAKMP (0): processing HASH payload. Message ID = 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 0 ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got a queue event... IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99 ISAKMP (0): SA has been authenticated ISAKMP (0): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange ISAKMP (0:0): Need XAUTH ISAKMP/xauth: request attribute XAUTH_TYPE ISAKMP/xauth: request attribute XAUTH_USER_NAME ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD ISAKMP (0:0): initiating peer config to 172.18.124.99. ID = 2218162690 (0x84367a02) return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 172.18.124.99. Message ID = 2156074032 ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS109005: Authentication succeeded for user 'pixb' from 172.18.124.99/0 to 0.0.0.0/0 on interface IKE-XAUTH ISAKMP (0:0): initiating peer config to 172.18.124.99. ID = 2218162690 (0x84367a02) 109005: Authentication succeeded for user 'pixb' from 172.18.124.157 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 172.18.124.99. Message ID = 2156497080 ISAKMP: Config payload CFG_ACK ISAKMP (0:0): initiating peer config to 172.18.124.99. ID = 393799466 (0x1778e72a) return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 172.18.124.99. Message ID = 2156156112 ISAKMP: Config payload CFG_ACK ISAKMP (0:0): peer accepted the address! return status is IKMP_NO_ERROR.99/0 to 0.0.0.0/0 on interface IKE-XAUTH crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. Message ID = 2323118710 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99, dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= ESP-Des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. Message ID = 2323118710 ISAKMP (0): processing ID payload. Message ID = 2323118710 ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0 ISAKMP (0): processing ID payload. Message ID = 2323118710 ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port 0 IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0xeeae8930(4004415792) for SA from 172.18.124.99 to 172.18.124.157 for prot 3 return status is IKMP_NO_ERROR4 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1 map_alloc_entry: allocating entry 2 ISAKMP (0): Creating IPSec SAs inbound SA from 172.18.124.99 to 172.18.124.157 (proxy 192.168.1.1 to 10.1.1.0) has spi 4004415792 and conn_id 1 and flags 4 outbound SA from 172.18.124.157 to 172.18.124.99 (proxy 10.1.1.0 to 192.168.1.1) has spi 1281287211 and conn_id 2 and flags 4 IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99, dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0xeeae8930(4004415792), conn_id= 1, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99, src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x4c5ee42b(1281287211), conn_id= 2, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR02101: decaps: rec'd IPSEC packet has invalid spi for destaddr=172.18.124.157, prot=esp, spi=0xeeae8930(0) 602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xeeae8930(4004415792), sa_trans= esp-des esp-md5-hmac, sa_conn_id= 1 602301: sa

created, (sa) sa_dest= 172.18.124.99, sa_prot= 50, sa_spi= 0x4c5ee42b(1281287211), sa_trans= esp-des esp-md5-hmac, sa_conn_id= 2 109011: Authen Session Start: user 'pixb', sid 5 109015: Authorization denied (acl=115) for user 'pixb' from 192.168.1.1/0 to 10.1.1.40/8 on interface outside 109015: Authorization denied (acl=115) for user 'pixb' from 192.168.1.1/0 to 10.1.1.40/8 on interface outside 109015: Authorization denied (acl=115) for user 'pixb' from 192.168.1.1/0 to 10.1.1.40/8 on interface outside 109015: Authorization denied (acl=115) for user 'pixb' from 192.168.1.1/0 to 10.1.1.40/8 on interface outside goss-pixb# goss-pixb#**show uauth** Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 ipsec user 'pixb' at 192.168.1.1, authenticated access-list 115 goss-pixb#**show access-list** access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=18) access-list 125 permit ip host 10.1.1.41 any (hitcnt=0) access-list dynacl4 permit ip 10.1.1.0 255.255.255.0 host 192.168.1.1 (hitcnt=0) access-list 115 permit ip any host 10.1.1.41 (hitcnt=0) access-list 115 deny ip any host 10.1.1.42 (hitcnt=0)

