تكوين L2TP عبر IPsec بين Windows 8 PC و ASA باستخدام مفاتيح مشترك مسبقا

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين بروتوكول الاتصال النفقي للطبقة 2 (L2TP) عبر IPsec باستخدام مفاتيح مشترك مسبقا بين جهاز الأمان القابل للتكيف (ASA) من Cisco والعميل الأصلي لنظام التشغيل Windows 8.

يوفر L2TP عبر أمان بروتوكول الإنترنت (IPsec) إمكانية نشر حل الشبكة الخاصة الظاهرية (VPN) لـ L2TP وإدارته بجانب خدمات VPN وجدار الحماية لـ IPsec في نظام أساسي واحد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- اتصال IP من جهاز العميل إلى ASA. الاختبار الاتصال، حاول إختبار اتصال عنوان IP الخاص ب ASA من نقطة نهاية العميل والعكس
- تضمنت أن UDP ميناء 500 و 4500 وبغلف أمن حمولة بروتوكول (ESP) لا يمنع في أي مكان على مسار التوصيل

القيود

- يدعم L2TP عبر IPsec فقط IKEv1. IKEv2 غير مدعوم.
- يتيح L2TP مع IPsec على ASA إمكانية تفاعل LNS مع عملاء VPN الأصليين المدمجين في أنظمة التشغيل مثل Windows و Mac OS X و Android و Cisco IOS. يتم دعم L2TP عبر IPsec فقط، ولا يتم دعم L2TP الأصلي نفسه على ASA.
- الحد الأدنى لفترة بقاء قترانأ مان IPsec الذي يدعمه عميل Windows هو 300 ثانية. إذا تم تعيين مدة البقاء على ASA إلى أقل من 300 ثانية، فإن عميل Windows يتجاهلها ويستبدلها بفترة حياة تبلغ 300 ثانية.
- يدعم ASA بروتوكول الاتصال من نقطة إلى نقطة (PPP) فقط مصادقة كلمة المرور من Microsoft، (CHAP) وبروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (PAP) و1 و2، على قاعدة البيانات المحلية. يتم تنفيذ بروتوكول المصادقة الإصداران. لذلك، إذا كان المستخدم البعيد ينتمي إلى مجموعة نفق تم تكوينها باستخدام أوامر **المصادقة eap-proxy** و **authentication chap**، وتم تكوين ASA لاستخدام قاعدة البيانات المحلية، فلن يمكن ذلك المستخدم الاتصال.

أنواع مصادقة PPP المدعومة

يوضح الجدول في ما يلي أنواع مصادقة PPP المدعومة إلى ASA عبر اتصالات IPsec عبر L2TP:

دعم خادم AAA لأنواع مصادقة PPP

أنواع مصادقة PPP المدعومة	نوع خادم AAA
MSCHAPv2 و MSCHAPv1 و PAP	محلي
EAP-Proxy و MSCHAPv2 و MSCHAPv1 و CHAP و PAP	RADIUS
MSCHAPv1 و CHAP و PAP	TACACS+
PAP	LDAP
PAP	NT
PAP	Kerberos
SDI	SDI

خصائص نوع مصادقة PPP

الخصائص	نوع المصادقة	الكلمة الأساسية
يستجيب لتحدي الخادم، يرجع العميل [challenge plus password] المشفر باسم مستخدم نصي واضح. هذا البروتوكول أكثر أمانا من PAP، ولكنه لا يوفر تشفير البيانات.	CHAP	**chap**
يتيح EAP الذي يسمح للجهاز الأمان بتوكيل عملية مصادقة PPP إلى خادم مصادقة RADIUS خارجي.	EAP	**eap proxy**
يشبه بروتوكول CHAP ولكن أكثر أمانا من حيث أنه يخزن كلمات المرور المشفرة وليس كلمات المرور النصية كما في بروتوكول CHAP. كما يعمل هذا البروتوكول على إنشاء مفاتيح تشفير البيانات باستخدام MPPE.	Microsoft CHAP، الإصدار 1 Microsoft CHAP، الإصدار 2	**ms-chap-v1** **ms-chap-v2**
يرجى إرسال اسم مستخدم وكلمة مرور نصية واضحة أثناء المصادقة وهي غير آمنة.	PAP	**pap**

المكونات المستخدمة

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

- Cisco 5515 Series ASA أن يركض البرمجية صيغة 9.4(1)
- عميل L2TP/IPSec (Windows 8)

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco ASA 5500 Series Security Appliance 8.3(1) وأ إصدار أحدث.

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية](#) للحصول على مزيد من المعلومات حول اصطلاحات المستندات

معلومات أساسية

بروتوكول الاتصال النفقي للطبقة 2 (L2TP) هو بروتوكول اتصال VPN النفقي الذي يسمح للعملاء عن بعد باستخدام شبكة IP العامة للاتصال بشكل آمن بخوادم شبكة الشركة الخاصة. يستخدم L2TP PPP عبر UDP (المنفذ 1701) لتقنية البيانات.

يستند بروتوكول L2TP إلى طراز العميل/الخادم. يتم تقسيم الوظيفة بين خادم شبكة L2TP (LNS) ومركز الوصول إلى L2TP (LAC). يعمل LNS عادة على بوابة شبكة مثل ASA في هذه الحالة، بينما يمكن أن يكون LAC خادم وصول إلى الشبكة عن طريق الطلب الهاتفي (NAS) أو جهاز نقطة نهاية مع عميل L2TP مجمع مثل Microsoft Windows أو Apple iPhone أو Android.

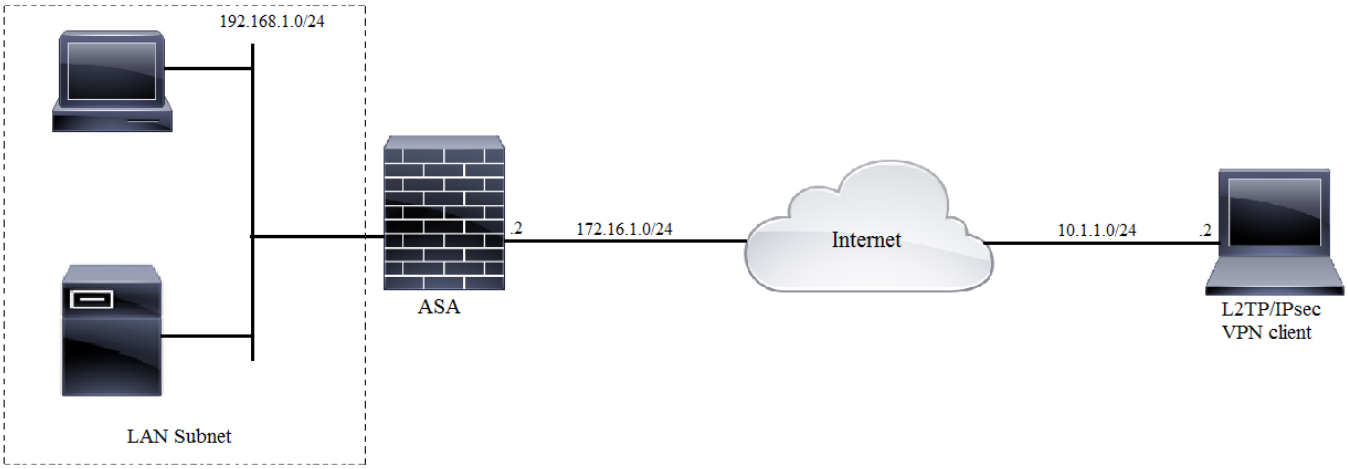
التكوين

يقدم هذا القسم 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 خاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

الرسم التخطيطي للشبكة

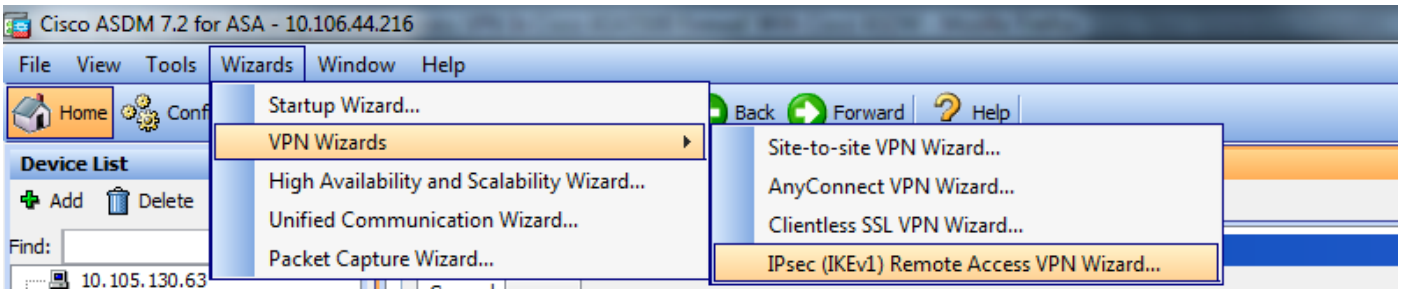


تكوين النفق الكامل

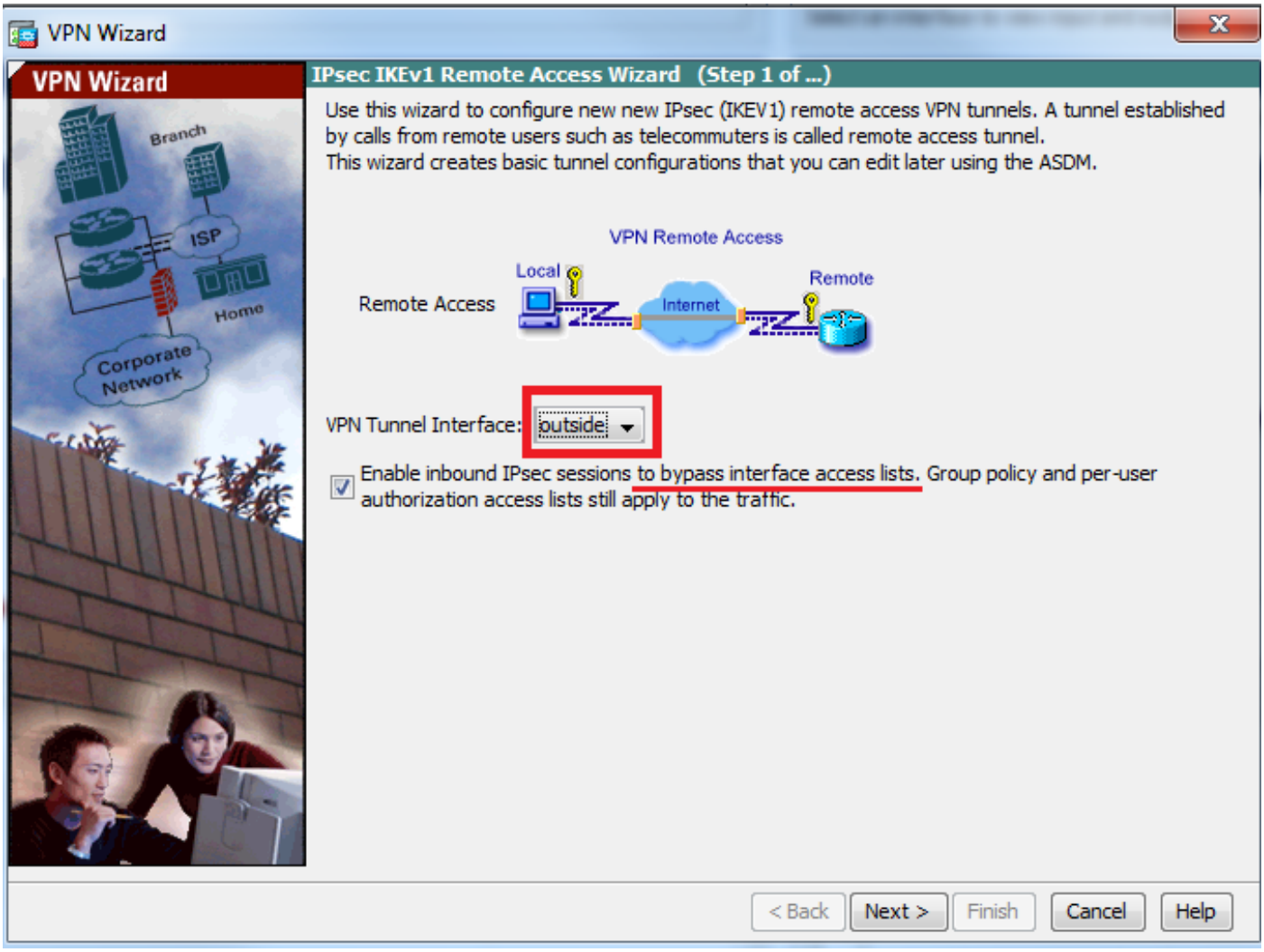
تكوين ASA باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM)

أكمل الخطوات التالية:

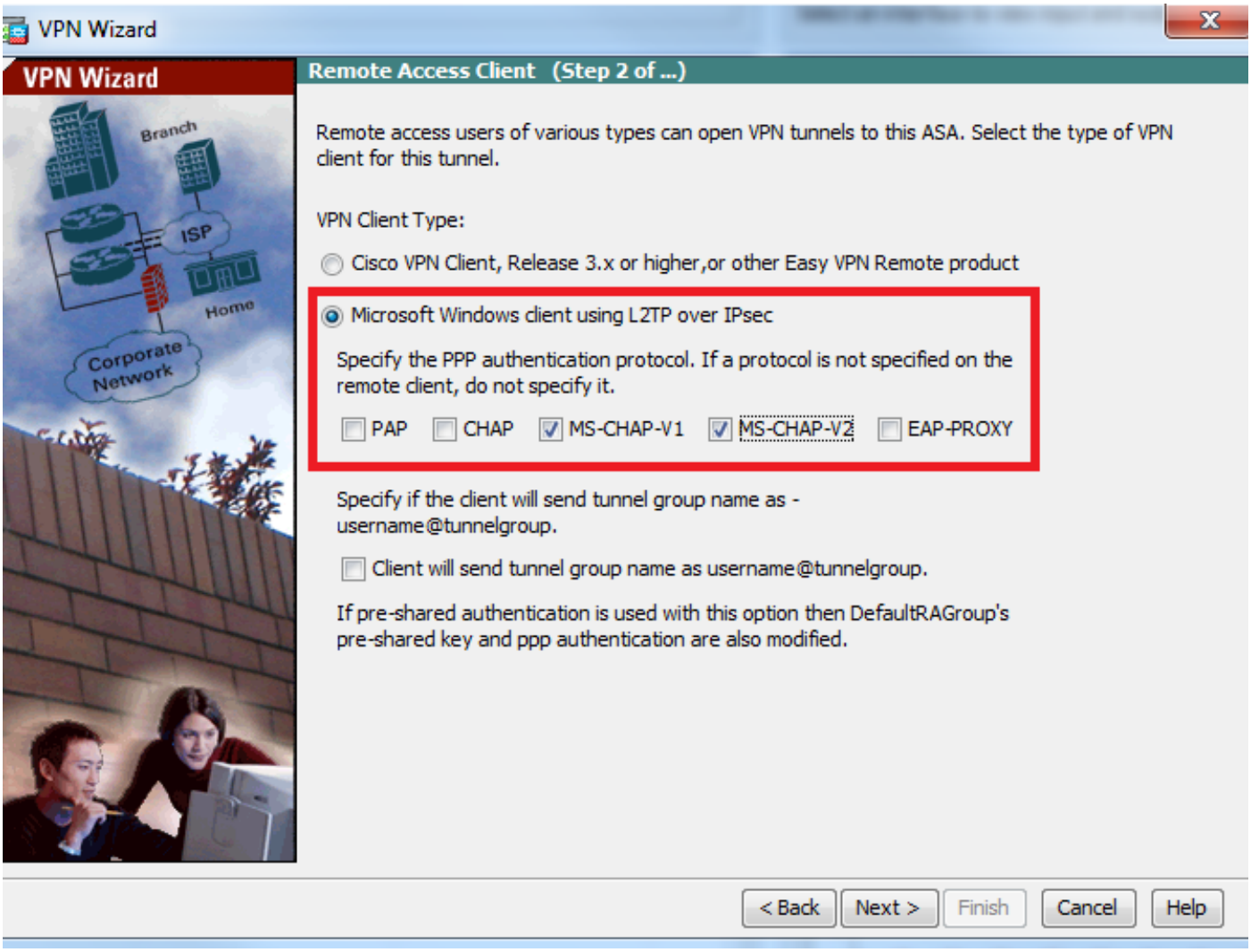
الخطوة 1. سجل الدخول إلى إدارة قاعدة بيانات المحول (ASDM)، وانتقل إلى **المعالجات > معالجات VPN > معالج IPsec (IKEv1) للوصول عن بعد إلى شبكة VPN**.



