عميل PIX/ASA و VPN لشبكة VPN العامة على مثال تكوين العصا

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد جهاز أمان ASA 7.2 والإصدارات الأحدث لتنفيذ IPsec على أحد العصا. ينطبق هذا الإعداد على حالة معينة حيث لا يسمح ASA بتقسيم خطوط اتصال، ويتصل المستخدمون مباشرة بجهاز ASA قبل السماح لهم بالانتقال إلى الإنترنت.

ملاحظة: في الإصدار 7.2 من PIX/ASA والإصدارات الأحدث، تسمح الكلمة الأساسية *intra-interface* لجميع حركة المرور بالدخول إلى نفس الواجهة والخروج منها، وليس فقط حركة مرور IPsec.

ارجع إلى Router وزبون الشبكة الخاصة الظاهرية (VPN) لشبكة الإنترنت العامة على مثال تكوين Stick لإكمال تكوين مماثل على موجه موقع مركزي.

ارجع إلى PIX/ASA 7.x Enhanced Talk-To-Client VPN مع مثال تكوين مصادقة TACACS+ لمعرفة المزيد حول السيناريو الذي يقوم فيه PIX الموزع بإعادة توجيه حركة مرور البيانات من عميل VPN إلى PIX الذي يتم التحدث به.

ملاحظة: لتجنب تداخل عناوين IP في الشبكة، قم بتعيين مجموعة مختلفة تماما من عناوين IP إلى عميل VPN (على سبيل المثال، x.x.x.10 و x.x.172.16 و x.x.192.168). يعد مخطط عنونة IP هذا مفيدا لاستكشاف أخطاء الشبكة وإصلاحها.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يحتاج جهاز أمان Hub PIX/ASA إلى تشغيل الإصدار 7.2 أو إصدار أحدث
- عميل شبكة VPN من Cisco، الإصدار x.5

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 8.0.2 من جهاز الأمان PIX أو ASA و Cisco VPN Client الإصدار 5.0.

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 Cisco PIX الإصدار 7.2 والإصدارات الأحدث.

الاصطلاحات

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

معلومات أساسية

تسريحة شعر أو دوران U

هذا سمة مفيد ل VPN حركة مرور أن يدخل قارن غير أن بعد ذلك وجهت خارج أن القارن نفسه. على سبيل المثال، إذا كانت لديك شبكة شبكة VPN تدعم تقنية المحاور، حيث يكون جهاز الأمان هو المركز، وكانت شبكات VPN البعيدة محددة، لكي يتمكن الشخص من الاتصال بالآخر الذي يتحدث، يجب أن تنتقل حركة مرور البيانات إلى جهاز الأمان ثم تعود مرة أخرى إلى الشبكة الأخرى التي تتحدث بها.

أستخدم الأمر **نفسه-security-traffic** للسماح لحركة المرور بالدخول والخروج من نفس الواجهة.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

ملاحظة: ينطبق **الفرز** حسب الحاجة أو الدوران إلى الخلف على اتصال عميل الشبكة الخاصة الظاهرية (VPN) أيضا.

التكوينات

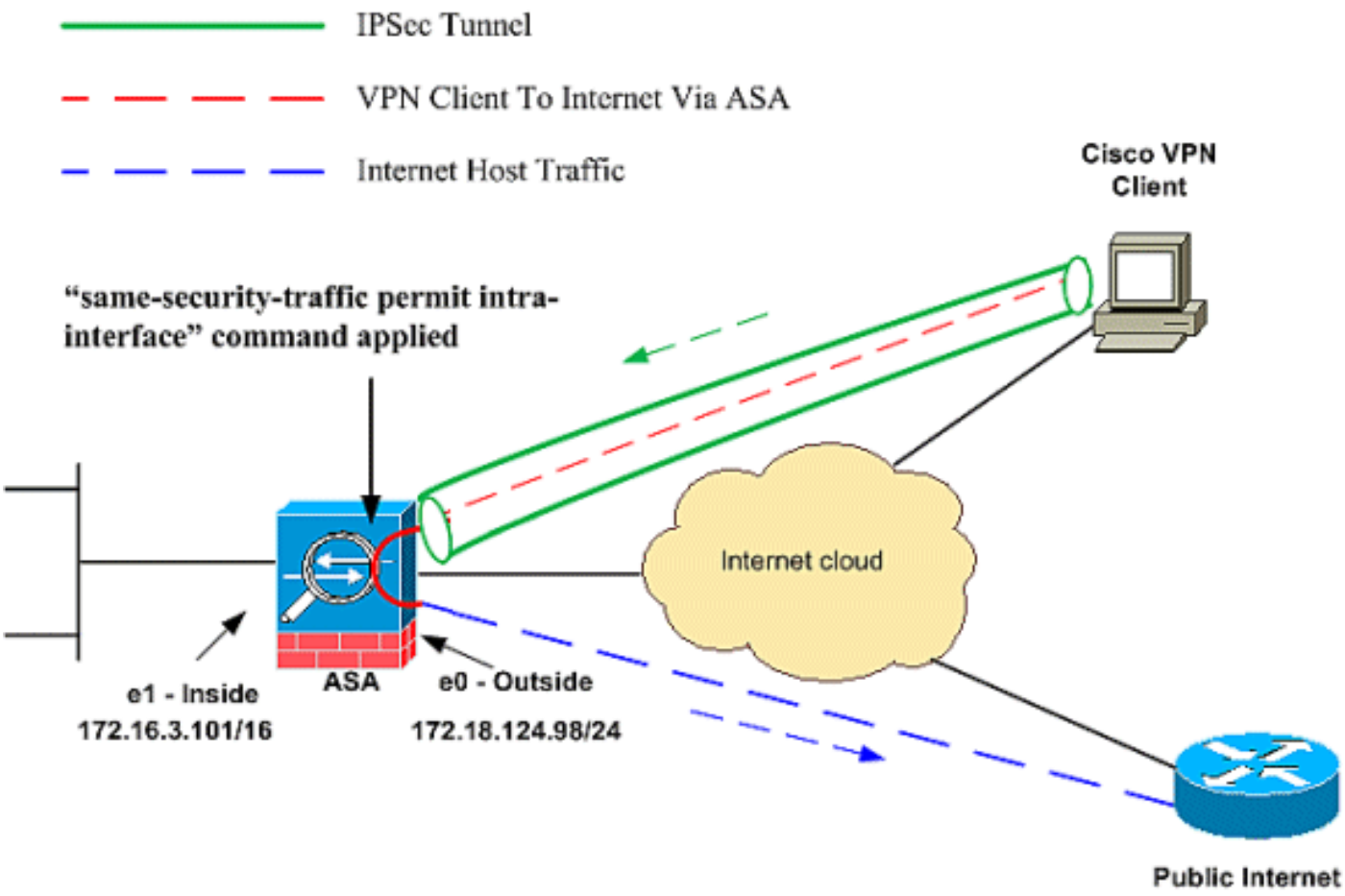
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر

المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تشكيل ال CLI PIX/ASA

- PIX/ASA

تشغيل التكوين على PIX/ASA

```
(PIX Version 8.0(2
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
```

```
                                                no ip address
                                                !
                                            interface Ethernet3
                                                shutdown
                                                no nameif
                                            no security-level
                                                no ip address
                                                !
                                            interface Ethernet4
                                                shutdown
                                                no nameif
                                            no security-level
                                                no ip address
                                                !
                                            interface Ethernet5
                                                shutdown
                                                no nameif
                                            no security-level
                                                no ip address
                                                !
                                    enable password 8Ry2YjIyt7RRXU24 encrypted
                                            passwd 2KFQnbNIdI.2KYOU encrypted
                                                hostname pixfirewall
                                                ftp mode passive
    Command that permits IPsec traffic to enter and ---!
   exit the same interface. same-security-traffic permit
                                                intra-interface
 access-list 100 extended permit icmp any any echo-reply
                                                pager lines 24
                                                logging enable
                                        logging buffered debugging
                                                mtu outside 1500
                                                mtu inside 1500

                                                ip local pool vpnpool
       mask 255.255.255.0 192.168.10.1-192.168.10.254

                                                no failover
                                        monitor-interface outside
                                        monitor-interface inside
                                        icmp permit any outside
                                        no asdm history enable
                                                arp timeout 14400
nat-control!--- The address pool for the VPN Clients. !-
   -- The global address for Internet access used by VPN
      Clients. !--- Note: Uses an RFC 1918 range for lab
     setup. !--- Apply an address from your public range
                                                .provided by your ISP

                                        global (outside) 1 172.18.124.166

   The NAT statement to define what to encrypt (the ---!
           addresses from the vpn-pool). nat (outside) 1
                                        192.168.10.0 255.255.255.0

                                    nat (inside) 1 0.0.0.0 0.0.0.0
       static (inside,outside) 172.16.3.102 172.16.3.102
                                        netmask 255.255.255.255
                                access-group 100 in interface outside
            route outside 0.0.0.0 0.0.0.0 172.18.124.98 1
                                        timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                                icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
```

