L2TP عبر IPsec بين Windows 2000/XP PC و PIX/ASA 7.2 باستخدام مثال تكوين مفاتيح مشتركة مسبقا

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين بروتوكول الاتصال النفقي للطبقة 2 (L2TP) عبر أمان IPsec من عملاء Microsoft Windows 2000/2003 و XP البعيدين إلى جهاز أمان PIX الخاص بمكتب الشركة باستخدام مفاتيح مشتركة مسبقا مع خادم RADIUS Microsoft Windows 2003 Internet Authentication Service (IAS) لمصادقة المستخدم. ارجع إلى Microsoft - قائمة التحقق: تكوين IAS للطلب الهاتفي والوصول إلى VPN للحصول على مزيد من المعلومات حول IAS.

تتمثل الميزة الأساسية لتكوين L2TP باستخدام IPsec في سيناريو الوصول عن بعد في أنه يمكن للمستخدمين عن بعد الوصول إلى شبكة VPN عبر شبكة IP عامة بدون بوابة أو خط مخصص. ويتيح ذلك الوصول عن بعد من أي مكان تقريبا باستخدام POTS. وهناك ميزة إضافية تتمثل في أن متطلبات العميل الوحيدة للوصول إلى الشبكة الخاصة

الظاهرية (VPN) هي إستخدام Windows 2000 مع شبكة الطلب الهاتفي من Microsoft (DUN). لا يلزم توفر برنامج عميل إضافي، مثل برنامج عميل شبكة VPN من Cisco.

يصف هذا المستند أيضا كيفية إستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco لتكوين جهاز الأمان من السلسلة PIX 500 Series ل L2TP عبر IPsec.

ملاحظة: بروتوكول الاتصال النفقي للطبقة 2 (L2TP) عبر IPsec مدعوم على برنامج جدار حماية PIX الآمن من Cisco الإصدار x.6 والإصدارات الأحدث.

لتكوين L2TP عبر IPsec بين PIX 6.x و Windows 2000، ارجع إلى تكوين L2TP عبر IPsec بين جدار حماية PIX و Windows 2000 PC باستخدام الشهادات.

من أجل تكوين عملاء L2TP عبر IPsec من نظام التشغيل Microsoft Windows 2000 و XP البعيد إلى موقع شركة باستخدام طريقة مشفرة، ارجع إلى تكوين عميل L2TP عبر IPsec من نظام التشغيل Windows 2000 أو XP إلى مركز Cisco VPN 3000 Series باستخدام مفاتيح مشتركة مسبقا.

المتطلبات الأساسية

المتطلبات

قبل إنشاء النفق الآمن، يلزم وجود اتصال IP بين الأقران.

تأكد من أن منفذ UDP 1701 غير محظور في أي مكان على مسار الاتصال.

أستخدم فقط مجموعة النفق الافتراضية ونهج المجموعة الافتراضي على Cisco PIX/ASA. لا تعمل السياسات والمجموعات المعرفة من قبل المستخدم.

ملاحظة: لا يقوم جهاز الأمان بإنشاء نفق L2TP/IPsec مع Windows 2000 في حالة تثبيت إما Cisco VPN Client 3.x أو Cisco VPN 3000 Client 2.5. قم بتعطيل خدمة Cisco VPN ل Cisco VPN Client 3.x، أو خدمة ANetIKE ل Cisco VPN 3000 Client 2.5 من لوحة الخدمات في Windows 2000. للقيام بذلك، أختر **Start (البدء) > Programs (البرامج) > Administrative Tools (الأدوات الإدارية) > Services (الخدمات)، ثم أعد تشغيل خدمة "وكيل سياسة IPsec" من لوحة الخدمات، وأعد تشغيل الجهاز.**

المكونات المستخدمة

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

- جهاز أمان PIX 515E مع إصدار البرنامج 7.2(1) أو إصدار أحدث
- 1)5.2 Adaptive Security Device Manager) أو إصدار أحدث
- نظام التشغيل Microsoft Windows 2000 Server
- نظام التشغيل Microsoft Windows XP Professional مع حزمة الخدمة SP2
- Windows 2003 Server مع IAS

ملاحظة: إذا قمت بترقية PIX 6.3 إلى الإصدار x.7، فتأكد من تثبيت SP2 في Windows XP (عميل L2TP).

ملاحظة: المعلومات الواردة في المستند صالحة أيضا لجهاز أمان ASA.

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان 1)7.2 Cisco ASA 5500 Series Security Appliance) أو إصدار أحدث.

الاصطلاحات

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

معلومات أساسية

أكمل هذه الخطوات لتكوين L2TP عبر IPsec.

1. قم بتكوين وضع نقل IPsec لتمكين IPsec باستخدام L2TP.يستخدم عميل Windows 2000 L2TP/IPsec وضع النقل IPsec — يتم تشفير حمولة IP فقط، وتترك رؤوس IP الأصلية كما هي. مزايا هذا الوضع هي أنه يضيف بضعة بايت فقط إلى كل حزمة ويسمح للأجهزة على الشبكة العامة برؤية المصدر والوجهة النهائيين للحزمة. لذلك، من أجل اتصال عملاء Windows 2000 L2TP/IPsec بجهاز الأمان، يجب تكوين وضع النقل IPsec لعملية تحويل (راجع الخطوة 2 في تكوين ASDM). مع هذه الإمكانية (النقل)، يمكنك تمكين معالجة خاصة (على سبيل المثال، جودة الخدمة) على الشبكة الوسيطة بناء على المعلومات الموجودة في رأس IP. ومع ذلك، يتم تشفير رأس الطبقة 4، مما يحد من فحص الحزمة. للأسف، يسمح نقل رأس IP في نص واضح، وضع النقل للمهاجم بإجراء بعض تحليل حركة المرور.
2. قم بتكوين L2TP باستخدام مجموعة شبكة الطلب الهاتفي الخاصة الظاهرية (VPDN).

يدعم تكوين L2TP مع IPsec الشهادات التي تستخدم المفاتيح المشتركة مسبقا أو طرق توقيع RSA، واستخدام خرائط التشفير الديناميكية (في مقابل خرائط التشفير الثابتة). يتم إستخدام المفتاح المشترك مسبقا كمصادقة لإنشاء نفق L2TP عبر IPsec.

التكوين

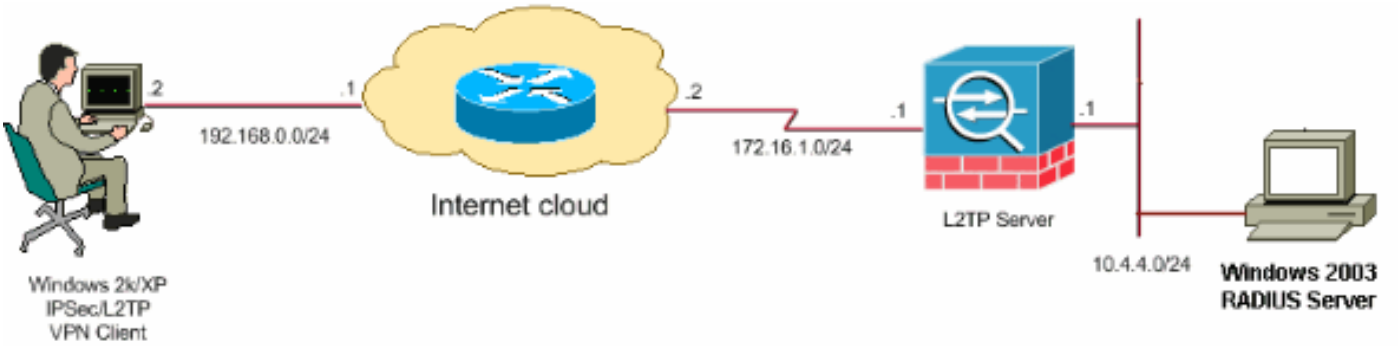
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين عميل Windows L2TP/IPsec
- خادم L2TP في تكوين PIX
- L2TP باستخدام تكوين ASDM
- Microsoft Windows 2003 Server مع تكوين IAS

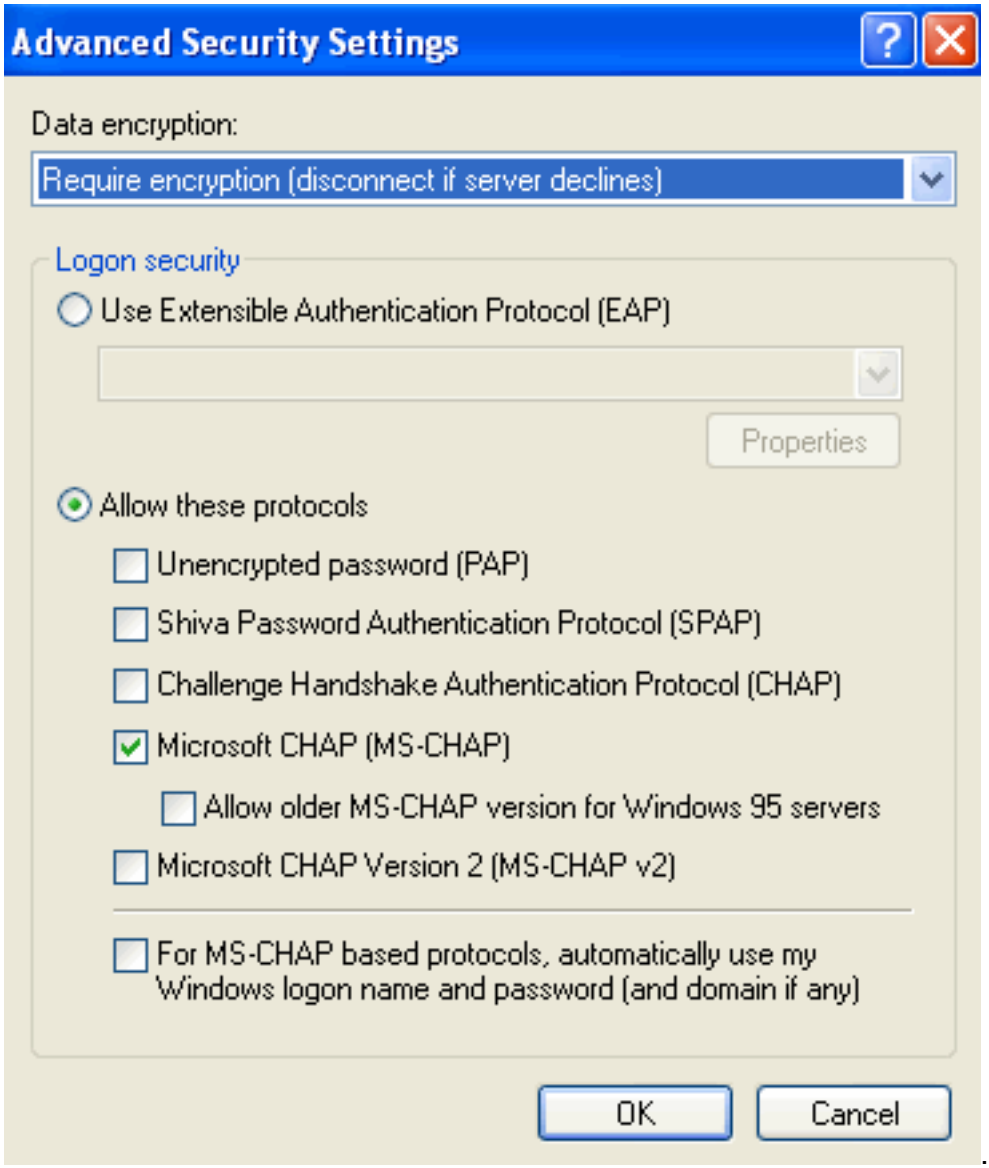
تكوين عميل Windows L2TP/IPsec

أكمل هذه الخطوات لتكوين L2TP عبر IPsec على Windows 2000. بالنسبة لنظام التشغيل Windows XP، يجب تخطي الخطوات 1 و 2 والبداية من الخطوة 3:

1. إضافة قيمة التسجيل هذه إلى جهاز Windows 2000:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. إضافة قيمة التسجيل هذه إلى هذا المفتاح:
   ```
   Value Name: ProhibitIpSec
   Data Type: REG_DWORD
   Value: 1
   ```

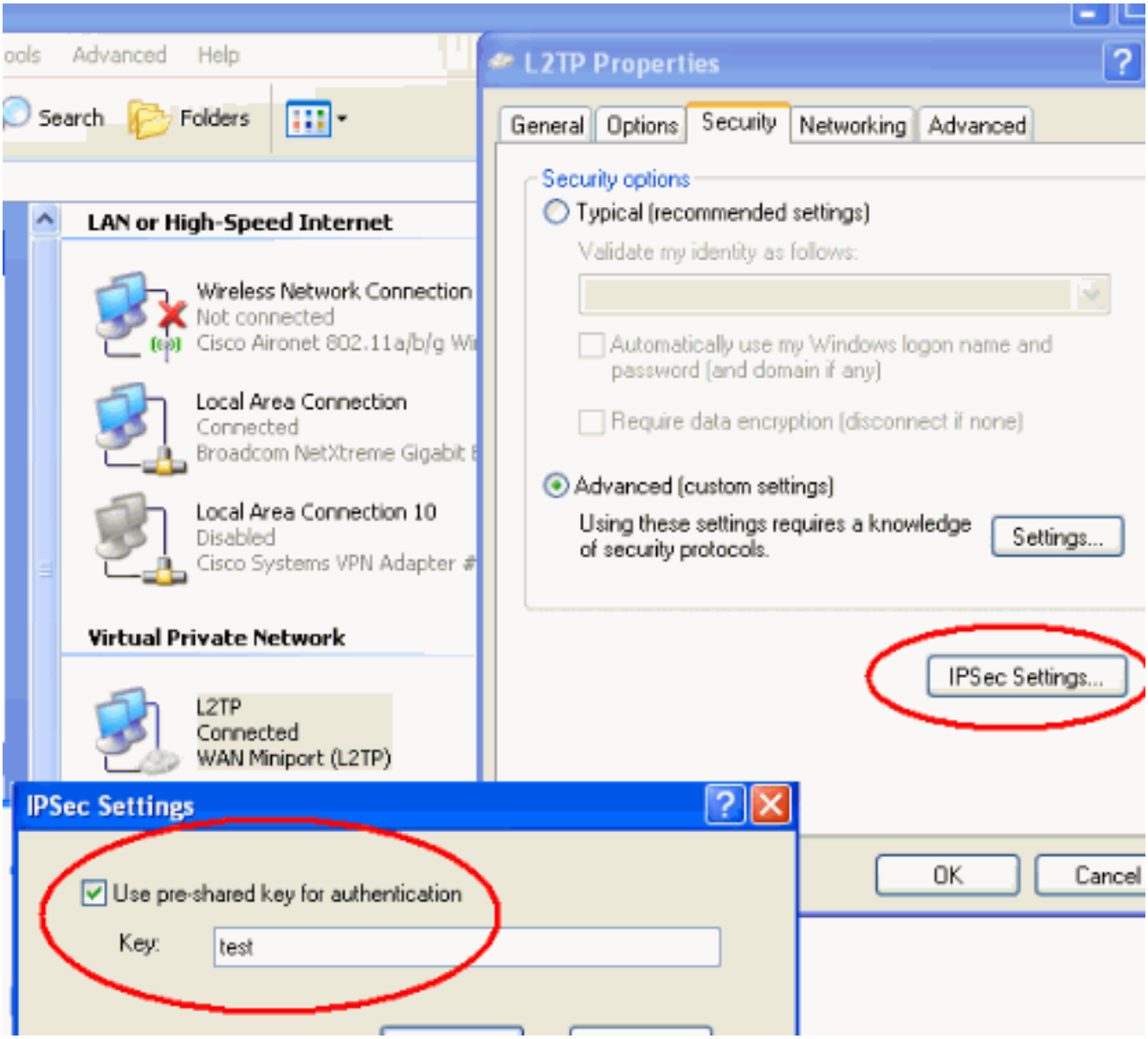
ملاحظة: في بعض الحالات (Windows XP SP2)، يبدو أن إضافة هذا المفتاح **(القيمة: 1)** تعطل الاتصال لأنه يجعل مربع XP يفاوض L2TP فقط بدلا من L2TP مع اتصال IPsec. من الضروري إضافة سياسة IPsec بالاقتران مع مفتاح التسجيل هذا. إذا تلقيت `800` عند محاولة إنشاء اتصال، فقم بإزالة المفتاح (القيمة 1) لجعل الاتصال يعمل.**ملاحظة:** يجب إعادة تشغيل جهاز Windows 2000/2003 أو XP حتى تصبح التغييرات نافذة المفعول. يحاول عميل Windows بشكل افتراضي إستخدام IPsec مع مرجع مصدق (CA). يمنع تكوين مفتاح التسجيل هذا من الحدوث. يمكنك الآن تكوين نهج IPsec على محطة Windows لمطابقة المعلمات التي تريدها على PIX/ASA. ارجع إلى كيفية تكوين اتصال L2TP/IPSec باستخدام مصادقة المفاتيح المشتركة مسبقا (Q240262) للحصول على تكوين مفصل لسياسة Windows IPsec.راجع تكوين مفتاح مشترك مسبقا للاستخدام مع إتصالات بروتوكول الاتصال النفقي للطبقة 2 في Windows XP (Q281555)\ للحصول على مزيد من المعلومات.

3. إنشاء الاتصال الخاص بك.
4. تحت إتصالات الشبكة والطلب الهاتفي، انقر بزر الماوس الأيمن على الاتصال واختر **خصائص**.انتقل إلى علامة التبويب "أمان" وانقر فوق **خيارات متقدمة**. أختر البروتوكولات كما تظهر هذه



الصورة.

5. **ملاحظة:** تنطبق هذه الخطوة على نظام التشغيل Windows XP فقط.انقر على **إعدادات IPSec**، وتحقق من **إستخدام مفتاح مشترك مسبقا للمصادقة** واكتب في المفتاح المشترك مسبقا لتعيين المفتاح المشترك مسبقا.في هذا المثال، يتم إستخدام الاختبار كمفتاح مشترك
مسبقا.



خادم L2TP في تكوين PIX

PIX 7.2
pixfirewall#**show run** (PIX Version 7.2(1 ! hostname pixfirewall domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! *Configures the outside and inside interfaces. ---!* interface Ethernet0 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! interface Ethernet1 nameif inside security-level 100 ip address 10.4.4.1 255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid **access-list nonat extended permit ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0** **nat (inside) 0 access-list nonat** pager lines 24

```
logging console debugging
mtu outside 1500
mtu inside 1500

Creates a pool of addresses from which IP addresses ---!
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

The global and nat command enable !--- the Port ---!
Address Translation (PAT) using an outside interface IP
.!--- address for all outgoing traffic

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0


route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

Create the AAA server group "vpn" and specify its ---!
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
key radiuskey

Identifies the group policy as internal. group- ---!
policy DefaultRAGroup internal
Instructs the security appliance to send DNS and !- ---!
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
wins-server value 10.4.4.99
dns-server value 10.4.4.99
Configures L2TP over IPsec as a valid VPN tunneling ---!
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
default-domain value cisco.com
Configure usernames and passwords on the device !-- ---!
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username

.


username test password DLaUiAX3l78qgoB5c7iVNw== nt-
```

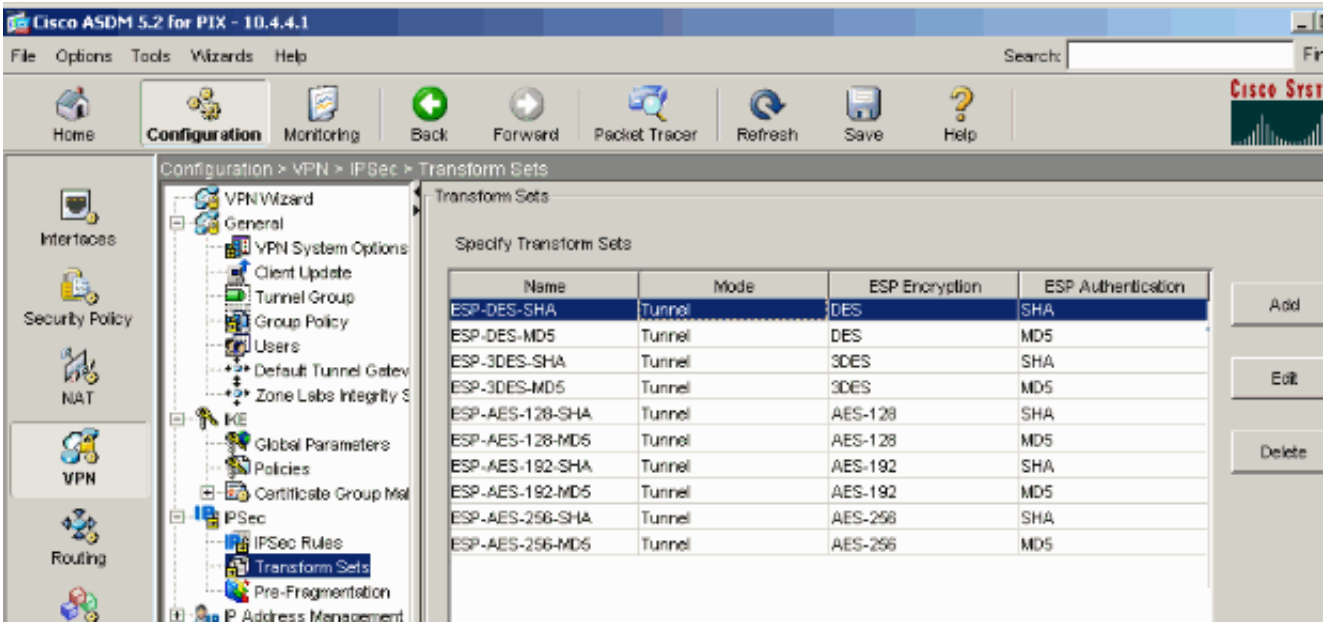
```
                                                    encrypted


                                    vpn-tunnel-protocol l2tp-ipsec

                                                  http server enable
                                        http 0.0.0.0 0.0.0.0 inside
                                            no snmp-server location
                                             no snmp-server contact
                snmp-server enable traps snmp authentication linkup
                                                    linkdown coldstart

Identifies the IPsec encryption and hash algorithms ---!
      !--- to be used by the transform set. crypto ipsec
  transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

Since the Windows 2000 L2TP/IPsec client uses IPsec ---!
transport mode, !--- set the mode to transport. !--- The
      default is tunnel mode. crypto ipsec transform-set
                                TRANS_ESP_3DES_MD5 mode transport




   Specifies the transform sets to use in a dynamic ---!
 crypto map entry. crypto dynamic-map outside_dyn_map 20
                                  set transform-set TRANS_ESP_3DES_MD5

    Requires a given crypto map entry to refer to a ---!
        pre-existing !--- dynamic crypto map. crypto map
     outside_map 20 ipsec-isakmp dynamic outside_dyn_map

  Applies a previously defined crypto map set to an ---!
     outside interface. crypto map outside_map interface
                                                    outside

                                  crypto isakmp enable outside
                                crypto isakmp nat-traversal 20

Specifies the IKE Phase I policy parameters. crypto ---!
                                                isakmp policy 10
                                      authentication pre-share
                                               encryption 3des
                                                      hash md5
                                                     group 2
                                                lifetime 86400

       Creates a tunnel group with the tunnel-group ---!
 command, and specifies the local !--- address pool name
     used to allocate the IP address to the client. !---
    Associate the AAA server group (VPN) with the tunnel
                                                    .group


                tunnel-group DefaultRAGroup general-attributes
                                        address-pool clientVPNpool
                                 authentication-server-group vpn

   Link the name of the group policy to the default ---!
  tunnel !--- group from tunnel group general-attributes
                 mode. default-group-policy DefaultRAGroup

 Use the tunnel-group ipsec-attributes command !--- ---!
     in order to enter the ipsec-attribute configuration
```

```
mode. !--- Set the pre-shared key. !--- This key should
       be the same as the key configured on the Windows
                                                .machine


            tunnel-group DefaultRAGroup ipsec-attributes
                                     * pre-shared-key

 Configures the PPP authentication protocol with the ---!
 authentication type !--- command from tunnel group ppp-
                                        .attributes mode


            tunnel-group DefaultRAGroup ppp-attributes
                                  no authentication chap
                               authentication ms-chap-v2

                                          telnet timeout 5
                                             ssh timeout 5
                                          console timeout 0
                                                        !
                                  class-map inspection_default
                              match default-inspection-traffic
                                                        !
                                                        !
                 policy-map type inspect dns preset_dns_map
                                               parameters
                                   message-length maximum 512
                                       policy-map global_policy
                                     class inspection_default
                                   inspect dns preset_dns_map
                                             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
                                        prompt hostname context
        Cryptochecksum:e1e0730fa260244caa2e2784f632accd
                                                end :
```