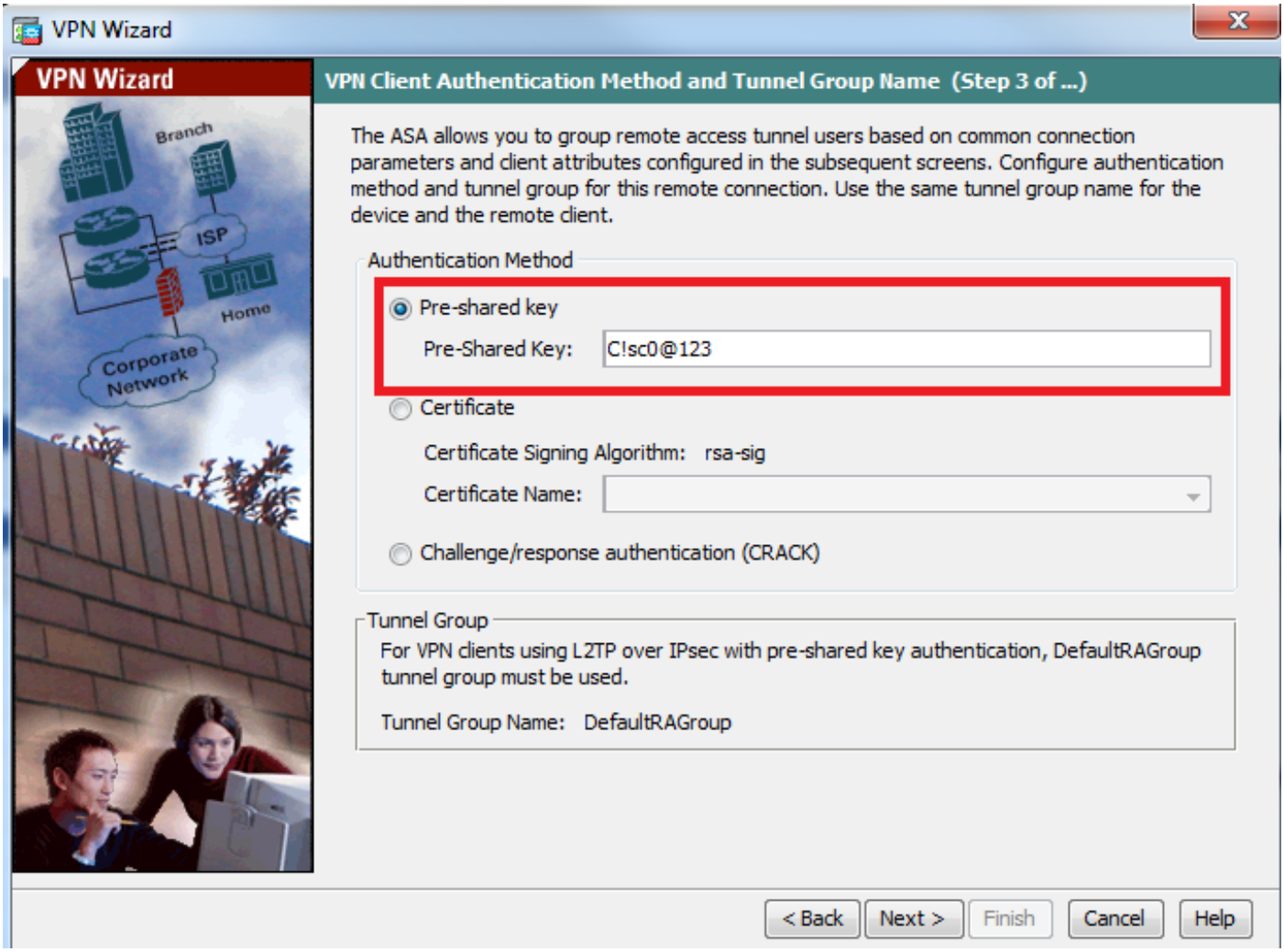
الخطوة 2. تظهر نافذة إعداد VPN للوصول عن بعد. من القائمة المنسدلة، أختر الواجهة التي يجب إنهاء نفق VPN عليها. في هذا المثال، يتم توصيل الواجهة الخارجية بشبكة WAN وبالتالي إنهاء أنفاق VPN على هذه الواجهة. الاحتفاظ بالمربع **تمكين جلسات عمل IPSec الواردة لتجاوز قوائم الوصول إلى الواجهة. لا يزال نهج المجموعة وقوائم الوصول إلى التخويل لكل مستخدم يتم تطبيقها على حركة المرور** التي تم فحصها بحيث لا يلزم تكوين قائمة الوصول الجديدة على الواجهة الخارجية للسماح للعملاء بالوصول إلى المواد الداخلية. انقر فوق **Next (التالي)**.



الخطوة 3. أخترت عرض في هذه الصورة، الزبون نوع **كعميل Microsoft Windows يستعمل** PAP غير آمن لأن PPP مصادقة كبروتوكول **MS-CHAP-V2** و**MS-CHAP-V1** و**IPSec عبر L2TP**. **بعد** نقر واحد مصادقة خادم محلية البيانات قاعدة مع مدعومة غير الأخرى المصادقة وأنواع **ذلك**.

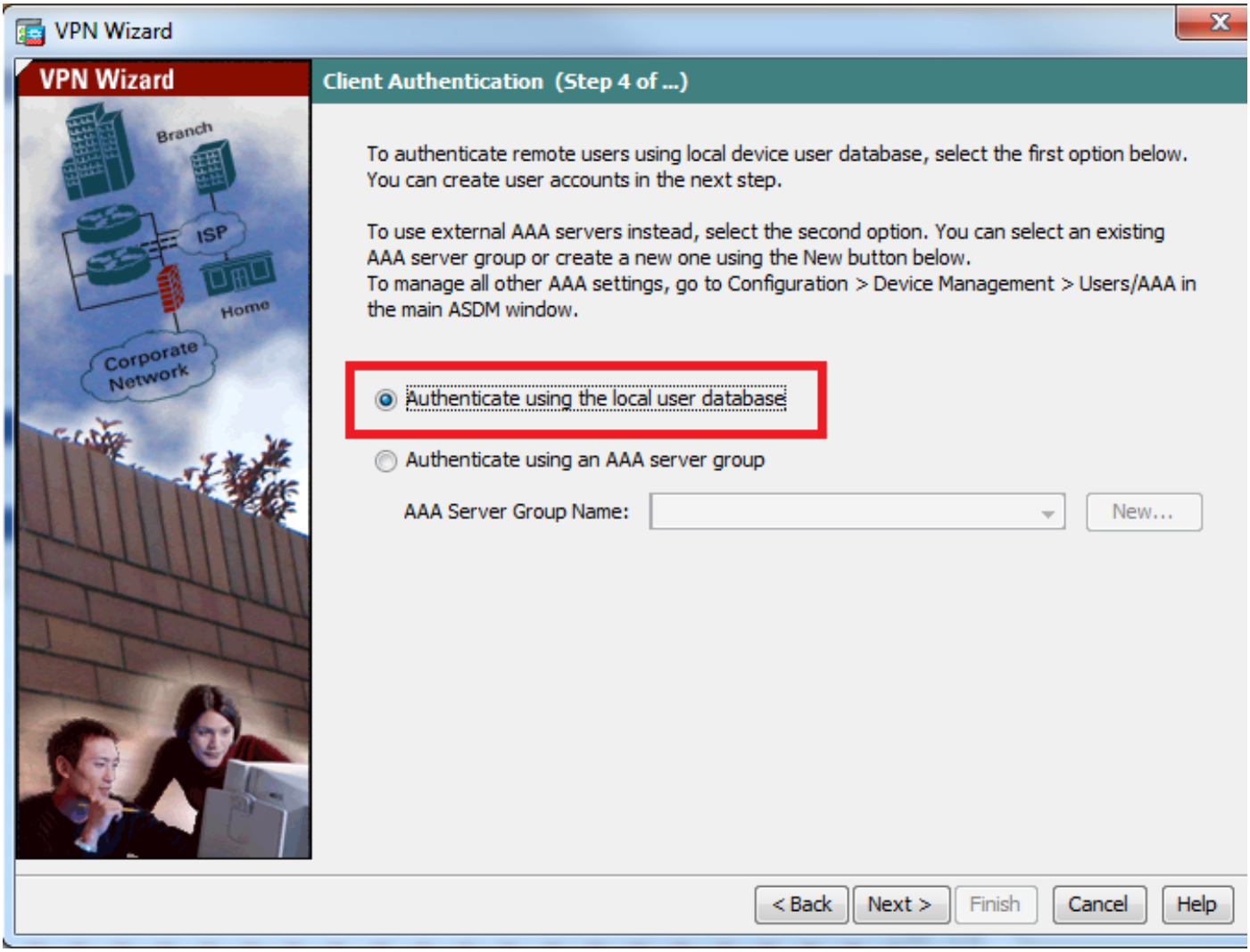


الخطوة 4. أختر أسلوب المصادقة كمفتاح **مشترك مسبقا** واكتب المفتاح المشترك مسبقا الذي يجب أن يكون مماثل على جانب العميل أيضا وانقر **بعد ذلك**، كما هو موضح في هذه الصورة.

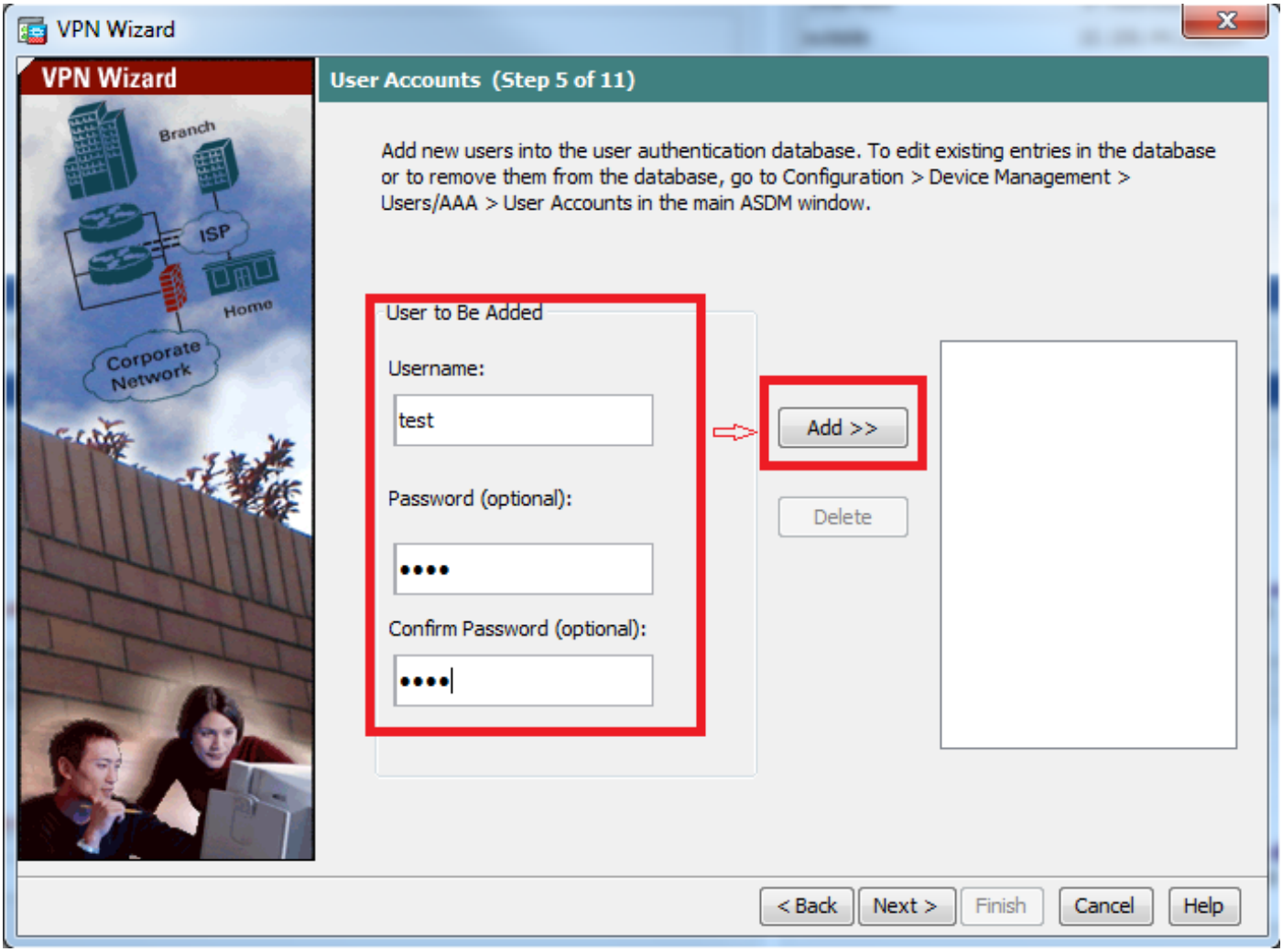


الخطوة 5. حدد طريقة لمصادقة المستخدمين الذين يحاولون L2TP عبر إتصالات IPsec. يمكن إستخدام خادم مصادقة AAA خارجي أو قاعدة بيانات محلية خاصة به. أخترت **يصدق يستعمل القاعدة معطيات مستعمل محلي** إن يريد أنت أن يصدق الزبون مقابل قاعدة معطيات محلي من ASA وطقطقة **بعد ذلك.**

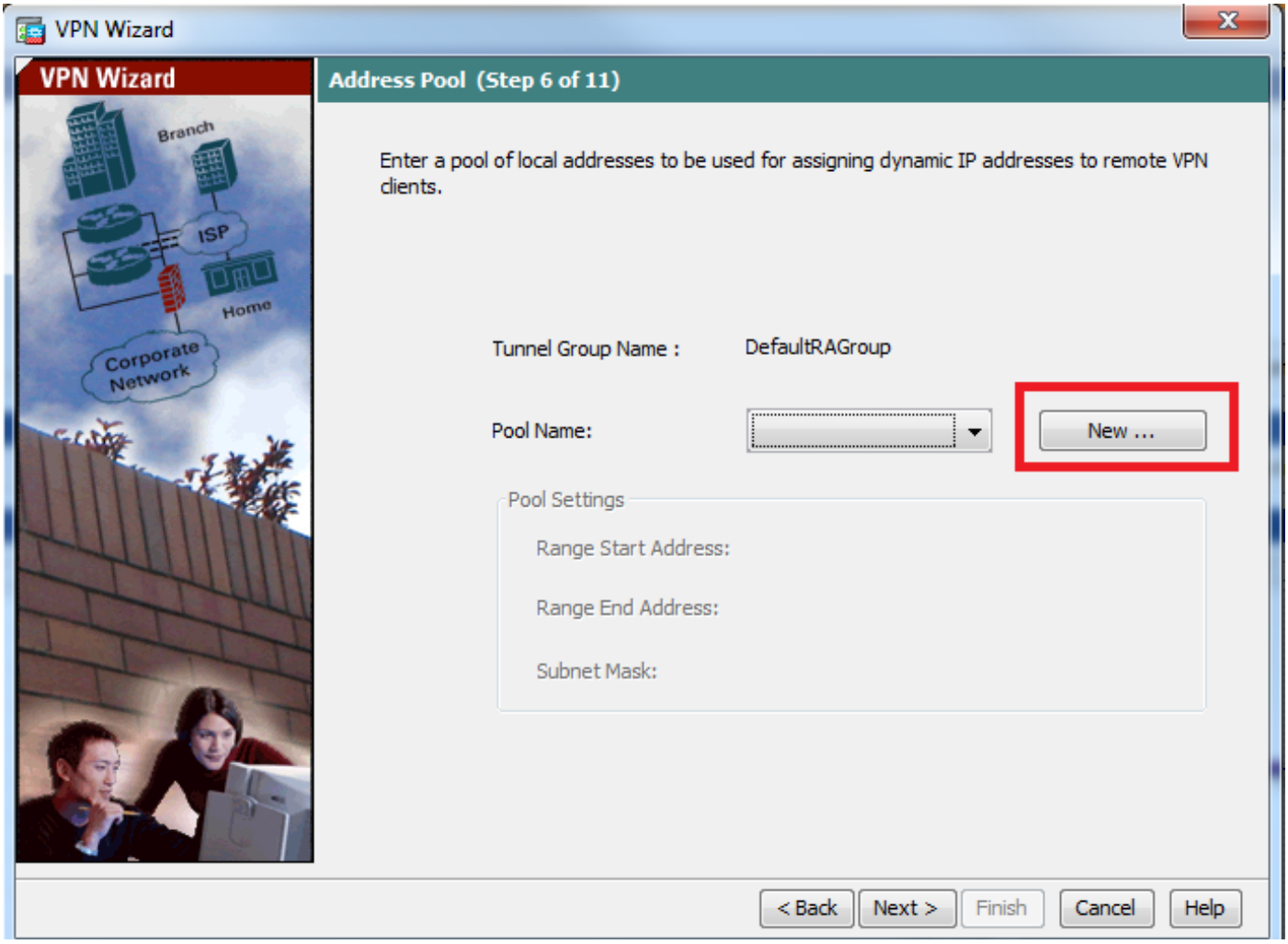
ملاحظة: يرجى الرجوع إلى تكوين مصادقة RADIUS لمستخدمي VPN لمصادقة المستخدمين باستخدام خادم AAA الخارجي.