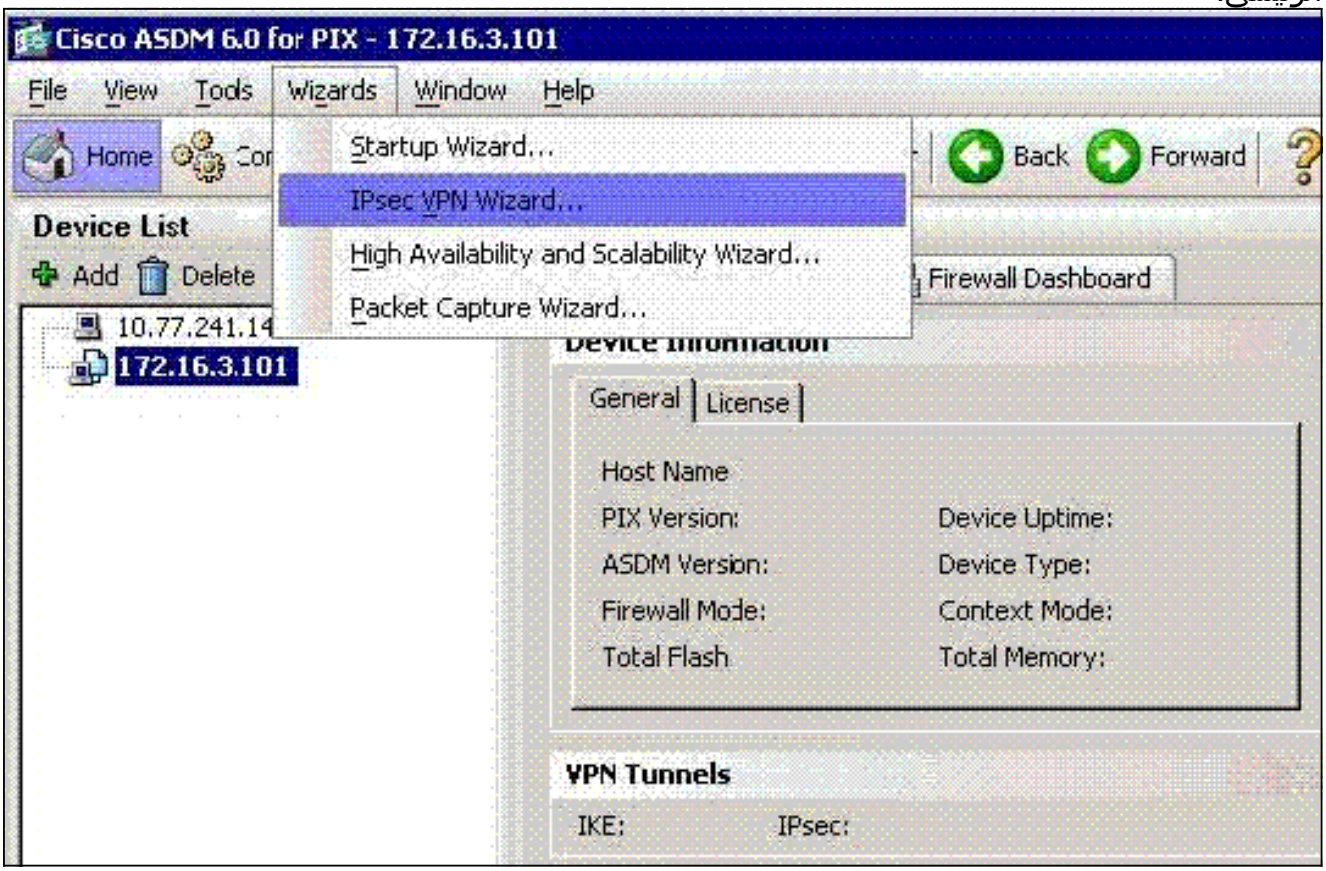
```
                                                0:05:00
  timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
                                timeout uauth 0:05:00 absolute

 The configuration of group-policy for VPN Clients. ---!
                                group-policy clientgroup internal
                                group-policy clientgroup attributes
                                                vpn-idle-timeout 20

    Forces VPN Clients over the tunnel for Internet ---!
                                access. split-tunnel-policy tunnelall


                                                no snmp-server location
                                                  no snmp-server contact
                                snmp-server enable traps snmp

       Configuration of IPsec Phase 2. crypto ipsec ---!
                                transform-set myset esp-3des esp-sha-hmac

      Crypto map configuration for VPN Clients that ---!
 connect to this PIX. crypto dynamic-map rtpdynmap 20 set
                                                transform-set myset

   Binds the dynamic map to the crypto map process. ---!
                                crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

 Crypto map applied to the outside interface. crypto ---!
                                map mymap interface outside

     Enable ISAKMP on the outside interface. isakmp ---!
                                                identity address
                                                isakmp enable outside

   Configuration of ISAKMP policy. isakmp policy 10 ---!
                                                authentication pre-share
                                isakmp policy 10 encryption 3des
                                                isakmp policy 10 hash sha
                                                isakmp policy 10 group 2
                                isakmp policy 10 lifetime 86400
                          isakmp policy 65535 authentication pre-share
                                   isakmp policy 65535 encryption 3des
                                          isakmp policy 65535 hash sha
                                          isakmp policy 65535 group 2
                                isakmp policy 65535 lifetime 86400
                                                telnet timeout 5
                                                   ssh timeout 5
                                                console timeout 0

          Configuration of tunnel-group with group ---!
 information for VPN Clients. tunnel-group rtptacvpn type
                                                ipsec-ra

      Configuration of group parameters for the VPN ---!
      Clients. tunnel-group rtptacvpn general-attributes
                                                address-pool vpnpool

 Disable user authentication. authentication-server- ---!
                                                group none


   Bind group-policy parameters to the tunnel-group ---!
       for VPN Clients. default-group-policy clientgroup
                                tunnel-group rtptacvpn ipsec-attributes
```

```
* pre-shared-key
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
end :
```

تكوين ASA/PIX باستخدام ASDM

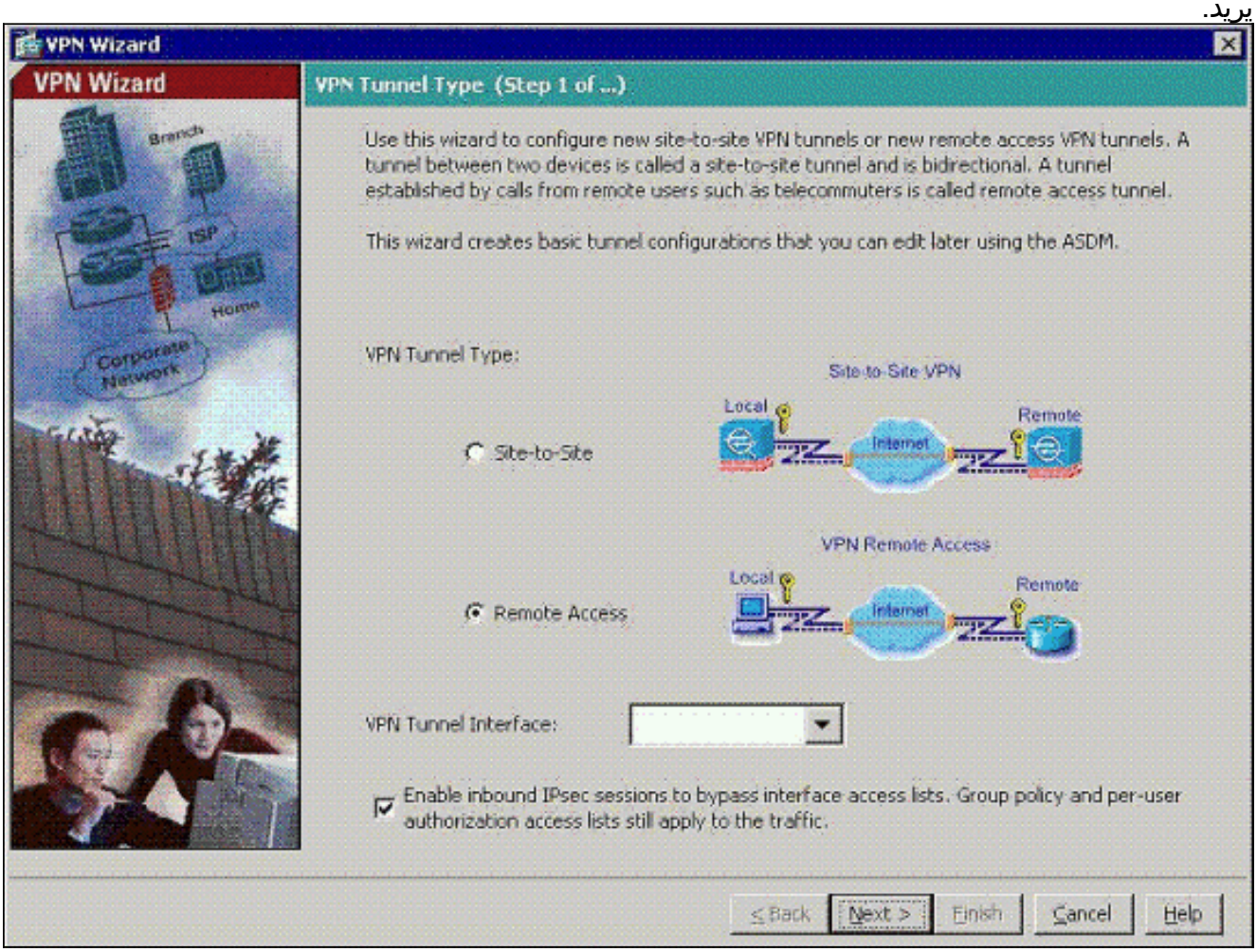
أتمت هذا steps in order to شكلت ال cisco ASA كنادل VPN بعيد مع ASDM:

1. أختر **المعالجات > معالج IPsec VPN** من الإطار الرئيسي.