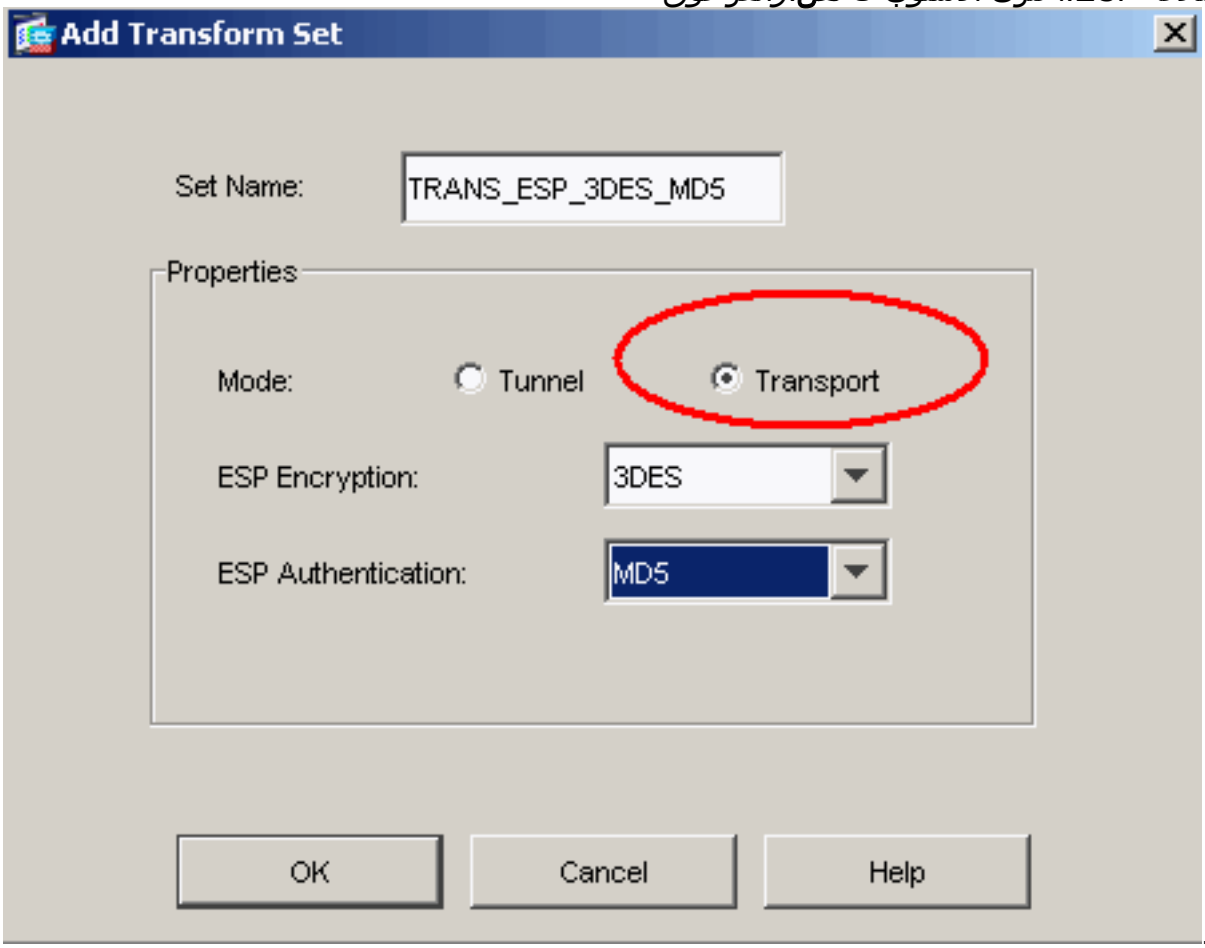
L2TP باستخدام تكوين ASDM

أكمل هذه الخطوات لتكوين جهاز الأمان لقبول إتصالات L2TP عبر IPsec:

1. قم بإضافة مجموعة تحويل IPsec وحدد IPsec لاستخدام وضع النقل بدلا من وضع النفق. أخترت in order to أتمت هذا، **تشكيل > IPSec > VPN > تحويل مجموعة** وطقطقة **يضيف**. تعرض لوحة مجموعات التحويل.

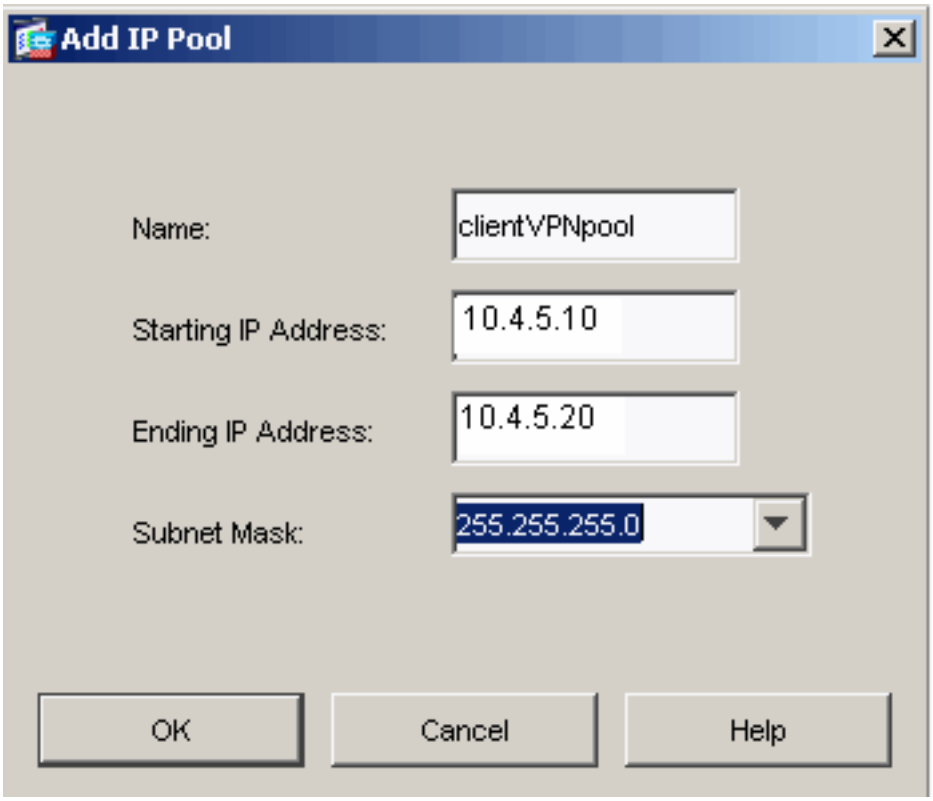


2. أتمت هذا steps in order to أضفت مجموعة تحويل:أدخل اسم لمجموعة التحويل.أختر طريقتي تشفير ESP ومصادقة ESP.أخترت الأسلوب ك **نقل**.وانقر فوق



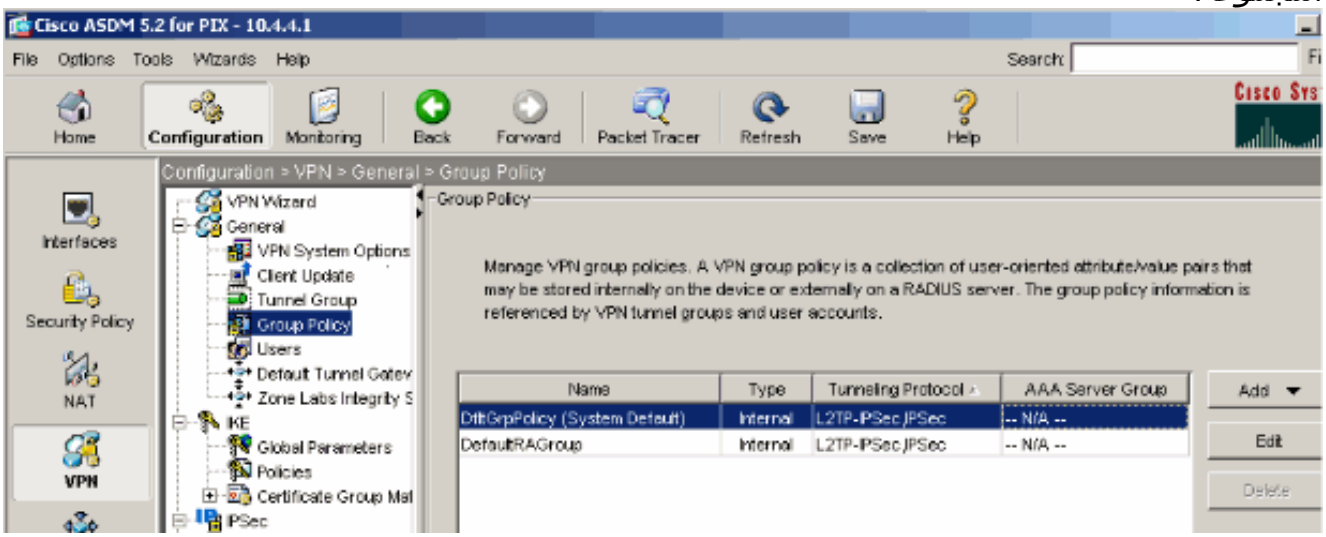
.OK

3. أتمت هذا steps in order to شكلت طريقة من العنوان تنازل. يستخدم هذا المثال تجمعات عناوين IP.أخترت **تشكيل>VPN>عنوان إدارة>IP بركة**.انقر فوق **إضافة (Add)**. يظهر مربع الحوار إضافة تجمع IP.أدخل اسم تجمع عناوين IP الجديد.أدخل عناوين IP البداية والنهاية.أدخل قناع الشبكة الفرعية وانقر فوق