الخطوة 6. لإضافة مستخدمين جدد إلى قاعدة البيانات المحلية لمصادقة المستخدم، أدخل اسم المستخدم وكلمة المرور ثم انقر على **إضافة** أو يمكن إستخدام حسابات مستخدمين موجودة أخرى في قاعدة البيانات، كما هو موضح في هذه الصورة. انقر فوق **Next (التالي)**.

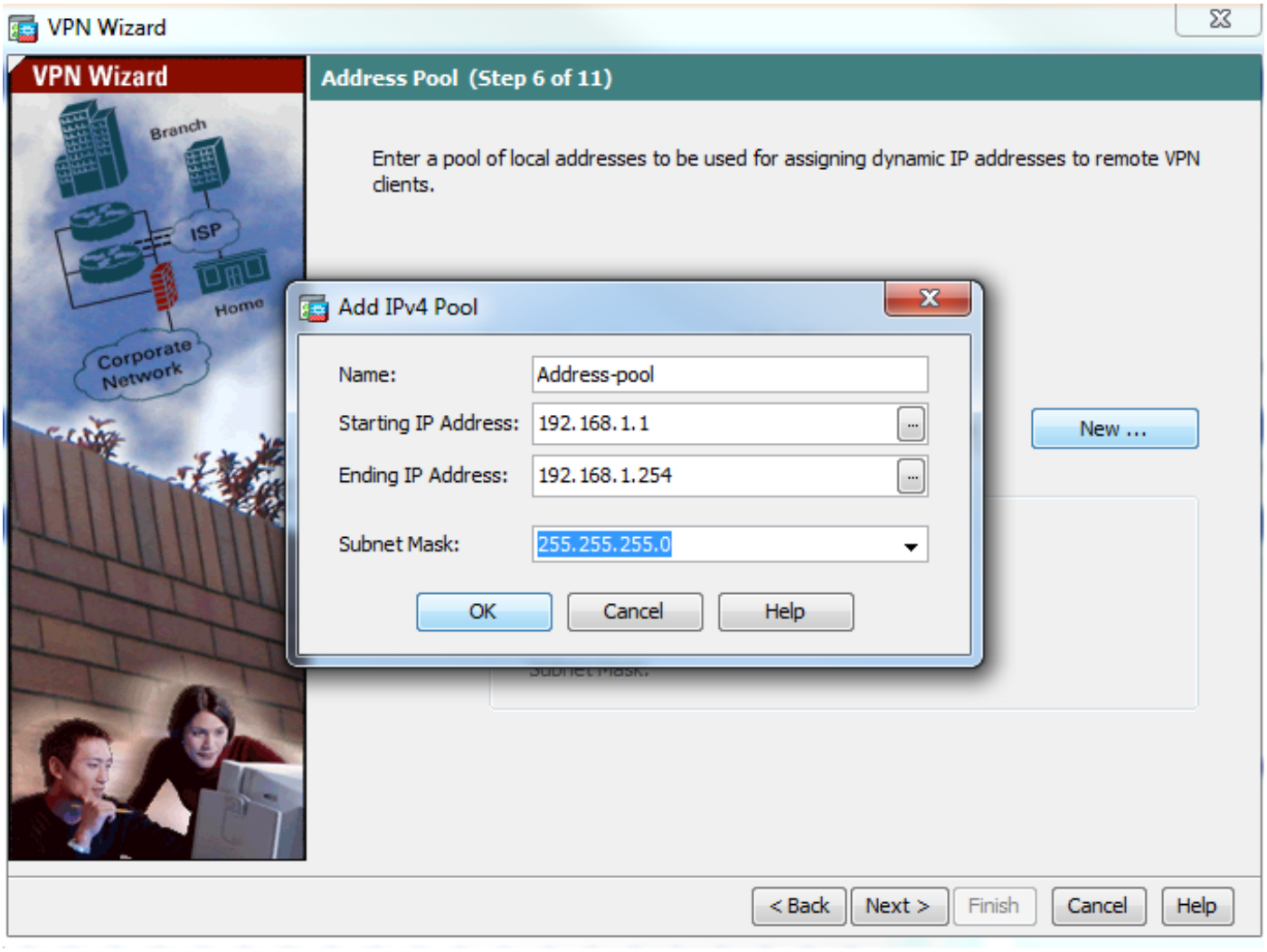


الخطوة 7. من القائمة المنسدلة، أختر تجمع العناوين الذي سيتم إستخدامه لتعيين عنوان IP إلى العملاء. لإنشاء تجمع عناوين جديد، انقر فوق **جديد**، كما هو موضح في هذه الصورة.

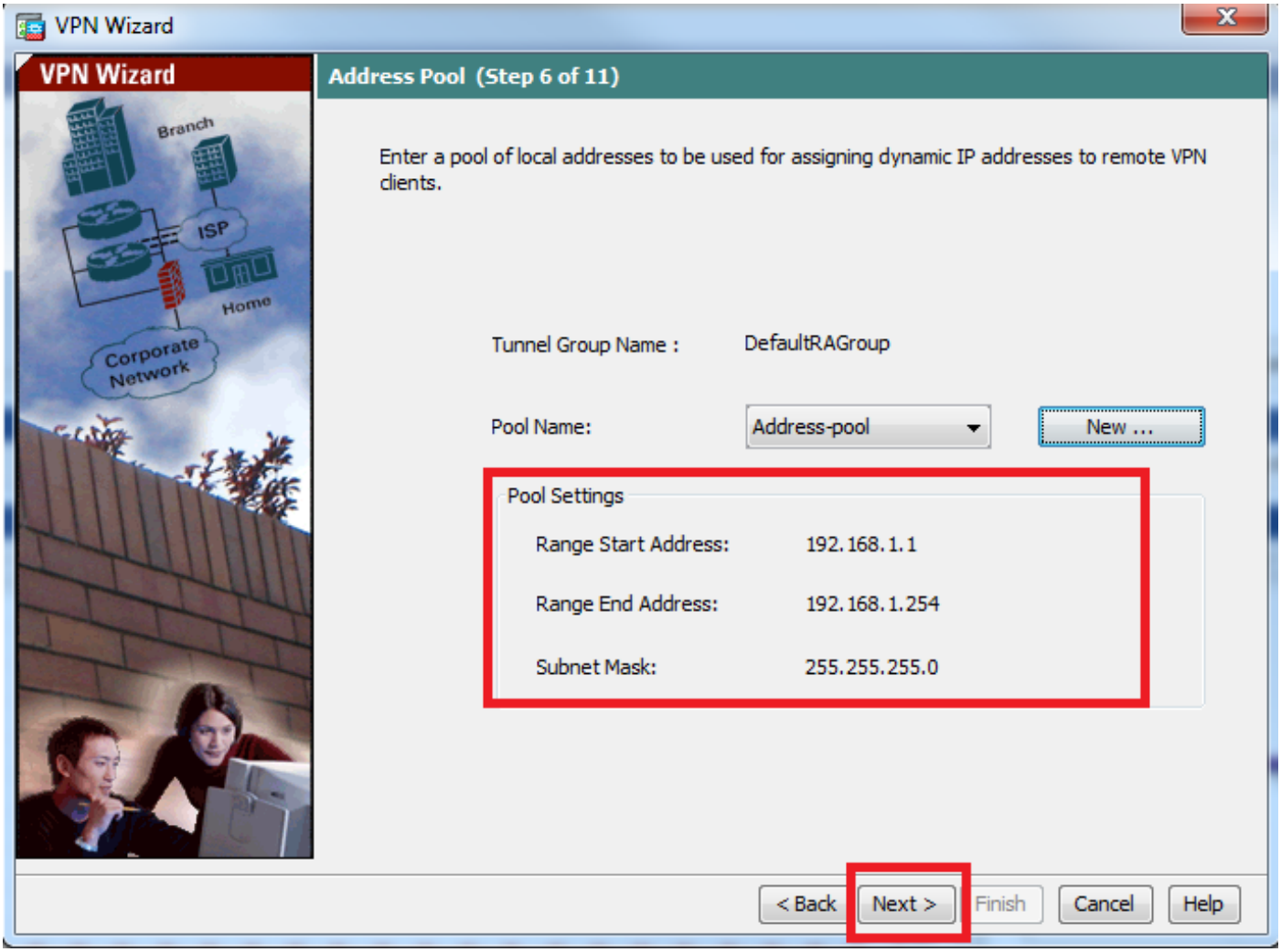


الخطوة 8. يظهر مربع الحوار **إضافة تجمع IPv4**.

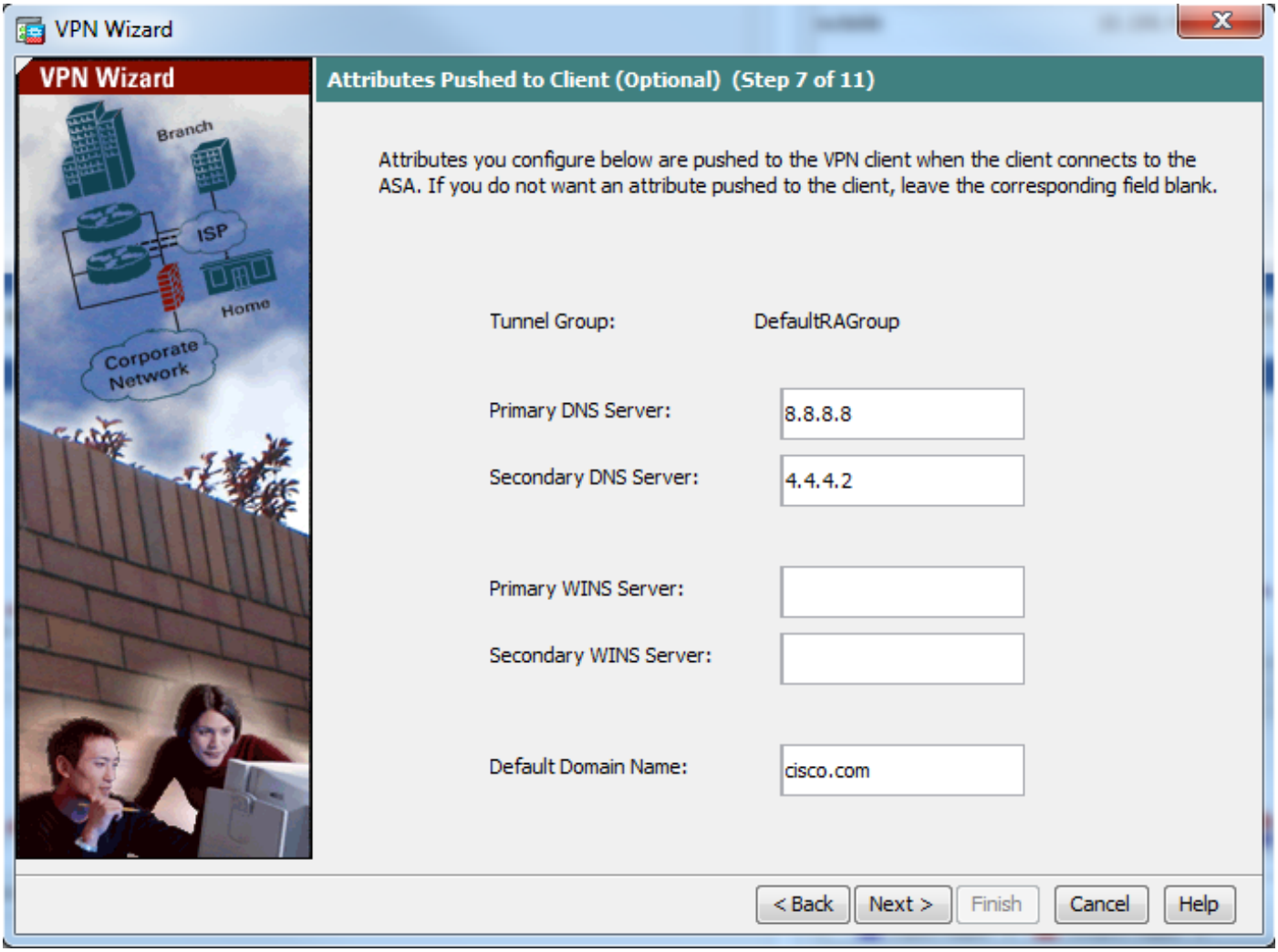
1. أدخل اسم تجمع عناوين IP الجديد.
2. أدخل عناوين IP البداية والنهاية.
3. أدخل قناع الشبكة الفرعية وانقر فوق **موافق**.



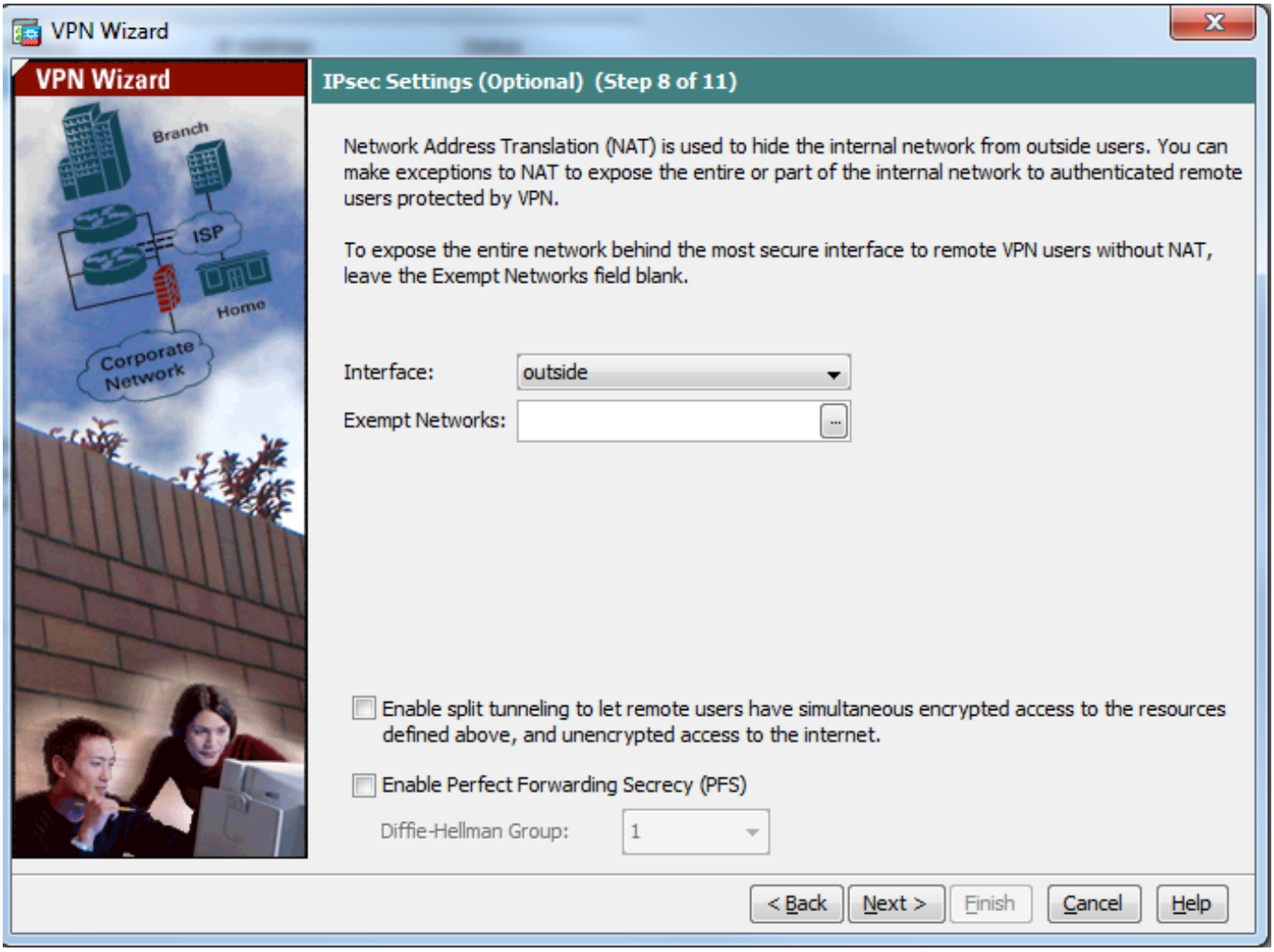
الخطوة 9. دقق التجمع عملية إعداد وطقطقة **بعد ذلك.**



