PIX/ASA كخادم VPN بعيد مع مصادقة موسعة باستخدام مثال تكوين CLI و ASDM

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 للعمل كخادم VPN بعيد باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) أو CLI (واجهة سطر الأوامر (CLI). يوفر برنامج إدارة قاعدة بيانات المحول (ASDM) إدارة ومراقبة أمان على مستوى عالمي من خلال واجهة إدارة سهلة الاستخدام قائمة على الويب. بمجرد اكتمال تكوين Cisco ASA، يمكن التحقق منه باستخدام عميل Cisco VPN.

ارجع إلى مثال تكوين المصادقة PIX/ASA 7.x و Cisco VPN Client 4.x مع Windows 2003 IAS RADIUS (مقابل Active Directory) لإعداد اتصال VPN للوصول عن بعد بين عميل Cisco VPN 4.x ل Windows) وجهاز الأمان PIX 500 Series 7.x. يقوم مستخدم عميل شبكة VPN البعيدة بالمصادقة مقابل خدمة Active Directory باستخدام خادم RADIUS لخدمة مصادقة الإنترنت (IAS) ل Microsoft Windows 2003.

ارجع إلى PIX/ASA 7.x و Cisco VPN Client 4.x لمثال تكوين مصادقة Cisco Secure ACS من أجل إعداد اتصال VPN للوصول عن بعد بين عميل Cisco VPN 4.x ل Windows) وجهاز الأمان PIX 500 Series 7.x باستخدام خادم التحكم في الوصول الآمن من Cisco (ACS الإصدار 3.2) للمصادقة الموسعة (Xauth).

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM أو CLI بإجراء تغييرات التكوين.

ملاحظة: ارجع إلى السماح بوصول HTTPS ل ASDM أو PIX/ASA 7.x: SSH على مثال تكوين الواجهة الداخلية والخارجية للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو SSH (Secure Shell).

المكونات المستخدمة

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

- برنامج جهاز الأمان القابل للتكيف الإصدار x.7 من Cisco والإصدارات الأحدث
- Adaptive Security Device Manager، الإصدار x.5 والإصدارات الأحدث
- Cisco VPN Client الإصدار x.4 والإصدارات الأحدث

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 x.7 والإصدارات الأحدث.

الاصطلاحات

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

معلومات أساسية

توفر تكوينات الوصول عن بعد الوصول الآمن عن بعد لعملاء Cisco VPN، مثل المستخدمين كثيري التنقل. تتيح الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد للمستخدمين البعيدين إمكانية الوصول الآمن إلى موارد الشبكة المركزية. يتوافق عميل شبكة VPN من Cisco مع بروتوكول IPSec وتم تصميمه خصيصا للعمل مع جهاز الأمان. ومع ذلك، يمكن أن يقوم جهاز الأمان بإنشاء إتصالات IPSec مع العديد من العملاء المتوافقين مع البروتوكول. ارجع إلى أدلة تكوين ASA للحصول على مزيد من المعلومات حول IPSec.

المجموعات والمستخدمين هم المفاهيم الأساسية في إدارة أمان الشبكات الخاصة الظاهرية (VPN) وفي تكوين جهاز الأمان. هم يعين شعار أن يحدد مستعمل منفذ إلى واستخدام ال VPN. المجموعة هي مجموعة من المستخدمين الذين يتم التعامل معهم ككيان واحد. يحصل المستخدمون على خصائصهم من نهج المجموعة. تحدد مجموعات النفق نهج المجموعة لاتصالات محددة. في حالة عدم تعيين نهج مجموعة معين لمستخدمين، يتم تطبيق نهج المجموعة الافتراضي للاتصال.

تتكون مجموعة النفق من مجموعة سجلات تحدد نهج اتصال النفق. تحدد هذه السجلات الخوادم التي تتم مصادقة مستخدمي النفق عليها، بالإضافة إلى خوادم المحاسبة، إن وجدت، التي يتم إرسال معلومات الاتصالات إليها. كما أنها تحدد نهج مجموعة افتراضي للاتصالات، وهي تحتوي على معلمات اتصال خاصة بالبروتوكول. تتضمن مجموعات الأنفاق عددا صغيرا من السمات المتعلقة بإنشاء النفق نفسه. تتضمن مجموعات النفق مؤشر لنهج المجموعة الذي يعرف السمات الموجهة للمستخدم.

