Cómo agregar la Autenticación AAA (Xauth) a PIX IPSec 5.2 y posteriores.

Contenido

Introducción

La autenticación y contabilización, y hasta cierto punto la autorización, de RADIUS y TACACS+ se hace para los túneles de Cisco Secure VPN Client 1.1 y Cisco VPN 3000 2.5 Hardware Client que terminan en el PIX. Cambia en el Autenticación ampliada (Xauth) PIX 5.2 y posterior sobre el de las versiones anteriores que incluyen el soporte de lista de acceso del Authentication, Authorization, and Accounting (AAA) para controlar qué usuarios autenticados pueden acceder y soportar para la terminación Xauth del Cliente Cisco VPN 3000 2.5. **El comando vpn group split-tunneling** permite al VPN 3000 Client para conectar con la red dentro del PIX así como de otras redes (por ejemplo, Internet) al mismo tiempo. En PIX 5.3 y posterior, el cambio AAA sobre las versiones de código anterior es que los puertos RADIUS son configurables. En PIX 6.0, el soporte para el cliente VPN 3.x se agrega. Esto requiere el grupo Diffie-Hellman 2.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software PIX versión 5.2.1
- Secure VPN Client 1.1 de Cisco
- VPN 3000 2.5 Client o VPN Client 3.x de Cisco**Nota:** La versión de Cliente Cisco VPN 3.0.x no funciona con las versiones de PIX anterior de 6.0. Refiera al Cisco Hardware y a los clientes VPN que soportan IPsec/PPTP/L2TP para más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

La versión de Software PIX Firewall 6.2 soporta la descarga del Listas de control de acceso (ACL) al firewall PIX de un Access Control Server (ACS). Esto permite a la configuración por usuario de los ACL en un servidor de AAA para proporcionar por usuario la autorización de ACL. Es entonces transferible con el ACS al firewall PIX. Esta característica se soporta para los servidores de RADIUS solamente. No se soporta para los servidores TACACS+.

Pasos del debug

Complete estos pasos del debug:

1. Aseegurese los trabajos de la configuración del Xauth PIX antes de que usted agregue la autenticación AAA.Si usted no puede pasar el tráfico antes de que usted implemente el AAA, usted no puede hacerlo luego.
2. Habilite algún tipo de registro en el PIX:No publique el **comando logging console debugging** en un sistema muy cargado.**El comando logging buffered debugging** puede ser publicado. Entonces publique el **comando show logging**.El registro puede también ser enviado a un servidor del registro de mensajes del sistema (Syslog) y ser examinado.
3. Activar la depuración en los servidores TACACS+ o RADIUS. Todos los servidores tienen esta opción.

Comandos debug en PIX

- **debug crypto ipsec sa** — Este comando debug visualiza los eventos del IPSec.
- **debug crypto isakmp sa** — Este comando debug visualiza los mensajes sobre los eventos del Internet Key Exchange (IKE).
- **debug crypto isakmp engine** — Este comando debug visualiza los mensajes sobre los eventos IKE.

Depuración del lado del cliente

Permita al Log Viewer para ver que los client-side debug en Cisco aseguran 1.1 o el VPN 3000 Client 2.5.

Perfiles de servidor AAA

Cisco UNIX seguro 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 for Windows TACACS+

El noacl, la necesidad de usuarios 3000full, y 3000partial solamente un nombre de usuario y una contraseña en el Cisco Secure ACS for Windows. Las necesidades de usuario del pixb un nombre de usuario, una contraseña, un shell/adentro grupo marcado ejecutivo, un ACL marcaron, y 115 en el cuadro.

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 for Windows RADIUS

El tipo de dispositivo es RADIUS/Cisco El noacl, la necesidad de usuarios 3000full, y 3000partial solamente un nombre de usuario y una contraseña en el Cisco Secure ACS for Windows. Las necesidades de usuario del pixb un nombre de usuario, una contraseña, y un control y acl=115 en cuadro rectangular de Cisco/RADIUS donde dice el Par AV 009\001 (específico del vendedor).

Nota: Usted necesita el Atributo del vendedor para el ACL. El atributo 11, filtro-identificación, es inválido. Este problema se asigna el Id. de bug Cisco CSCdt50422 (clientes registrados solamente). Se repara en el software PIX versión 6.0.1.