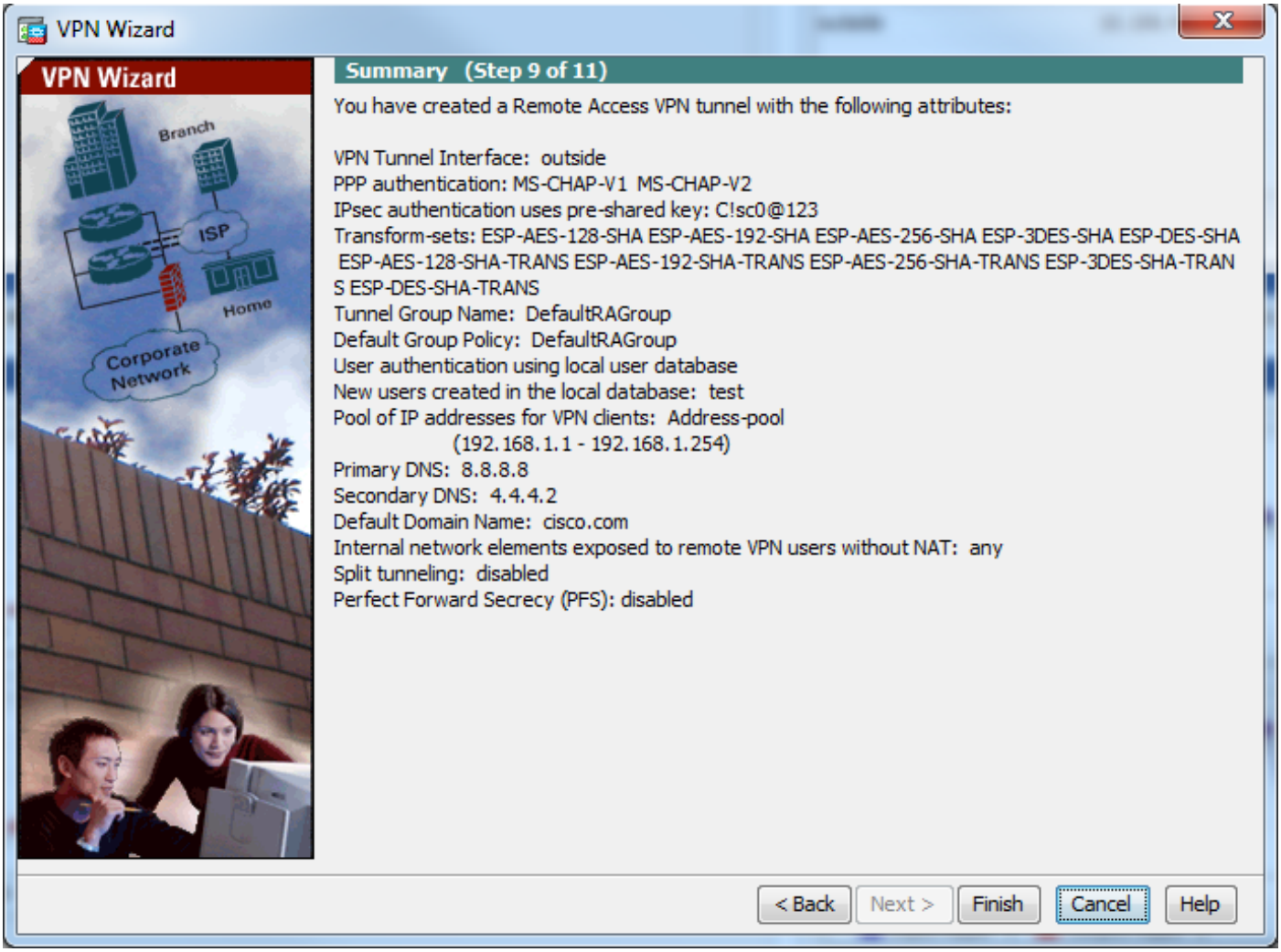
الخطوة 10. قم بتكوين السمات التي سيتم دفعها إلى العملاء أو أتركها فارغة ثم انقر فوق **التالي**.



الخطوة 11: تأكد من أن مربع **تمكين سرية إعادة التوجيه الكاملة (PFS)** غير محدد لأن بعض أنظمة العملاء الأساسية لا تدعم هذه الميزة. **قم بتمكين الاتصال النفقي المنقسم للسماح للمستخدمين البعيدين بالوصول المشفر المتزامن إلى الموارد المحددة أعلاه،** ويتم إلغاء تحديد **الوصول غير المشفر إلى** مربع **الإنترنت** مما يعني تمكين الاتصال النفقي الكامل حيث يتم إرسال جميع حركات مرور البيانات (بما في ذلك حركة مرور الإنترنت) من جهاز العميل إلى ASA عبر نفق VPN. انقر فوق **Next (التالي).**



الخطوة 12. راجع معلومات الملخص ثم انقر فوق **إنهاء**.



تكوين ASA باستخدام CLI

الخطوة 1. تكوين معلمات نهج المرحلة الأولى ل IKE.

يتم إستخدام هذه السياسة لحماية حركة مرور البيانات بين الأقران (أي أنها تحمي المفاتيح المشترك مسبقا ومفاوضات المرحلة 2)

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

الخطوة 2. تكوين مجموعة التحويل.

يحتوي على معلمات نهج المرحلة 2 ل IKE التي يتم إستخدامها لحماية حركة مرور البيانات. نظرا لأن عميل Windows L2TP/IPsec يستخدم وضع النقل IPsec، قم بتعيين الوضع على النقل. الوضع الافتراضي هو وضع النفق

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

الخطوة 3. تكوين الخريطة الديناميكية.

مع حصول عملاء Windows على عنوان IP ديناميكي ل ISP أو خادم DHCP محلي (مثال مودم)، ال

يعلم ASA عن عنوان IP النظير وهذا يسبب مشكلة في تكوين نظير ساكن إستاتيكي على نهاية ASA. لذلك، يجب التعامل مع تكوين التشفير الديناميكي حيث لا يتم بالضرورة تعريف جميع المعاملات ويتم التعرف بشكل ديناميكي على المعاملات المفقودة لاحقا، نتيجة لمفاوضات IPSec من العميل.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA
```

الخطوة 4. ربط الخريطة الديناميكية بخريطة التشفير الثابتة وتطبيق خريطة التشفير وتمكين IKEv1 على الواجهة الخارجية

لا يمكن تطبيق خريطة التشفير الديناميكية على واجهة وبالتالي ربطها بخريطة التشفير الثابتة. يجب أن تكون مجموعات التشفير الديناميكية أقل خرائط التشفير أولوية في مجموعة خريطة التشفير (أي يجب أن تحتوي على أعلى أرقام التسلسل) حتى يتمكن ASA من تقييم خرائط التشفير الأخرى أولا. إنه يفحص مجموعة خريطة التشفير الديناميكية فقط عندما لا تتطابق الإدخالات الخريطة الأخرى (الثابتة).

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

الخطوة 5. إنشاء تجمع عناوين IP

قم بإنشاء مجموعة من العناوين التي يتم من خلالها تعيين عناوين IP بشكل ديناميكي إلى عملاء VPN البعيدة. تجاهل هذه الخطوة لاستخدام التجمع الموجود على ASA.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

الخطوة 6. تكوين نهج المجموعة

تعريف نهج المجموعة كنهج داخلي مما يعني سحب السمات من قاعدة البيانات المحلية.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

> **ملاحظة**: يمكن تكوين اتصالات L2TP/IPsec باستخدام نهج المجموعة الافتراضي (DfltGrpPolicy) أو نهج مجموعة معرف من قبل المستخدم. في تلك الحالتين، يجب تكوين نهج المجموعة لاستخدام بروتوكول الاتصال النفقي ل L2TP/IPsec. قم بتكوين l2tp-ipSec على سمة بروتوكول VPN على نهج المجموعة الافتراضي الذي سيتم توريثه إلى نهج المجموعة المعرف من قبل المستخدم إذا لم يتم تكوين السمة VPN-protocol عليه.

قم بتكوين السمات مثل بروتوكول نفق VPN (في حالتنا، هو l2tp-ipsSec)، واسم المجال، وعنوان IP الخاص بخادم WINS وعنوان IP الخاص بخادم WINS وحسابات المستخدم الجديدة

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

تكوين أسماء المستخدمين وكلمات المرور على الجهاز بالإضافة إلى استخدام المصادقة والتفويض والمحاسبة (AAA). إذا كان المستخدم يعمل عميل L2TP يستخدم Microsoft CHAP الإصدار 1 أو الإصدار 2، وتم تكوين ASA للمصادقة مقابل قاعدة البيانات المحلية، فيجب تضمين الكلمة الأساسية mschap. على سبيل المثال، اسم المستخدم <username> كلمة المرور <password> mschap.

```
ciscoasa(config-group-policy)# username test password test mschap
```

الخطوة 7. تكوين مجموعة النفق

قم بإنشاء مجموعة نفق باستخدام الأمر **tunnel-group**، وحدد اسم تجمع العناوين المحلي المستخدم لتخصيص عنوان IP إلى العميل. إذا كانت طريقة المصادقة هي مفتاح مشترك مسبقا، فيجب أن يكون اسم مجموعة النفق DefaultRAGgroup حيث لا يوجد خيار على العميل لتحديد مجموعة النفق وبالتالي يقع على مجموعة النفق الافتراضية فقط. ربط نهج المجموعة بمجموعة النفق باستخدام الأمر default-group-policy

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

> **ملاحظة**: يجب تكوين ملف تعريف الاتصال الافتراضي (مجموعة النفق)، DefaultRAGgroup، في حالة إجراء مصادقة تستند إلى مفتاح مشترك مسبقا. في حالة إجراء مصادقة قائمة على الشهادة، يمكن إختيار توصيف توصيل معرف من قبل المستخدم بناء على معرفات الشهادات

أستخدم الأمر **tunnel-group ipSec-attributes** لإدخال وضع تكوين سمة IPsec لتعيين المفتاح المشترك مسبقا.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)#  ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

قم بتكوين بروتوكول مصادقة PPP باستخدام أمر **عون المصادقة** من وضع سمات PPP لمجموعة النفق. تعطيل CHAP الذي يتم تمكينه بشكل افتراضي لأنه غير مدعوم في حالة تكوين خادم AAA كقاعدة بيانات محلية.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

الخطوة 8. تكوين إستثناء NAT

قم بتكوين إستثناء NAT حتى يتمكن العملاء من الوصول إلى الموارد الداخلية المتصلة بالواجهات الداخلية (في هذا المثال، يتم توصيل الموارد الداخلية بالواجهة الداخلية).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

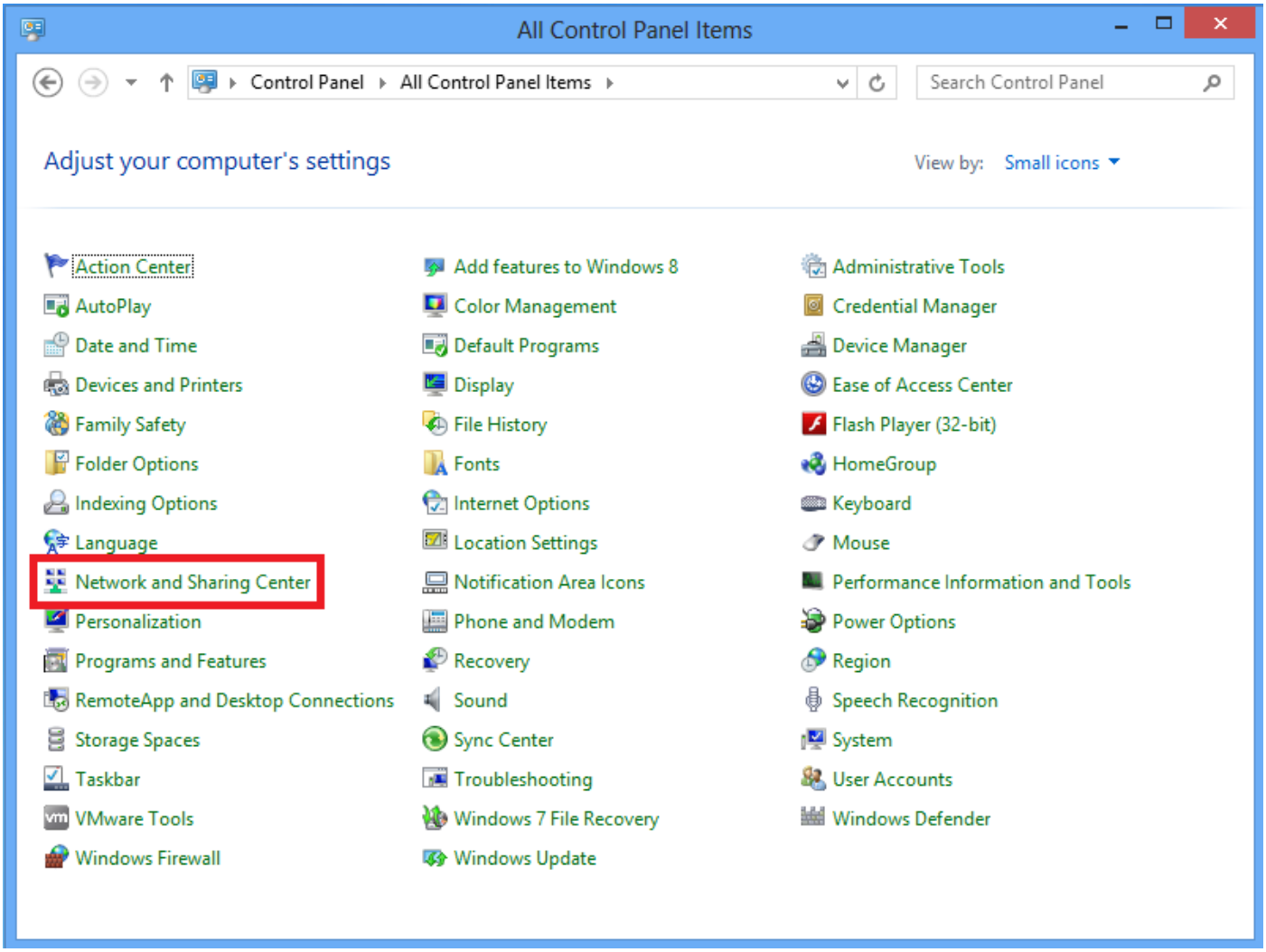
إكمال نموذج التكوين

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

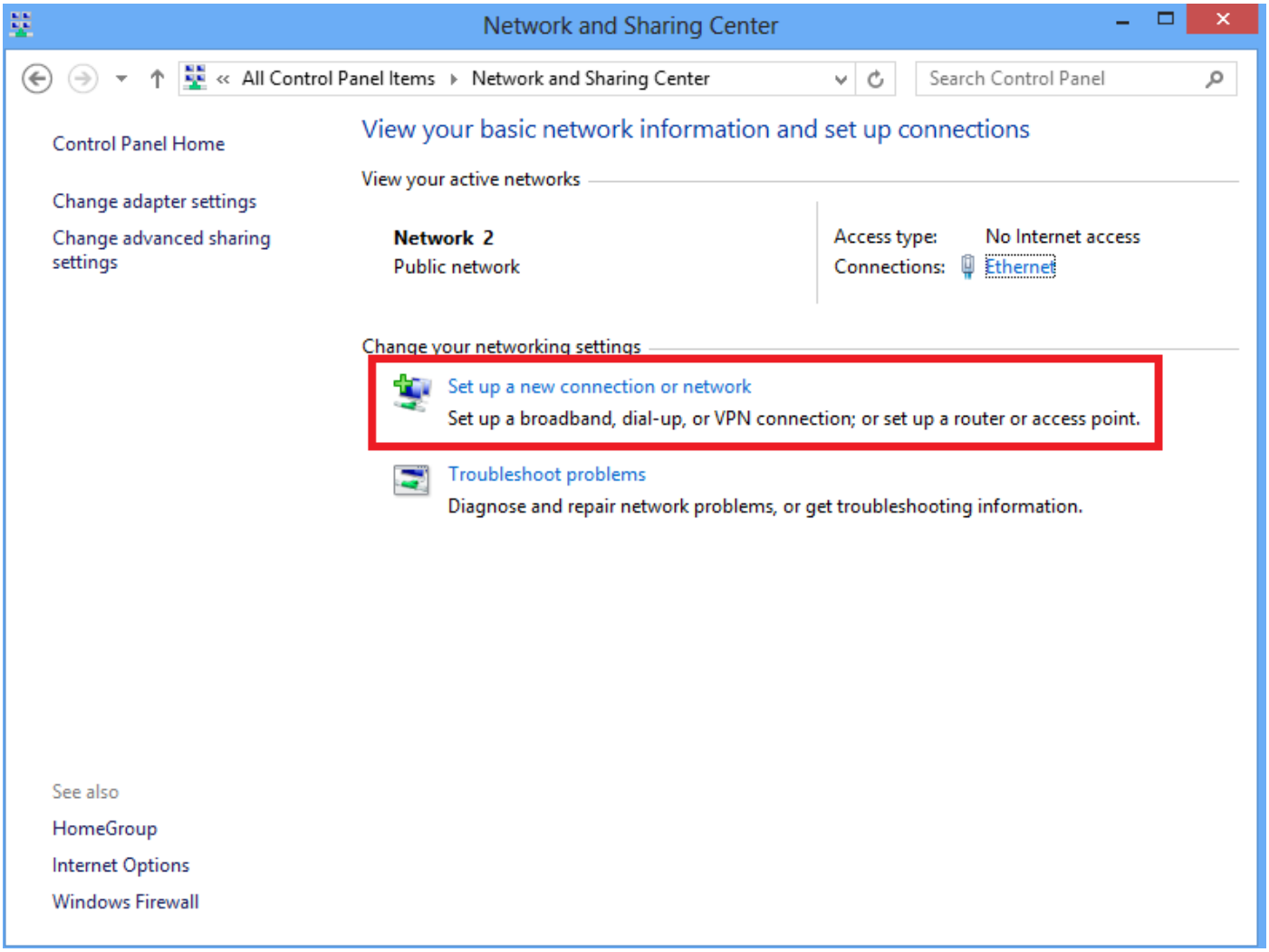
```
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