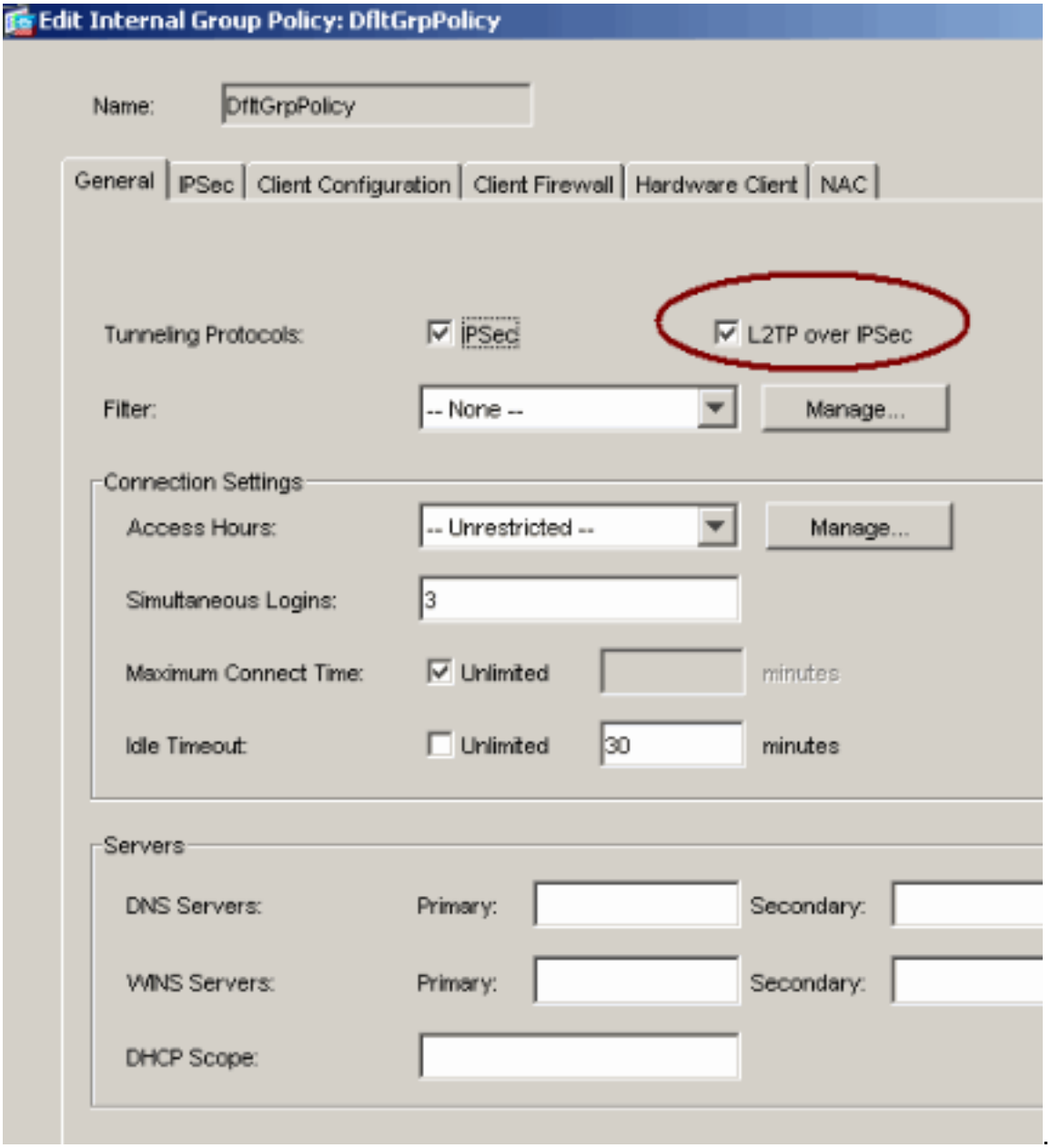


موافق.

4. أخترت **تشكيل>VPN>عام>مجموعة سياسة** in order to شكلت L2TP عبر IPsec بما أن شرعي VPN tunneling بروتوكول ل المجموعة سياسة. يظهر جزء نهج المجموعة.

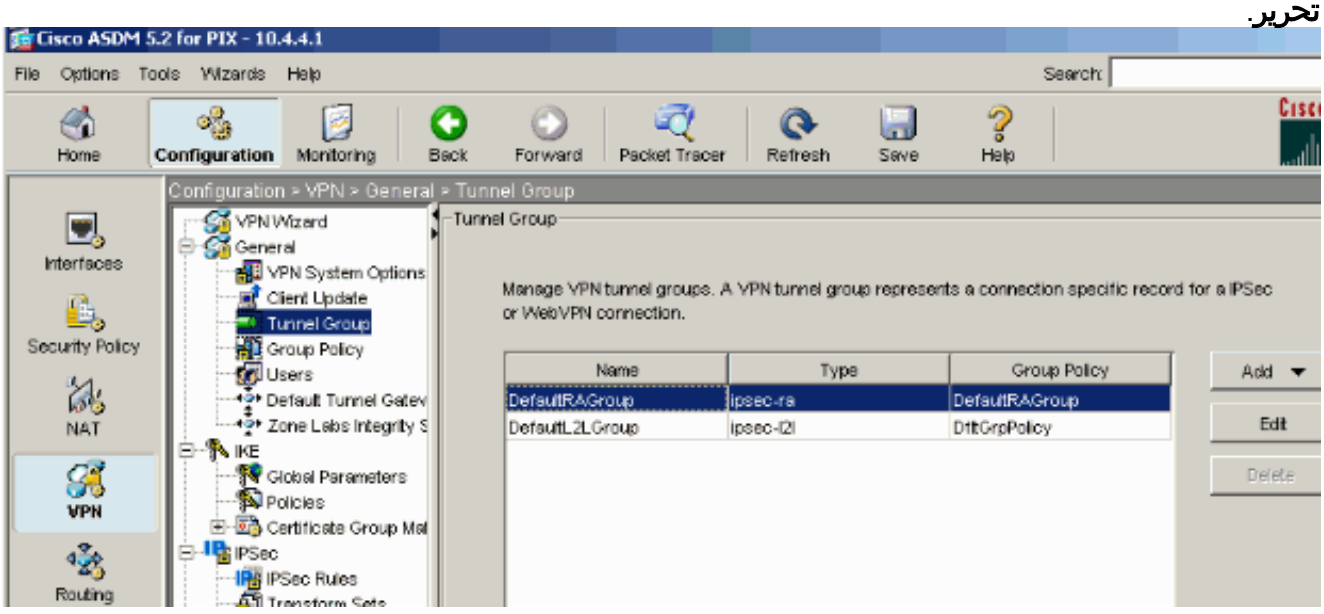


5. حدد نهج مجموعة (DiffGrpPolicy) وانقر فوق **تحرير**.يتم عرض مربع الحوار "تحرير نهج المجموعة". تحقق من **L2TP عبر IPSec** لتمكين البروتوكول لنهج المجموعة ثم انقر فوق



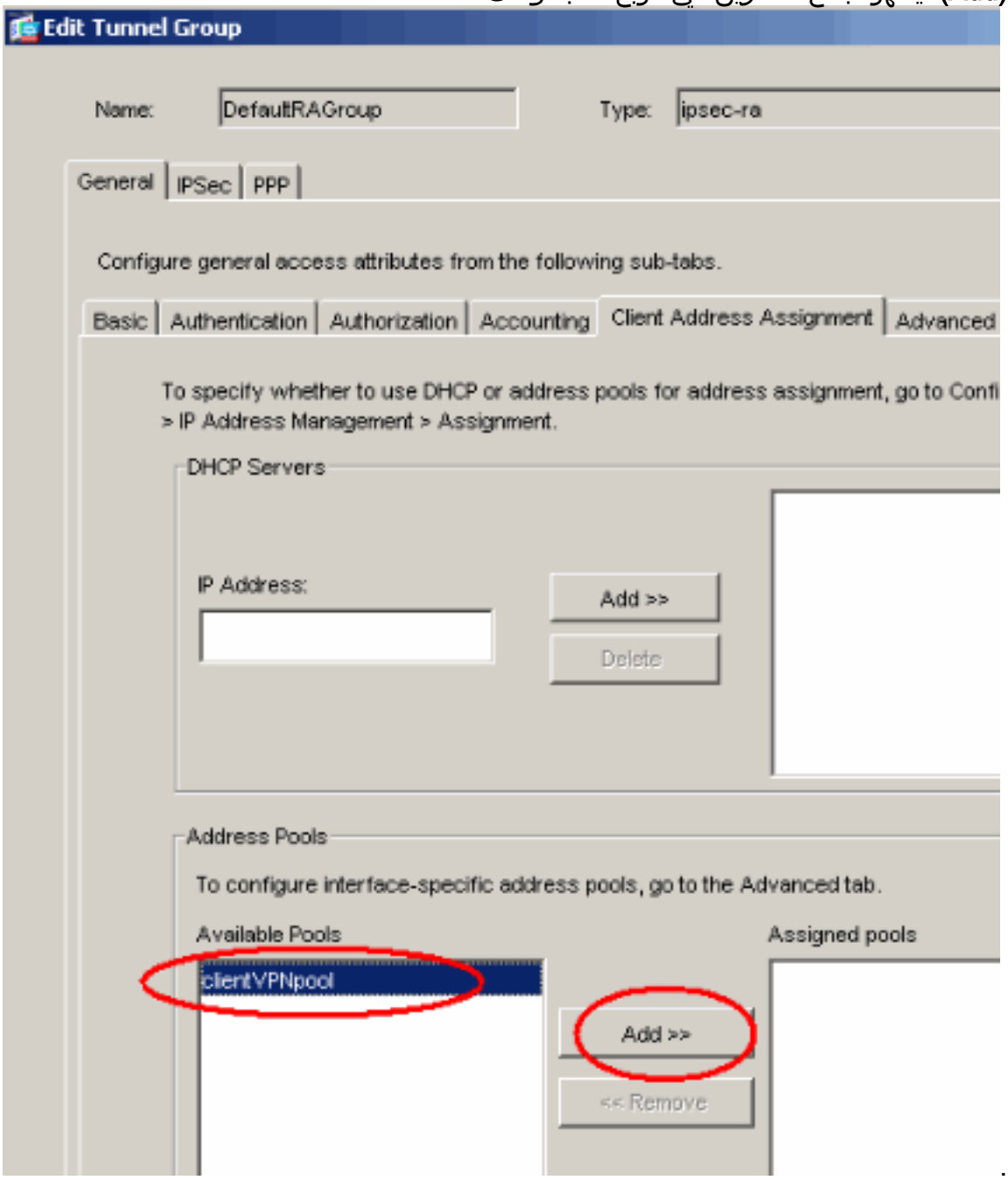
موافق.

6. أتمت هذا steps in order to عينت العنوان بركة إلى نفق مجموعة:أخترت **تشكيل>VPN>عام>نفق مجموعة**.بعد أن يظهر جزء مجموعة النفق، حدد مجموعة نفق (DefaultRAGroup) في الجدول.انقر فوق **تحرير**.



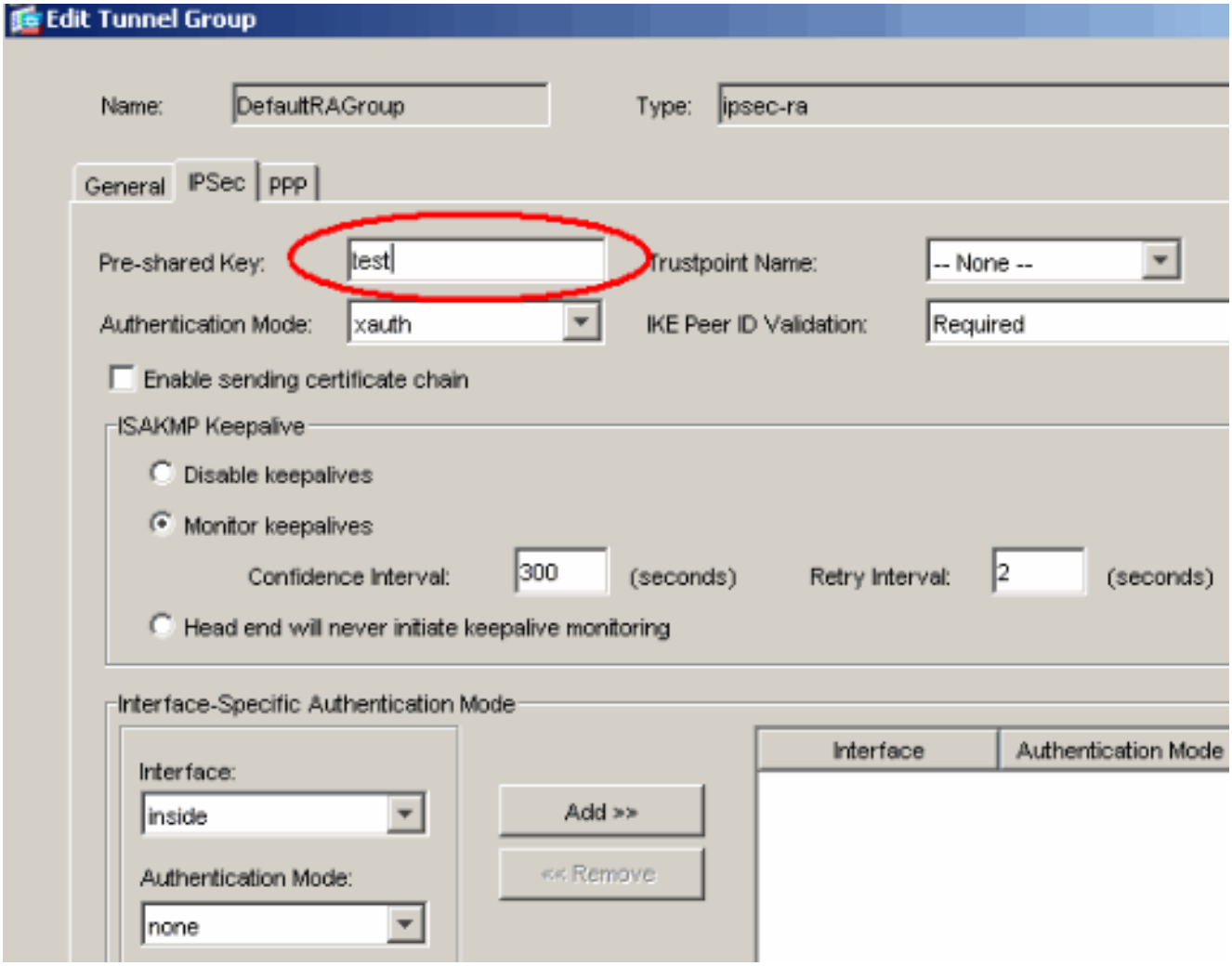
7. أتمت هذا steps عندما يظهر ال edit نفق مجموعة نافذة:من علامة التبويب "عام"، انتقل إلى علامة التبويب "تعيين عنوان العميل".في منطقة تجمعات العناوين، أختر تجمع عناوين لتعيينه على مجموعة النفق.انقر فوق