Merit RADIUS (Soporte de pares AV de Cisco)

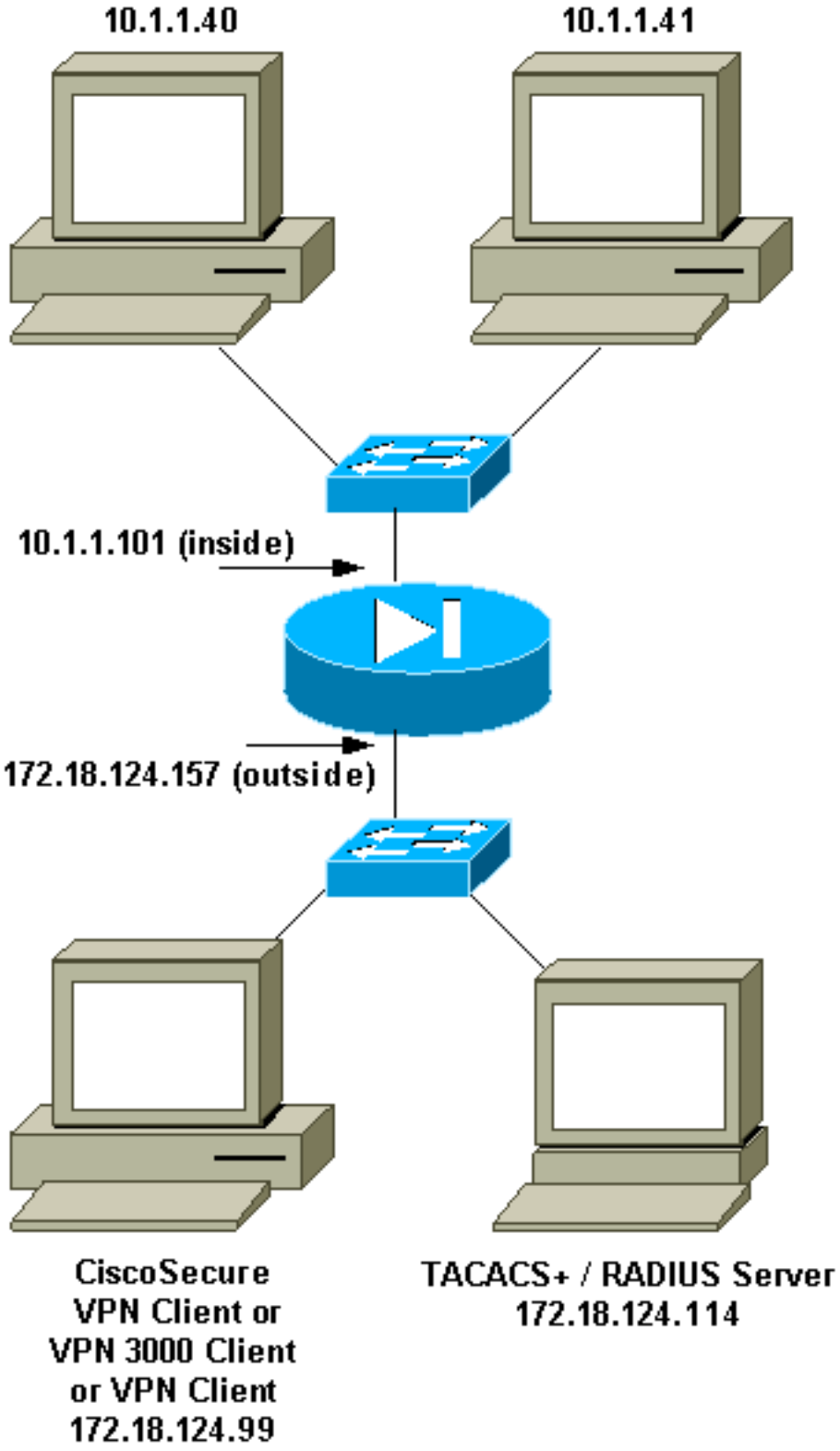
```
noacl Password= "noacl"

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

3000full Password= "3000full"

3000partial Password= "3000partial"
```

Diagrama de la red



Puertos RADIUS configurables (5.3 y posteriores)