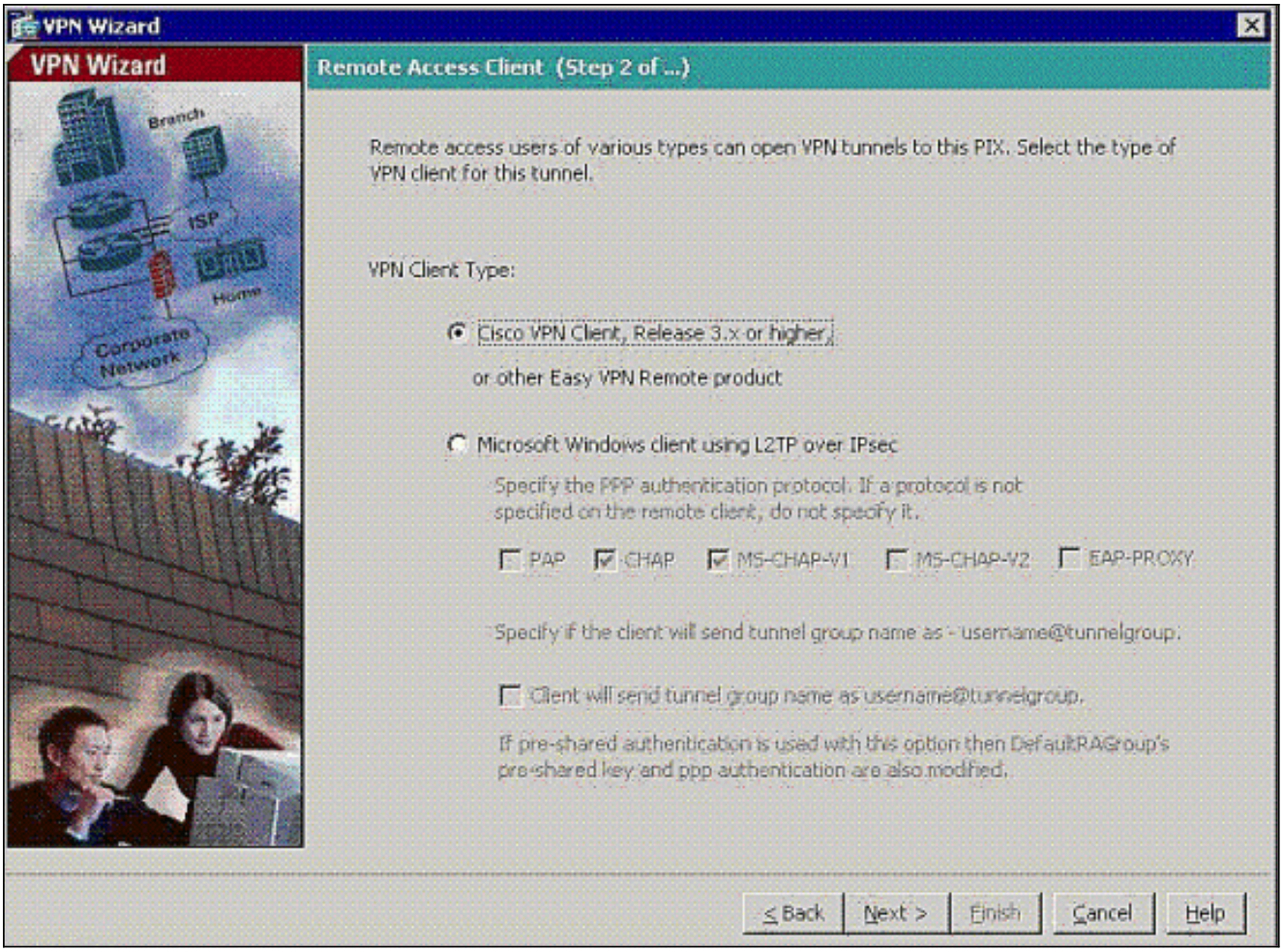


2. أخترت **الوصول عن بعد** VPN نفق نوع، وتأكد أن ال VPN نفق قارن ثبت بما

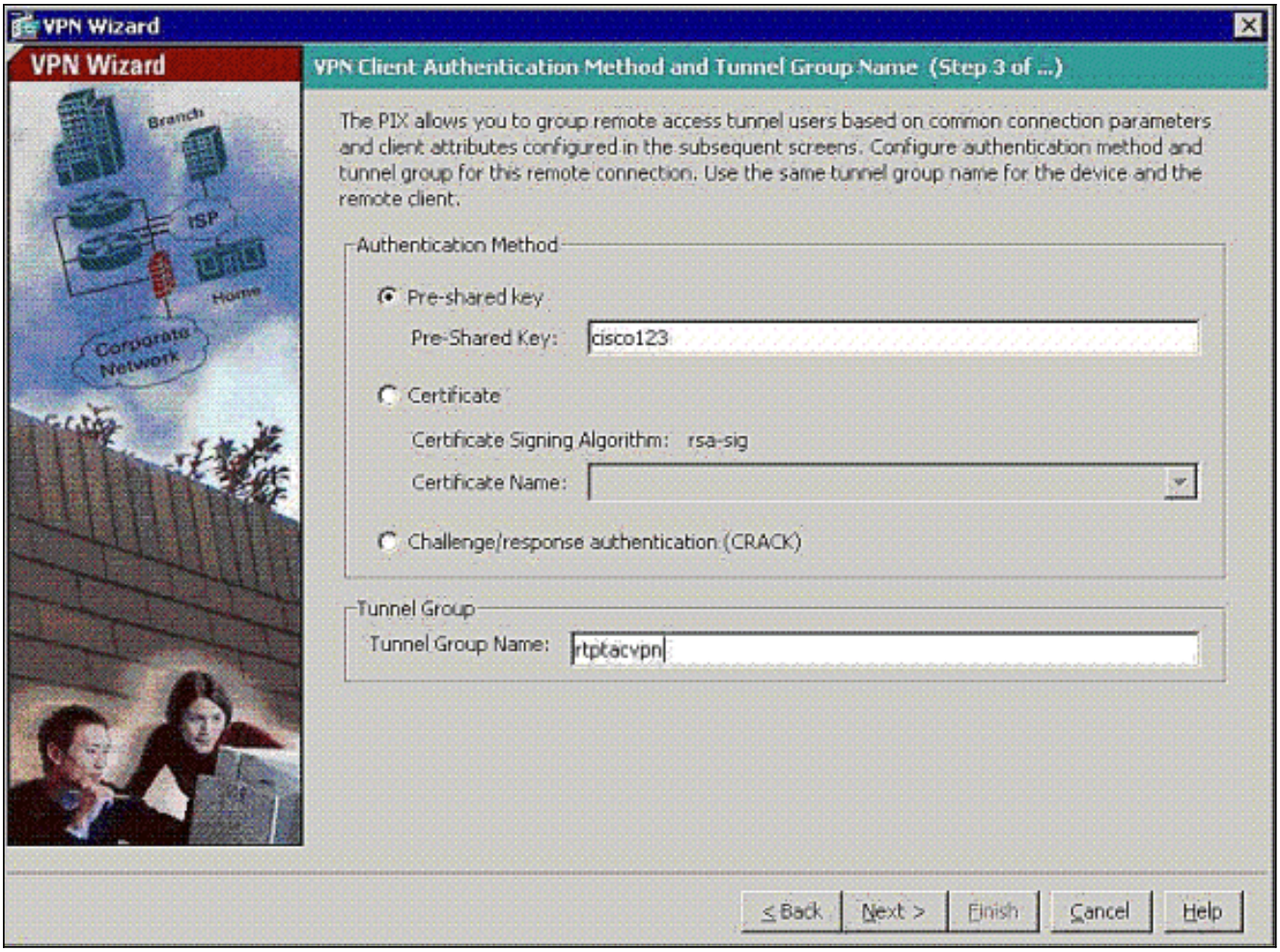
يريد.



3. تم بالفعل إختيار نوع عميل شبكة VPN الوحيد المتاح. انقر فوق **Next (التالي)**.

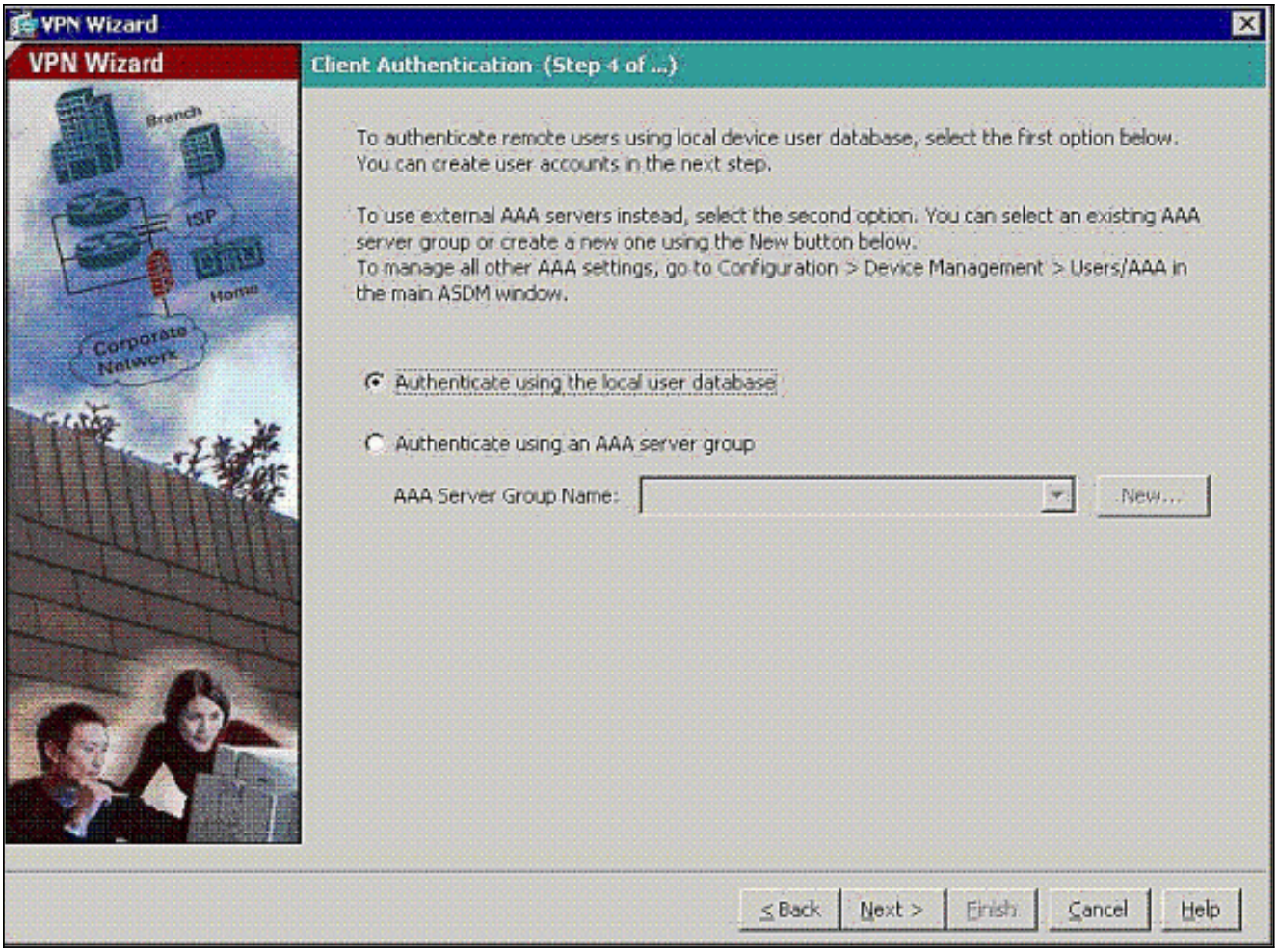


4. أدخل اسما لاسم مجموعة النفق. قم بتوفير معلومات المصادقة لاستخدامها.يتم إختيار **المفتاح المشترك مسبقا** في هذا
المثال.

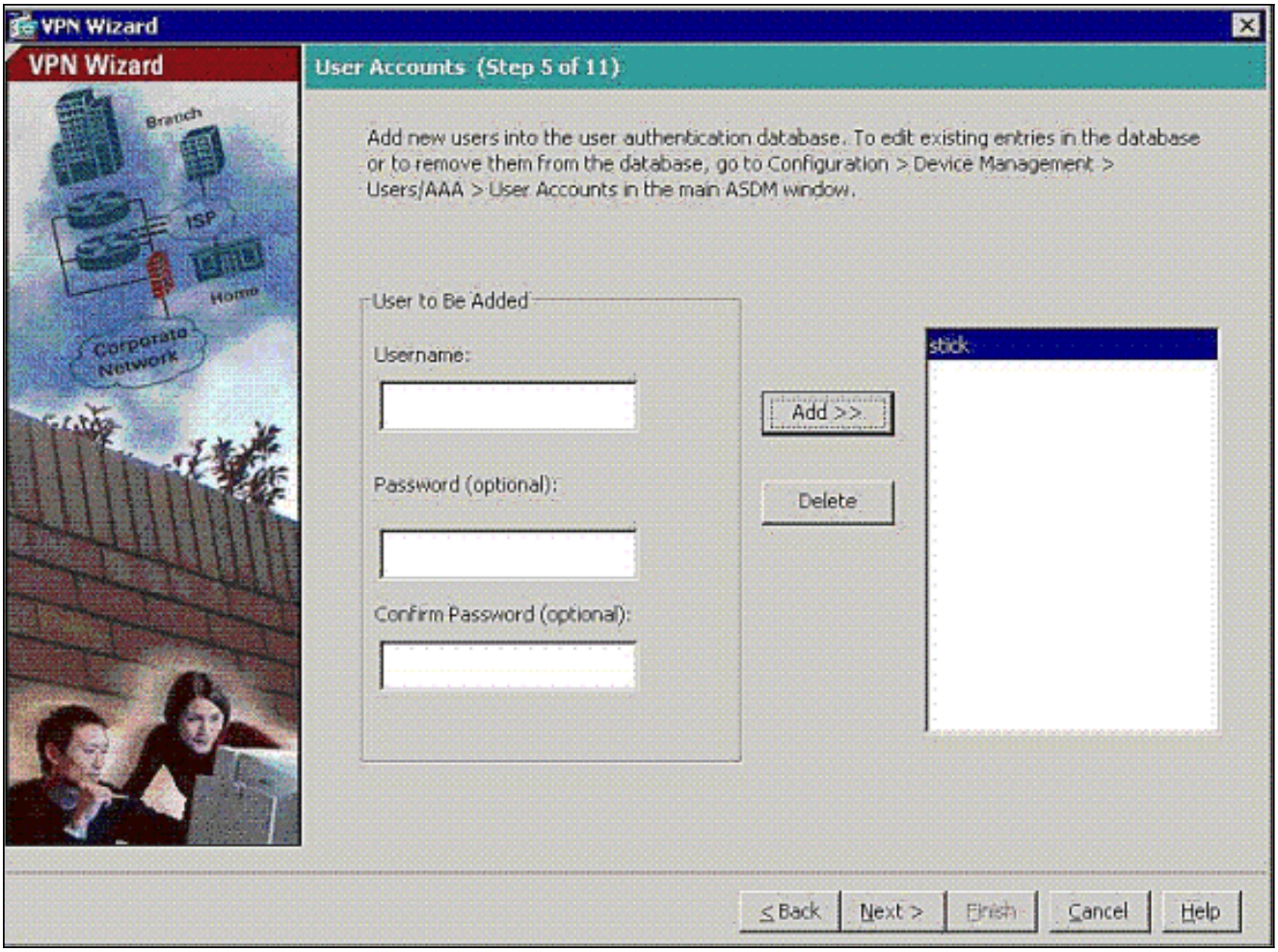


ملاحظة: لا توجد طريقة لإخفاء/تشفير المفتاح المشترك مسبقا على ASDM. السبب هو أنه يجب إستخدام ASDM فقط من قبل الأشخاص الذين يقومون بتكوين ASA أو الأشخاص الذين يساعدون العميل في هذا التكوين.