إضافة (Add). يظهر تجمع العناوين في مربع المجموعات

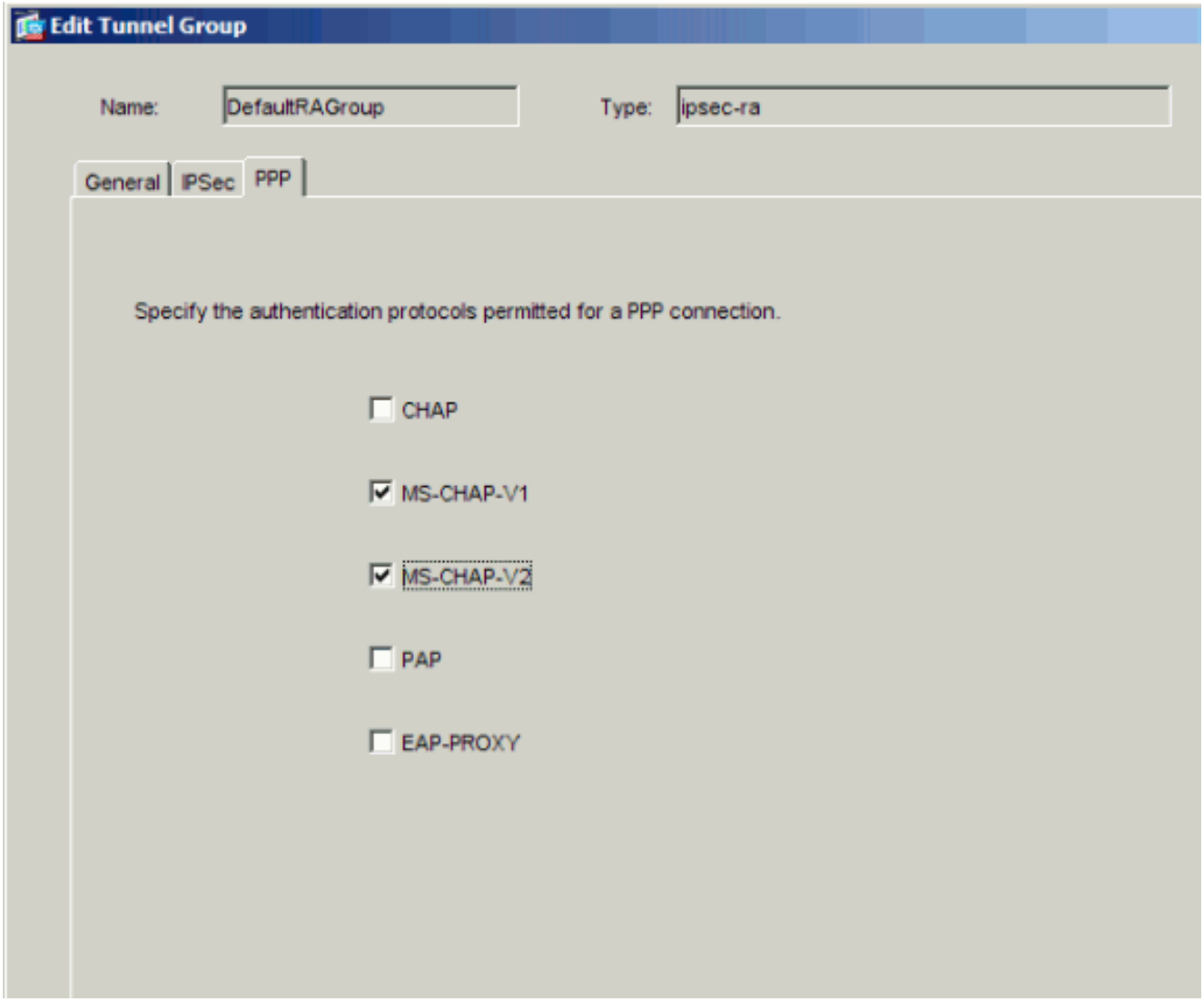


المعينة.

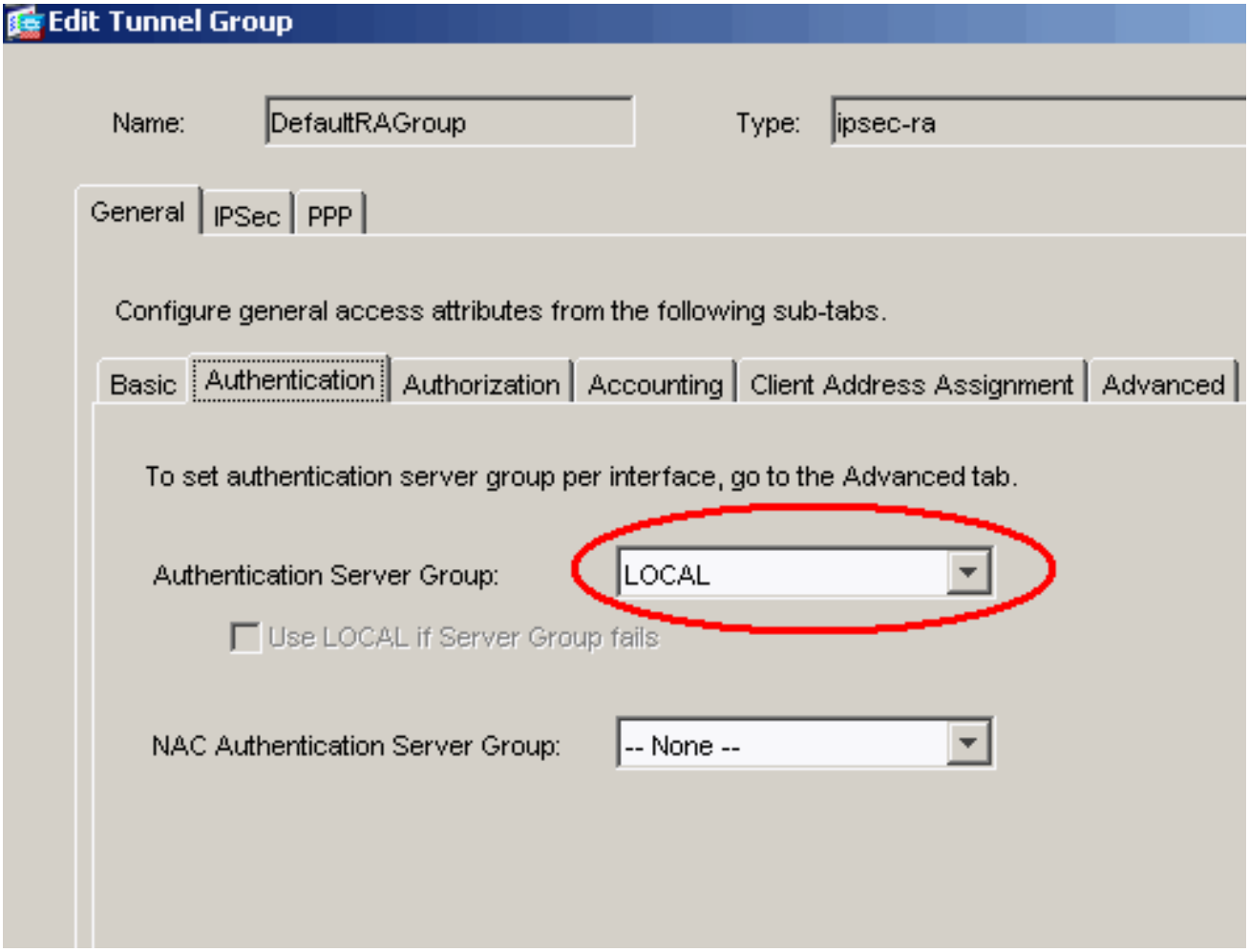
8. لتعيين المفتاح المشترك مسبقا، انتقل إلى علامة التبويب IPSec، وأدخل **المفتاح المشترك مسبقا**، وانقر **موافق**.



9. يستخدم L2TP عبر IPsec بروتوكولات مصادقة PPP. حدد البروتوكولات المسموح بها لاتصالات PPP في علامة التبويب PPP الخاصة بمجموعة النفق. حدد بروتوكول **MS-CHAP-V1** للمصادقة.