ملاحظة: في نموذج التكوين في هذا المستند، يتم إستخدام حسابات المستخدمين المحليين للمصادقة. إذا كنت ترغب في إستخدام خدمة أخرى، مثل LDAP و RADIUS، ارجع إلى تكوين خادم RADIUS خارجي للتخويل والمصادقة.

بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP)، المسمى أيضا IKE، هو بروتوكول التفاوض الذي يستضيف الاتفاق على كيفية إنشاء اقتران أمان IPSec. وينقسم كل تفاوض من مفاوضات ISAKMP إلى قسمين،

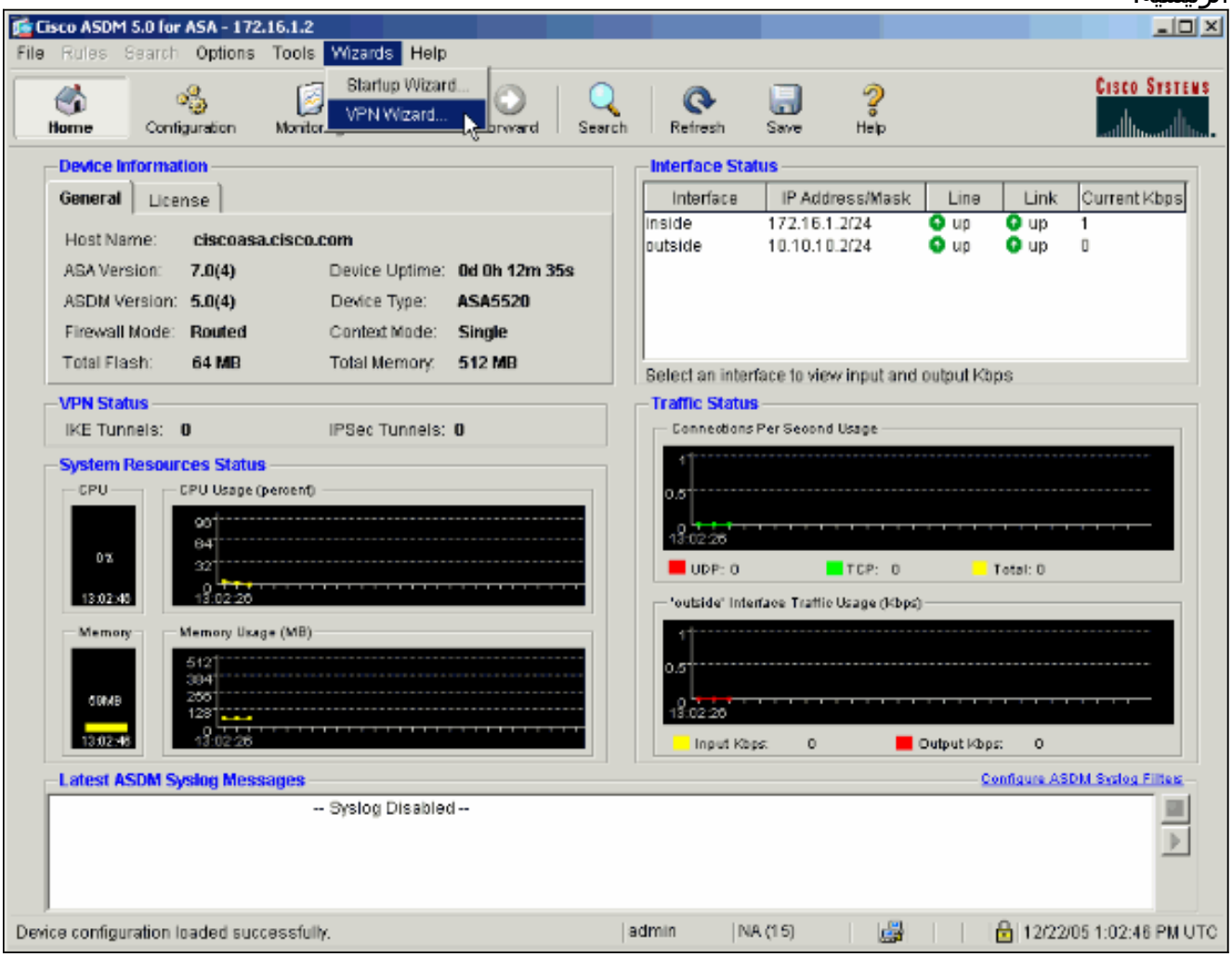
المرحلة 1 والمرحلة 2. تنشئ المرحلة 1 النفق الأول لحماية رسائل تفاوض ISAKMP اللاحقة. تقوم المرحلة 2 بإنشاء النفق الذي يحمي البيانات التي تتنقل عبر الاتصال الآمن. راجع الكلمات الأساسية لسياسة ISAKMP لأوامر CLI للحصول على مزيد من المعلومات حول ISAKMP.

