كيفية إضافة مصادقة AAA (Xauth) إلى PIX IPSec 5.2 والإصدارات الأحدث

المحتويات

المقدمة

يتم إجراء مصادقة ومحاسبة RADIUS و TACACS+، وإلى حد ما، التخويل، ل Cisco Secure VPN Client 1.1 و Cisco VPN 3000 2.5 Hardware Client tunnels التي تنتهي عند PIX. تغييرات في PIX 5.2 والمصادقة الموسعة اللاحقة (Xauth) مقارنة بدعم قائمة الوصول (AAA) للمصادقة والتفويض والمحاسبة (AAA) للتحكم في ما يمكن للمستخدمين المصدق عليهم الوصول إليه ودعمه لعميل Cisco VPN 3000 الإصدار 2.5. يتيح الأمر **vpn group split-tunneling** لعميل VPN 3000 الاتصال بالشبكة داخل PIX بالإضافة إلى الشبكات الأخرى (على سبيل المثال، الإنترنت) في نفس الوقت. في PIX 5.3 والإصدارات الأحدث، يكون تغيير المصادقة والتفويض والمحاسبة (AAA) عبر الإصدارات السابقة من الرمز أن منافذ RADIUS قابلة للتكوين. في PIX 6.0، تتم إضافة دعم عميل VPN 3.x. يتطلب هذا مجموعة Diffie-Hellman رقم 2.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج PIX الإصدار 5.2.1
- Cisco Secure VPN Client 1.1
- عميل Cisco VPN 3000 2.5 أو VPN Client 3.x**ملاحظة:** لا يعمل الإصدار x.3.0 من عميل Cisco VPN مع إصدارات PIX الأقدم من 6.0. راجع أجهزة Cisco وعملاء VPN الذين يدعمون IPsec/PPTP/L2TP للحصول على مزيد من المعلومات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يدعم الإصدار 6.2 من برنامج جدار الحماية ل PIX تنزيل قوائم التحكم في الوصول (ACL) إلى جدار حماية PIX من خادم التحكم في الوصول (ACS). وهذا يمكن تكوين قوائم التحكم في الوصول (ACL) لكل مستخدم على خادم AAA لتوفير تفويض قوائم التحكم في الوصول (ACL) لكل مستخدم. ويمكن بعد ذلك تنزيله من خلال ACS إلى جدار حماية PIX. هذه الميزة مدعومة لخوادم RADIUS فقط. وهو غير مدعوم لخوادم TACACS+.

خطوات التصحيح

أكمل خطوات تصحيح الأخطاء التالية:

1. تأكد من عمل تكوين PIX Xauth قبل إضافة مصادقة AAA.إذا لم تكن قادرا على تمرير حركة المرور قبل تنفيذ المصادقة والتفويض والمحاسبة (AAA)، فلن تكون قادرا على القيام بذلك بعد ذلك.

2. تمكين نوع ما من التسجيل في PIX:لا تقم بإصدار الأمر **logging console debugging** على نظام محمل بشكل ثقيل.يمكن إصدار أمر **تصحيح الأخطاء المخزن مؤقتا للتسجيل**. ثم قم بإصدار الأمر **show logging**.يمكن أيضا إرسال التسجيل إلى خادم سجل رسائل النظام (syslog) وفحصه.
3. قم بتشغيل تصحيح الأخطاء على خوادم TACACS+ أو RADIUS. كافة الخوادم لها هذا الخيار.

أوامر تصحيح الأخطاء على PIX

- **debug crypto ipSec**— يعرض أمر تصحيح الأخطاء هذا أحداث IPsec.
- **debug crypto isakmp sa**— يعرض أمر تصحيح الأخطاء هذا رسائل حول أحداث Internet Key Exchange (IKE).
- **debug crypto isakmp engine**— يعرض أمر تصحيح الأخطاء هذا رسائل حول أحداث IKE.

تصحيح أخطاء جانب العميل

قم بتمكين عارض السجل لعرض تصحيح أخطاء جانب العميل في Cisco Secure 1.1 أو VPN 3000 Client 2.5.

ملفات تعريف خادم AAA

بروتوكول UNIX TACACS+ الآمن من Cisco

```
                    }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
                                    {
                                    {
```

مصدر المحتوى الإضافي الآمن من Cisco ل Windows TACACS+

لا يحتاج المستخدمون غير المتفرغون و 3000 و 3000 الجزئيون إلا إلى اسم مستخدم وكلمة مرور في ACS الآمن من Cisco لنظام Windows. يحتاج مستخدم Pixb اسم مستخدم، كلمة مرور، shell/exec تدقيق في مجموعة، قائمة تحكم بالوصول (ACL)، و 115 في المربع.