Algunos servidores RADIUS utilizan puertos RADIUS diferentes a 1645/1646 (generalmente 1812/1813). En PIX 5.3 y posterior, la autenticación de RADIUS y los puertos de contabilidad se pueden cambiar a los puertos con excepción del 1645/1646 predeterminado con estos comandos:

- aaa-server radius-authport
- aaa-server radius-acctport #

Cómo autenticar con el Xauth sin los grupos VPN

En este ejemplo, autentican a los tres clientes VPN con el Xauth. Sin embargo, los clientes VPN pueden acceder solamente la red dentro del PIX, pues el Túnel dividido es parado. Vea cómo autenticar el Xauth con grupo de VPN para más información sobre el Túnel dividido. Los ACL pasajeros abajo del servidor de AAA se aplican a cualquier cliente VPN. En este ejemplo, la meta está para que el noacl del usuario conecte y consiga a todos los recursos dentro del PIX. El usuario que el pixb conecta, pero porque el ACL 115 se pasa abajo del servidor de AAA durante el proceso del Xauth, el usuario puede conseguir solamente a 10.1.1.40. El acceso a 10.1.1.41 y al resto de interior de los IP Addresses se niega.

Nota: Se requiere el software PIX versión 6.0 para apoyo de VPN Client 3.0.

Cliente Cisco Secure VPN 1.1 puesto - Xauth sin los grupos 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
```

Abra una ventana de la negación de servicio (DOS) y publique el **comando ping - t - - - -**. Cuando aparece la ventana xauth, teclee el nombre de usuario y contraseña que está de acuerdo con el que está con el servidor de AAA.

VPN 3000 Client 2.5 o cliente VPN 3.x puesto - Xauth sin los grupos VPN

Complete estos pasos:

1. Seleccione el **Option (Opciones) > Properties (Propiedades) > Group Name (Nombre de grupo)**.
2. El nombre del grupo es no hace _care y la contraseña está de acuerdo con la que está con el PIX en el **comando isakmp key**. El nombre de la computadora principal es 172.18.124.157.
3. Haga clic en Connect (Conectar)
4. Cuando sube la ventana xauth, teclee el nombre de usuario y contraseña que está de acuerdo con el que está con el servidor de AAA.

Xauth sin los grupos VPN - Configuración 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]
```

Cómo autenticar con el Xauth con grupo de VPN

En este ejemplo, el 3.0 del VPN 3000 Client 2.5 o del cliente VPN se puede autenticar con el Xauth, y el Túnel dividido está en efecto. En virtud de la calidad de miembro de grupo VPN, un ACL se pasa del PIX al VPN 3000 Client. Especifica que solamente la red dentro del PIX tiene un túnel encriptado. El otro tráfico (quizás a Internet) no se cifra.

En este ejemplo, un cliente VPN, con el nombre de usuario 3000full (en el servidor de AAA), en el grupo vpn3000-all (en el PIX) accede la red entera 10.1.1.X dentro del PIX al mismo tiempo que Internet. El cliente VPN recibe el triunfo-servidor, el dns-servidor, y la información sobre el nombre del dominio. El otro cliente VPN, con el nombre de usuario 3000partial (en el AAA-servidor), en el grupo vpn3000-41 (en el PIX) accede solamente una dirección IP dentro de la red (10.1.1.40) en virtud del perfil del grupo. Este cliente VPN no recibe la información de los triunfos y del dns-servidor, sino todavía hace el Túnel dividido.

Nota: Se requiere el software PIX versión 6.0 para apoyo de VPN Client 3.0.

Cliente VPN 2.5 o 3.0 puesto - Xauth con grupo de VPN

Complete estos pasos:

Nota: El VPN 2.5 o la configuración del cliente del 3.0 depende del usuario implicado.

1. Seleccione Opciones > Propiedades > Autenticación.
2. El nombre del grupo y el group password hacen juego el nombre del grupo en el PIX como en: ******** de la contraseña del vpngroup vpn3000-all o ******** de la contraseña del vpngroup vpn3000-41. El nombre de la computadora principal es 172.18.124.157.
3. Haga clic en Connect (Conectar)
4. Cuando aparezca la ventana Xauth, ingrese el nombre de usuario y la contraseña que correspondan con los valores que figuran en el servidor de AAA.