Debug et exposition - Xauth avec des groupes VPN

crypto_isakmp_process_block: src 172.18.124.96,
dest 172.18.124.157
goss-pixb#**show debug** debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get Off put Off verify Off switch Off fail Off fmsg Off goss-pixb# crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_AG exchange ISAKMP (0): processing SA payload. message ID = 0 ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy ISAKMP: encryption DES-CBC ISAKMP: hash MD5 ISAKMP: default group 1 ISAKMP: auth pre-share ISAKMP (0): atts are acceptable. Next payload is 3 ISAKMP (0): processing KE payload. message ID = 0 ISAKMP (0): processing NONCE payload. message ID = 0 ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing vendor id payload ISAKMP (0): speaking to a VPN3000 client ISAKMP (0): ID payload next-payload : 10 type : 1 protocol : 17 port : 500 length : 8 ISAKMP (0): Total payload length: 12 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_AG exchange ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0): SA has been authenticated return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange ISAKMP (0:0): Need XAUTH ISAKMP/xauth: request attribute XAUTH_TYPE ISAKMP/xauth: request attribute XAUTH_USER_NAME ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD ISAKMP (0:0): initiating peer config to 172.18.124.99. ID = 1396280702 (0x53398d7e) return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 172.18.124.99. message ID = 2156608344 ISAKMP: Config payload CFG_REPLY return status is IKMP_ERR_NO_RETRANS10 ISAKMP (0:0): initiating peer config to 172.18.124.99. ID = 1396280702 (0x53398d7e)9 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 172.18.124.99. message ID = 2156115984 ISAKMP: Config payload CFG_ACK ISAKMP (0:0): peer accepted the address! ISAKMP (0:0): processing saved QM. oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 1697984837 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99, dest_proxy= 172.18.124.157/255.255.255.255/0/0 (type=1), src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 1697984837 ISAKMP (0): processing ID payload. message ID = 1697984837 ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0 ISAKMP (0): processing ID payload. message ID = 1697984837 ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.157 prot 0 port 0 ISAKMP (0): processing NOTIFY payload 24578 protocol 1 spi 0, message ID = 1697984837 ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got a queue event... IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP IPSEC(key_engine_delete_sas): delete all SAs shared with 172.18.124.99 IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0x6a9d3f79(1788690297) for SA from 172.18.124.99 to 172.18.124.157 for prot 3 return status is IKMP_NO_ERROR0 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1 map_alloc_entry: allocating entry 2 ISAKMP (0): Creating IPSec SAs inbound SA from 172.18.124.99 to 172.18.124.157 (proxy 192.168.1.1 to 172.18.124.157) has spi 1788690297 and conn_id 1 and flags 4 outbound SA from 172.18.124.157 to 172.18.124.99 (proxy 172.18.124.157 to 192.168.1.1) has spi 2854452814 and conn_id 2 and flags 4 IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest=

172.18.124.157, src= 172.18.124.99, dest_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1), src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x6a9d3f79(1788690297), conn_id= 1, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99, src_proxy= 172.18.124.157/0.0.0.0/0/0 (type=1), dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0xaa237e4e(2854452814), conn_id= 2, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR05: Authentication succeeded for user 'pixc' from 172.18.124.99/0 to 0.0.0.0/0 on interface IKE-XAUTH 602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0x6a9d3f79(1788690297), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 1 602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50, sa_spi= 0xaa237e4e(2854452814), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2 109011: Authen Session Start: user 'pixc', sid 19 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing SA payload. message ID = 3361949217 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1, ESP_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5 ISAKMP: encaps is 1 ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99, dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.1.1/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0): processing NONCE payload. message ID = 3361949217 ISAKMP (0): processing ID payload. message ID = 3361949217 ISAKMP (0): ID_IPV4_ADDR src 192.168.1.1 prot 0 port 0 ISAKMP (0): processing ID payload. message ID = 3361949217 ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.1.1.0/255.255.255.0 prot 0 port 0 IPSEC(key_engine): got a queue event... IPSEC(spi_response): getting spi 0xfec4c3aa(4274308010) for SA from 172.18.124.99 to 172.18.124.157 for prot 3 return status is IKMP_NO_ERROR4 crypto_isakmp_process_block: src 172.18.124.99, dest 172.18.124.157 OAK_QM exchange oakley_process_quick_mode: OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 4 map_alloc_entry: allocating entry 3 ISAKMP (0): Creating IPSec SAs inbound SA from 172.18.124.99 to 172.18.124.157 (proxy 192.168.1.1 to 10.1.1.0) has spi 4274308010 and conn_id 4 and flags 4 outbound SA from 172.18.124.157 to 172.18.124.99 (proxy 10.1.1.0 to 192.168.1.1) has spi 798459812 and conn_id 3 and flags 4 IPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.99, dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0xfec4c3aa(4274308010), conn_id= 4, keysize= 0, flags= 0x4 IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.157, dest= 172.18.124.99, src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 192.168.1.1/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x2f9787a4(798459812), conn_id= 3, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR02101: decaps: rec'd IPSEC packet has invalid spi for destaddr=172.18.124.157, prot=esp, spi=0xfec4c3aa(0) 602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xfec4c3aa(4274308010), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 4 602301: sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50, sa_spi= 0x2f9787a4(798459812), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3 goss-pixb#**show uauth** Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 ipsec user 'pixc' at 192.168.1.1, authenticated goss-pixb#**show crypto ipsec sa** interface: outside Crypto map tag: mymap, local addr. 172.18.124.157 local ident (addr/mask/prot/port): (172.18.124.157/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 172.18.124.99 dynamic allocated peer ip: 192.168.1.1 PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.157, remote crypto endpt.: 172.18.124.99 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: aa237e4e inbound esp sas: spi: 0x6a9d3f79(1788690297) transform: esp-des esp-md5-hmac , <--- More ---> in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4608000/28519) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xaa237e4e(2854452814) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4608000/28510) IV size: 8 bytes replay detection support: Y outbound ah sas: <--- More ---> outbound pcp sas: local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 172.18.124.99 dynamic allocated peer ip: 192.168.1.1 PERMIT, flags={} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.157, remote crypto endpt.:172.18.124.99 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 2f9787a4 inbound esp sas: spi:

```
0xfec4c3aa(4274308010) <--- More ---> transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 4, crypto map: mymap sa timing: remaining key lifetime (k/sec):
(4607999/27820) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0x2f9787a4(798459812) transform: esp-des esp-md5-hmac , in use settings
={Tunnel, } slot: 0, conn id: 3, crypto map: mymap sa timing: remaining key lifetime (k/sec):
(4607999/27820) IV size: 8 bytes replay detection support: Y <--- More ---> outbound ah sas:
outbound pcp sas:
```