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

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

تكوين عميل Windows 8 L2TP/IPsec

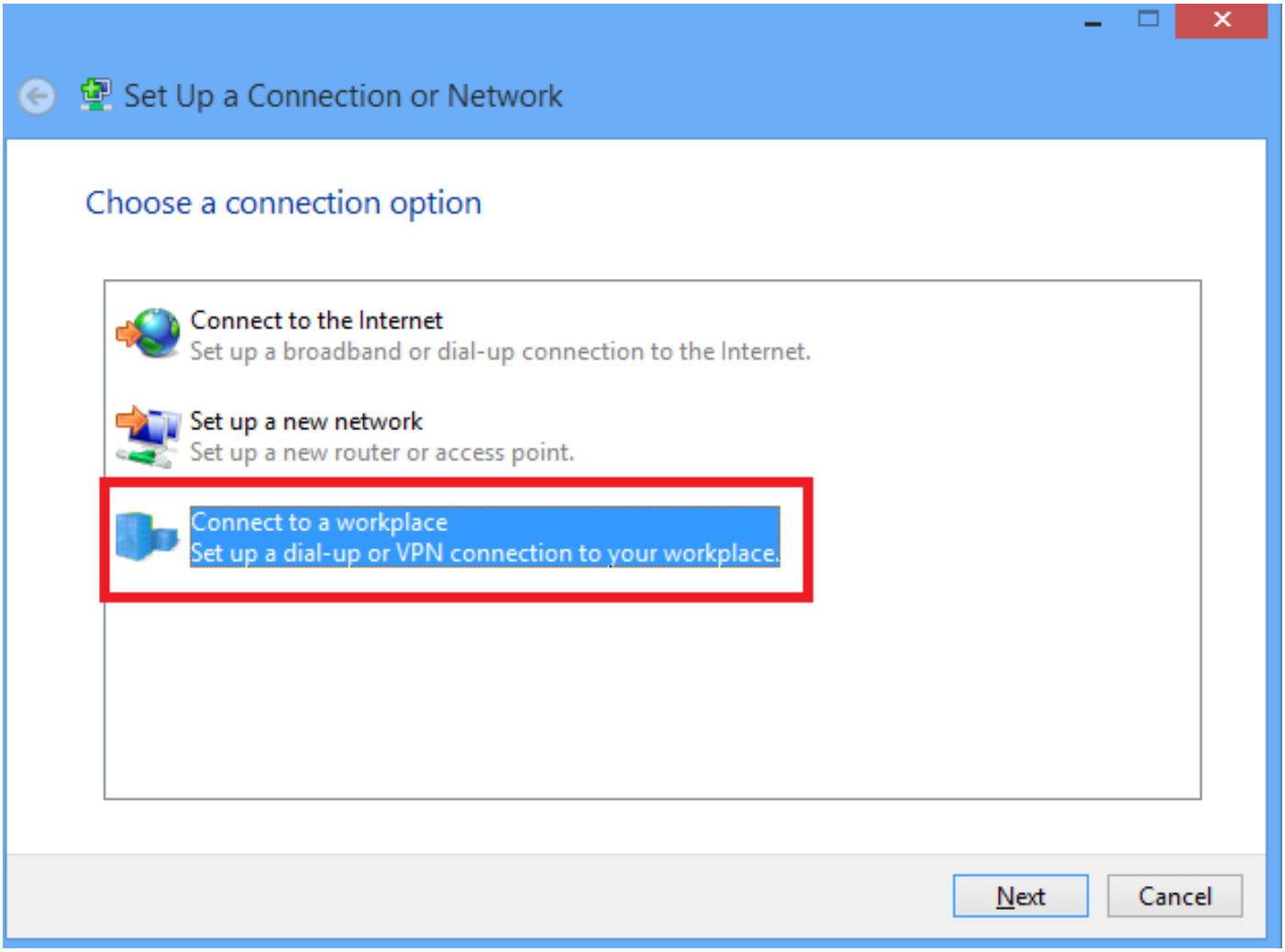
1. افتح "لوحة التحكم" وحدد "مركز الشبكات والمشاركة".



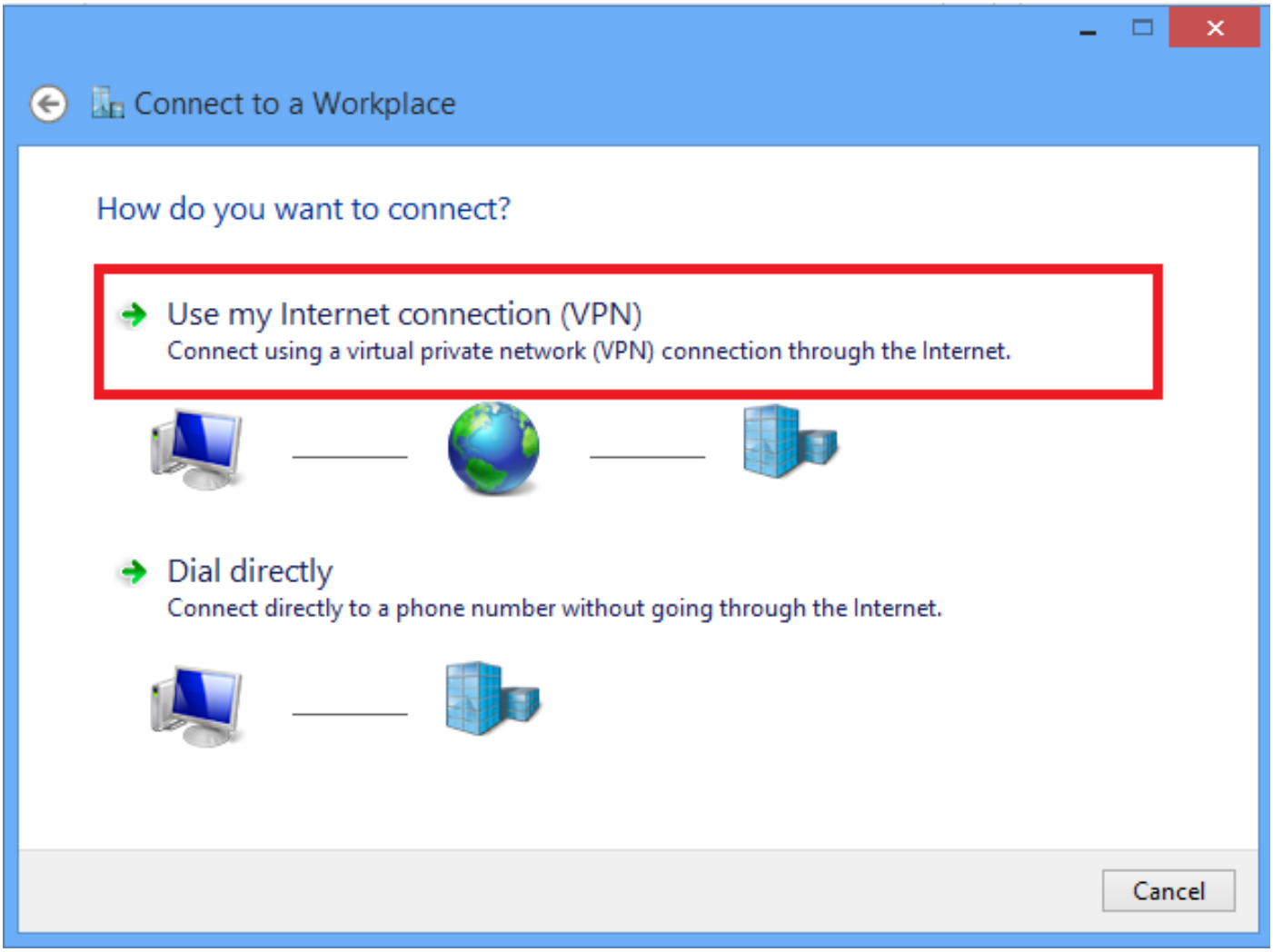
2. أختر **إعداد توصيل جديد أو** خيار **شبكة**.



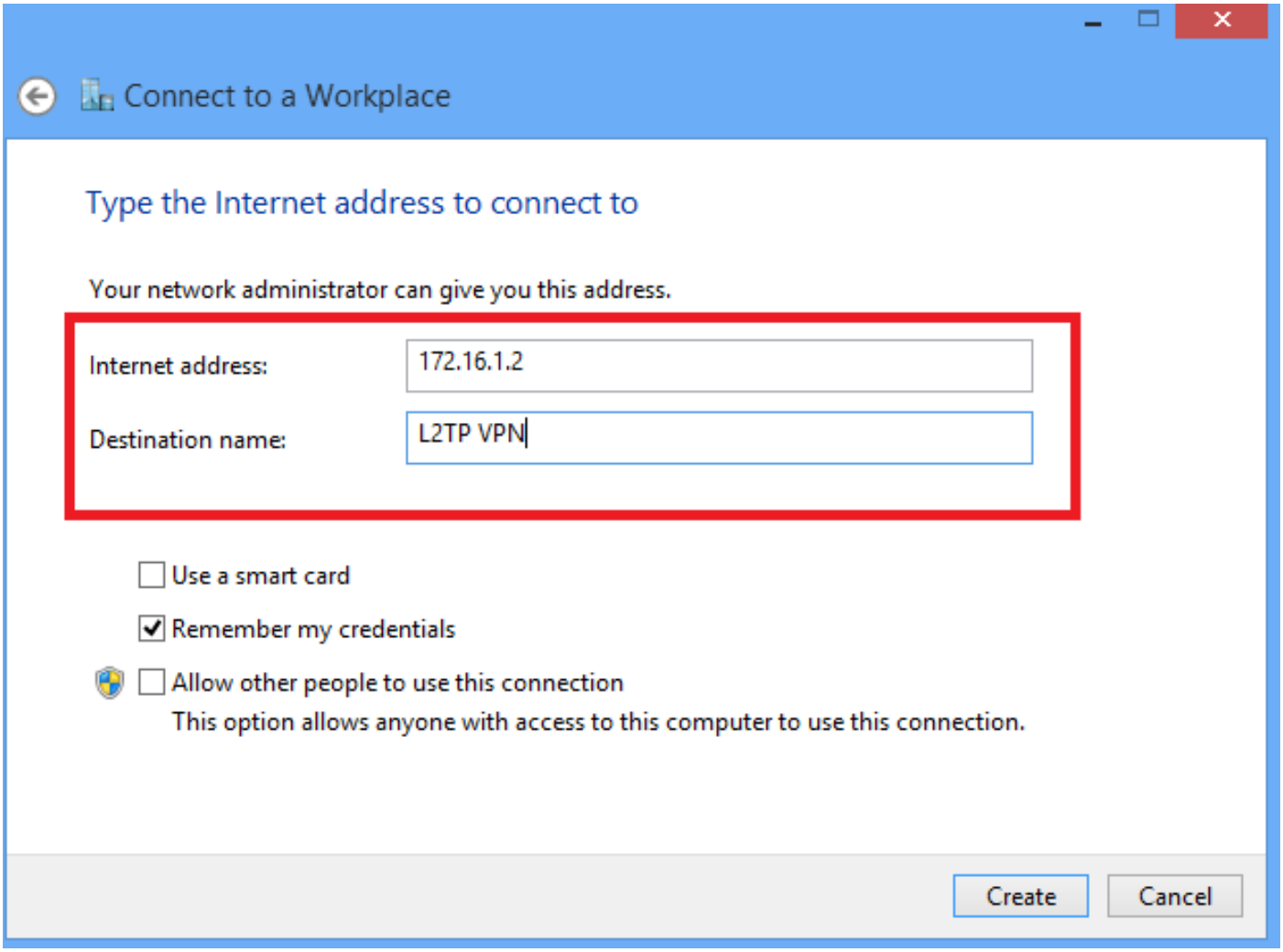
3. أختر **الاتصال** بخيار **مكان العمل** وانقر **فوق التالي.**



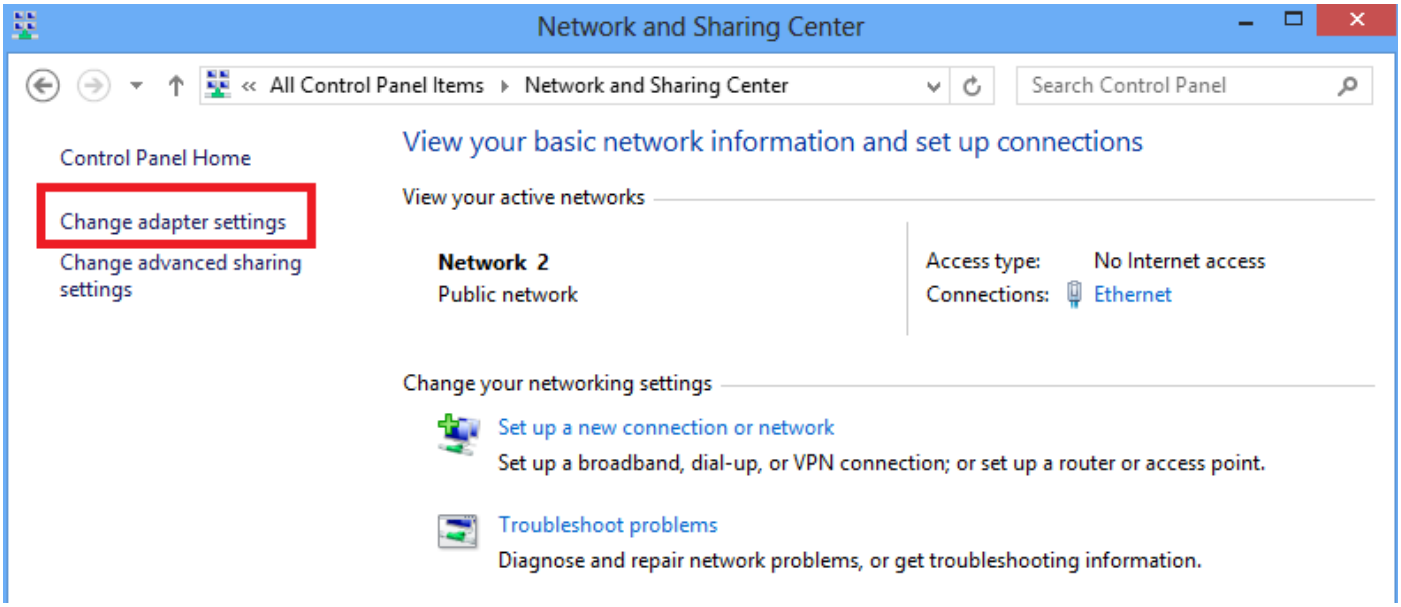
4.انقر فوق **استخدام** خيار **اتصال الإنترنت (VPN)**.