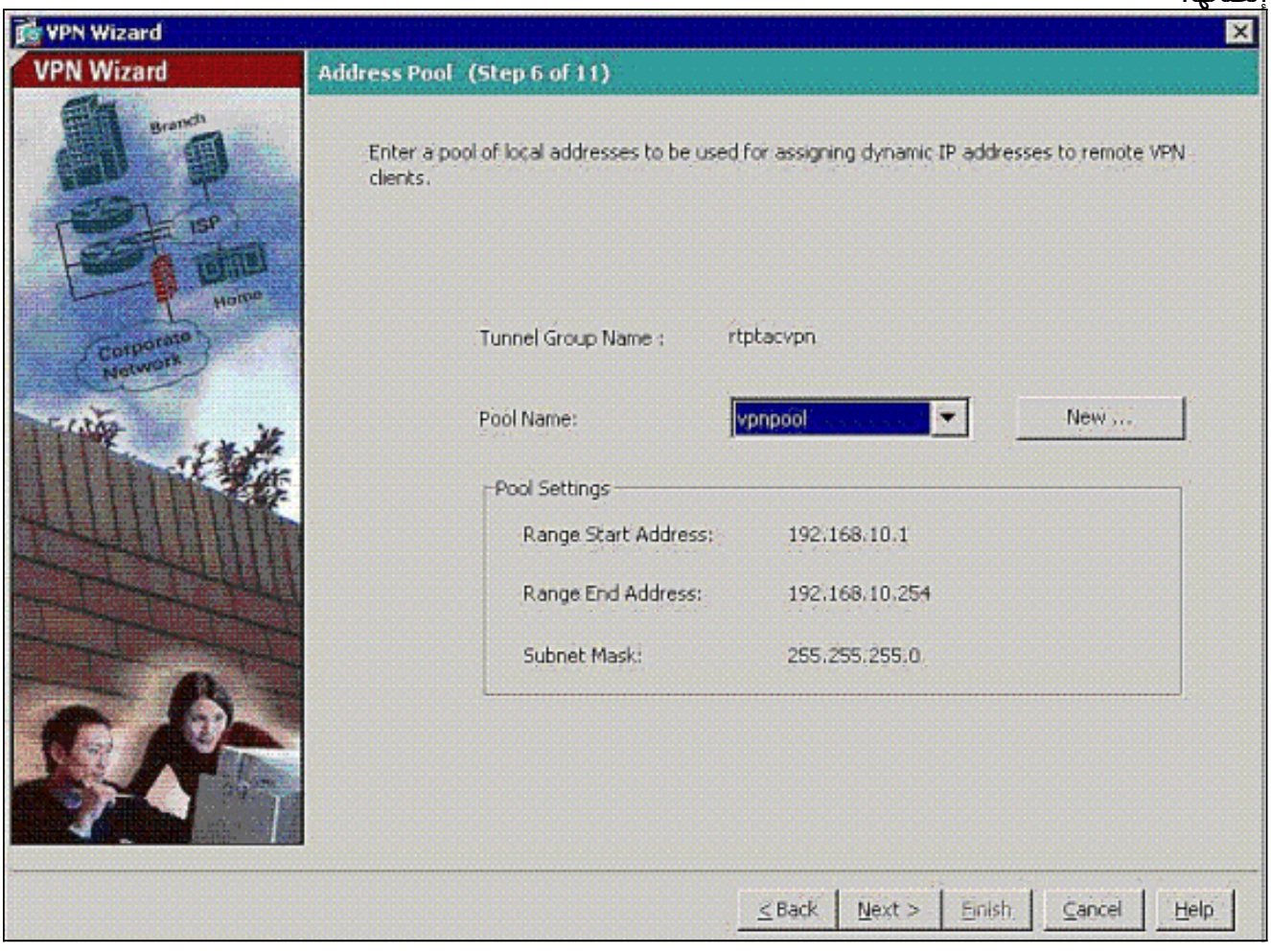
5. أختر ما إذا كنت تريد مصادقة المستخدمين عن بعد إلى قاعدة بيانات المستخدم المحلية أو إلى مجموعة خوادم AAA خارجية.**ملاحظة:** يمكنك إضافة مستخدمين إلى قاعدة بيانات المستخدم المحلية في الخطوة 6.**ملاحظة:** ارجع إلى مجموعات خوادم المصادقة والتفويض الخاصة ب PIX/ASA 7.x لمستخدمي VPN عبر مثال تكوين ASDM للحصول على معلومات حول كيفية تكوين مجموعة خوادم AAA الخارجية من خلال ASDM.



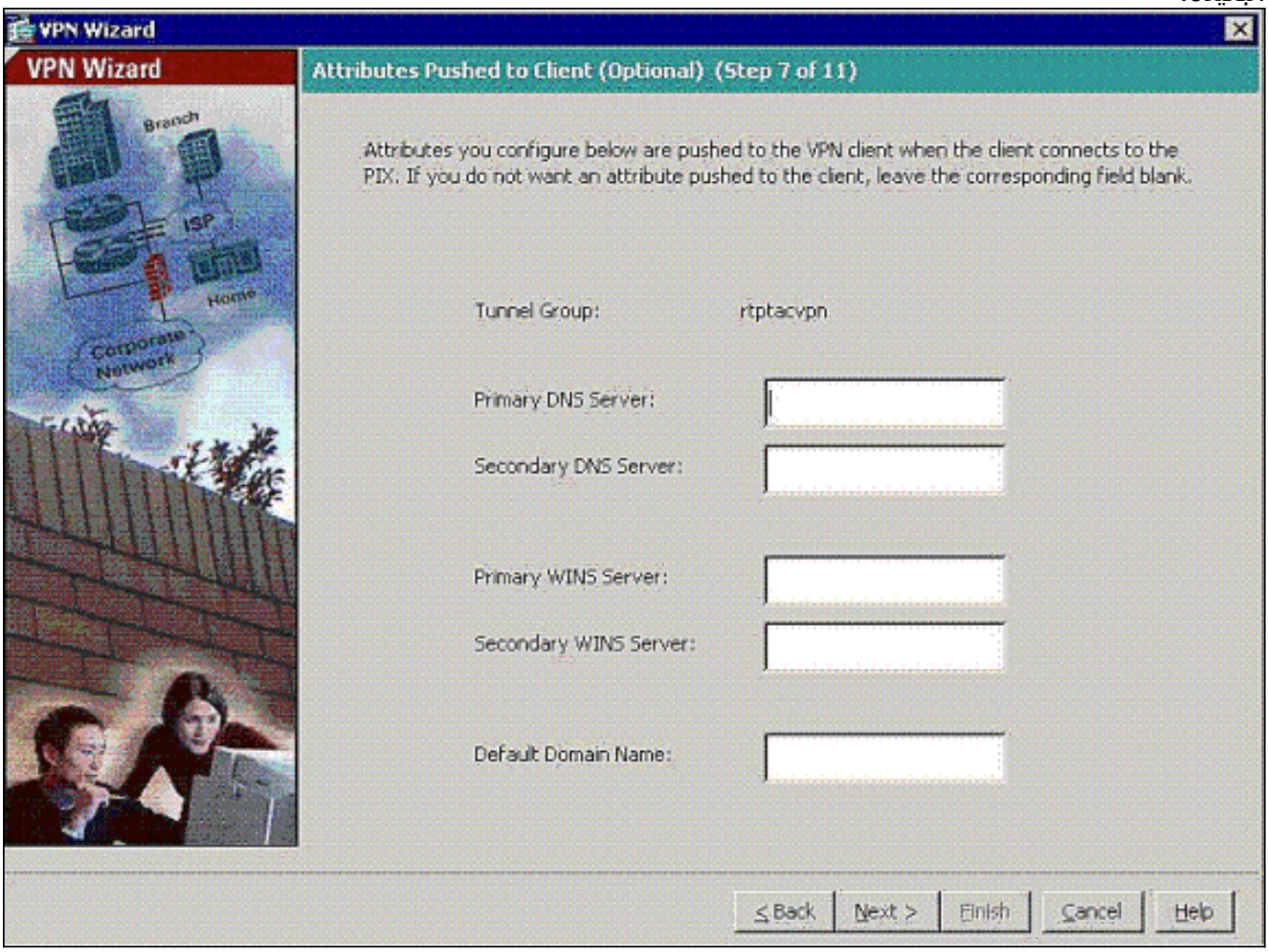
6. قم بإضافة مستخدمين إلى قاعدة البيانات المحلية، إذا لزم الأمر.**ملاحظة:** لا تقم بإزالة المستخدمين الحاليين من هذا الإطار. أختر **تكوين > إدارة الأجهزة > إدارة > حسابات المستخدمين في نافذة ASDM الرئيسية** لتحرير الإدخالات الموجودة في قاعدة البيانات أو لإزالتها من قاعدة البيانات.



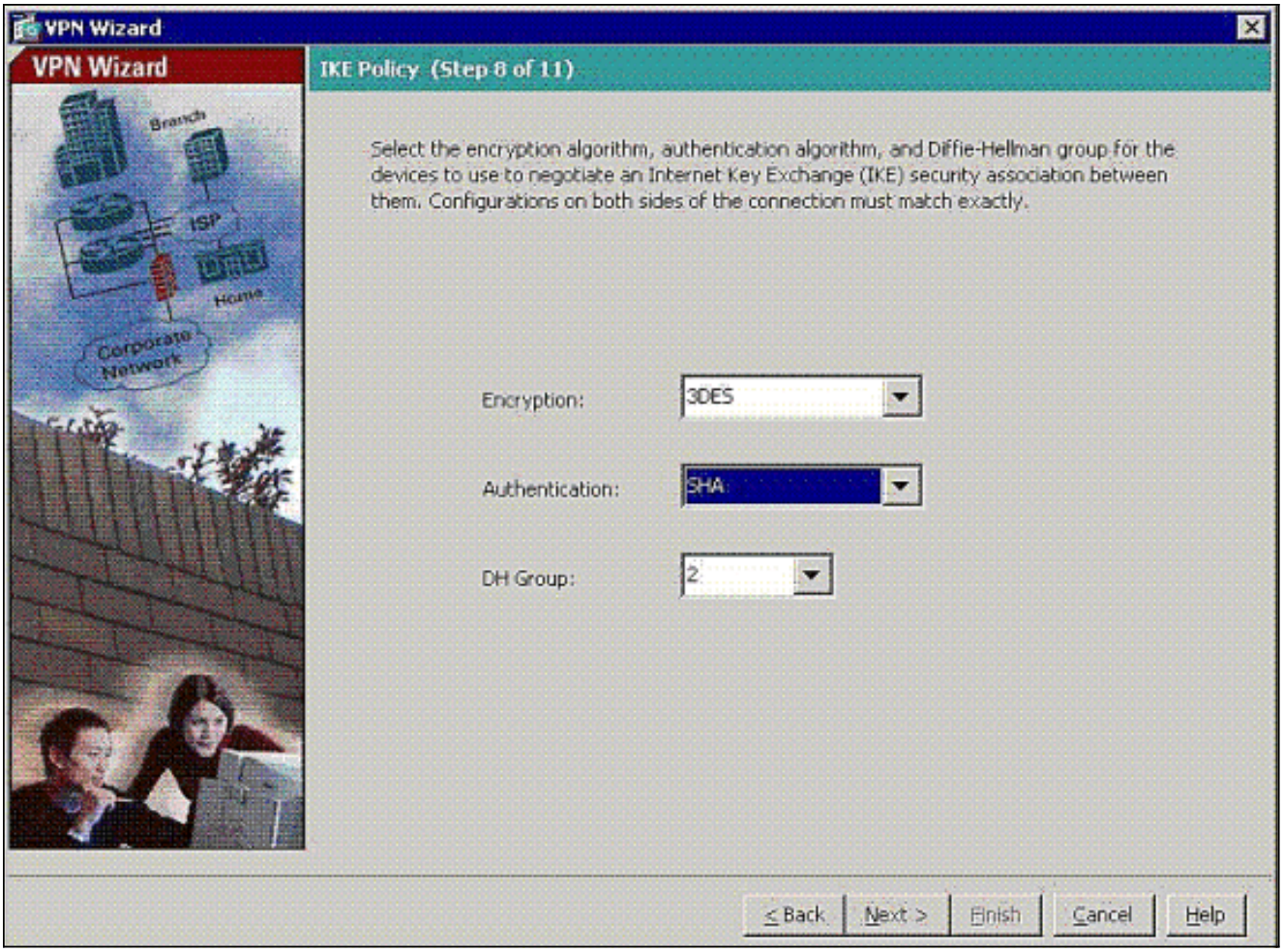
7. حدد مجموعة من العناوين المحلية ليتم تعيينها ديناميكيا لعملاء شبكات VPN البعيدة عند إتصالها.