Debug et exposition - Xauth avec le Par-utilisateur ACLs téléchargeable

```
crypto_isakmp_process_block: src 10.66.79.229,
dest 10.66.79.69
VPN Peer: ISAKMP: Added new peer: ip:10.66.79.229
Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:10.66.79.229 Ref cnt incremented to:1
Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 20 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 20 policy
ISAKMP: encryption DES-CBC
```

```
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP (0): ID payload
next-payload : 10
type : 2
protocol : 17
port : 500
length : 10
ISAKMP (0): Total payload length: 14
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
spi 0, message ID = 0RADIUS_GET_PASS
RADIUS_REQUEST
raidus.c: rad_mkpkt_authen
attribute:
type 1, length 10, content:
80917fb0: 74 65 73 74 75 73 65 72 | testuser
attribute:
type 4, length 6, content:
80917fb0: 0a 42 | .B
80917fc0: 4f 45 | OE
attribute:
type 5, length 6, content:
80917fd0: 00 00 00 01 | ....

ISAKMP (0): processing notify INITIAL_CONTACTrip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
session_id 0x5d5ba513
request_id 0x2
user 'testuser'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 8, length 6, content:
```

```
809186f0: ff ff | ..
80918700: ff ff | ..
RADIUS_RCVD
attribute:
type 26, length 67, content:
Vendor ID 0 0 0 9, type=1, len=61:
80918700: 41 43 53 3a 43 69 | ACS:Ci
80918710: 73 63 6f 53 65 63 75 72 65 2d 44 65 66 69 6e 65
| scoSecure-Define
80918720: 64 2d 41 43 4c 3d 23 41 43 53 41 43 4c 23 2d 50
| d-ACL=#ACSACL#-P
80918730: 49 58 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33
| IX-VPNClient-3d3
80918740: 32 37 38 31 35 | 27815
RADIUS_RCVD
RADIUS_REQUEST
raidus.c: rad_mkpkt_authen
attribute:
type 1, length 33, content:
809186d0: 23 41 43 53 41 43 4c 23 2d 50 49 58 | #ACSACL#-PIX
809186e0: 2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33 32 37
| -VPNClient-3d327
809186f0: 38 31 35 | 815
attribute:
type 4, length 6, content:
809186f0: 0a 42 4f 45 | .BOE
attribute:
type 5, length 6, content:
80918700: 00 00 00 | ...
80918710: 02 | .
IPSEC(key_engine): got a queue event...rip 0x80791f00
: chall_state ''
: state 0x7
: timer 0x0
: info 0x5d5ba513
session_id 0x5d5ba513
request_id 0x3
user '#ACSACL#-PIX-VPNClient-3d327815'
app 0
reason 2
sip 10.66.79.244
type 1
rad_procpkt: ACCEPT
attribute:
type 26, length 46, content:
Vendor ID 0 0 0 9, type=1, len=40:
80918e20: 69 70 3a 69 6e 61 63 6c 23 31 3d 70 | ip:inacl#1=p
80918e30: 65 72 6d 69 74 20 69 70 20 61 6e 79 20 68 6f 73
| ermit ip any hos
80918e40: 74 20 31 30 2e 31 2e 31 2e 32 | t 10.1.1.2
RADIUS_RCVD
RADIUS_RCVD
RADIUS_ACCESS_ACCEPT:normal termination
RADIUS_DELETE

IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 10.66.79.229

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP (0): sending phase 1 RESPONDER_LIFETIME notify
ISAKMP (0): sending NOTIFY message 24576 protocol 1
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
```

```
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 3250273953 (0xc1bb3ea1)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
 message ID = 2167001532
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 10.66.79.229.
ID = 1530000247 (0x5b31f377)
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.66.79.229.
message ID = 2167001532
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute IP4_ADDRESS (1)
ISAKMP: attribute IP4_NETMASK (2)
ISAKMP: attribute IP4_DNS (3)
ISAKMP: attribute IP4_NBNS (4)
ISAKMP: attribute ADDRESS_EXPIRY (5)