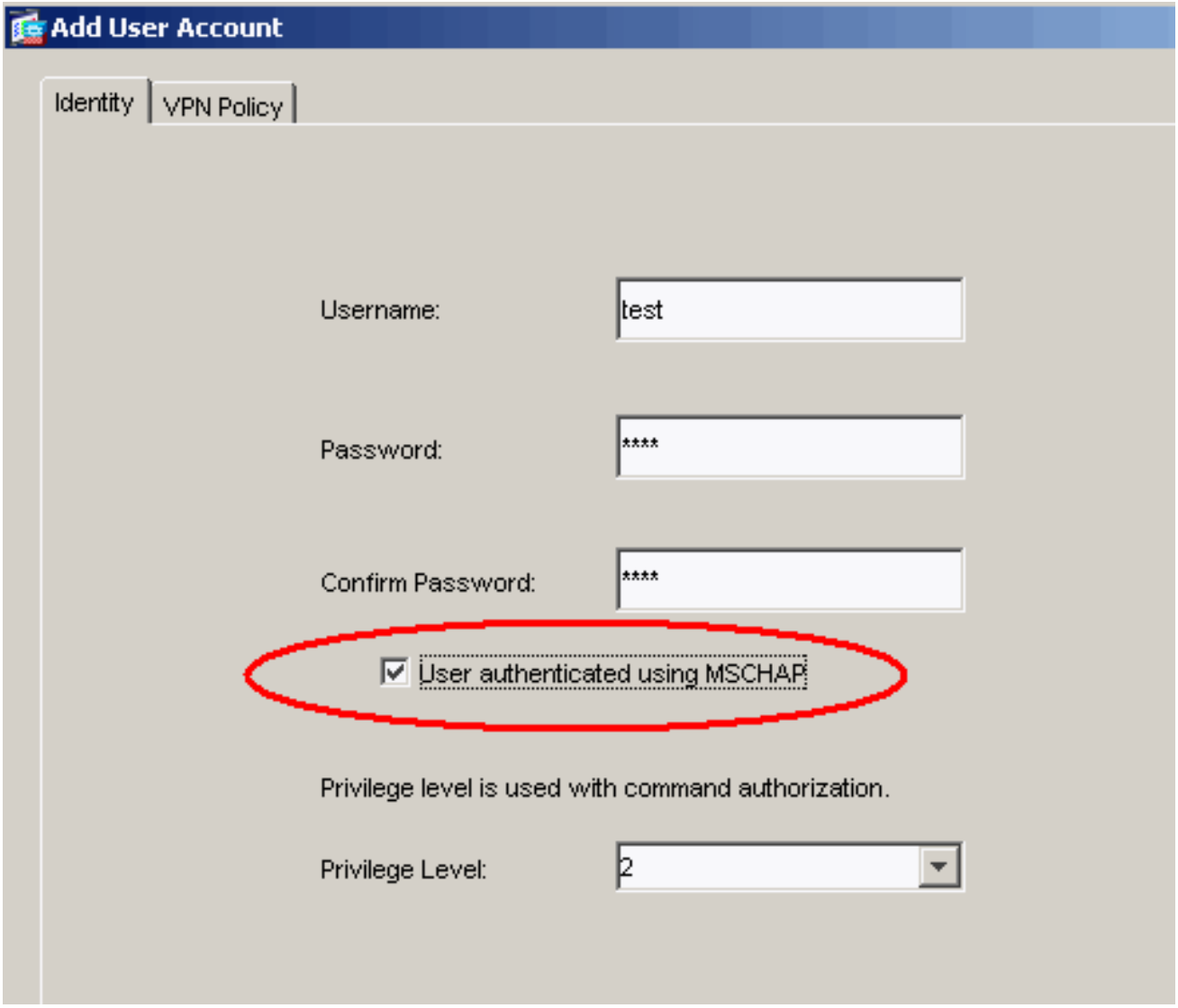


10. حدد طريقة لمصادقة المستخدمين الذين يحاولون L2TP عبر إتصالات IPsec.يمكنك تكوين جهاز الأمان لاستخدام خادم المصادقة أو قاعدة البيانات المحلية الخاصة به. للقيام بذلك، انتقل إلى علامة تبويب المصادقة الخاصة بمجموعة النفق. وبشكل افتراضي، يستخدم جهاز الأمان قاعدة البيانات المحلية الخاصة به. تعرض القائمة المنسدلة لمجموعة خوادم المصادقة بيانات محلية. لاستخدام خادم مصادقة، حدد خادما من القائمة.**ملاحظة:** يدعم جهاز الأمان فقط مصادقة PPP و Microsoft CHAP الإصدار 1 و 2 على قاعدة البيانات المحلية. يتم تنفيذ EAP و CHAP بواسطة خوادم مصادقة الوكيل. لذلك، إذا كان المستخدم البعيد ينتمي إلى مجموعة نفق تم تكوينها باستخدام EAP أو CHAP، وتم تكوين جهاز الأمان لاستخدام قاعدة البيانات المحلية، فإن ذلك المستخدم غير قادر على
الاتصال.

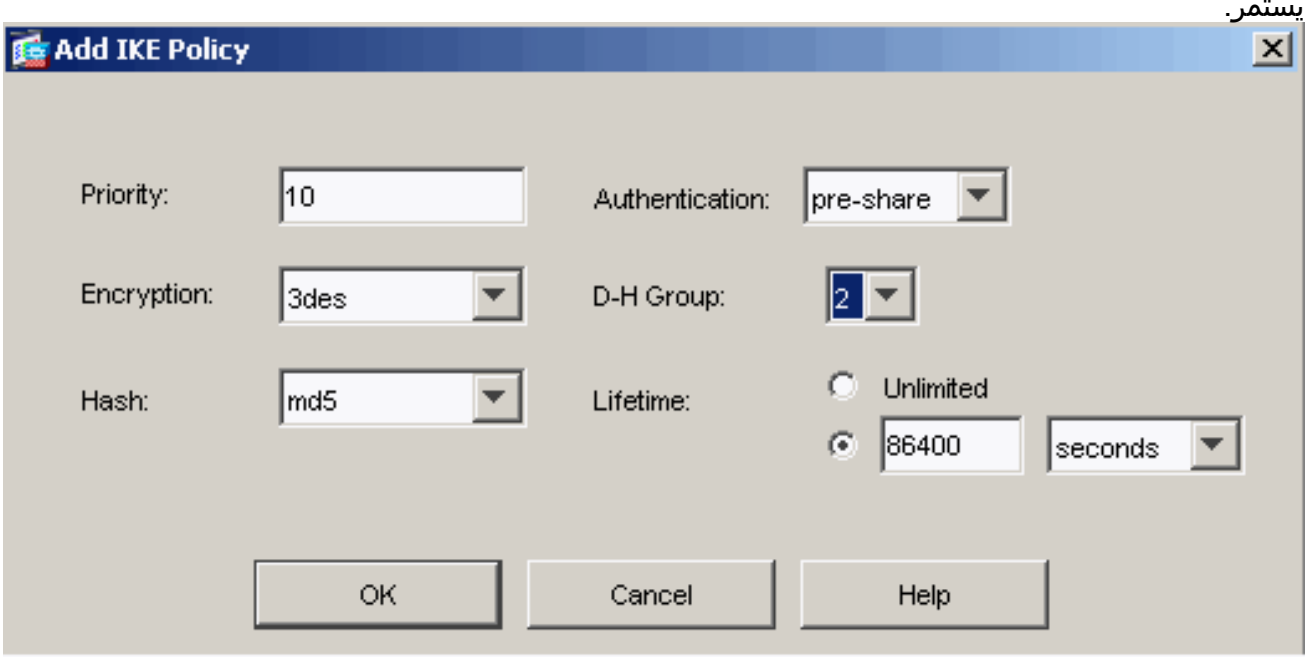


ملاحظة: أختر **التكوين > VPN > عام > مجموعة النفق** للعودة إلى تكوين مجموعة النفق حتى يمكنك ربط سياسة المجموعة بمجموعة النفق وتمكين تحويل مجموعة النفق (إختياري). عندما تظهر لوحة مجموعة النفق، أختر مجموعة النفق وانقر **تحرير**.**ملاحظة:** يمكن تحويل مجموعة النفق جهاز الأمان من إقران مستخدمين مختلفين يقومون بإنشاء إتصالات L2TP عبر IPsec مع مجموعات النفق المختلفة. ونظرا لأن كل مجموعة نفق تحتوي على مجموعة خوادم AAA وتجميعات عناوين IP الخاصة بها، يمكن مصادقة المستخدمين من خلال أساليب خاصة بمجموعة النفق الخاصة بهم. باستخدام هذه الميزة، بدلا من إرسال اسم مستخدم فقط، يرسل المستخدم اسم مستخدم واسم مجموعة بالتنسيق username@group_name، حيث يمثل "@" محدد يمكنك تكوينه، واسم المجموعة هو اسم مجموعة أنفاق تم تكوينها على جهاز الأمان.**ملاحظة:** يتم تمكين تحويل مجموعة النفق بواسطة معالجة مجموعة الشريط، التي تمكن جهاز الأمان من تحديد مجموعة النفق لاتصالات المستخدم من خلال الحصول على اسم المجموعة من اسم المستخدم الذي يقدمه عميل VPN. ثم يرسل جهاز الأمان جزء المستخدم فقط لاسم المستخدم للتخويل والمصادقة. وإلا (في حالة تعطيلها)، يرسل جهاز الأمان اسم المستخدم بالكامل، بما في ذلك النطاق. لتمكين تحويل مجموعة النفق، تحقق من **قطع النطاق من اسم المستخدم قبل تمريره إلى خادم AAA**، وفحص **قطع المجموعة من اسم المستخدم قبل تمريره إلى خادم AAA**. ثم انقر فوق **OK**.

11. أتمت هذا steps in order to خلقت مستعمل في القاعدة معطيات محلي:أخترت **تشكيل >خصائص>أداة إدارة>مستعمل حساب**.انقر فوق **إضافة (Add)**.إذا كان المستخدم عميل L2TP يستخدم Microsoft CHAP الإصدار 1 أو 2، وتم تكوين جهاز الأمان للمصادقة مقابل قاعدة البيانات المحلية، فيجب عليك التحقق من **مصادقة المستخدم باستخدام MSCHAP** لتمكين MSCHAP.وانقر فوق **OK**.



12. أخترت **تشكيل>IKE>VPN>نهج** وطقطقة **يضيف** in order to خلقت IKE سياسة للمرحلة i. طقطقة **ok** أن يستمر.



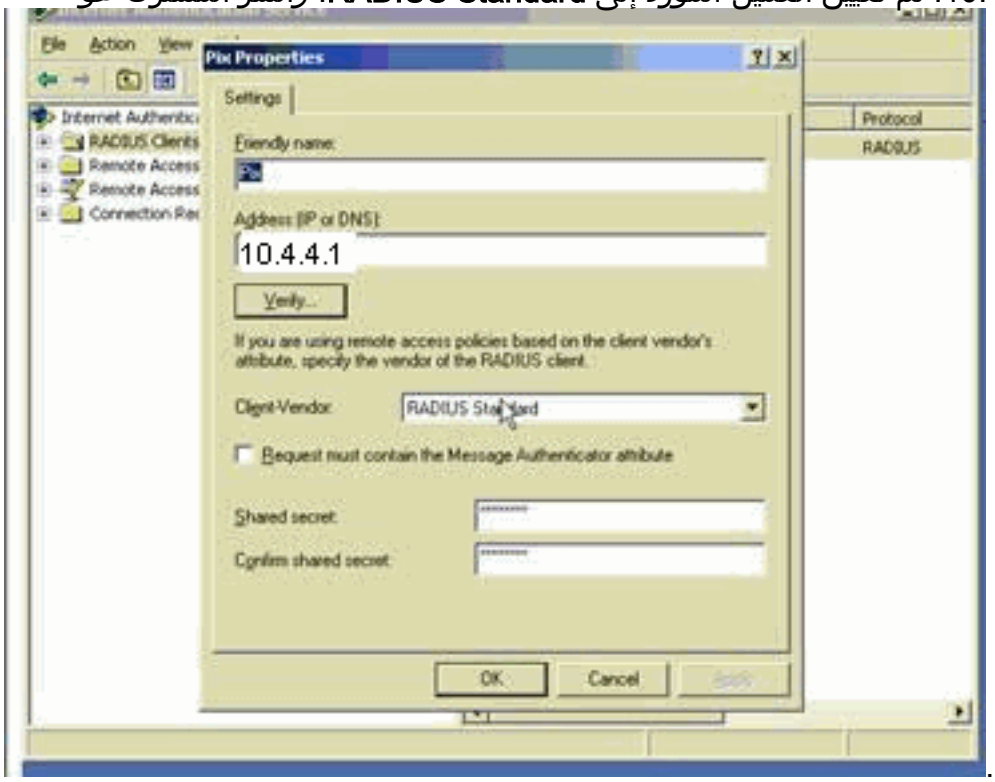
13. (إختياري) إذا كنت تتوقع أن يقوم العديد من عملاء L2TP خلف جهاز NAT بمحاولة L2TP عبر IPsec من الاتصالات بجهاز الأمان، فيجب عليك تمكين إجتياز NAT حتى يمكن لحزم ESP المرور عبر جهاز واحد أو أكثر من أجهزة NAT. أتمت هذا steps in order to أنجزت هذا:أخترت **تشكيل>IKE>VPN>شامل معلم**.تأكد من تمكين **ISAKMP** على واجهة.تدقيق **تمكين IPSec عبر NAT-T**.وانقر فوق **OK**.