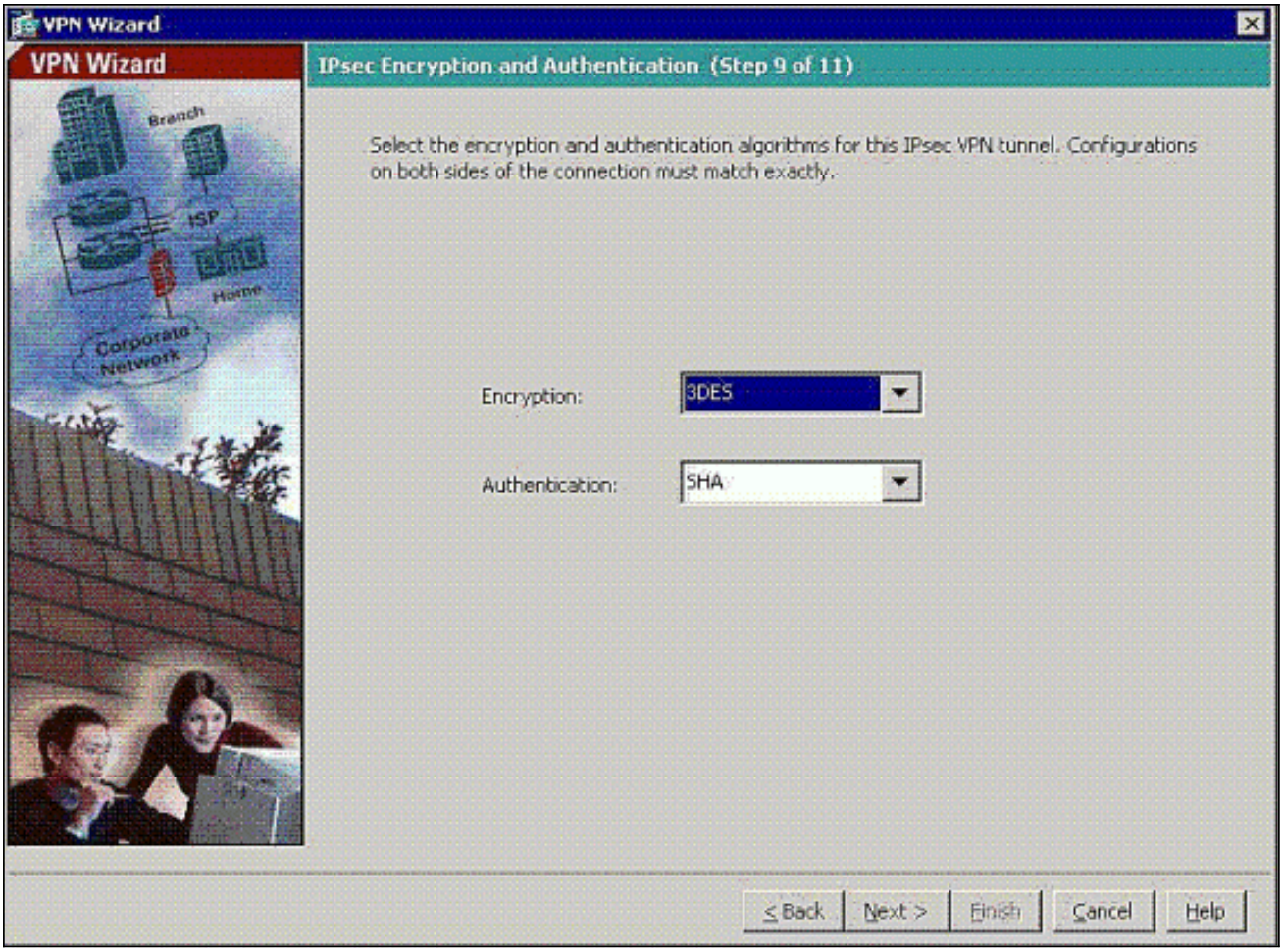
8. *إختياري:* حدد معلومات خادم DNS و WINS واسم مجال افتراضي ليتم دفعه إلى عملاء VPN البعيدة.



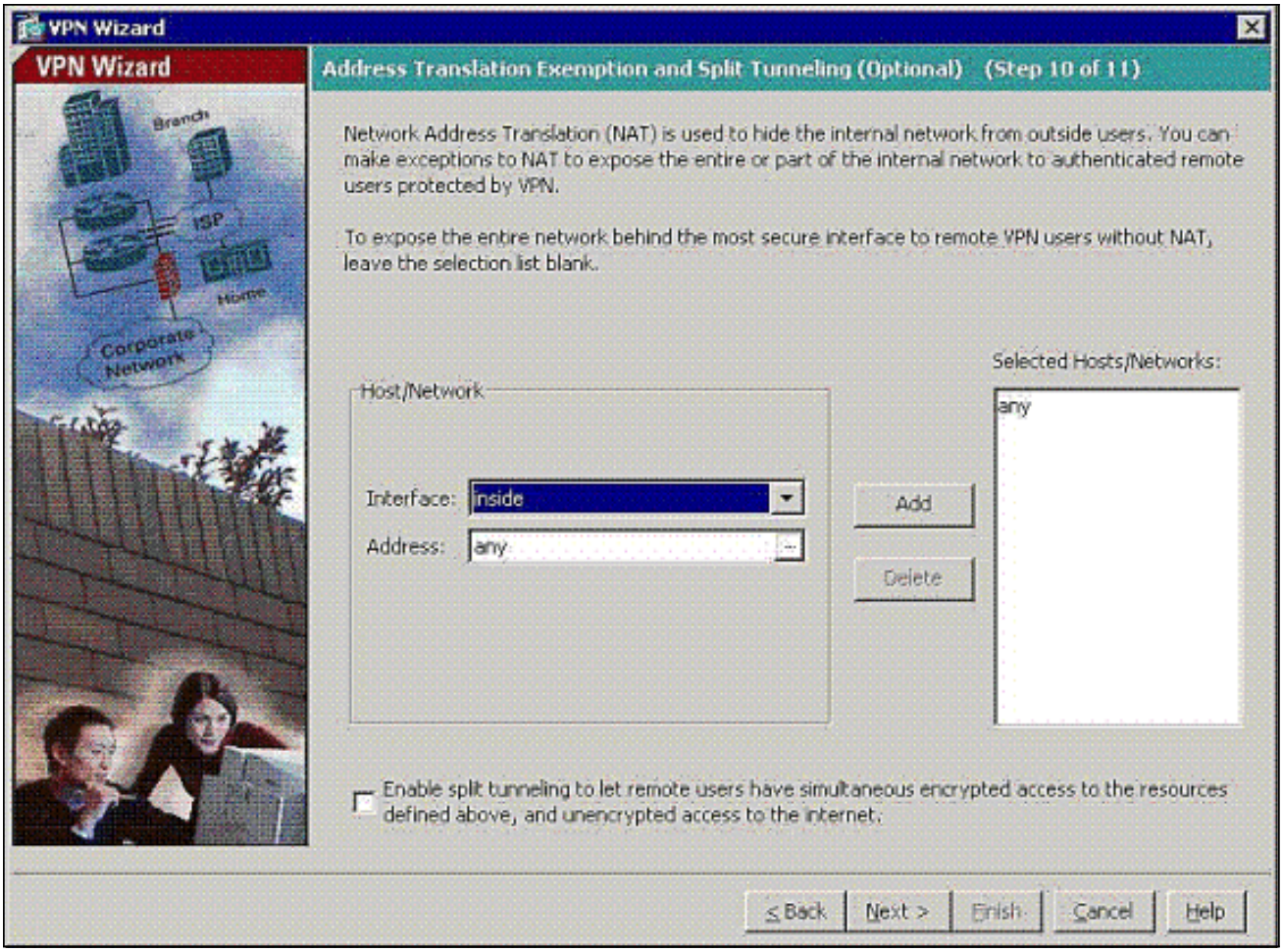
9. حدد معلمات IKE، المعروفة أيضا بالمرحلة 1 من IKE.يجب أن تتطابق التكوينات على كلا جانبي النفق تماما، ولكن يختار عميل Cisco VPN التكوين المناسب لنفسه تلقائيا. لا يلزم تكوين IKE على كمبيوتر العميل.



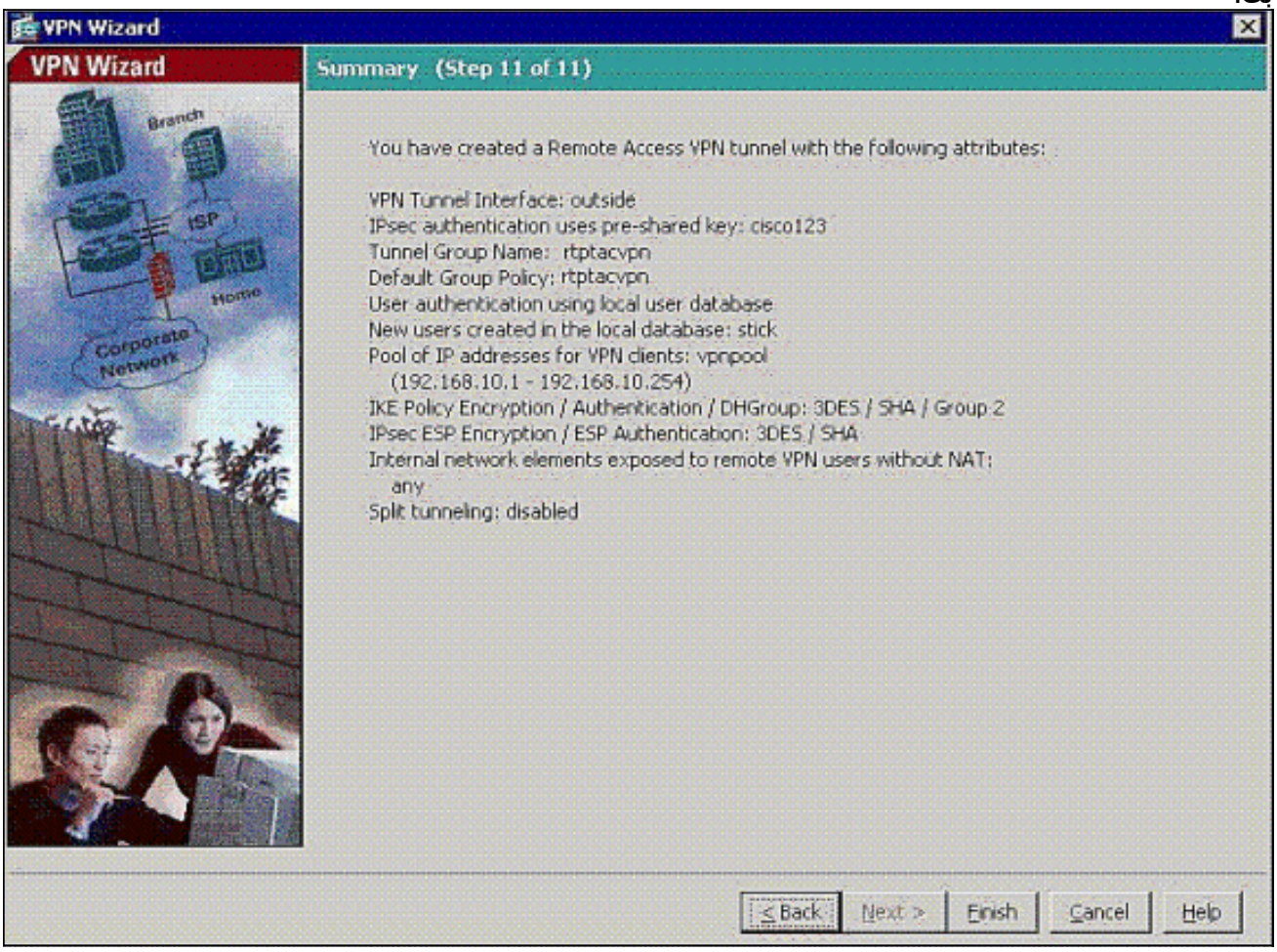
10. حدد معلمات IPSec، المعروفة أيضا باسم المرحلة 2 من IKE.يجب أن تتطابق التكوينات على كلا جانبي النفق تماما، ولكن يختار عميل Cisco VPN التكوين المناسب لنفسه تلقائيا. لا يلزم تكوين IKE على كمبيوتر العميل.