Cisco Secure UNIX RADIUS

```
}user = noacl
```

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

مصدر المحتوى الإضافي الآمن من Cisco ل Windows RADIUS

RADIUS/Cisco هو نوع الجهاز. لا يحتاج المستخدمون غير المتفرغون و 3000 و 3000 الجزئيون إلا إلى اسم مستخدم وكلمة مرور في ACS الآمن من Cisco لنظام Windows. يحتاج مستخدم Pixb إلى اسم مستخدم وكلمة مرور وفحص و acl=115 في المربع المستطيل Cisco/RADIUS حيث يقول 009\001 AV-pair (خاص بالمورد).

ملاحظة: تحتاج إلى سمة المورد لقائمة التحكم في الوصول (ACL). السمة 11، معرف عامل التصفية، غير صالحة. عينت هذا إصدار cisco بق CSCdt50422 id (يسجل زبون فقط). تم تثبيته في برنامج PIX، الإصدار 6.0.1.

Merit RADIUS (دعم أزواج Cisco AV)

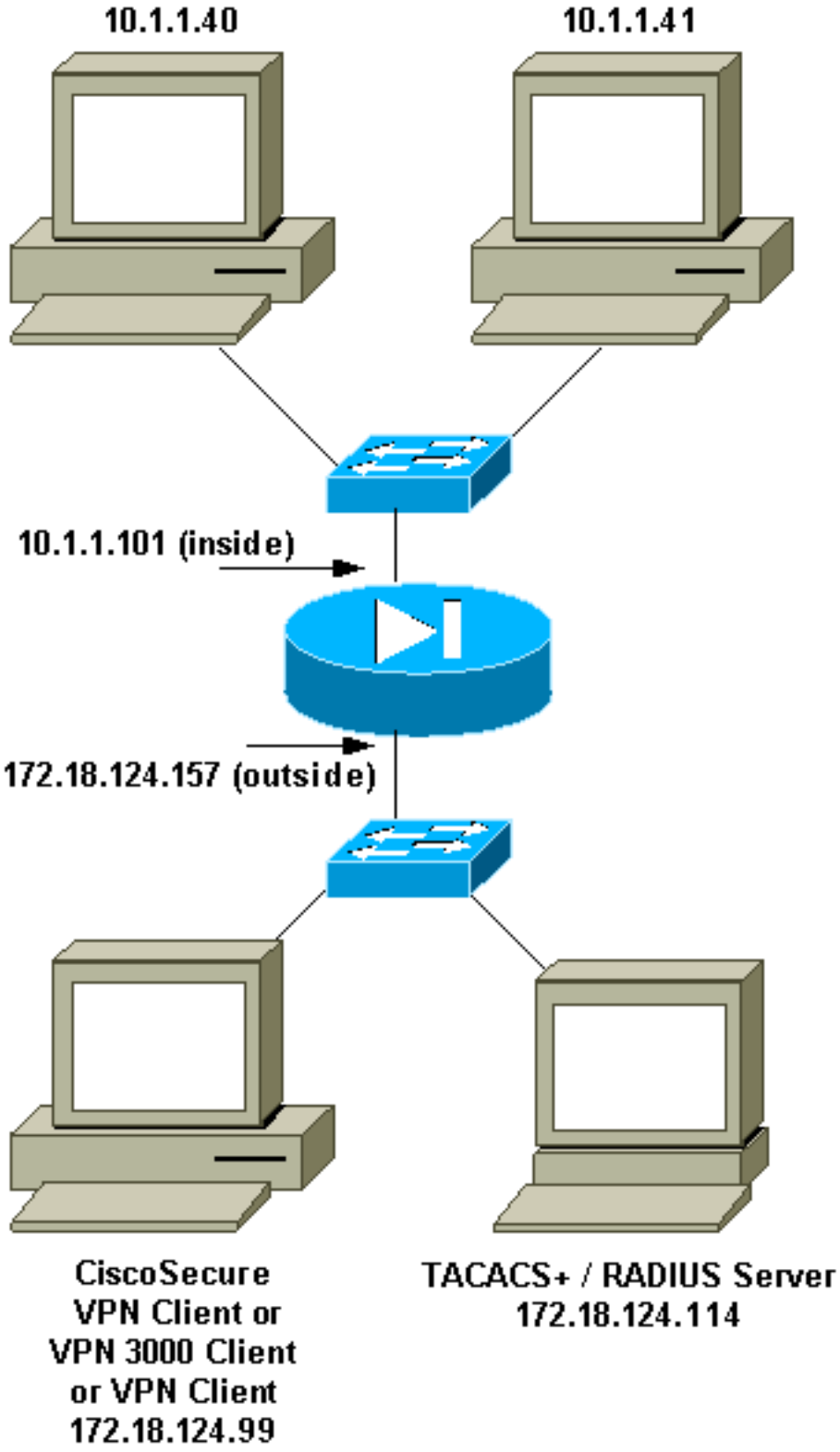
```
"noacl Password= "noacl

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

"3000full Password= "3000full

"3000partial Password= "3000partial
```