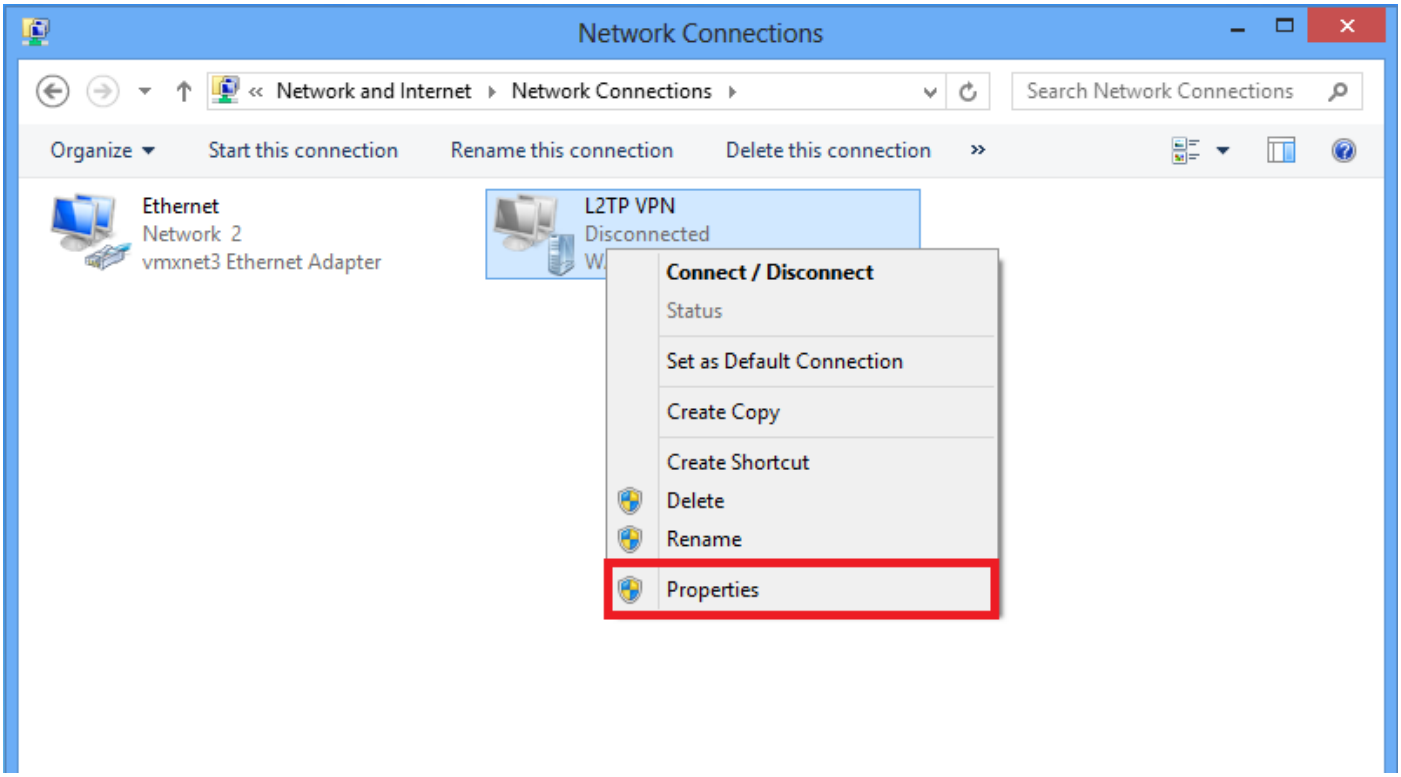
5. أدخل عنوان IP لواجهة WAN أو FQDN الخاصة بـ ASA وأي اسم لمهايئ VPN المهم محليا وانقر على **إنشاء**.



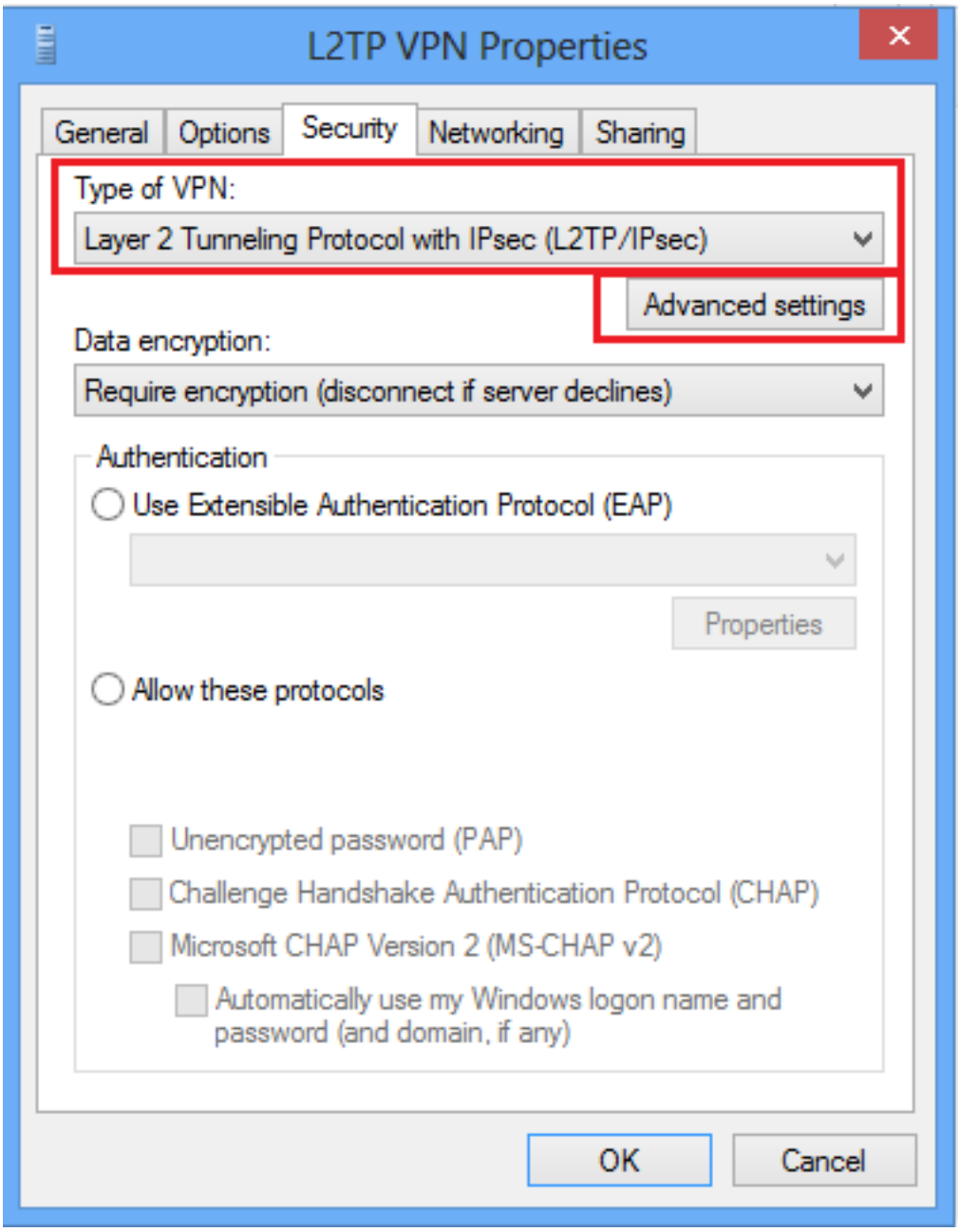
6. في مركز الشبكات والمشاركة، أختر **تغيير** خيار **إعدادات المحول** في الجزء الأيسر من الإطار.



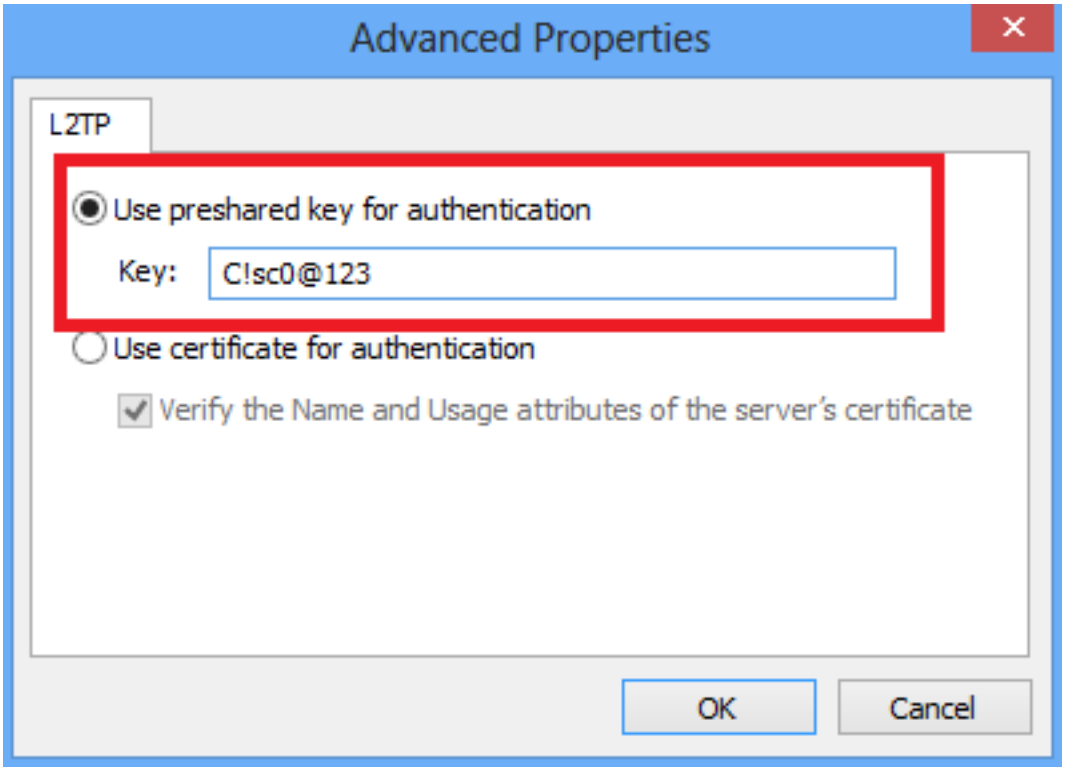
7. انقر بزر الماوس الأيمن فوق المهايئ الذي تم إنشاؤه مؤخرا لشبكة VPN الخاصة بالطرز L2TP واختر **الخصائص**.



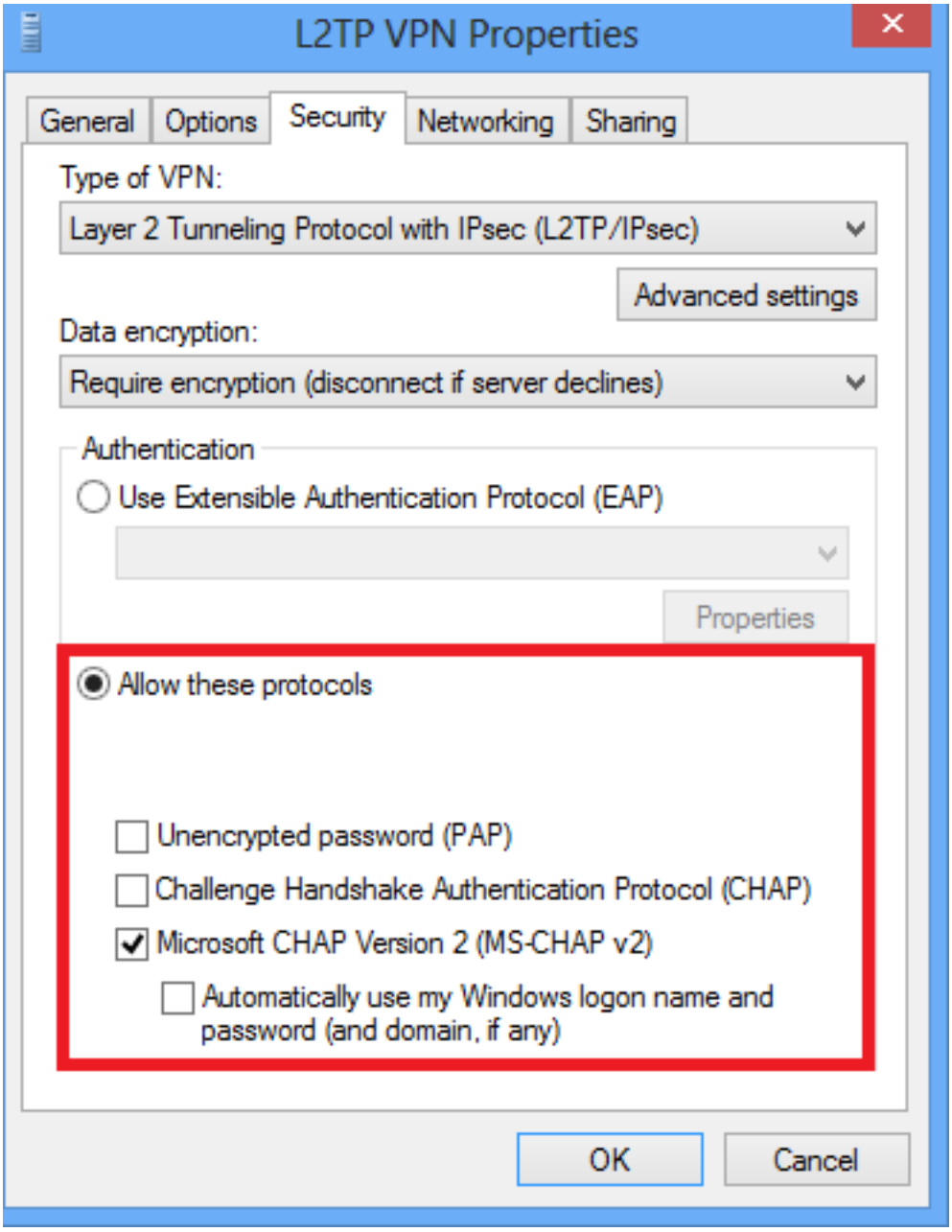
8. انتقل إلى علامة التبويب **الأمان**، واختر نوع شبكة VPN **كبروتوكول الاتصال النفقي للطبقة 2 مع IPsec (L2TP/IPsec)** ثم انقر فوق **الإعدادات المتقدمة**.



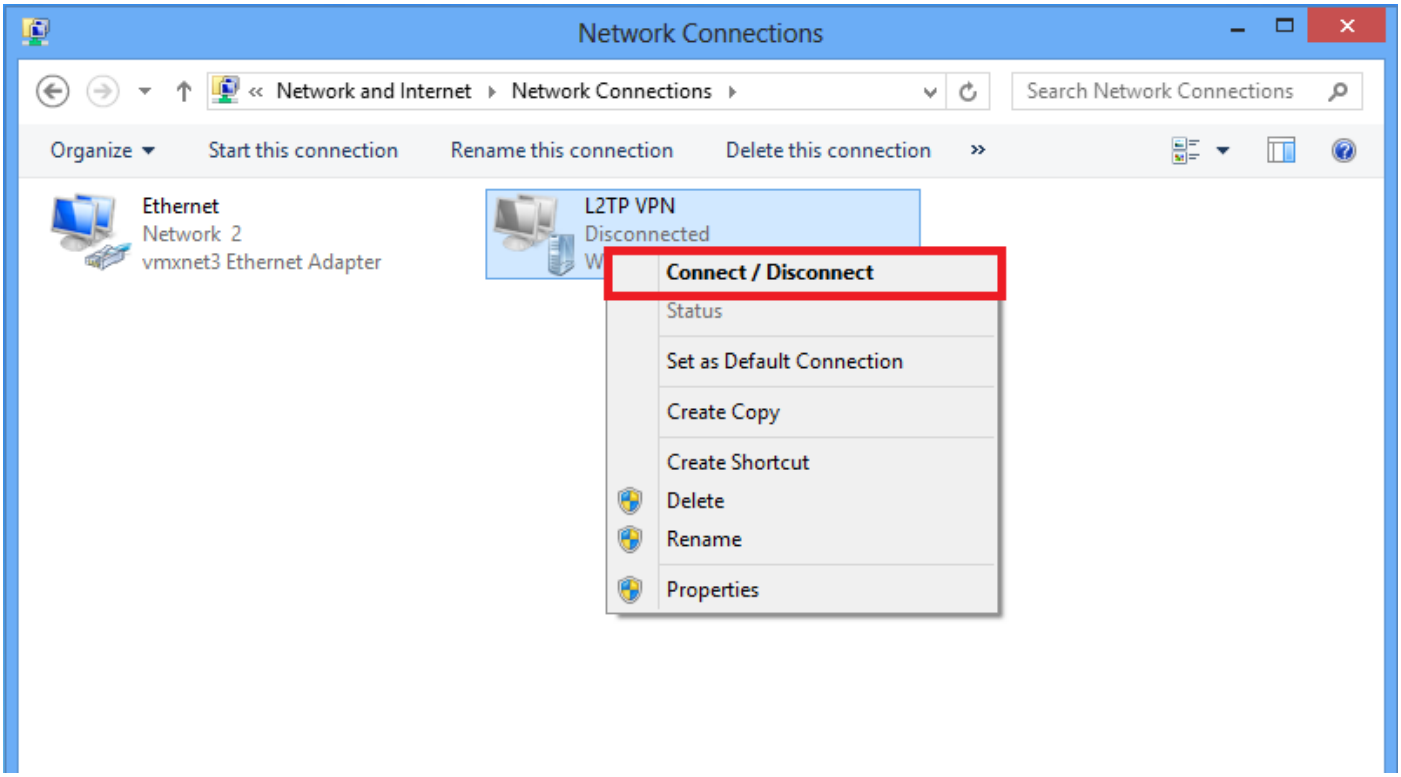
9. أدخل المفتاح المشترك مسبقا كما هو مذكور في Tunnel-group **DefaultRAGgroup** وانقر فوق **موافق**. في هذا المثال، يتم إستخدام C!sc0@123 كمفتاح مشترك مسبقا.