Unsupported Attr: 5
ISAKMP: attribute APPLICATION_VERSION (7)
Unsupported Attr: 7
ISAKMP: attribute UNKNOWN (28672)
Unsupported Attr: 28672
ISAKMP: attribute UNKNOWN (28673)
Unsupported Attr: 28673
ISAKMP: attribute ALT_DEF_DOMAIN (28674)
ISAKMP: attribute ALT_SPLIT_INCLUDE (28676)
ISAKMP: attribute ALT_PFS (28679)
ISAKMP: attribute UNKNOWN (28680)
Unsupported Attr: 28680
ISAKMP: attribute UNKNOWN (28677)
Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 10.66.79.229.
ID = 2397668523
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2858414843

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
```

```
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal
(prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (2)
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b IPSEC
(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2)
not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
crypto_isakmp_process_block: src 10.66.79.229, dest 10.66.79.69
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#
sv2-4(config)#show uauth Current Most Seen Authenticated Users 1 1 Authen In Progress 0 1 ipsec
user 'testuser' at 192.168.1.1, authenticated access-list #ACSACL#-PIX-VPNClient-3d327815 sv2-
```

```
4(config)#show access-list access-list 108; 1 elements access-list 108 permit ip 10.1.1.0
255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=38) access-list #ACSACL#-PIX-VPNClient-3d327815;
1 elements access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any host 10.1.1.2 (hitcnt=15)
access-list dynacl4; 1 elements access-list dynacl4 permit ip host 10.66.79.69 host 192.168.1.1
(hitcnt=0) access-list dynacl5; 1 elements access-list dynacl5 permit ip any host 192.168.1.1
(hitcnt=15) sv2-4(config)#show access-list access-list 108; 1 elements access-list 108 permit ip
10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 (hitcnt=42) access-list #ACSACL#-PIX-VPNClient-
3d327815; 1 elements access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any host 10.1.1.2
(hitcnt=17) access-list dynacl4; 1 elements access-list dynacl4 permit ip host 10.66.79.69 host
192.168.1.1 (hitcnt=0) access-list dynacl5; 1 elements access-list dynacl5 permit ip any host
192.168.1.1 (hitcnt=17) sv2-4(config)#show crypto map Crypto Map: "mymap" interfaces: { outside
} client configuration address respond client authentication AuthInbound Crypto Map "mymap" 10
ipsec-isakmp Dynamic map template tag: dynmap Crypto Map "mymap" 20 ipsec-isakmp Peer =
10.66.79.229 access-list dynacl6; 1 elements access-list dynacl6 permit ip host 10.66.79.69 host
192.168.1.1 (hitcnt=0) dynamic (created from dynamic map dynmap/10) Current peer: 10.66.79.229
Security association lifetime: 4608000 kilobytes/28800 seconds PFS (Y/N): N Transform sets={
myset, } Crypto Map "mymap" 30 ipsec-isakmp Peer = 10.66.79.229 access-list dynacl7; 1 elements
access-list dynacl7 permit ip any host 192.168.1.1 (hitcnt=0) dynamic (created from dynamic map
dynmap/10) Current peer: 10.66.79.229 Security association lifetime: 4608000 kilobytes/28800
seconds PFS (Y/N): N Transform sets={ myset, } sv2-4(config)
```

Informations connexes

- Page de support PIX
- Références des commandes du pare-feu PIX
- Demandes de commentaires (RFC)
- Cisco Secure ACS pour la page de support UNIX
- Cisco Secure ACS pour la page d'assistance de Windows
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Page d'assistance RADIUS
- Support et documentation techniques - Cisco Systems