En este ejemplo, una vez que autentican al usuario 3000full, coge la información del grupo vpn3000-all. El usuario 3000partial coge la información del grupo vpn3000-41. La ventana muestra que la **negociación de los perfiles de seguridad** y **su link es segura ahora**.

El usuario 3000full utiliza la contraseña para el grupo vpn3000-all. La lista de acceso 108 se asocia a ese grupo para los fines de tunelización dividida. El túnel se forma a la red 10.1.1.x. Flujos de tráfico unencrypted a los dispositivos no en la lista de acceso 108 (por ejemplo, Internet). Éste es Túnel dividido.

Ésta es la salida para la ventana de estado de la conexión de cliente VPN para el usuario 3000full:

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

El usuario 3000partial utiliza la contraseña para el grupo vpn3000-41. La lista de acceso 125 se asocia a ese grupo para los fines de tunelización dividida. El túnel se forma al dispositivo de 10.1.1.41. Flujos de tráfico unencrypted a los dispositivos no en la lista de acceso 125 (por ejemplo, Internet). Sin embargo, el tráfico no fluye al dispositivo de 10.1.1.40 porque este tráfico es unroutable. No se especifica en la lista de túneles de encripción.

Ésta es la salida para la ventana de estado de la conexión de cliente VPN para el usuario 3000partial:

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

Xauth con grupo de VPN - Configuración de PIX

Nota: El Cliente Cisco Secure VPN 1.1 no trabaja con esto porque no hay clave del Internet Security Association and Key Management Protocol (ISAKMP). Agregue el comando de **0.0.0.0 del netmask de 0.0.0.0 del direccionamiento del ******** de la clave del isakmp** de hacer que todos los clientes VPN trabajan.

```
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
```