الرسم التخطيطي للشبكة



منافذ RADIUS القابلة للتكوين (5.3 ومتأخر)

تستخدم بعض خوادم RADIUS منافذ RADIUS بخلاف 1646/1645 (عادة 1813/1812). في PIX 5.3 والإصدارات الأحدث، يمكن تغيير منافذ مصادقة RADIUS ومحاسبته إلى منافذ أخرى غير المنافذ الافتراضية 1646/1645 باستخدام هذه الأوامر:

- خادم # AAA-radius-authport
- منفذ # AAA-server radius

كيفية المصادقة مع Xauth دون مجموعات VPN

في هذا المثال، تتم مصادقة جميع عملاء VPN الثلاثة باستخدام Xauth. ومع ذلك، يمكن لعملاء شبكة VPN الوصول إلى الشبكة داخل PIX فقط، نظرا لأن تقسيم الاتصال النفقي غير مستخدم. راجع كيفية مصادقة Xauth مع مجموعات VPN للحصول على مزيد من المعلومات حول تقسيم الاتصال النفقي. يتم تطبيق قوائم التحكم في الوصول (ACL) التي تم تمريرها من خادم AAA على أي من عملاء شبكة VPN. في هذا المثال، الهدف هو تمكين المستخدم من الاتصال بجميع الموارد الموجودة داخل PIX والوصول إليها. يتصل المستخدم Pixb، ولكن نظرا لأن قائمة التحكم في الوصول (ACL) رقم 115 تم تمريرها من خادم AAA أثناء عملية Xauth، يمكن للمستخدم الوصول إلى 10.1.1.40 فقط. يتم رفض الوصول إلى 10.1.1.41 وجميع عناوين IP الأخرى داخل.

ملاحظة: يلزم توفر برنامج PIX الإصدار 6.0 لدعم عميل VPN 3.0.

إعداد Xauth - Cisco Secure VPN Client 1.1 بدون مجموعات 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
```

افتح نافذة رفض الخدمة (DoS) وأصدر الأمر **ping -t #.#.#.#**. عندما تظهر نافذة Xauth، اكتب اسم المستخدم وكلمة المرور اللذين يتفقان مع الواحد على خادم AAA.

إعداد VPN 3000 Client 2.5 أو Xauth - VPN Client 3.x بدون مجموعات VPN

أكمل الخطوات التالية:

1. حدد **خيارات > خصائص > مصادقة > اسم المجموعة**.
2. اسم المجموعة هو no_care وكلمة المرور تتفق مع اسم المجموعة على PIX في الأمر **isakmp key**. اسم المضيف هو 172.18.124.157.
3. انقر على **توصيل**.
4. عندما تظهر نافذة Xauth، اكتب اسم المستخدم وكلمة المرور اللذين يتفقان مع الواحد على خادم AAA.

إعداد PIX - VPN بدون مجموعات Xauth