التكوينات

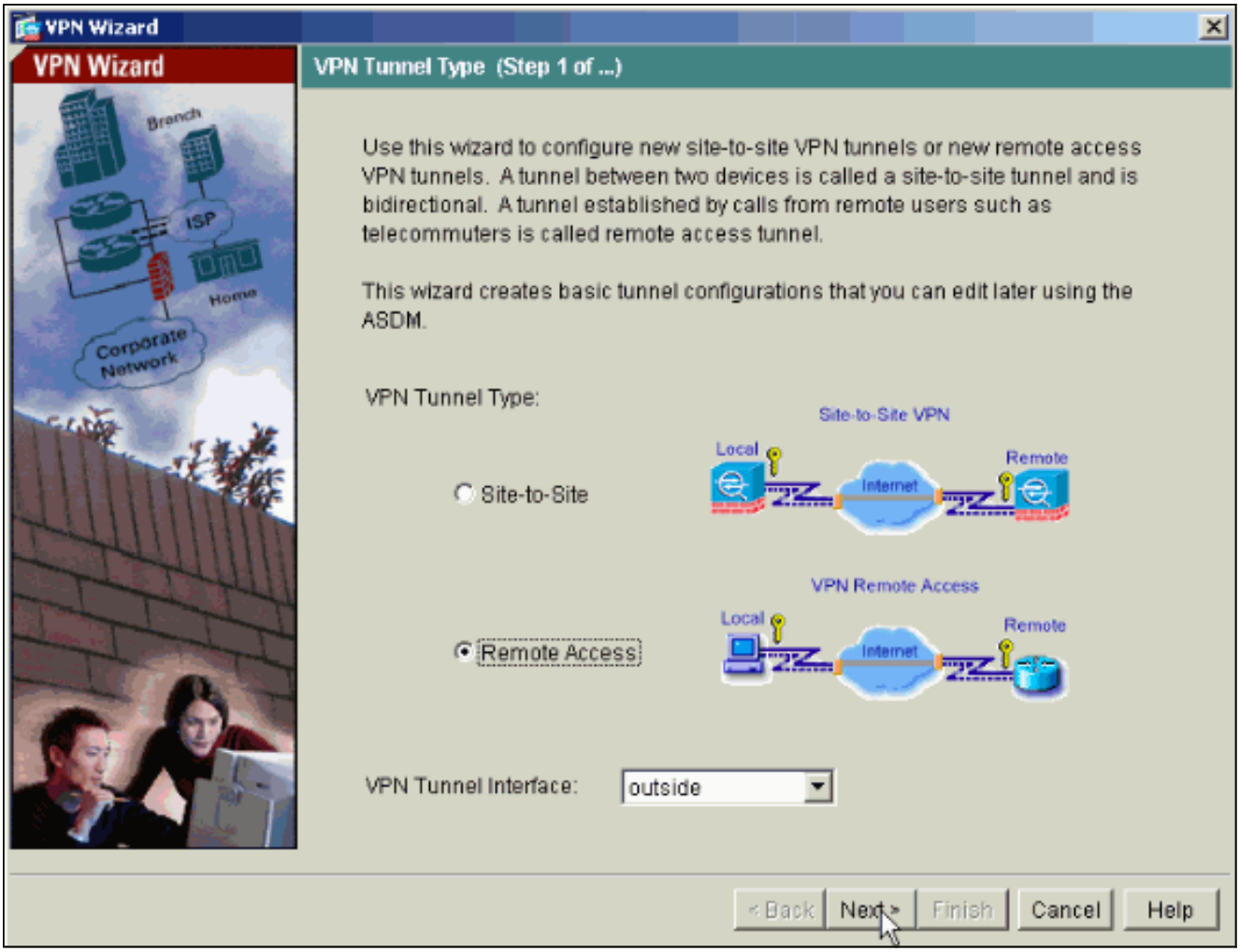
تكوين ASA/PIX كخادم VPN بعيد باستخدام ASDM