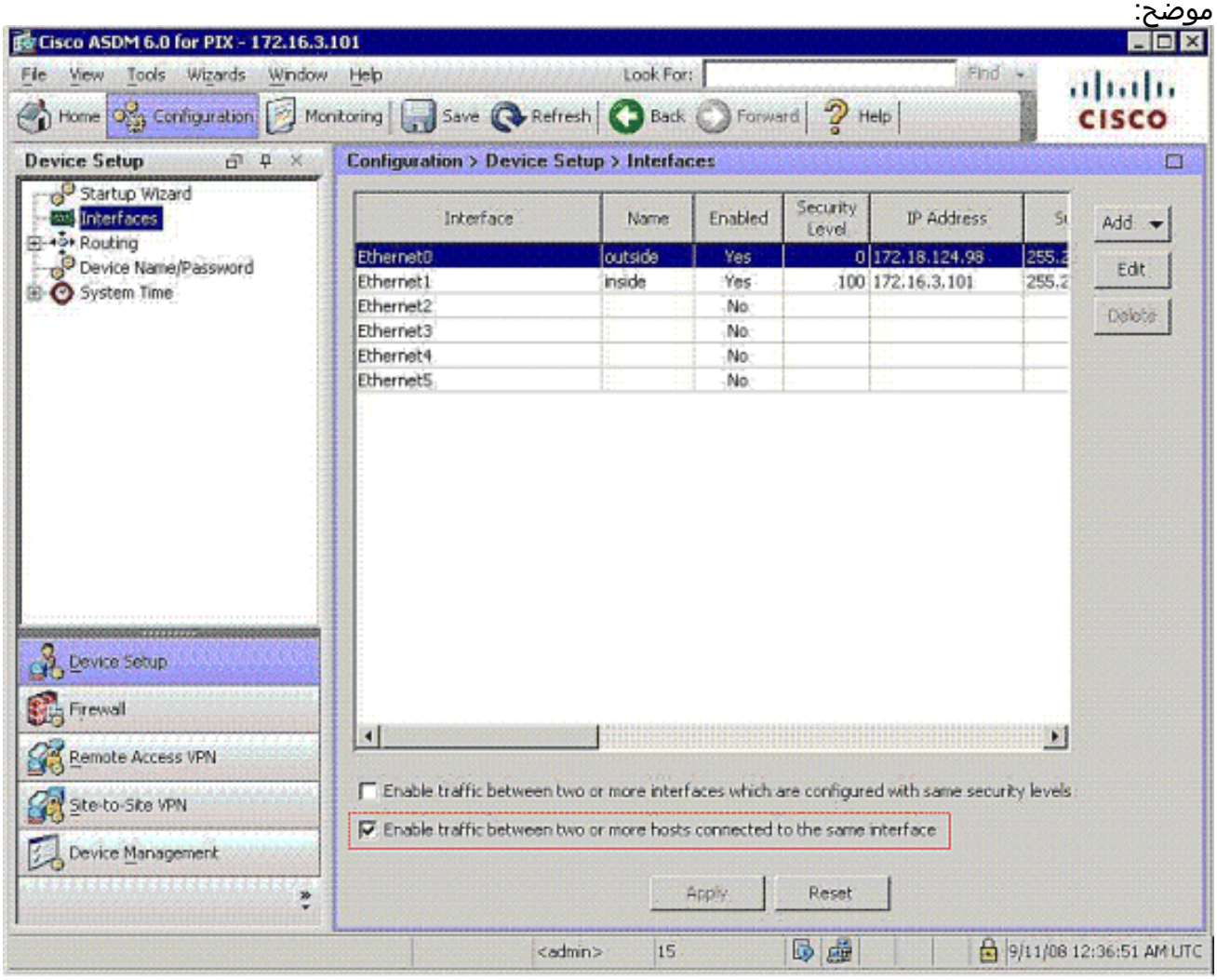
11. حدد أي البيئات المضيفة الداخلية أو الشبكات، إن وجدت، يمكن أن تتعرض لمستخدمي شبكات VPN البعيدة.إن يترك أنت هذا قائمة فارغ، هو يسمح بعيد VPN مستعمل أن ينفذ الكامل داخل شبكة من ال ASA.أنت يستطيع أيضا مكنت انقسام tunneling على هذا نافذة. يقوم تقسيم الاتصال النفقي بتشفير حركة مرور البيانات إلى الموارد المحددة مسبقا في هذا الإجراء وتوفير وصول غير مشفر إلى الإنترنت بشكل عام من خلال عدم إنشاء قنوات لحركة مرور البيانات هذه. إن لا يمكن انقسام tunneling يكون، كل حركة مرور من بعيد VPN مستعمل أنفاق إلى ال ASA. يمكن أن يشكل ذلك نطاقا ترديا عريضا جدا ومعالجا مكثفا، وذلك بناء على عملية التهيئة
لديك.



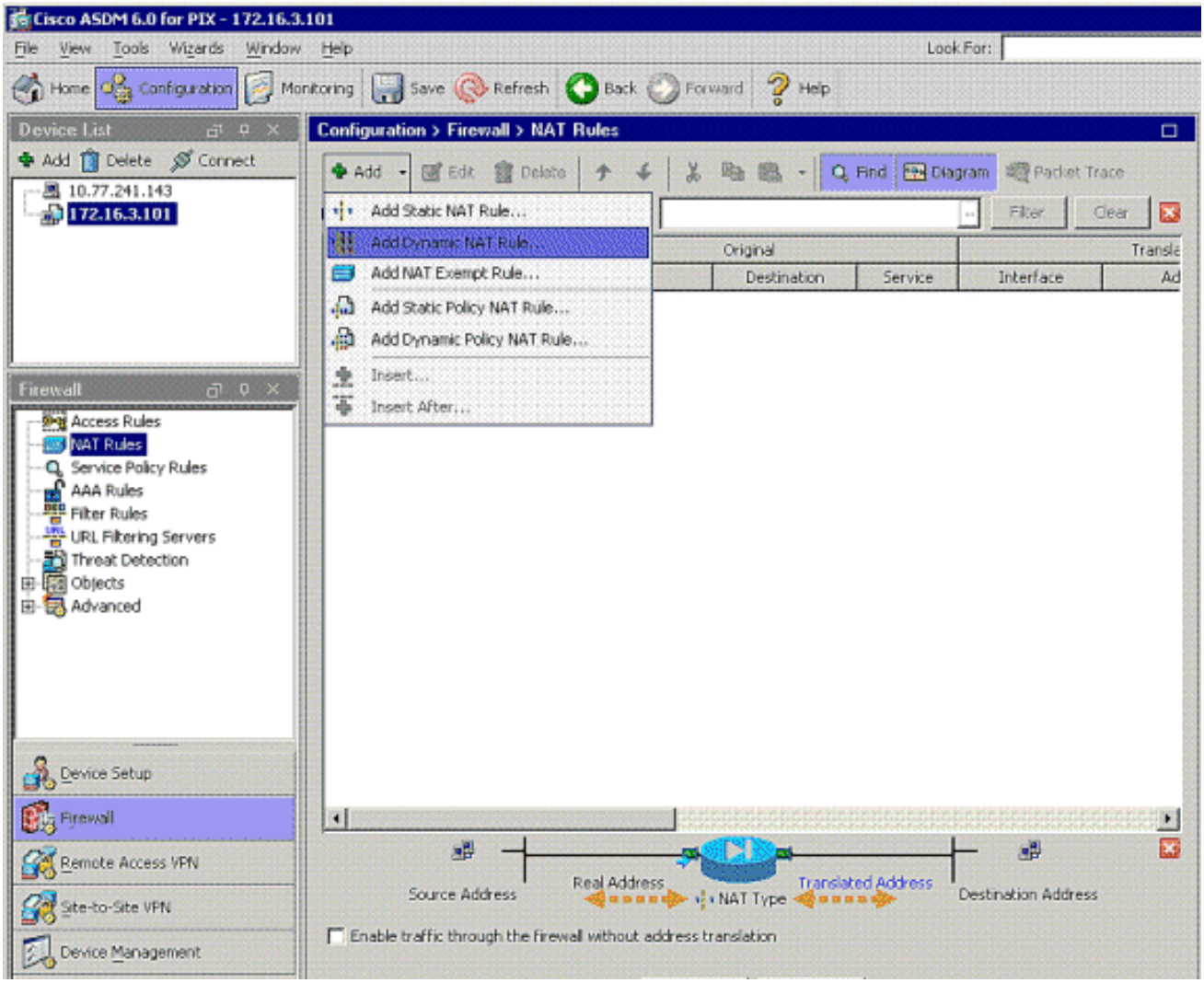
12. تعرض هذه النافذة ملخصا للإجراءات التي اتخذتها. انقر فوق **إنهاء** إذا كنت راضيا عن التكوين الخاص بك.



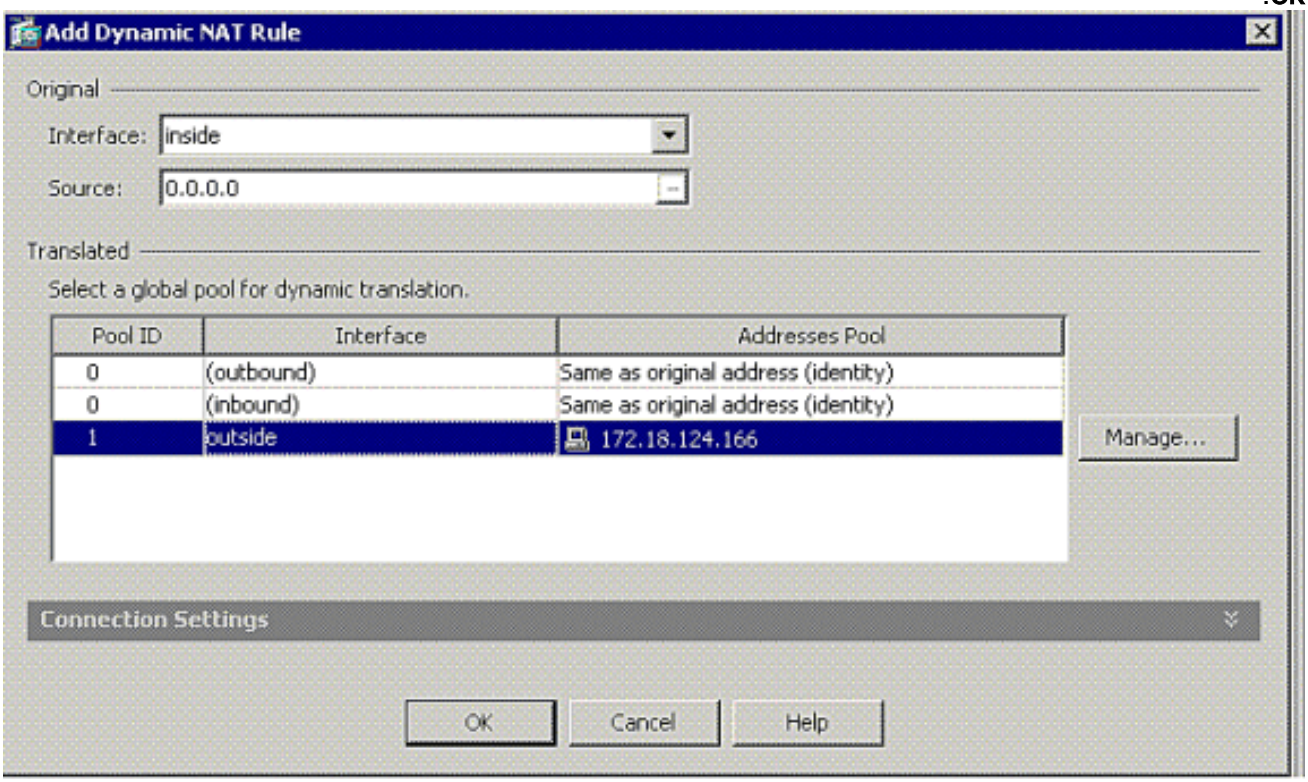
13. قم بتكوين الأمر **نفسه-security-traffic** لتمكين حركة مرور البيانات بين جهازين مضيفين أو أكثر موصولين بنفس الواجهة عند النقر فوق خانة الاختيار كما هو موضح:



14. أخترت **تشكيل>جدار حماية >nat قاعدة**، **ويضيف حركي nat قاعدة** in order to خلقت هذا ترجمة حركية مع الإستعمالمن ASDM.

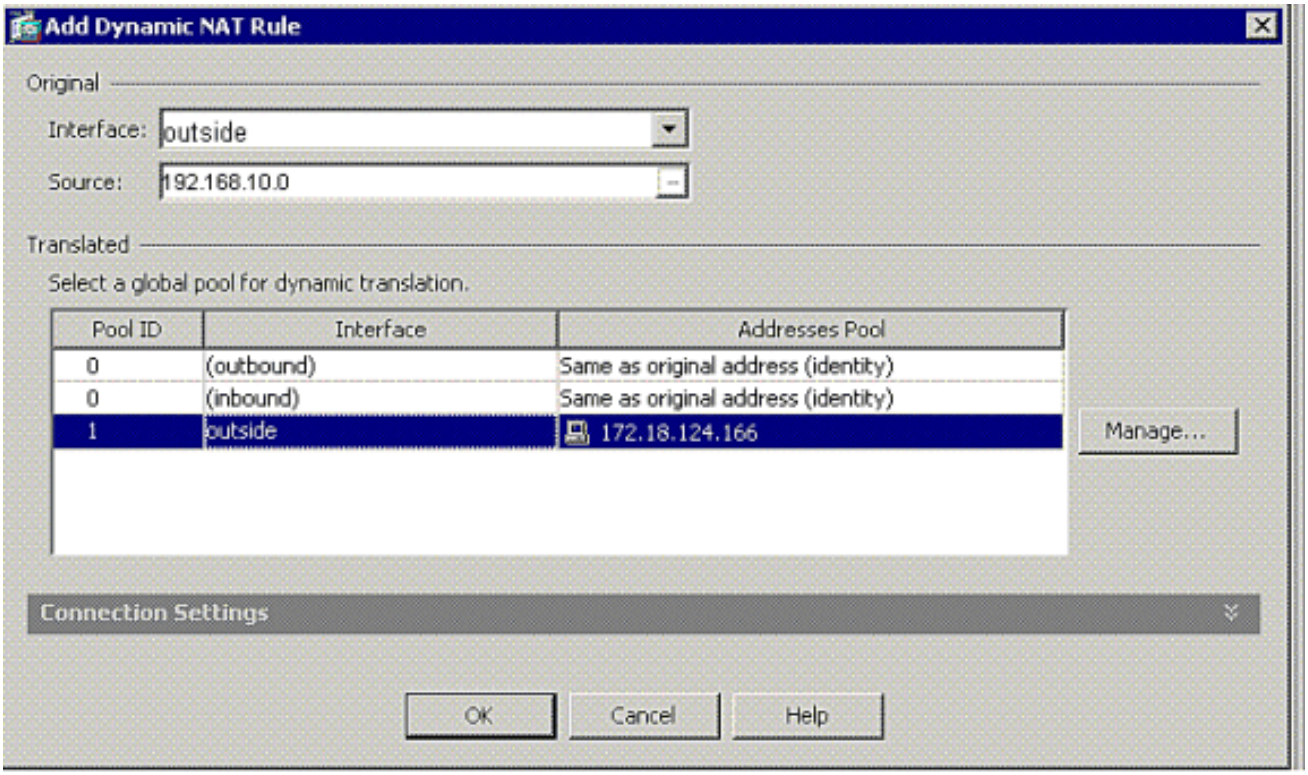


15. أخترت **داخلي** كمصدر قارن، ودخلت العنوان أنت تريد أن nat. أخترت ل ترجمة عنوان على قارن، **خارج** وطقطقة **ok**.

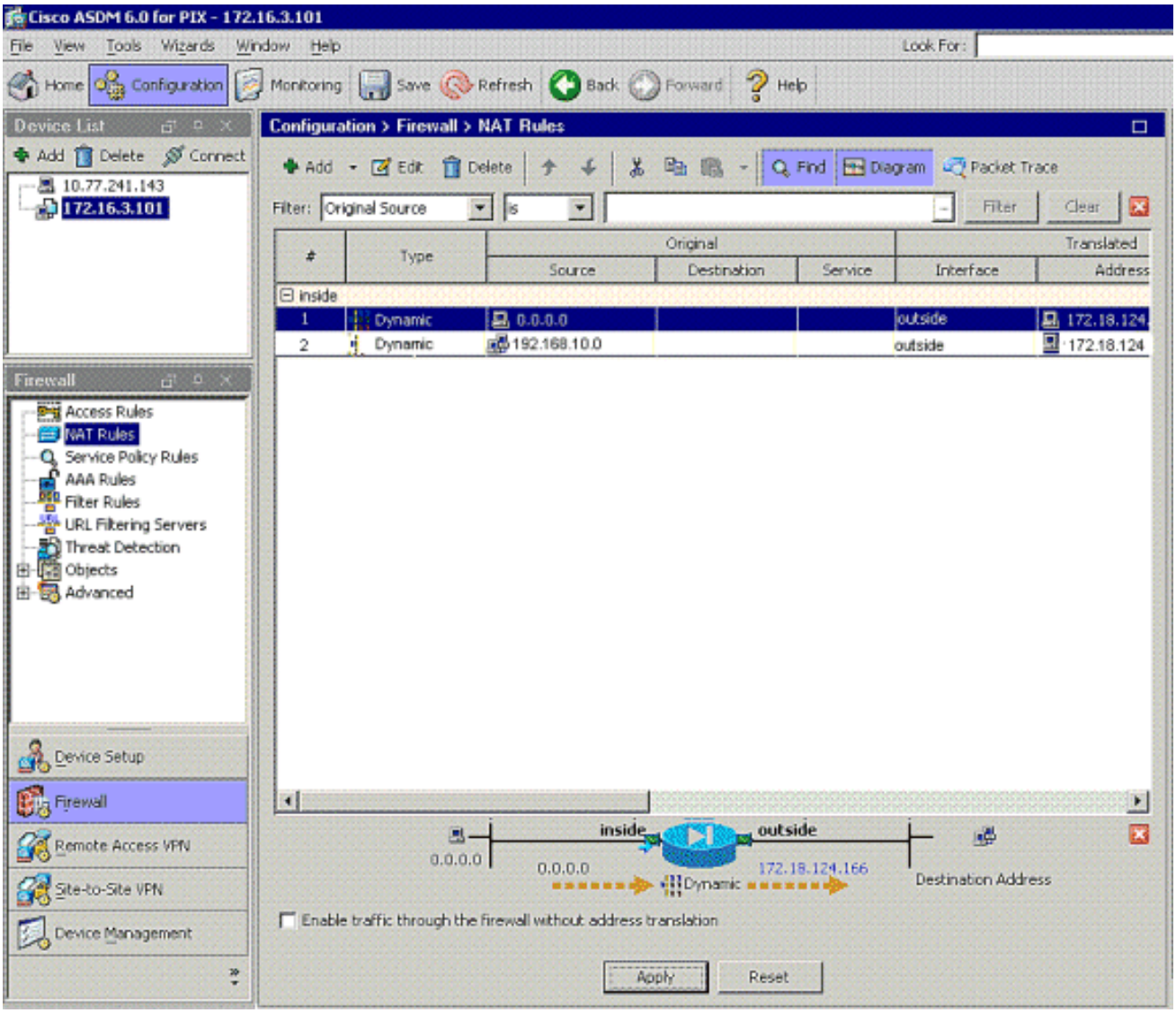


16. أخترت **خارجي** كمصدر قارن، ودخلت العنوان أنت تريد أن nat. أخترت ل ترجمة عنوان على قارن، **خارج** وطقطقة

.**ok**



17. يظهر الترجمة في الترجمة قاعدة في **تشكيل > جدار حماية >nat قاعدة**.



ملاحظة 1: يلزم تكوين الأمر sysopt connection allowed-vpn. يتحقق الأمر show running-config sysopt إذا تم تكوينه.