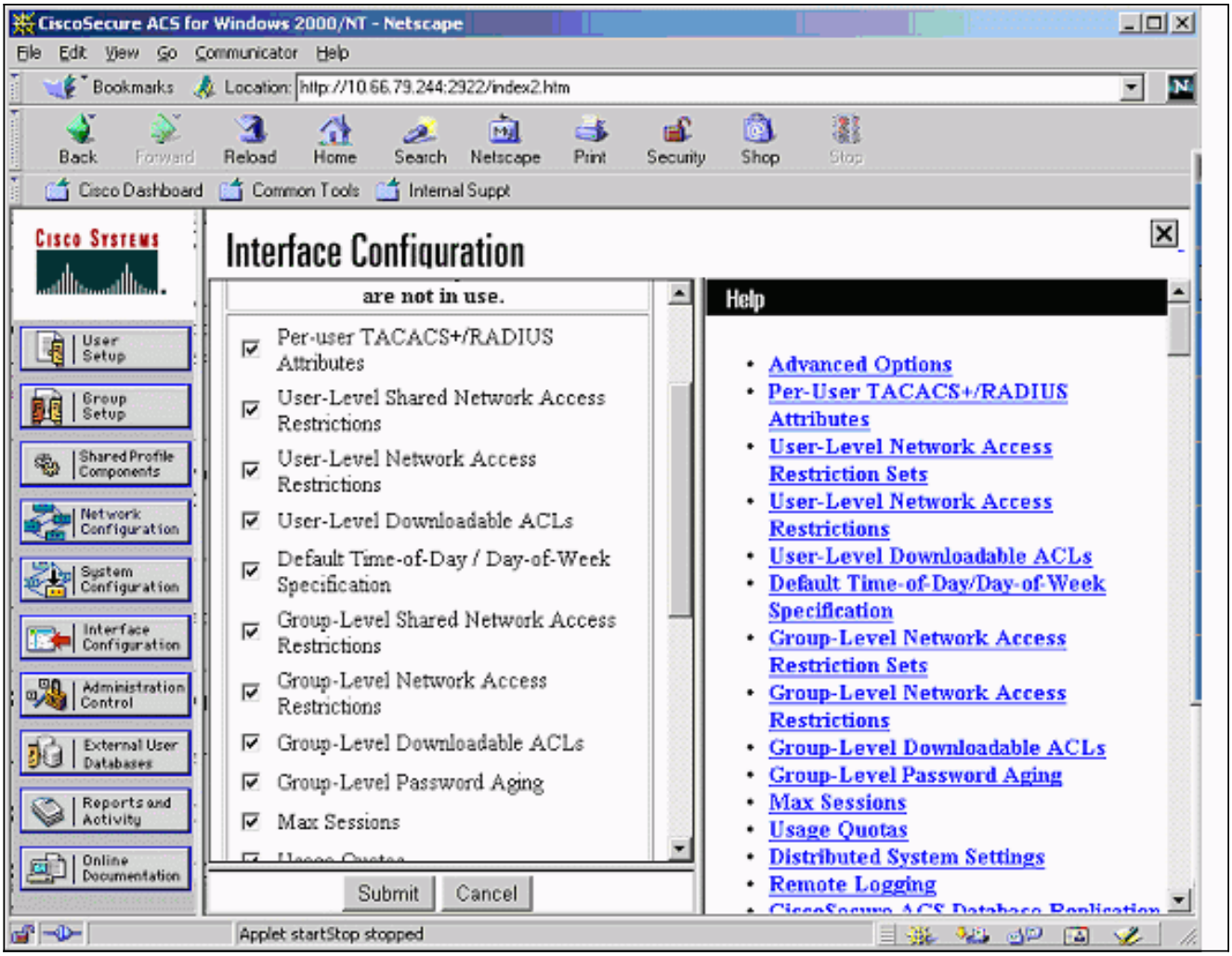
```
access-list 108 permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 access-list 125
permit ip host 10.1.1.41 any pager lines 24 logging on no logging timestamp no logging standby
logging console debugging no logging monitor no logging buffered logging trap debugging no
logging history logging 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 con grupo de VPN y ACL por usuario transferibles - Configuración ACS

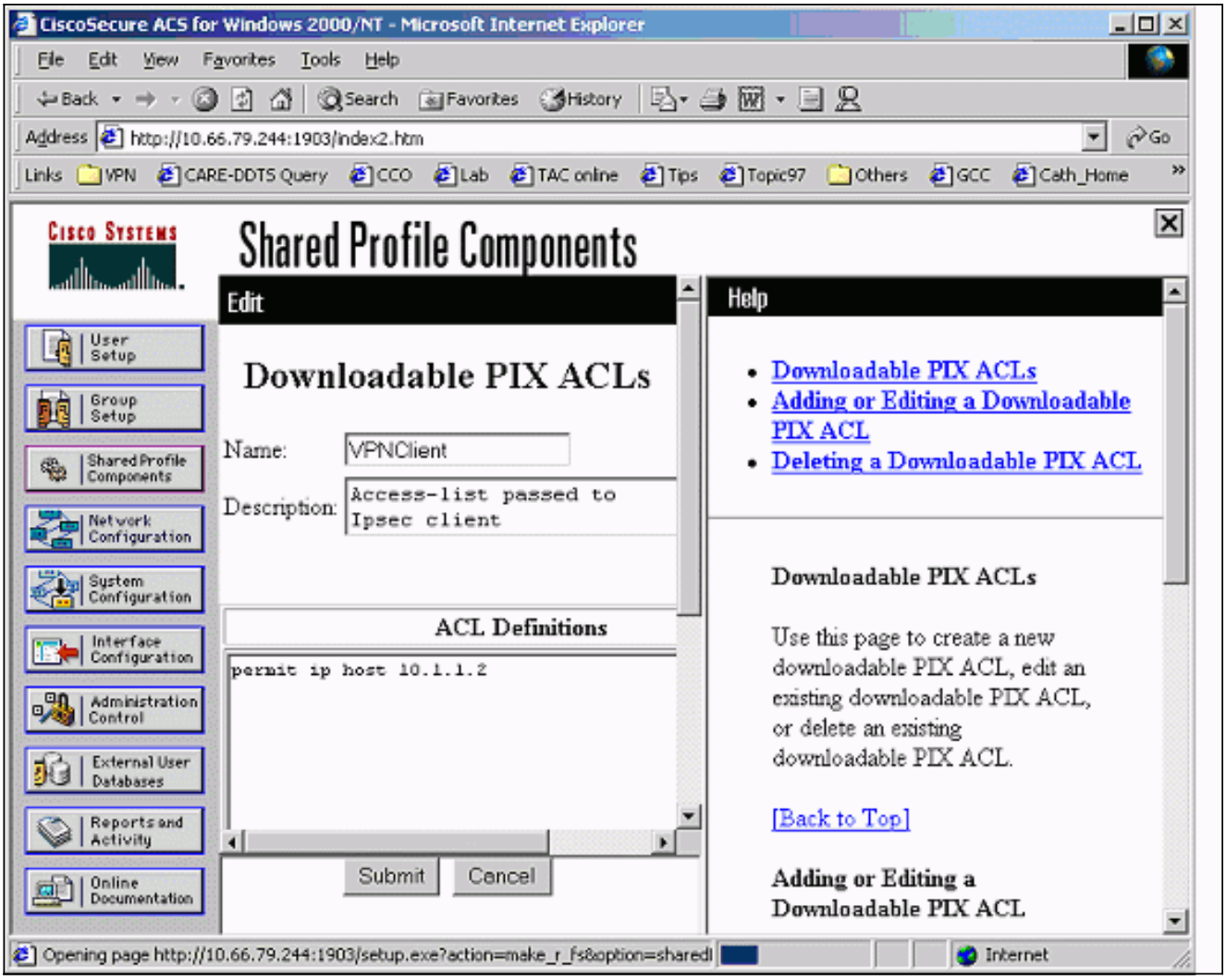
Configure el Cisco Secure ACS

Complete estos pasos:

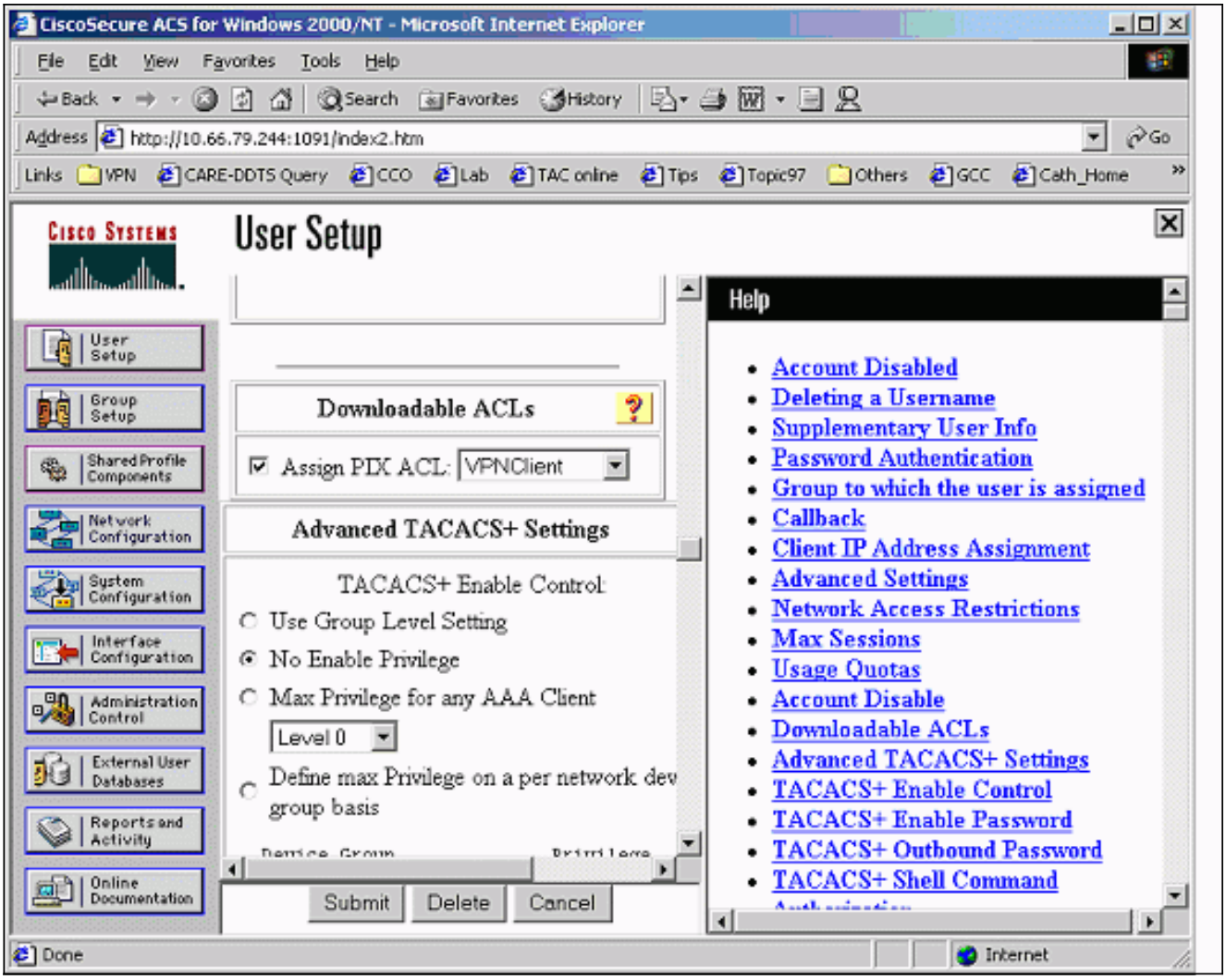
1. Haga clic en Configuración de la interfaz y seleccione la opción para las ACL descargables a nivel del
   usuario.



2. Haga clic en Shared Profile Components (Componentes de perfil compartidos) y defina un ACL que pueda
descargarse.



3. Haga clic en User Setup (Configuración de usuario). Seleccione la opción **para asignar PIX ACL**. Elija el ACL correcto de la lista desplegable.



Xauth con grupo de VPN y ACL por usuario transferibles - Configuración PIX 6.x

Si usted quiere conducir un ACL descargable por usuario del usuario para la autorización, utilice la versión 6.2(2) del Software PIX Firewall. Refiera al Id. de bug Cisco CSCdx47975 (clientes registrados solamente).