```
(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
255.255.255.0 192.168.1.0
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]
```

كيفية المصادقة مع Xauth مع مجموعات VPN

في هذا المثال، يمكن مصادقة VPN 3000 Client 2.5 أو VPN Client 3.0 مع Xauth، وتكون انقسام-tunneling فعالة. بموجب عضوية مجموعة VPN، يتم تمرير قائمة تحكم في الوصول (ACL) من PIX إلى عميل VPN 3000. وهو يحدد أن الشبكة داخل PIX فقط تحتوي على نفق مشفر. لا يتم تشفير حركة مرور أخرى (ربما إلى الإنترنت).

في هذا المثال، يقوم عميل شبكة VPN واحد، باسم المستخدم full 3000 (على خادم AAA)، في مجموعة VPN3000-all (على PIX) بالوصول إلى شبكة X.10.1.1 بالكامل داخل PIX في نفس وقت وصول الإنترنت. يستقبل عميل VPN معلومات wins-server و dns-server واسم المجال. لا يصل عميل VPN الآخر، باسم المستخدم 3000 جزئي (على خادم AAA)، في مجموعة VPN3000-41 (على PIX) إلا إلى عنوان IP واحد داخل الشبكة (10.1.1.40) بفضل ملف تعريف المجموعة. لا يتلقى عميل شبكة VPN هذا معلومات WINS-و DNS-server، ولكنه لا يزال يقوم بتقسيم الاتصال النفقي.

ملاحظة: يلزم توفر برنامج PIX الإصدار 6.0 لدعم عميل VPN 3.0.

إعداد VPN Client 2.5 أو 3.0 - Xauth مع مجموعات VPN

أكمل الخطوات التالية:

ملاحظة: يعتمد إعداد عميل VPN 2.5 أو 3.0 على المستخدم المعني.

1. حدد **خيارات > خصائص > مصادقة**.
2. يتطابق اسم المجموعة وكلمة مرور المجموعة مع اسم المجموعة على PIX كما هو الحال في: vpnGroup VPN3000-all password ******** أو vpn3000-41 password ********. اسم المضيف هو 172.18.124.157.
3. انقر على **توصيل**.
4. عند ظهور نافذة Xauth، أدخل اسم المستخدم وكلمة المرور اللذين يتفقان مع الواحد على خادم AAA.

في هذا المثال، بمجرد مصادقة المستخدم full 3000، فإنه يلتقط المعلومات من مجموعة VPN3000-all. المستخدم 3000 يلتقط جزءا من المعلومات من مجموعة VPN3000-41. يظهر الإطار **التفاوض على ملفات تعريف الأمان والارتباط آمن الآن**.

يستخدم المستخدم full3000 كلمة المرور للمجموعة VPN3000-all. يتم إقران قائمة الوصول 108 بتلك المجموعة لأغراض تقسيم الاتصال النفقي. يتم تكوين النفق لشبكة x.10.1.1. تتدفق حركة المرور غير مشفرة إلى الأجهزة غير الموجودة في قائمة الوصول 108 (على سبيل المثال، الإنترنت). هذا انقسام-tunneling.

هذا هو مخرج نافذة حالة اتصال عميل VPN للمستخدم full 3000:

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

يستعمل مستعمل 3000 جزئي الكلمة للمجموعة VPN3000-41. يتم إقران قائمة الوصول 125 بتلك المجموعة لأغراض تقسيم الاتصال النفقي. يتم تكوين النفق للجهاز 10.1.1.41. تتدفق حركة المرور غير مشفرة إلى الأجهزة غير الموجودة في قائمة الوصول 125 (على سبيل المثال، الإنترنت). ومع ذلك، لا تتدفق حركة المرور إلى الجهاز 10.1.1.40 لأن حركة المرور هذه غير قابلة للتوجيه. غير محدد في قائمة أنفاق التشفير.

هذا هو مخرج نافذة حالة اتصال عميل VPN للمستخدم 3000 جزئي:

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

Xauth مع مجموعات VPN - إعداد PIX

ملاحظة: لا يعمل عميل VPN الآمن 1.1 من Cisco مع هذا الأمر بسبب عدم وجود مفتاح بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP). قم بإضافة **الأمر isakmp key ******* عنوان 0.0.0.0 0.0.0.0 netmask** لجعل جميع عملاء شبكات VPN يعملون.