ملاحظة 2: إضافة هذا الإخراج لنقل UDP الاختياري:

```
group-policy clientgroup attributes vpn-idle-timeout 20
ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

ملاحظة 3: قم بتكوين هذا الأمر في التكوين العام لجهاز PIX للاتصال بعملاء VPN عبر IPsec عبر TCP:

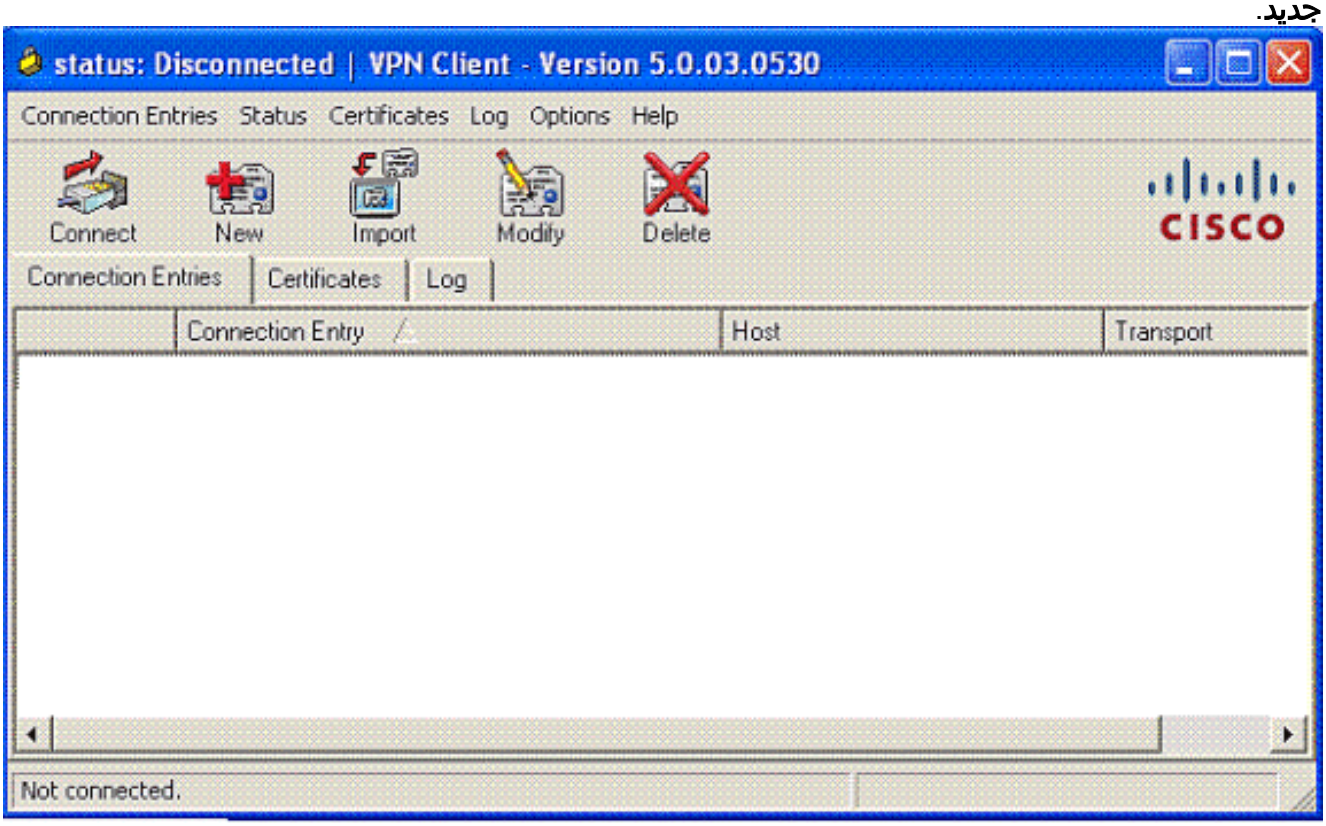
```
isakmp ipsec-over-tcp port 10000
```

ملاحظة: راجع فيديو شد الشعر على Cisco ASA للحصول على مزيد من المعلومات حول سيناريوهات مختلفة حيث يمكن إستخدام شد الشعر.

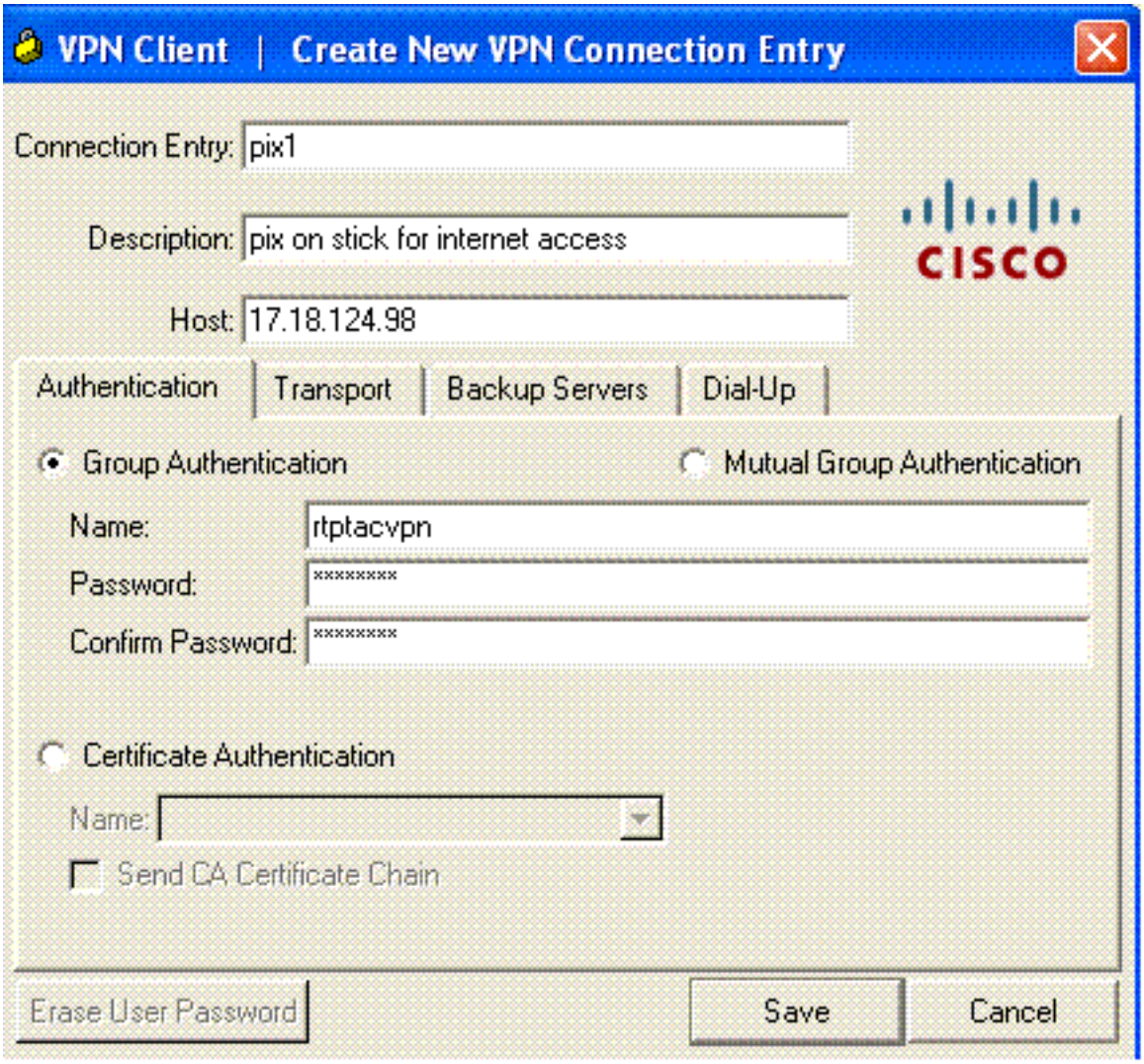
تكوين عميل شبكة VPN

أتمت هذا steps أن يشكل ال VPN زبون:

1. أختر **جديد**.

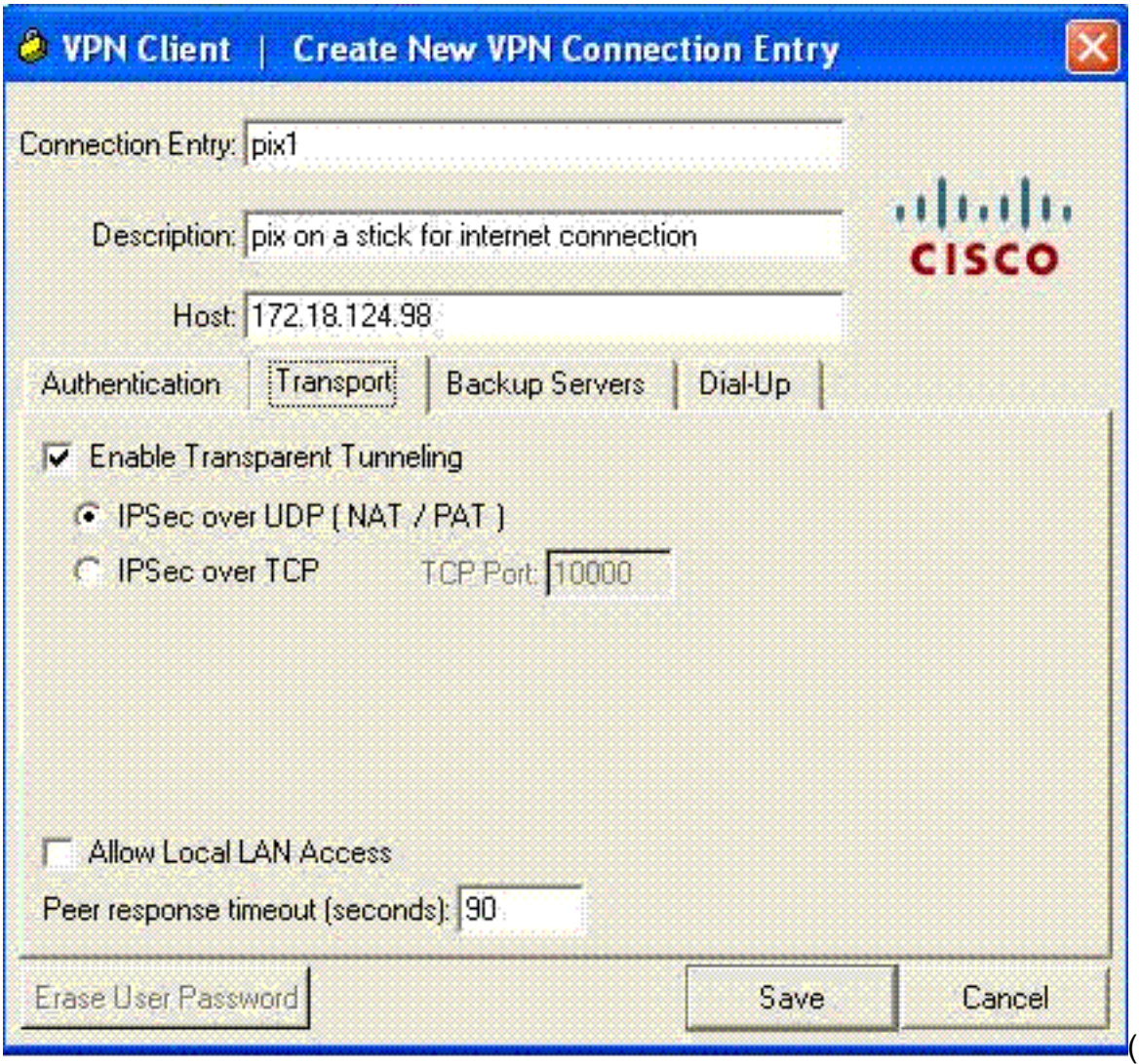


2. أدخل عنوان PIX الخارجي للواجهة واسم مجموعة النفق مع كلمة المرور



للمصادقة.

3. (*إختياري*) انقر فوق **تمكين الاتصال النفقي الشفاف** أسفل علامة التبويب نقل. (هذا إختياري ويتطلب تكوين PIX/ASA الإضافي المذكور في الملاحظة



(2.

4. احفظ التوصيف.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- show crypto isakmp sa — يعرض جميع اقترانات أمان IKE (SAs) الحالية في نظير.
- show crypto ipSec — يعرض جميع معرفات الخدمة الحالية. ابحث عن تشفير الحزم وفك تشفيرها على SA التي تعرف حركة مرور عميل VPN.

حاول إختبار الاتصال أو الاستعراض إلى عنوان IP عام من العميل (على سبيل المثال، www.cisco.com).

ملاحظة: لا يمكن إدخال الواجهة الداخلية ل PIX لتكوين نفق ما لم يتم تكوين الأمر management-access في وضع التأكيد العام.

```
PIX1(config)#management-access inside
PIX1(config)#show management-access

management-access inside
```

التحقق من عميل شبكة VPN

أتمت هذا steps in order to دققت ال VPN عميل.

1. انقر بزر الماوس الأيمن فوق رمز قفل عميل شبكة VPN الموجود في درج النظام بعد اتصال ناجح واختر خيار **الإحصائيات** لعرض التشفير وفك التشفير.
2. انقر فوق علامة التبويب تفاصيل المسار للتحقق من عدم تمرير قائمة النفق المقسم إلى أسفل من الجهاز.

استكشاف الأخطاء وإصلاحها

ملاحظة: للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء VPN وإصلاحها، ارجع إلى حلول أستكشاف أخطاء VPN وإصلاحها .

معلومات ذات صلة

- مثال تكوين شبكة VPN المحسنة المتصلة بالعميل ل PIX Security Appliance، الإصدار 7.0
- عميل شبكة VPN من Cisco
- مفاوضة IPSec/بروتوكولات IKE
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- تثبيت الشعر على Cisco ASA
- طلبات التعليقات (RFCs)
- 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).