```
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 con grupo de VPN y ACL por usuario transferibles - ASA/PIX configuración 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
```

Cómo configurar el Xauth local para la conexión de cliente VPN

Estos comandos se requieren configurar el Xauth local para la conexión de cliente VPN:

- **protocol local de la servidor-***etiqueta del AAA***-servidor**
- ***AAA-servidor-nombre de la* autenticación de cliente del *nombre de asignación de la* correspondencia de criptografía**

Publique el **comando username** de definir a los usuarios locales en el PIX.

Para utilizar la base de datos de autenticación de usuario del escudo de protección de PIX local, ingrese el **LOCAL** para el parámetro de la servidor-*etiqueta* para el **comando aaa-server**. Publican el **comando aaa-server** con el **comando crypto map** de establecer una asociación de autenticación para autenticar los clientes VPN cuando acceden el firewall PIX.

Cómo agregar contabilidad

Éste es el sintaxis del comando de agregar las estadísticas:

- ***acctg_service de las* estadísticas aaa|excepto de entrada|saliente/if_name local_ip local_mask foreign_ip foreign_mask tacacs+|radio**;

o (nuevo en 5.2):

- **las estadísticas aaa incluyen el *acctg_service* entrante|*server_tag* saliente de la coincidencia**

En la configuración PIX, esto es el comando agregado:

- **las estadísticas aaa incluyen cualquier AuthInbound entrante de 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0**;

o (nuevo en 5.2):

- **access-list 150 permit ip any any aaa accounting match 150 outside AuthInbound**

Nota: El comando sysopt connection permit-ipsec, no el sysopt ipsec pl-compatible, es necesario para que la contabilidad Xauth funcione. La cuenta Xauth no funciona sólo con el comando sysopt ipsec pl-compatible. La contabilidad de Xauth es válida para las conexiones TCP. Es inválida para el Internet Control Message Protocol (ICMP) o el User Datagram Protocol (UDP).

Ejemplo de contabilidad de 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
```

Ejemplo de contabilidad 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 and show - Xauth sin grupos 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 y show - Xauth con grupo de 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 y show - Xauth con los ACL por usuario transferibles

```
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)
```

Información Relacionada

- Página de Soporte de PIX
- Referencias de Comando PIX
- Solicitudes de Comentarios (RFC)
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- Página de soporte de RADIUS
- Soporte Técnico y Documentación - Cisco Systems