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

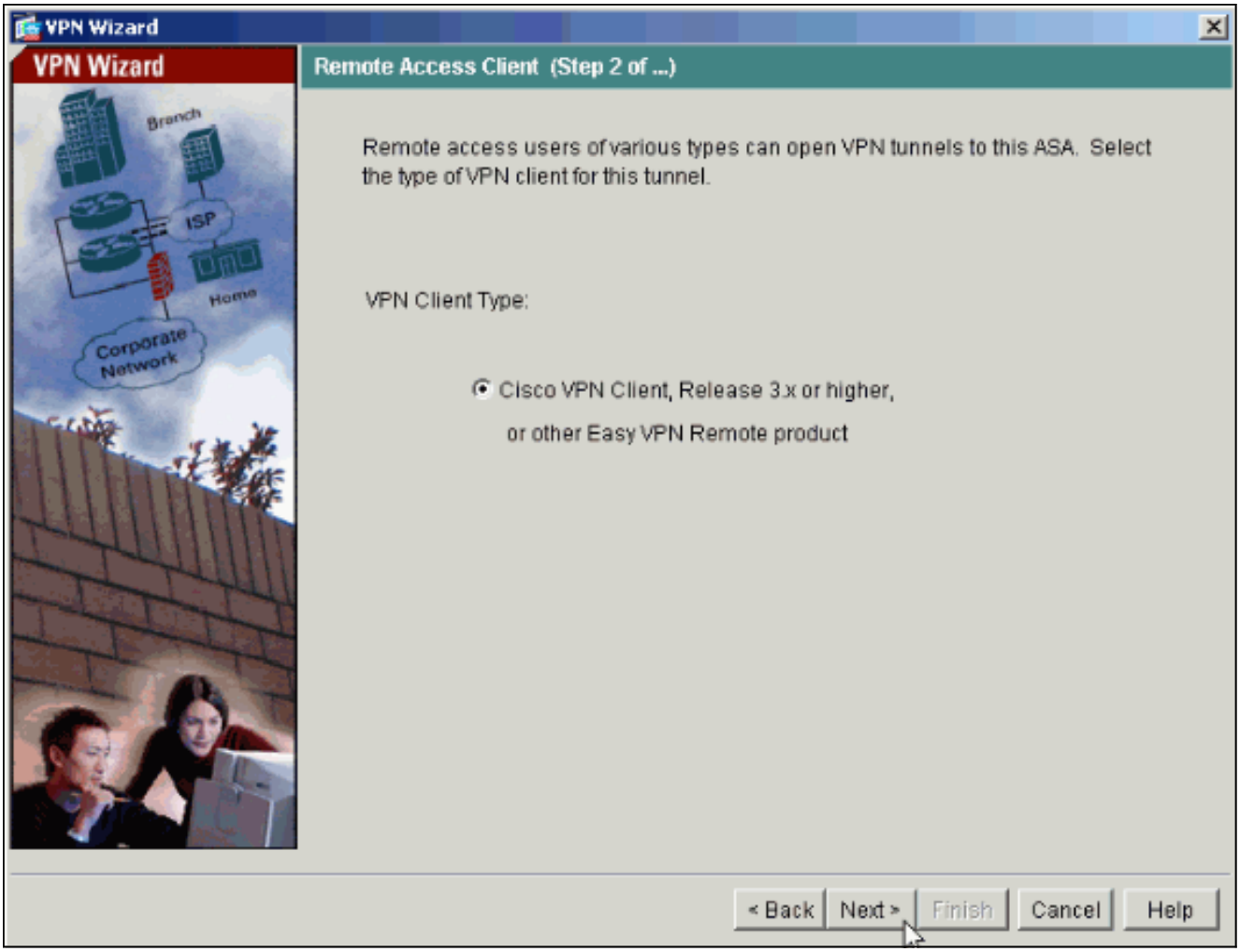
1. حدد **معالجات > معالج VPN** من النافذة الرئيسية.