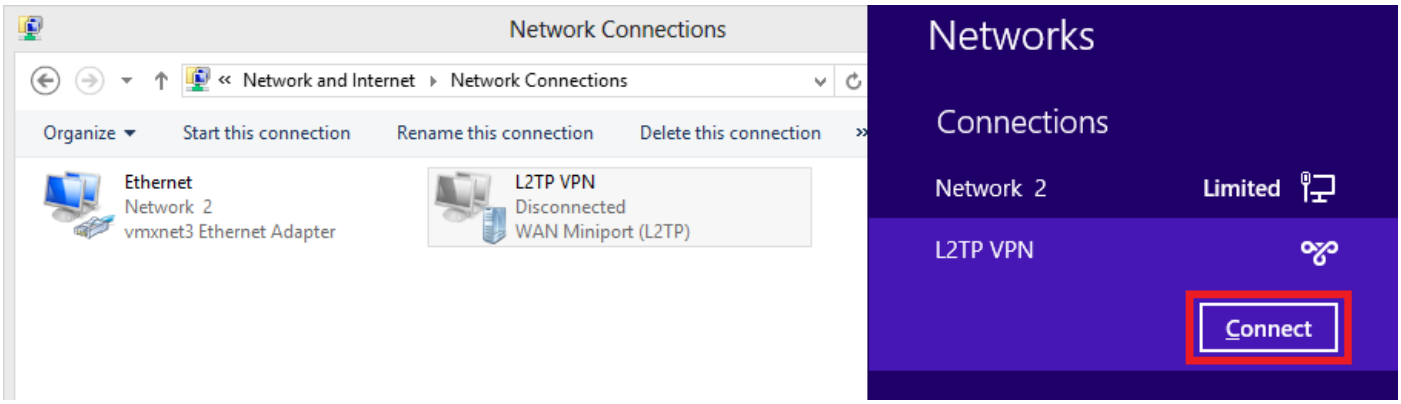
10. أختر طريقة المصادقة للسماح بهذه البروتوكولات وتأكد من تحديد خانة الاختيار **Microsoft CHAP الإصدار 2 (MS-CHAP v2)** فقط وانقر فوق **موافق**.



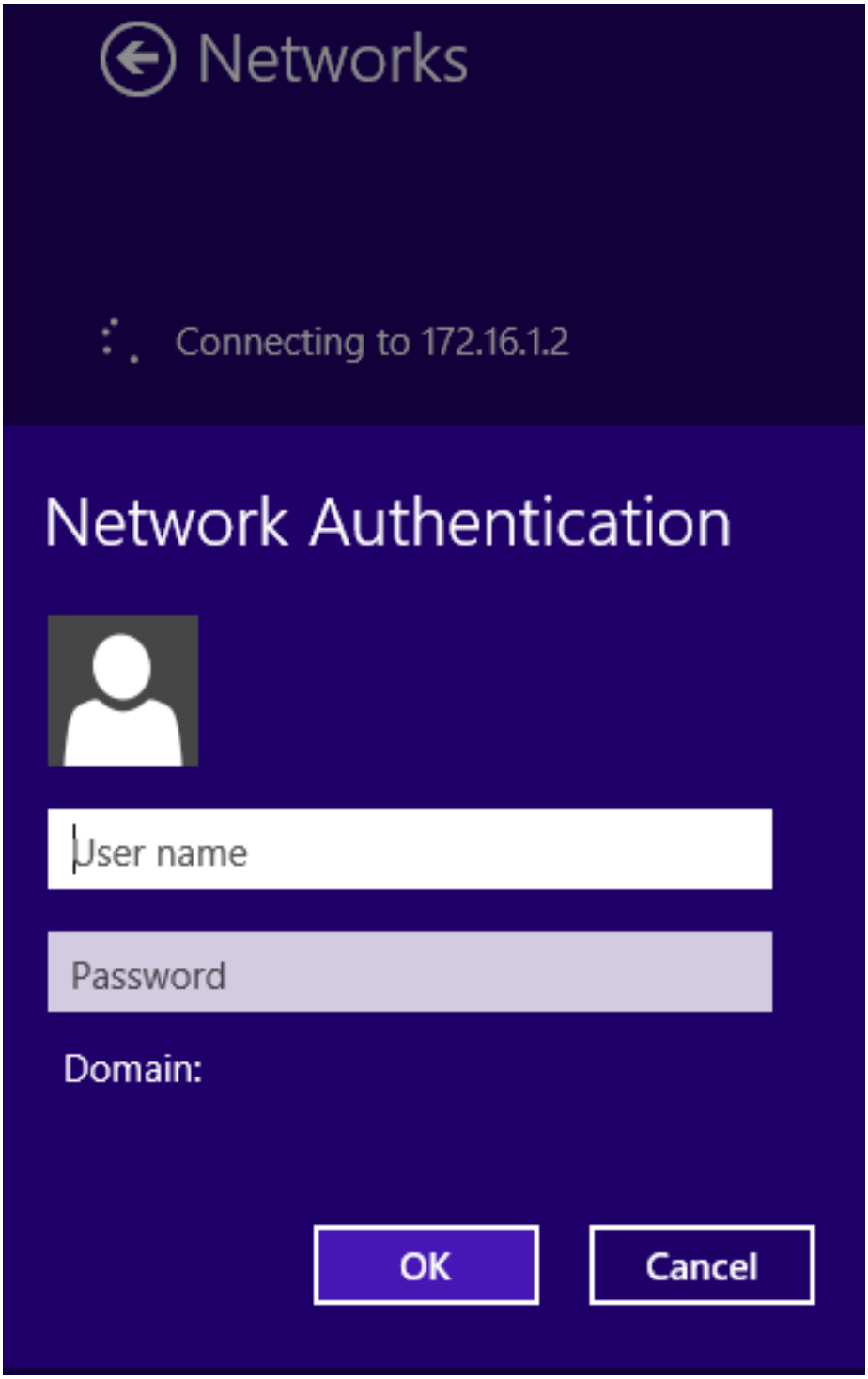
11. تحت إتصالات الشبكة، انقر بزر الماوس الأيمن على موائ L2TP VPN واختر **الاتصال/قطع الاتصال.**



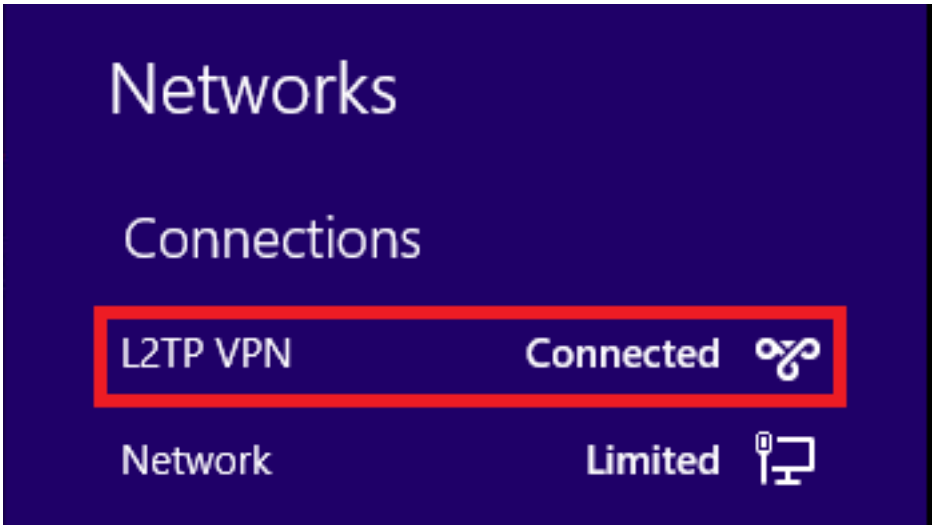
12. سيظهر رمز الشبكات ثم انقر على **اتصال** على اتصال L2TP VPN.



13. أدخل بيانات اعتماد المستخدم وانقر فوق **موافق**.



في حالة تطابق المعلمات المطلوبة على كل النهايتين، سيتم إنشاء اتصال L2TP/IPsec.



تكوين نفق التقسيم

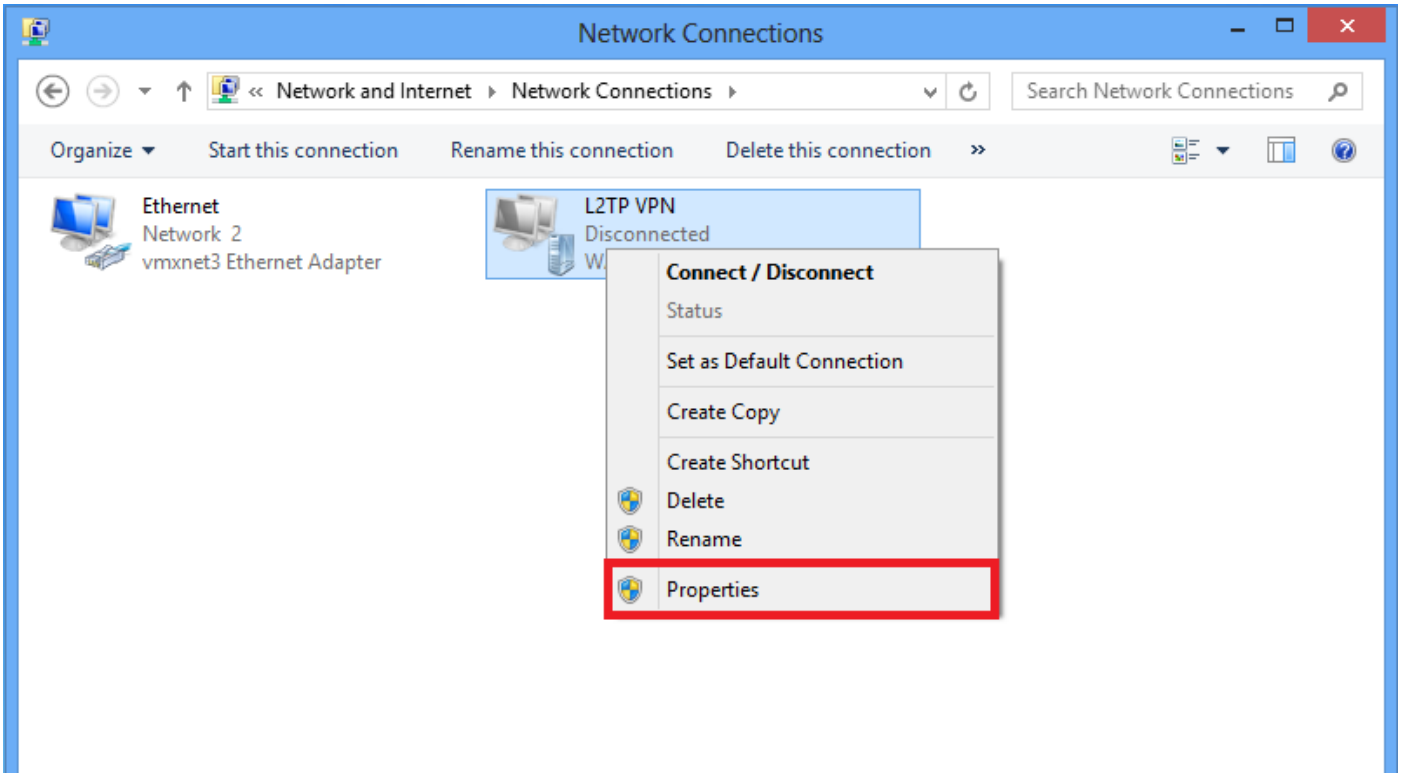
انقسام الاتصال النفقي هي ميزة يمكنك إستخدامها لتحديد حركة مرور البيانات للشبكات الفرعية أو الأجهزة المضيفة التي يجب تشفيرها. وهذا يتضمن تكوين قائمة التحكم في الوصول (ACL) المقترنة بهذه الميزة. يتم تشفير حركة مرور البيانات للشبكات الفرعية أو الأجهزة المضيفة المحددة على قائمة التحكم في الوصول (ACL) هذه عبر النفق من نهاية العميل، ويتم تثبيت المسارات لهذه الشبكات الفرعية على جدول توجيه الكمبيوتر الشخصي. يعترض ASA رسالة DHCPenform من عميل ويرد باستخدام قناع الشبكة الفرعية واسم المجال والمسارات الثابتة دون فئات.

التكوين على ASA

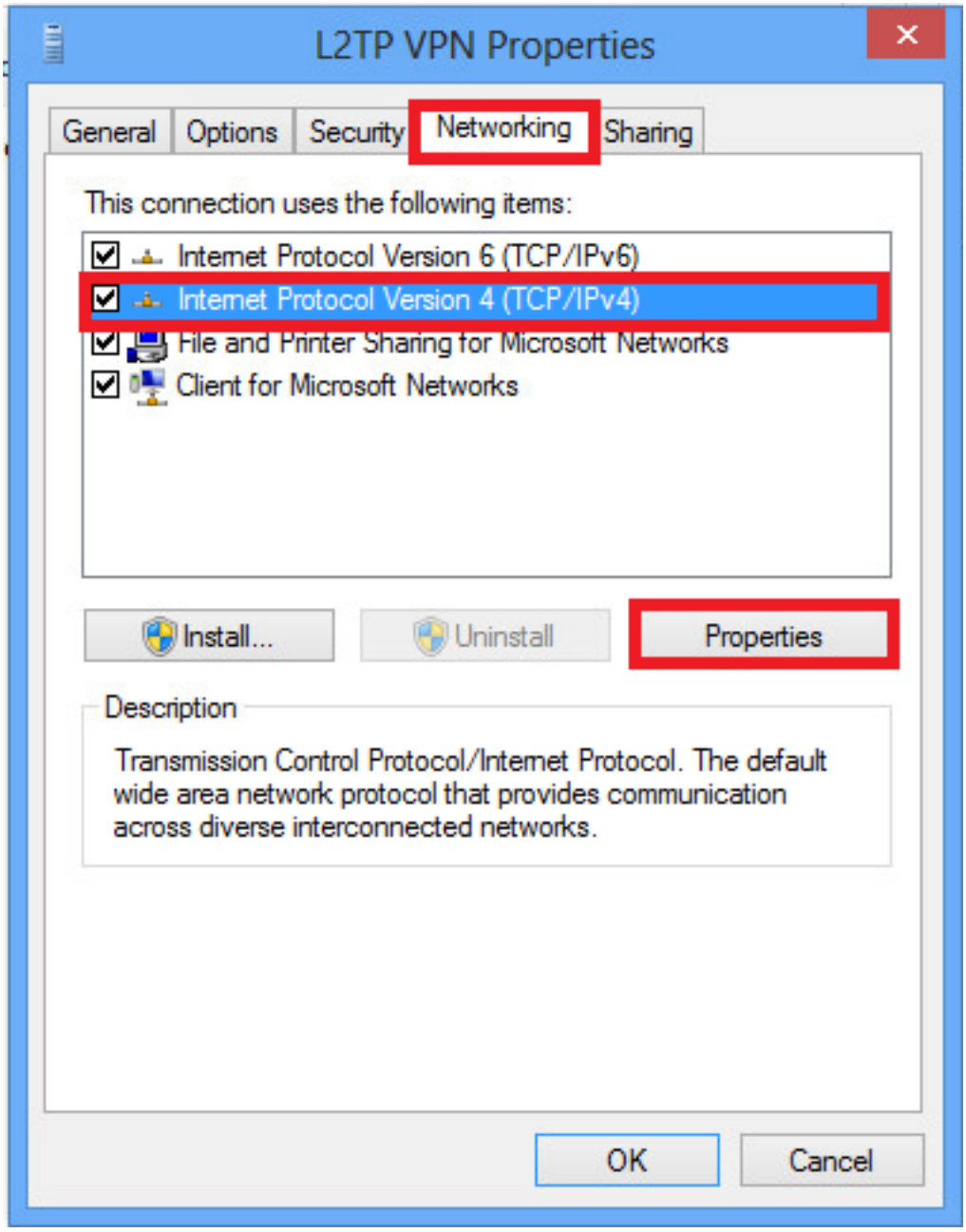
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