```
                                (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
                                255.255.255.0 192.168.1.0
        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
```

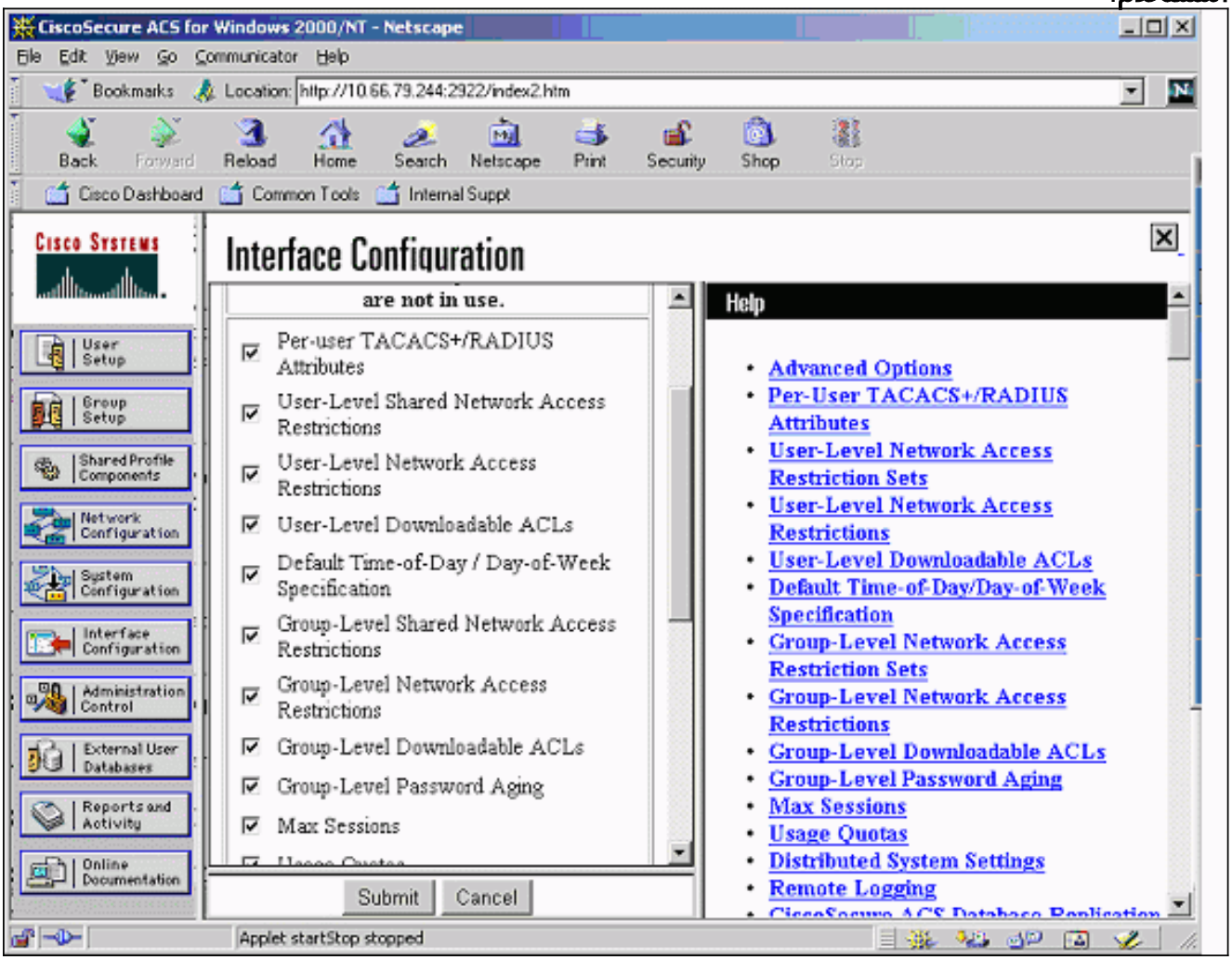
end :

Xauth مع مجموعات VPN وقوائم التحكم في الوصول (ACL) القابلة للتنزيل لكل مستخدم - إعداد ACS

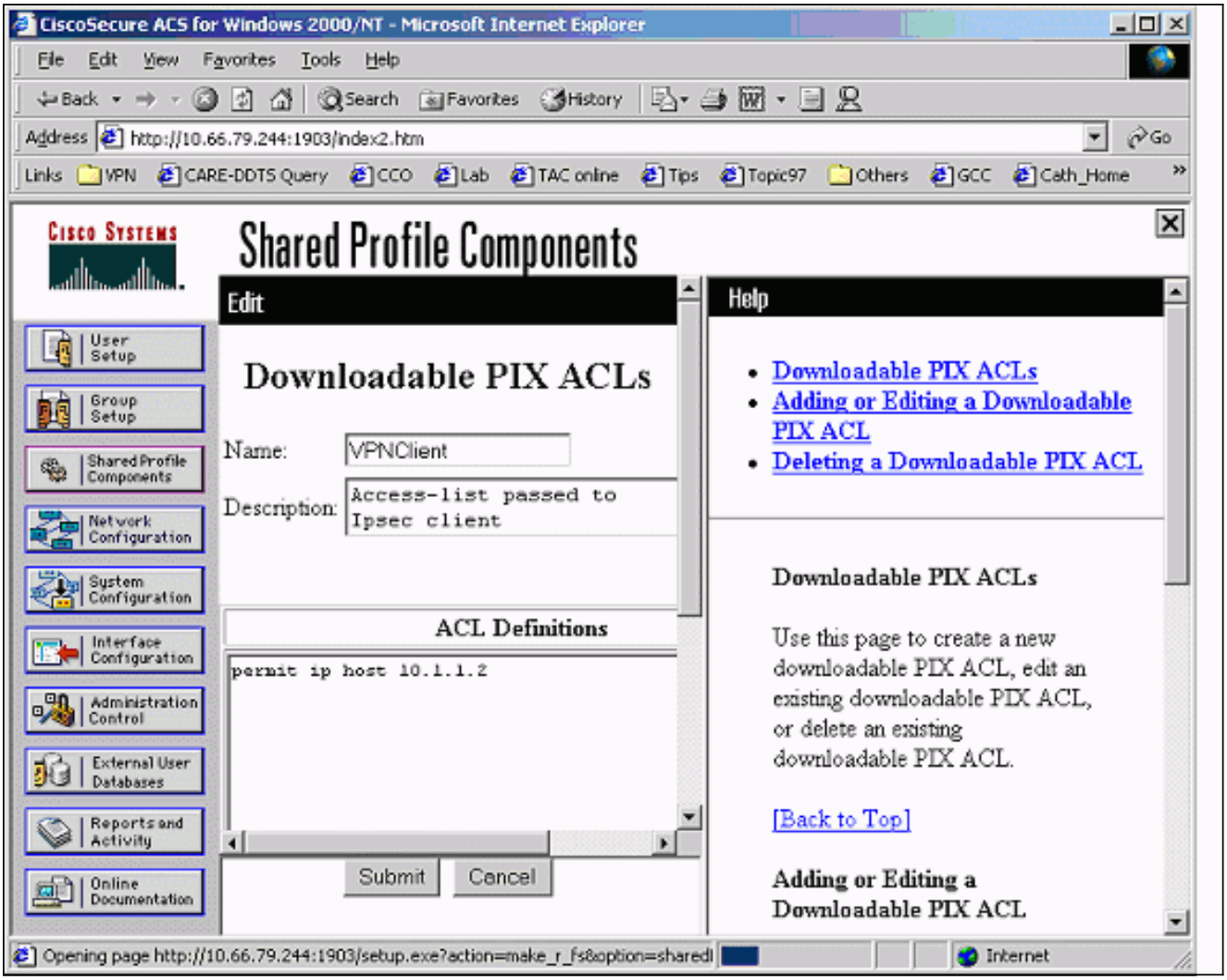
إعداد مصدر المحتوى الإضافي الآمن من Cisco

أكمل الخطوات التالية:

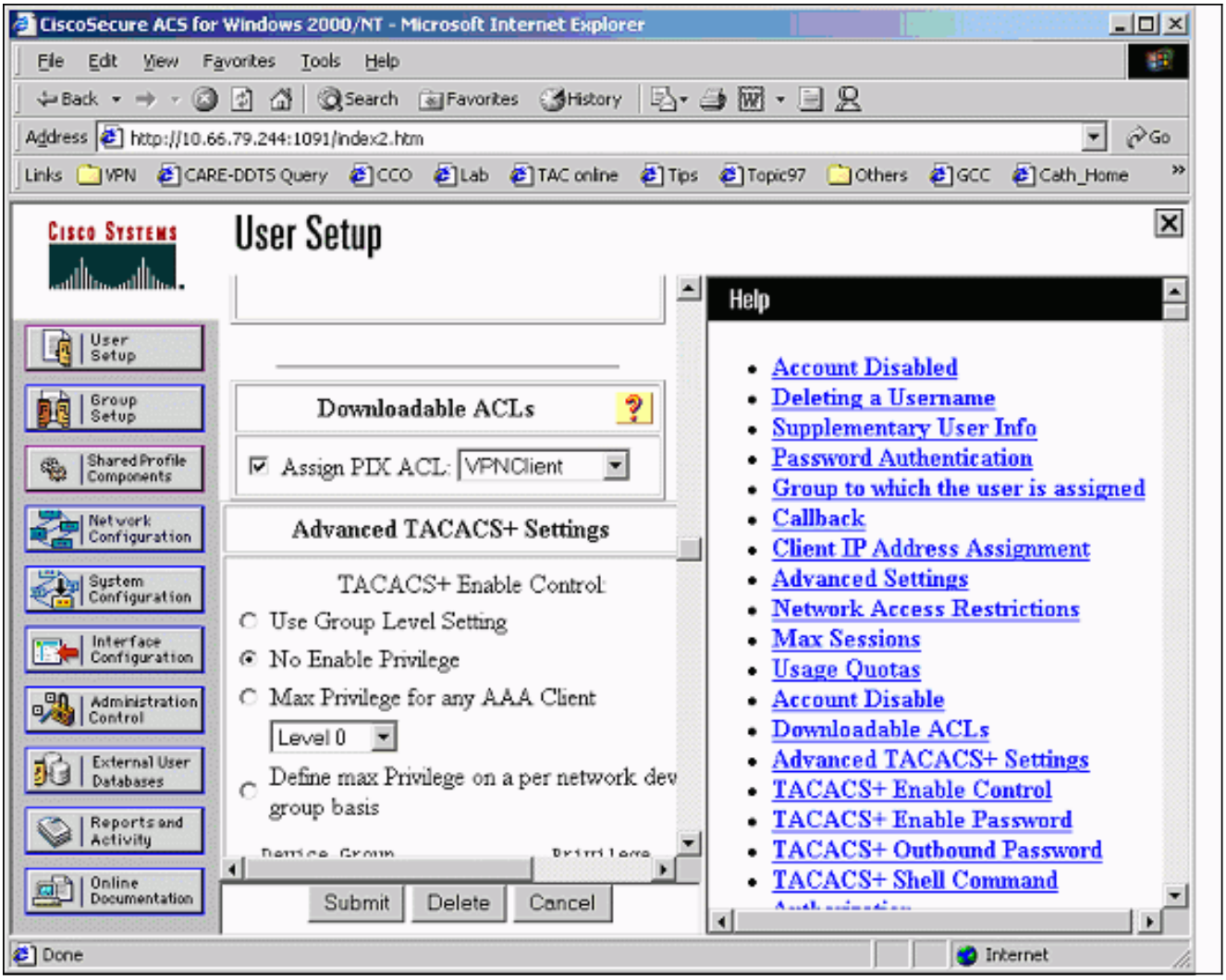
1. انقر فوق **تكوين الواجهة** وحدد الخيار لقوائم التحكم في الوصول (ACL) القابلة للتنزيل **على مستوى المستخدم**.



2. انقر على **مكونات ملف التعريف المشترك** وحدد قائمة تحكم في الوصول (ACL) قابلة للتنزيل.



3. انقر فوق **إعداد المستخدم**. حدد الخيار الخاص **بتعيين قائمة التحكم بالوصول (ACL) الخاصة ب PIX**. أختر قائمة التحكم في الوصول (ACL) الصحيحة من القائمة المنسدلة.



Xauth مع مجموعات VPN وقوائم التحكم في الوصول (ACL) القابلة للتنزيل لكل مستخدم - إعداد PIX 6.x

إذا كنت ترغب في تشغيل قائمة تحكم في الوصول (ACL) قابلة للتنزيل لكل مستخدم للتخويل، فاستخدم الإصدار 6.2(2) من برنامج جدار حماية PIX. أحلت cisco بق CSCdx47975 id (يسجل زبون فقط).