Microsoft Windows 2003 Server مع تكوين IAS

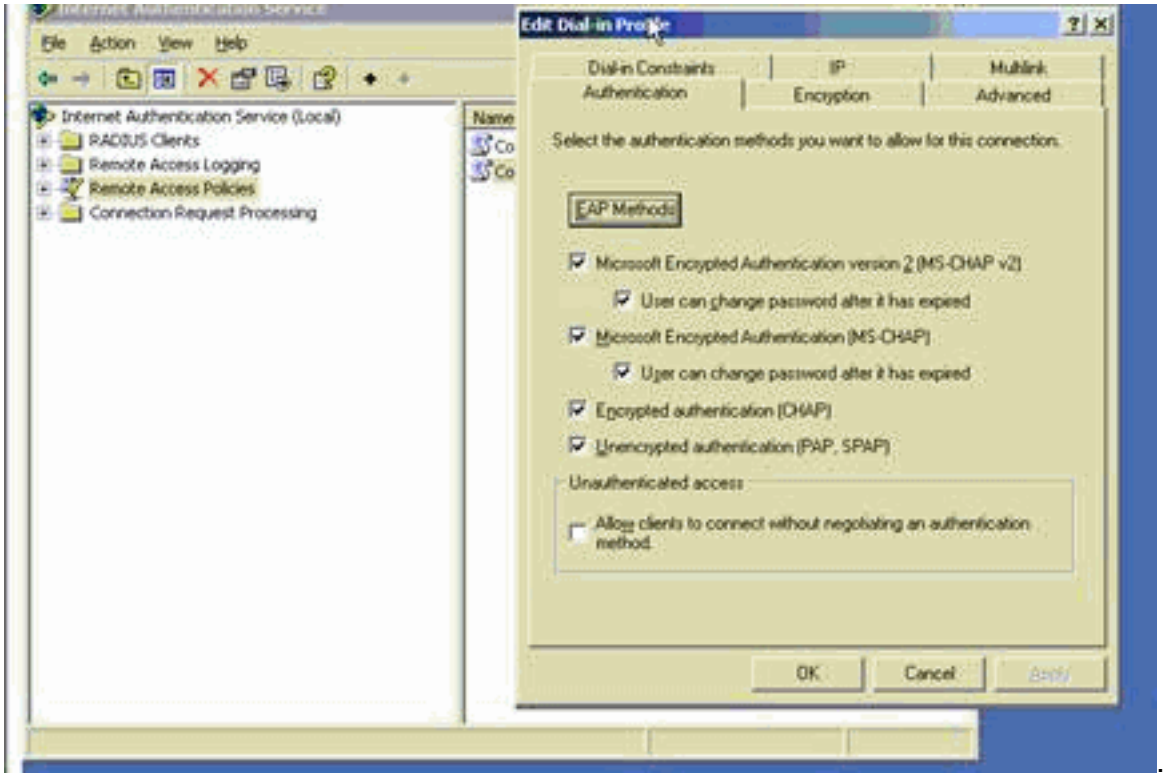
أكمل هذه الخطوات لتكوين خادم Microsoft Windows 2003 باستخدام IAS.

ملاحظة: تفترض هذه الخطوات أن IAS مثبت بالفعل على الجهاز المحلي. وإذا لم تكن هناك مساحة، فقم بإضافة هذا من خلال **لوحة التحكم > إضافة/إزالة البرامج**.

1. أختر **أدوات إدارية > خدمة مصادقة الإنترنت** وانقر بزر الماوس الأيمن على **عميل RADIUS** لإضافة عميل RADIUS جديد. بعد كتابة معلومات العميل، انقر فوق **موافق**.يوضح هذا المثال عميل مسمى "PIX" بعنوان IP بقيمة 10.4.4.1. تم تعيين العميل-المورد إلى **RADIUS Standard**، والسر المشترك هو **radiuskey**.

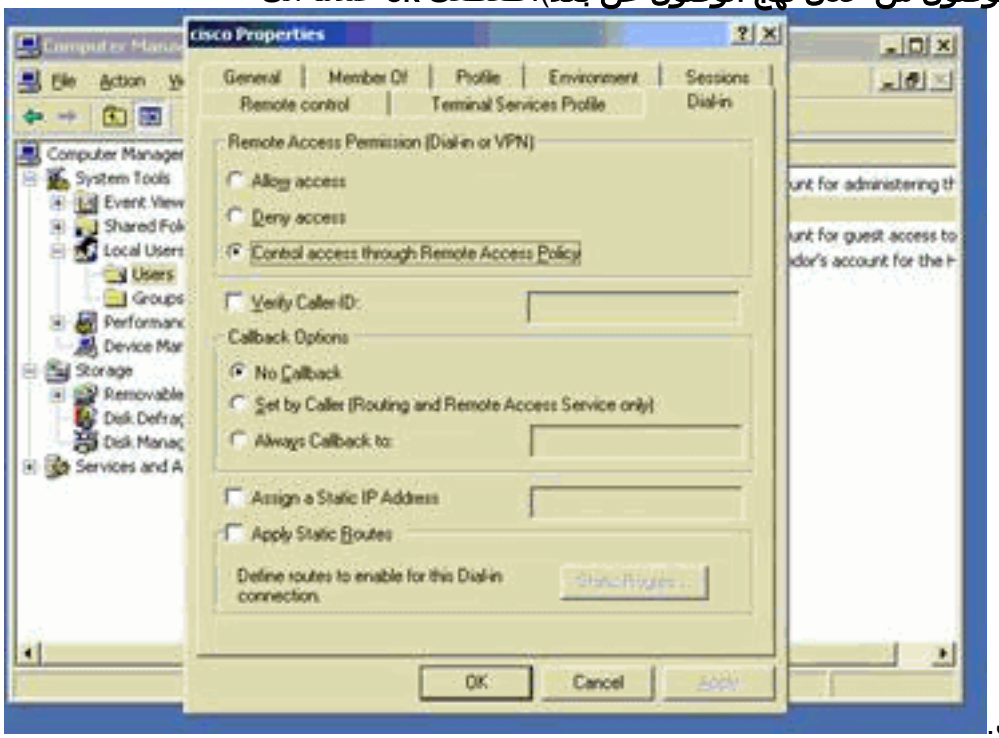


2. أختر **سياسات الوصول عن بعد**، وانقر بزر الماوس الأيمن فوق **الاتصالات بخوادم الوصول الأخرى**، وحدد **الخصائص**.
3. تأكد من أن خيار **منح أذونات الوصول عن بعد** محدد.
4. انقر على **تحرير التوصيف** وتحقق من الإعدادات التالية:في علامة تبويب المصادقة، تحقق من **المصادقة غير المشفرة (PAP، SPAP)**.في علامة تبويب التشفير، تأكد من تحديد خيار **عدم التشفير**.طقطقت **ok** عندما أنت



إنتهيت.

5. أختر **أدوات إدارية > إدارة الكمبيوتر > أدوات النظام > المستخدمون المحليون والمجموعات المحلية**، وانقر بزر الماوس الأيمن فوق **المستخدمين** وحدد **المستخدمين الجدد** لإضافة مستخدم إلى حساب الكمبيوتر المحلي.
6. أضفت مستعمل مع cisco كلمة **مرور 1** وفحصت هذا توصيف معلومة:على علامة التبويب "عام"، تأكد من تحديد خيار **كلمة المرور التي لا تنتهي صلاحيتها أبدا** بدلا من الخيار الخاص ب المستخدم الذي يجب عليه تغيير كلمة المرور.في علامة التبويب "الطلب الهاتفي"، حدد الخيار ل **السماح بالوصول** (أو أترك الإعداد الافتراضي ل **التحكم في الوصول من خلال نهج الوصول عن بعد**).طقطقت **ok** عندما أنت



إنتهيت.

المصادقة الموسعة ل L2TP عبر IPSec باستخدام Active Directory

أستخدم هذا التكوين على ASA للسماح بإجراء المصادقة لاتصال L2TP من Active Directory:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
```

```
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

أيضا، على ال L2TP زبون، ذهبت إلى **متقدم أمن عملية إعداد (مخصص)** واخترت فقط الخيار ل **لا يشفر كلمة (PAP)**.

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر العرض.

- **show crypto ipSec**—يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.

```
pixfirewall#show crypto ipsec sa
                                     interface: outside
        Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1

                access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
      (local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0
(remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701
                                  current_peer: 192.168.0.2, username: test
                                       dynamic allocated peer ip: 10.4.5.15

                                pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23#
                              pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93#
                                          pkts compressed: 0, #pkts decompressed: 0#
    pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0#
    post-frag successes: 0, #post-frag failures: 0, #fragments created: 0#
  PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                               send errors: 0, #recv errors: 0#

                          local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

                                    path mtu 1500, ipsec overhead 58, media mtu 1500
                                          current outbound spi: C16F05B8

                                                          :inbound esp sas
                                                  (spi: 0xEC06344D (3959829581
                                              transform: esp-3des esp-md5-hmac
                                            { ,in use settings ={RA, Transport
                        slot: 0, conn_id: 3, crypto-map: outside_dyn_map
                           sa timing: remaining key lifetime (sec): 3335
                                                        IV size: 8 bytes
                                               replay detection support: Y

                                                         :outbound esp sas
                                                  (spi: 0xC16F05B8 (3245278648
                                              transform: esp-3des esp-md5-hmac
                                            { ,in use settings ={RA, Transport
                        slot: 0, conn_id: 3, crypto-map: outside_dyn_map
                           sa timing: remaining key lifetime (sec): 3335
                                                        IV size: 8 bytes
                                               replay detection support: Y
```

- **show crypto isakmp sa**— يعرض جميع شبكات IKE الحالية في نظير.

```
pixfirewall#show crypto isakmp sa

                                                        Active SA: 1
    (Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
```

```
                                                    Total IKE SA: 1

                                                IKE Peer: 192.168.0.2   1
                                  Type    : user            Role    : responder
                                  Rekey   : no              State   : MM_ACTIVE
```

- **show vpn-sessiondb**— يتضمن عوامل تصفية البروتوكول التي يمكنك إستخدامها لعرض معلومات تفصيلية حول L2TP عبر إتصالات IPsec. الأمر الكامل من وضع التكوين العام هو **show vpn-sessoindb بروتوكول التصفية عن بعد التفصيلي l2tpOverIpSec**.يوضح هذا المثال تفاصيل اتصال L2TP واحد عبر IPsec:

```
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec

                                                Session Type: Remote Detailed

                                                    Username     : test
                                                       Index        : 1
                                Assigned IP  : 10.4.5.15          Public IP    : 192.168.0.2
                                       Protocol     : L2TPOverIPSec          Encryption   : 3DES
                                                                              Hashing      : MD5
                                             Bytes Tx     : 1336              Bytes Rx     : 14605
                                                   :   Client Type  :                      Client Ver
                                                                  Group Policy : DefaultRAGroup
                                                                  Tunnel Group : DefaultRAGroup
                                                       Login Time   : 18:06:08 UTC Fri Jan 1 1993
                                                           Duration     : 0h:04m:25s
                                                                       :  Filter Name
                                                                  NAC Result   : N/A
                                                                      :Posture Token

                                                                IKE Sessions: 1
                                                               IPSec Sessions: 1
                                                           L2TPOverIPSec Sessions: 1


                                                                                :IKE
                                                                    Session ID   : 1
                                             UDP Src Port : 500              UDP Dst Port : 500
                                       IKE Neg Mode : Main             Auth Mode    : preSharedKeys
                                             Encryption   : 3DES             Hashing      : MD5
                                       Rekey Int (T): 28800 Seconds    Rekey Left(T): 28536 Seconds
                                                                       D/H Group    : 2

                                                                                :IPSec
                                                                    Session ID   : 2
                                                  Local Addr   : 172.16.1.1/255.255.255.255/17/1701
                                                 Remote Addr  : 192.168.0.2/255.255.255.255/17/1701
                                             Encryption   : 3DES              Hashing      : MD5
                                                                           Encapsulation: Transport
                                       Rekey Int (T): 3600 Seconds     Rekey Left(T): 3333 Seconds
                                         Idle Time Out: 30 Minutes       Idle TO Left : 30 Minutes
                                              Bytes Tx     : 1336             Bytes Rx     : 14922
                                                Pkts Tx      : 25               Pkts Rx      : 156


                                                                             :L2TPOverIPSec
                                                                    Session ID   : 3
                                                                   Username     : test
                                                                 Assigned IP  : 10.4.5.15
                                           Encryption   : none             Auth Mode    : msCHAPV1
                                         Idle Time Out: 30 Minutes       Idle TO Left : 30 Minutes
                                              Bytes Tx     : 378              Bytes Rx     : 13431
                                                Pkts Tx      : 16               Pkts Rx      : 146
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات لاستكشاف أخطاء التكوين وإصلاحها. يتم عرض إخراج تصحيح الأخطاء للعينة أيضا.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض الأوامر بواسطة أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر تصحيح الأخطاء وأستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها قبل أن تستخدم أوامر **debug**.

- **debug crypto ips 7**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp 7**—يعرض مفاوضات ISAKMP للمرحلة 1.

إخراج تصحيح الأخطاء للعينة

جدار حماية PIX

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
 age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
                                                 NONE (0) total length : 256 + (13)
          Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
  Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
        Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
        Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
    Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
        Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
                                                                            ID
     Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
                                    acceptable  Matches global IKE entry # 2 2 #
 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
                                                    extended capabilities payload +
 (Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0
       with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
(Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0
       with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
         Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
      Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
       Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
       Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
    Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
                                                                          yload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo
                                                                            ad
                    Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V
                          (endor ID payload (version: 1.0.0, capabilities: 20000001
      Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco
                                                                    ASA GW VID
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
                                                                  aultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
```

```
...ing keys for Responder
 (Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0
) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR
VENDOR (13) + NONE (0) total length : 256 + (13
(Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0
with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def
aultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ
ously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi
ng hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
cting dpd vid payload
 (Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0
: with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length
80
```