التكوين على عميل L2TP/IPsec

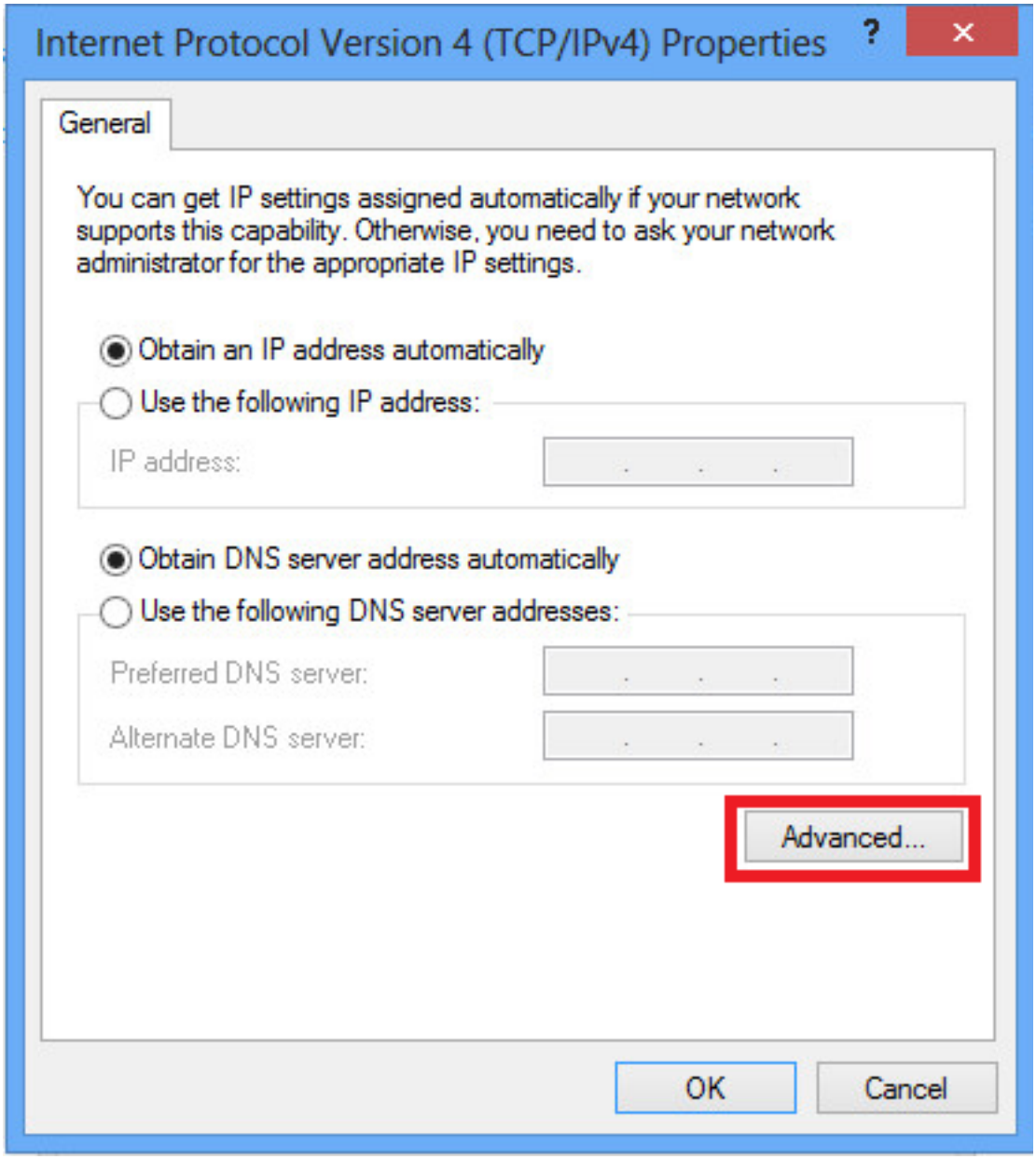
1. انقر بزر الماوس الأيمن على محول L2TP VPN واختر **خصائص**.



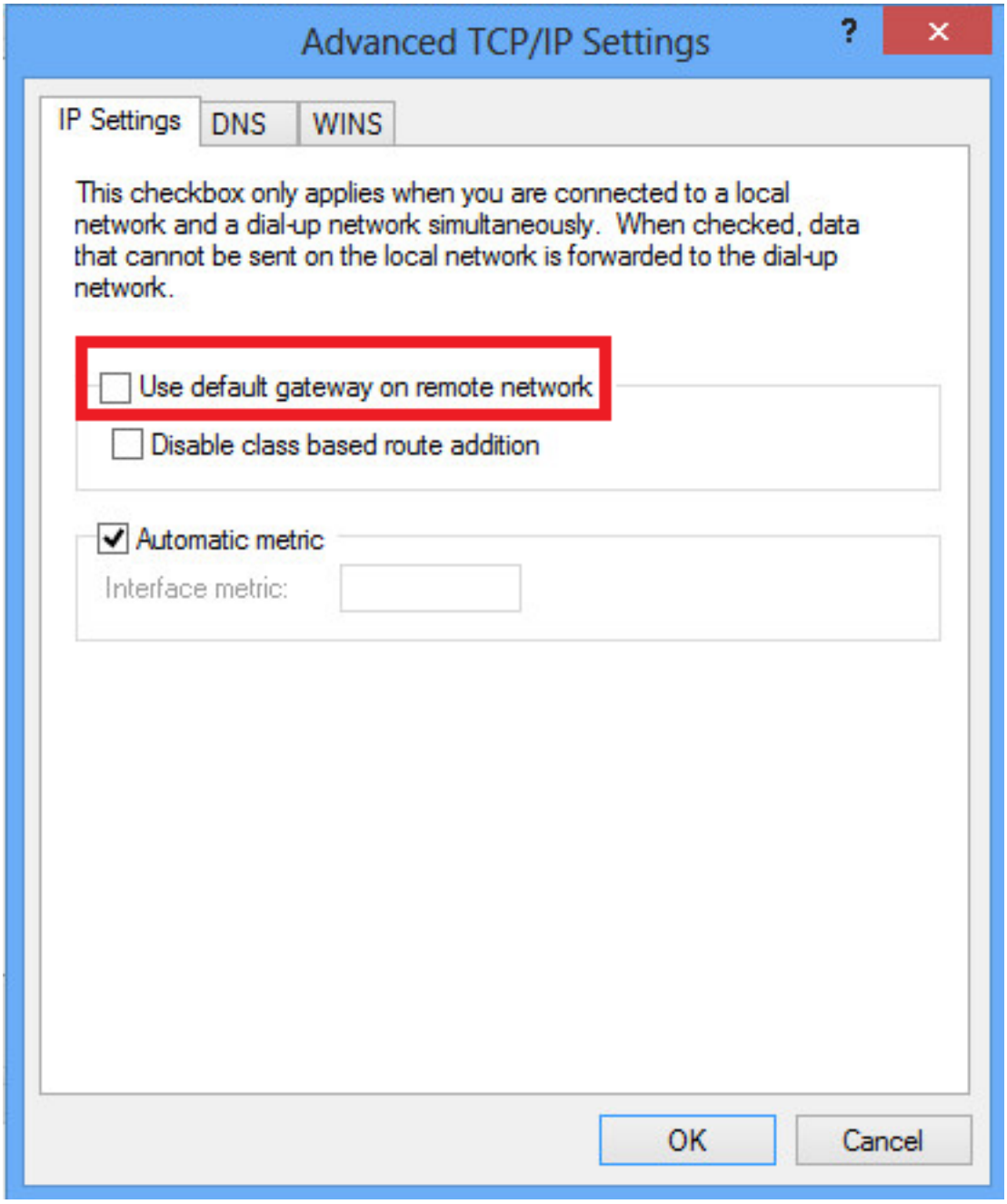
2. انتقل إلى علامة تبويب الشبكة، واختر الإصدار 4 من بروتوكول الإنترنت (TCP/IPv4) ثم انقر فوق **خصائص**.



3. انقر فوق خيار **خيارات متقدمة**.



4. قم بإلغاء تحديد **إستخدام البوابة الافتراضية على** خيار **الشبكة البعيدة** وانقر فوق **موافق**.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

> **ملاحظة**: تدعم أداة مترجم الإخراج (العملاء المسجلون فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمخرجات الأمر **show**.

- **show crypto ikev1 sa** - يعرض جميع شبكات IKE الحالية في نظير.

```
ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

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

```
1   IKE Peer:

10.1.1.2


   Type    : user            Role    : responder
   Rekey   : no

State   : MM_ACTIVE
```

- show crypto ipSec - يعرض جميع معرفات فئات خدمة IPsec الحالية في نظير.

```
ciscoasa# show crypto ipsec sa
interface: outside
   Crypto map tag:

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

     local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)
     remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)


current_peer: 10.1.1.2, username: test




dynamic allocated peer ip: 192.168.1.1


     dynamic allocated peer ip(ipv6): 0.0.0.0



#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29




      #pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118


     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 29, #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
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
     path mtu 1500, ipsec overhead 58(36), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: E8AF927A
     current inbound spi : 71F346AB

   inbound esp sas:
     spi: 0x71F346AB (1911768747)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000003
   outbound esp sas:
     spi: 0xE8AF927A (3903820410)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

- show vpn-sessiondb detail ra-ikev1-ipsSec filter protocol l2tpOverIpSec - يعرض معلومات تفصيلية حول L2TP عبر اتصالات IPsec.

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed



Username     : test

                  Index        : 1


Assigned IP  : 192.168.1.1           Public IP    : 10.1.1.2


Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 1574                  Bytes Rx     : 12752
Pkts Tx      : 29                    Pkts Rx      : 118
Pkts Tx Drop : 0                     Pkts Rx Drop : 0


Group Policy : L2TP-VPN              Tunnel Group : DefaultRAGroup


Login Time   : 23:32:48 UTC Sat May 16 2015
Duration     : 0h:04m:05s
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1
```

IKEv1:

```
 Tunnel ID    : 1.1
 UDP Src Port : 500                    UDP Dst Port : 500
 IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
 Encryption   : 3DES                   Hashing      : SHA1
 Rekey Int (T): 28800 Seconds          Rekey Left(T): 28555 Seconds
 D/H Group    : 2
 Filter Name  :
```

IPsec:

```
 Tunnel ID    : 1.2
 Local Addr   : 172.16.1.2/255.255.255.255/17/1701
 Remote Addr  : 10.1.1.2/255.255.255.255/17/1701
 Encryption   : 3DES                   Hashing      : SHA1
 Encapsulation: Transport
 Rekey Int (T): 3600 Seconds           Rekey Left(T): 3576 Seconds
 Rekey Int (D): 250000 K-Bytes         Rekey Left(D): 250000 K-Bytes
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Bytes Tx     : 1574                   Bytes Rx     : 12752
 Pkts Tx      : 29                     Pkts Rx      : 118
```

L2TPOverIPsec:

```
 Tunnel ID    : 1.3
```

Username : test

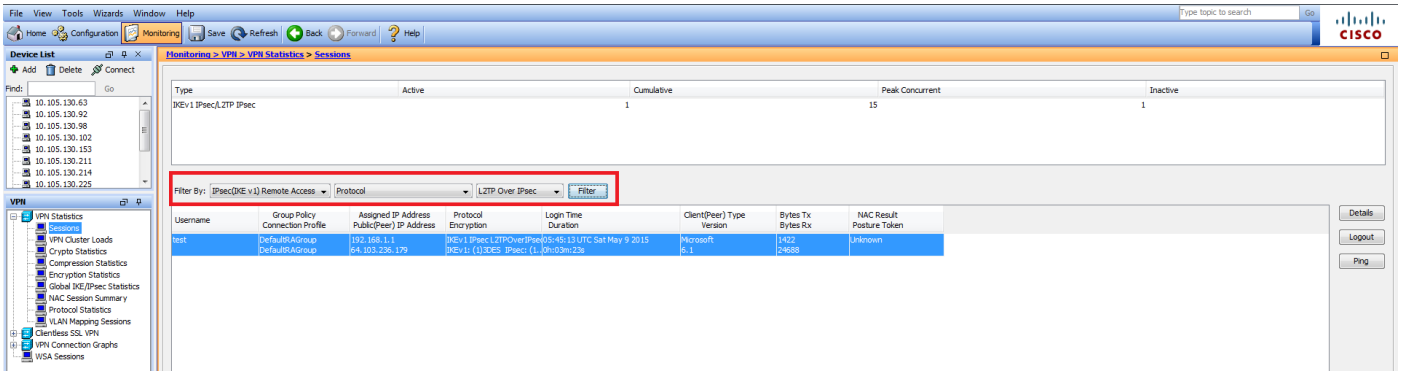
Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

```
 Encryption   : none                   Hashing      : none
```

```
Auth Mode     : msCHAPV2

Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
Client OS     : Microsoft
Client OS Ver: 6.2
Bytes Tx      : 475                  Bytes Rx     : 9093
Pkts Tx       : 18                   Pkts Rx      : 105
```

في ASDM، تحت **المراقبة > VPN > إحصائيات VPN > جلسات** العمل يمكن رؤية المعلومات العامة المتعلقة بجلسة شبكة VPN. يمكن تصفية L2TP عبر جلسات عمل IPsec بواسطة **IPsec (IKEv1) الوصول عن بعد > البروتوكول > L2TP عبر IPsec**.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل إستخدام أوامر **debug**.

تحذير: على ASA، يمكنك تعيين مستويات تصحيح أخطاء متنوعة؛ بشكل افتراضي، يتم إستخدام المستوى 1. إذا قمت بتغيير مستوى تصحيح الأخطاء، فقد تتزايد درجة توسع تصحيح الأخطاء. نفذ ذلك بحذر، خاصة في بيئات الإنتاج!

أستخدم **أوامر تصحيح الأخطاء** التالية **مع توخي الحذر** لاستكشاف أخطاء نفق VPN وإصلاحها

- **debug crypto ikev1** - يعرض معلومات تصحيح الأخطاء حول IKE
- **debug crypto ipSec** - يعرض معلومات تصحيح الأخطاء حول IPsec

فيما يلي إخراج تصحيح الأخطاء لاتصال L2TP ناجح عبر اتصال IPSec:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
```

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

Connection landed on tunnel_group DefaultRAGroup

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
```

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

  Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI   : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:
SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick
mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

  Remote host: 10.1.1.2 Protocol 17 Port 1701

  Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
   SCB: 0xE13ABD20,
   Direction: outbound
   SPI   : 0x8C14FD70
   Session ID: 0x00001000

```
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00000000
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   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 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   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: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User ()  Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA   : 0x00007fffe13ab260
   SPI  : 0x7AD72E0D
   MTU  : 0 bytes
   VCID : 0x00000000
   Peer : 0x000028D4
   SCB  : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00004174
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
```

```
   Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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 inbound tunnel flow rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

```
PHASE 2 COMPLETED

 (msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1
```

يتم عرض بعض الأخطاء المرتبطة بشبكة VPN التي تشاهد بشكل شائع على عميل Windows في هذا الجدول

رمز الخطأ	حل ممكن
691	تأكد من صحة اسم المستخدم وكلمة المرور المدخلين
789,835	تأكد من أن المفاتيح المشترك مسبقا الذي تم تكوينه على جهاز العميل كان مماثل لما هو عليه في ASA
800	1. تأكد من تعيين نوع VPN على "بروتوكول نفق الطبقة 2 (L2TP)" 2. تأكد من تكوين المفاتيح المشترك مسبقا بشكل صحيح
809	تأكد من أن منفذ UDP 500 و 4500 (في حالة ما إذا كان العميل أو الخادم خلف جهاز NAT) ولم يتم حظر حركة مرور ESP

معلومات ذات صلة

- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances]
- [حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPsec للوصول عن بعد و L2L الأكثر شيوعا]
- [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).