```
(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
255.255.255.0 192.168.1.0
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
sip_media 0:02:00 0:30:00
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 مع مجموعات VPN وقوائم التحكم في الوصول (ACL) القابلة للتنزيل لكل مستخدم - إعداد 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 :
```

كيفية تكوين مصادقة محلية لاتصال عميل VPN

يتطلب هذا أمر أن يشكل Xauth محلي ل VPN زبون توصيل:

- **بروتوكول *server-tag*-AAA للخادم محلي**
- **مصادقة عميل خريطة *التشفير* *aaa-server-name***

قم بإصدار الأمر **username** لتعريف المستخدمين المحليين على PIX.

لاستخدام قاعدة بيانات مصادقة المستخدم لجدار حماية PIX المحلي، أدخل **LOCAL** لمعلمة *server-tag* الخاصة بالأمر **aaa-server**. يتم إصدار الأمر **aaa-server** باستخدام الأمر **crypto map** لإنشاء اقتران مصادقة حتى تتم مصادقة عملاء VPN عند الوصول إلى جدار حماية PIX.

كيفية إضافة المحاسبة

هذه هي الصياغة الخاصة بالأمر لإضافة المحاسبة:

- **محاسبة *acctg_service* AAA|باستثناء الوارد|الصادر *if_name local_ip local_mask foreign_ip*|*foreign_mask* tacacs+|radius**؛

أو (جديد في 5.2):

- **تتضمن محاسبة *acctg_service* AAA الوارد|تطابق الصادر *server_tag***

في تكوين PIX، هذا هو الأمر الذي تمت إضافته:

- **تتضمن محاسبة AAA أي الوارد AuthInbound 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0** ؛

أو (جديد في 5.2):

- **السماح ب Access-list 150 أي تطابق محاسبة AAA خارج AuthInbound**

ملاحظة: يعد الأمر **sysopt connection permit-ipPSec**، وليس الأمر **sysopt ips pl** المتوافق، ضروريا لكي تعمل محاسبة Xauth. لا تعمل محاسبة Xauth مع الأمر **sysopt ipSec** المتوافق مع **pl** فقط. محاسبة Xauth صالحة لاتصالات TCP. غير صالح لبروتوكول رسائل التحكم في الإنترنت (ICMP) أو بروتوكول مخطط بيانات المستخدم (UDP).

مثال محاسبة 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
```