Phase 1 completed succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = *---!*

```
192.168.0.2, PHASE 1 COMPL
ETED
:Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection
None
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do
(es not support keep-alives (type = None
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
.g P1 rekey timer: 21600 seconds
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
 + (b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5
NONE (0) total length : 164
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo
  te Proxy Host data in ID Payload:  Address 192.168.0.2, Protocol 17, Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca
    l Proxy Host data in ID Payload:  Address 172.16.1.1, Protocol 17, Port 1701
```

PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP *---!*

```
= 192.168.0.2, L2TP/IPSec se
.ssion detected
 Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed
old sa not found by addr
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe
er configured for crypto map: outside_dyn_map
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
ing IPSec SA payload
```

```
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S
    A Proposal # 1, Transform # 1 acceptable  Matches global IPSec SA entry # 20
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti
                                                                        !ng SPI
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
                                                SPI from key engine: SPI = 0xce9f6e19
```

Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP *---!*

```
                                                                = 192.168.0.2, oakley
                                                              constucting quick mode
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
                                                             cting blank hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
                                                               cting IPSec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
                                                            cting IPSec nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
                                                                    cting proxy ID
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi
                                                                   :tting Proxy Id
                                    Remote host: 192.168.0.2  Protocol 17  Port 1701
                                     Local host:  172.16.1.1  Protocol 17  Port 1701
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru
                                                               cting qm hash payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b
84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N
                                                          ONE (0) total length : 144
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1
              b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process
                                                                  ing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading
                                                                    all IPSEC SAs
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
                                                                !ing Quick Mode Key
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat
                                                                !ing Quick Mode Key
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego
 tiation complete for User ()  Responder, Inbound SPI = 0xce9f6e19, Outbound SPI
                                                                    0xd08f711b =
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got
                                              a KEY_ADD msg for SA: SPI = 0xd08f711b
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher
                                               received KEY_UPDATE, spi 0xce9f6e19 :
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin
                                                  .g P2 rekey timer: 3059 seconds
```

Phase 2 completes succesfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = *---!*

```
192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add
 L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#debug crypto
                                                                        ipsec 7
                          pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09
                                                                Rule ID: 0x028D78D8
                                    IPSEC: Deleted inbound permit rule, SPI 0x71933D09
                                                                Rule ID: 0x02831838
                               IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
                                                                Rule ID: 0x029134D8
                                    IPSEC: Deleted inbound VPN context, SPI 0x71933D09
                                                              VPN handle: 0x0048B284
                                 IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
                                                                Rule ID: 0x028DAC90
                                   IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
                                                                Rule ID: 0x02912AF8
                                   IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
```

```
                                        VPN handle: 0x0048468C
                    ,IPSEC: New embryonic SA created @ 0x01BFCF80
                                            ,SCB: 0x01C262D0
                                       Direction: inbound
                                     SPI      : 0x45C3306F
                                    Session ID: 0x0000000C
                                    VPIF num  : 0x00000001
                                           Tunnel type: ra
                                          Protocol   : esp
                                  Lifetime   : 240 seconds
                    ,IPSEC: New embryonic SA created @ 0x0283A3A8
                                            ,SCB: 0x028D1B38
                                     Direction: outbound
                                     SPI      : 0x370E8DD1
                                    Session ID: 0x0000000C
                                    VPIF num  : 0x00000001
                                           Tunnel type: ra
                                          Protocol   : esp
                                  Lifetime   : 240 seconds
                IPSEC: Completed host OBSA update, SPI 0x370E8DD1
              IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
                                          Flags: 0x00000205
                                          SA   : 0x0283A3A8
                                          SPI  : 0x370E8DD1
                                          MTU  : 1500 bytes
                                          VCID : 0x00000000
                                          Peer : 0x00000000
                                          SCB  : 0x028D1B38
                                       Channel: 0x01693F08
             IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
                                        VPN handle: 0x0048C164
                 IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
                                     Src addr: 172.16.1.1
                                Src mask: 255.255.255.255
                                    Dst addr: 192.168.0.2
                                Dst mask: 255.255.255.255
                                             Src ports
                                       Upper: 1701
                                       Lower: 1701
                                      Op   : equal
                                           Dst ports
                                       Upper: 1701
                                       Lower: 1701
                                      Op   : equal
                                        Protocol: 17
                                    Use protocol: true
                                       SPI: 0x00000000
                                        Use SPI: false
           IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
                                         Rule ID: 0x02826540
                IPSEC: New outbound permit rule, SPI 0x370E8DD1
                                     Src addr: 172.16.1.1
                                Src mask: 255.255.255.255
                                    Dst addr: 192.168.0.2
                                Dst mask: 255.255.255.255
                                             Src ports
                                          Upper: 0
                                          Lower: 0
                                      Op   : ignore
                                           Dst ports
                                          Upper: 0
                                          Lower: 0
                                      Op   : ignore
                                        Protocol: 50
```

```
                                                  Use protocol: true
                                                     SPI: 0x370E8DD1
                                                      Use SPI: true
                          IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
                                                  Rule ID: 0x028D78D8
                             IPSEC: Completed host IBSA update, SPI 0x45C3306F
                           IPSEC: Creating inbound VPN context, SPI 0x45C3306F
                                                  Flags: 0x00000206
                                                  SA   : 0x01BFCF80
                                                  SPI  : 0x45C3306F
                                                     MTU  : 0 bytes
                                                  VCID : 0x00000000
                                                  Peer : 0x0048C164
                                                  SCB  : 0x01C262D0
                                                 Channel: 0x01693F08
                         IPSEC: Completed inbound VPN context, SPI 0x45C3306F
                                                VPN handle: 0x0049107C
        IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
                                                  Flags: 0x00000205
                                                  SA   : 0x0283A3A8
                                                  SPI  : 0x370E8DD1
                                                  MTU  : 1500 bytes
                                                  VCID : 0x00000000
                                                  Peer : 0x0049107C
                                                  SCB  : 0x028D1B38
                                                 Channel: 0x01693F08
                          IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
                                                VPN handle: 0x0048C164
                           IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
                                                  Rule ID: 0x02826540
                      IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
                                                  Rule ID: 0x028D78D8
                           IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
                                                Src addr: 192.168.0.2
                                             Src mask: 255.255.255.255
                                                  Dst addr: 172.16.1.1
                                             Dst mask: 255.255.255.255
                                                      Src ports
                                                    Upper: 1701
                                                    Lower: 1701
                                                   Op   : equal
                                                      Dst ports
                                                    Upper: 1701
                                                    Lower: 1701
                                                   Op   : equal
                                                     Protocol: 17
                                                  Use protocol: true
                                                     SPI: 0x00000000
                                                      Use SPI: false
                       IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F
                                                  Rule ID: 0x02831838
                          IPSEC: New inbound decrypt rule, SPI 0x45C3306F
                                                Src addr: 192.168.0.2
                                             Src mask: 255.255.255.255
                                                  Dst addr: 172.16.1.1
                                             Dst mask: 255.255.255.255
                                                      Src ports
                                                    Upper: 0
                                                    Lower: 0
                                                   Op   : ignore
                                                      Dst ports
                                                    Upper: 0
                                                    Lower: 0
                                                   Op   : ignore
```

```
                                    Protocol: 50
                                Use protocol: true
                                   SPI: 0x45C3306F
                                     Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
                                 Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
                                Src addr: 192.168.0.2
                             Src mask: 255.255.255.255
                                 Dst addr: 172.16.1.1
                             Dst mask: 255.255.255.255
                                      Src ports
                                    Upper: 0
                                    Lower: 0
                                Op    : ignore
                                     Dst ports
                                    Upper: 0
                                    Lower: 0
                                Op    : ignore
                                   Protocol: 50
                                Use protocol: true
                                   SPI: 0x45C3306F
                                     Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
                                 Rule ID: 0x02912E50
```

أستكشاف الأخطاء وإصلاحها باستخدام ASDM

يمكنك إستخدام ASDM لتمكين التسجيل وعرض السجلات.

1. أخترت **تشكيل>خصائص>تسجيل>تسجيل إعداد**، **يمكن تسجيل**، وطقطقة **يطبق** in order to مكنت تسجيل.
2. أختر **مراقبة > تسجيل > مخزن السجل المؤقت > على مستوى التسجيل**، وحدد **مخزن التسجيل المؤقت**، وانقر فوق **عرض** لعرض السجلات.

المشكلة: الانقطاعات المتكررة

وضع الخمول / مهلة جلسة العمل

إذا تم تعيين مهلة الخمول على 30 دقيقة (الافتراضي)، فهذا يعني أنها تسقط النفق بعد عدم مرور حركة المرور عبرها لمدة 30 دقيقة. يتم قطع اتصال عميل VPN بعد 30 دقيقة بغض النظر عن إعداد مهلة الخمول ويصادف رسالة خطأ `.PEER_DELETE-IKE_DELETE_SPECIFIED`

قم بتكوين مهلة وضع الخمول ومهلة جلسة العمل كلا شيء لجعل النفق دائما قيد التشغيل حتى لا يتم إسقاط النفق أبدا.

دخلت ال **vpn-idle-timeout** أمر في مجموعة-policy تشكيل أسلوب أو في username تشكيل أسلوب in order to شكلت المستعمل مهلة فترة:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

شكلت الحد الأقصى وقت ل VPN توصيل مع ال **vpn-session-timeout** أمر في مجموعة-policy تشكيل أسلوب أو في username تشكيل أسلوب:

```
hostname(config)#group-policy DfltGrpPolicy attributes
```

```
hostname(config-group-policy)#vpn-session-timeout none
```

أستكشاف أخطاء Windows Vista وإصلاحها

مستخدم متزامن

أدخل Windows Vista L2TP/IPsec بعض التغييرات المعمارية التي منعت أكثر من مستخدم واحد متزامن من الاتصال بمعرف PIX/ASA طرفي طرفي الرأس. لا يحدث هذا السلوك على Windows 2K/XP. قامت Cisco بتنفيذ حل بديل لهذا التغيير بدءا من الإصدار 7.2(3) والإصدارات الأحدث.

يتعذر على كمبيوتر Vista الاتصال

إذا لم يتمكن كمبيوتر Windows Vista من توصيل خادم L2TP، فتحقق من تكوين MSCHAP-V2 فقط أسفل سمات PPP على DefaultRAGgroup.

معلومات ذات صلة

- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- دعم منتج برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- صفحة دعم RADIUS
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- طلبات التعليقات (RFCs)
- بروتوكول نفق الطبقة الثانية (L2TP)
- 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).