مثال محاسبة 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
```

show و debug - Xauth بدون مجموعات 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
Authentication succeeded for user 'pixb' from 172.18.124.157 :109005
 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
 ,sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50 :602301
,sa_spi= 0xeeae8930(4004415792), sa_trans= esp-des esp-md5-hmac
                                                    sa_conn_id= 1

  ,sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50 :602301
,sa_spi= 0x4c5ee42b(1281287211), sa_trans= esp-des esp-md5-hmac
                                                    sa_conn_id= 2

                      Authen Session Start: user 'pixb', sid 5 :109011
    Authorization denied (acl=115) for user 'pixb' from :109015
                    to 10.1.1.40/8 on interface outside 192.168.1.1/0
    Authorization denied (acl=115) for user 'pixb' from :109015
                    to 10.1.1.40/8 on interface outside 192.168.1.1/0
    Authorization denied (acl=115) for user 'pixb' from :109015
                    to 10.1.1.40/8 on interface outside 192.168.1.1/0
    Authorization denied (acl=115) for user 'pixb' from :109015
                    to 10.1.1.40/8 on interface outside 192.168.1.1/0

                                                      #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
                                        (hitcnt=18) 255.255.255.0
        (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
                                        (hitcnt=0) 192.168.1.1
        (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
```

show و debug - Xauth مع مجموعات 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
           ,sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50 :602301
        , sa_spi= 0x6a9d3f79(1788690297), sa_trans= esp-des esp-md5-hmac
                                                            sa_conn_id= 1

            ,sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50 :602301
        , sa_spi= 0xaa237e4e(2854452814), sa_trans= esp-des esp-md5-hmac
                                                            sa_conn_id= 2

                              Authen Session Start: user 'pixc', sid 19 :109011

     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
                     ,sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50 :602301
                   , sa_spi= 0xfec4c3aa(4274308010), sa_trans= esp-des esp-md5-hmac
                                                                sa_conn_id= 4

                       ,sa created, (sa) sa_dest= 172.18.124.99, sa_prot= 50 :602301
                     , 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
```

تصحيح الأخطاء والعرض - Xauth مع قوائم التحكم في الوصول (ACL) القابلة للتنزيل لكل مستخدم

```
,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
                                                          .. | ff ff :80918700
                                                                   RADIUS_RCVD
                                                                   :attribute
                                              :type 26, length 67, content
                                         :Vendor ID 0 0 0 9, type=1, len=61
                                     3a 43 69 | ACS:Ci 53 43 41 :80918700
   6f 53 65 63 75 72 65 2d 44 65 66 69 6e 65 63 73 :80918710
                                                    scoSecure-Define |
   2d 41 43 4c 3d 23 41 43 53 41 43 4c 23 2d 50 64 :80918720
                                                    d-ACL=#ACSACL#-P |
   2d 56 50 4e 43 6c 69 65 6e 74 2d 33 64 33 58 49 :80918730
                                                    IX-VPNClient-3d3 |
                                         27815 | 35 31 38 37 32 :80918740
                                                                   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
                                                ... | 00 00 00 :80918700
                                                         . | 02 :80918710
       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
                                           (hitcnt=38) 255.255.255.0
          access-list #ACSACL#-PIX-VPNClient-3d327815; 1 elements
 access-list #ACSACL#-PIX-VPNClient-3d327815 permit ip any host
                                                (hitcnt=15) 10.1.1.2
                                       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
                               (hitcnt=42) 255.255.255.0 192.168.1.0
          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
                                                (hitcnt=0) 192.168.1.1
                                       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
```

معلومات ذات صلة

- صفحة دعم PIX
- مراجع أوامر PIX
- طلبات التعليقات (RFCs)
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- صفحة دعم TACACS/TACACS+
- TACACS+ في وثائق IOS
- صفحة دعم RADIUS
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).