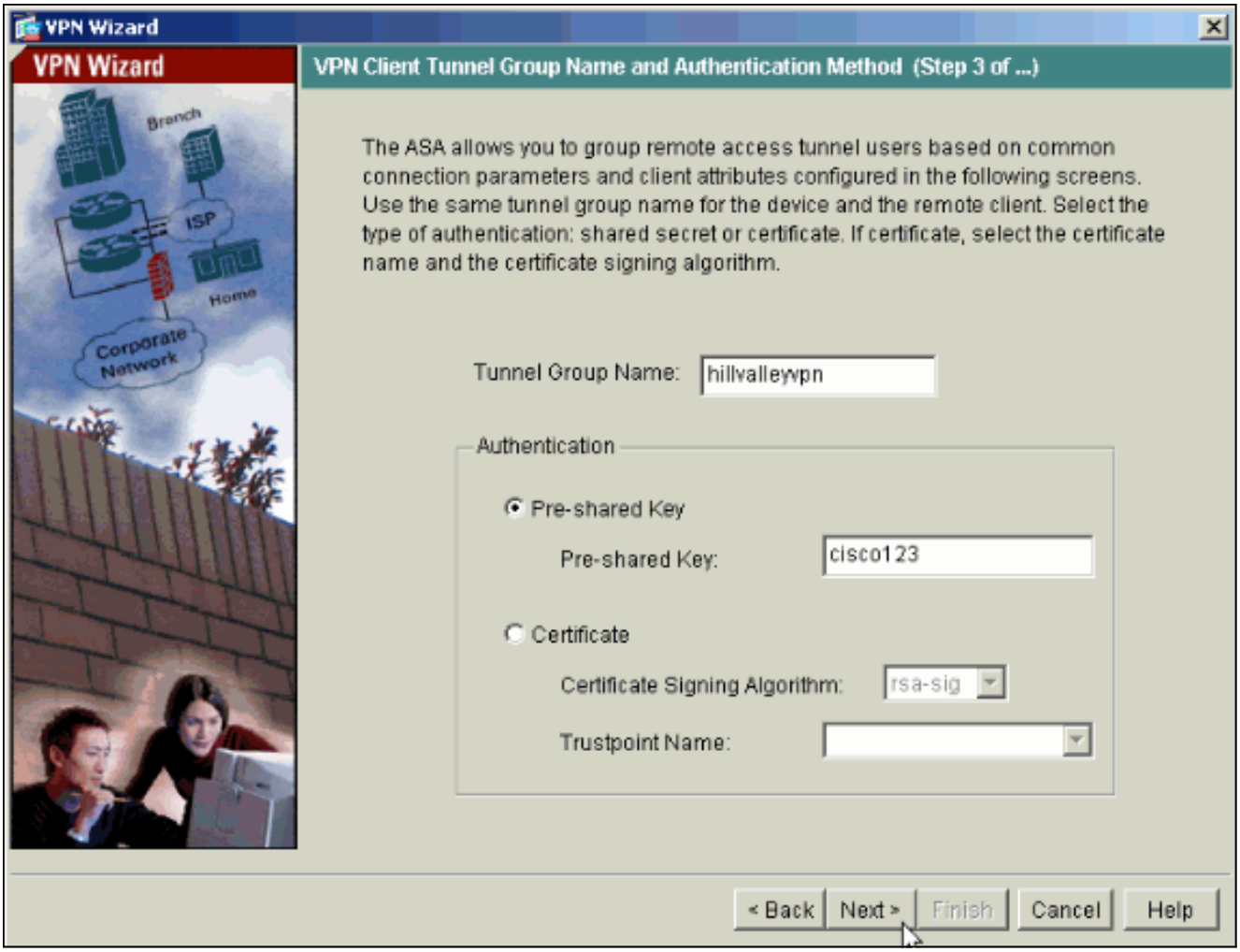
2. حدد نوع نفق VPN **Remote Access** وتأكد من تعيين واجهة نفق VPN على النحو المطلوب.



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

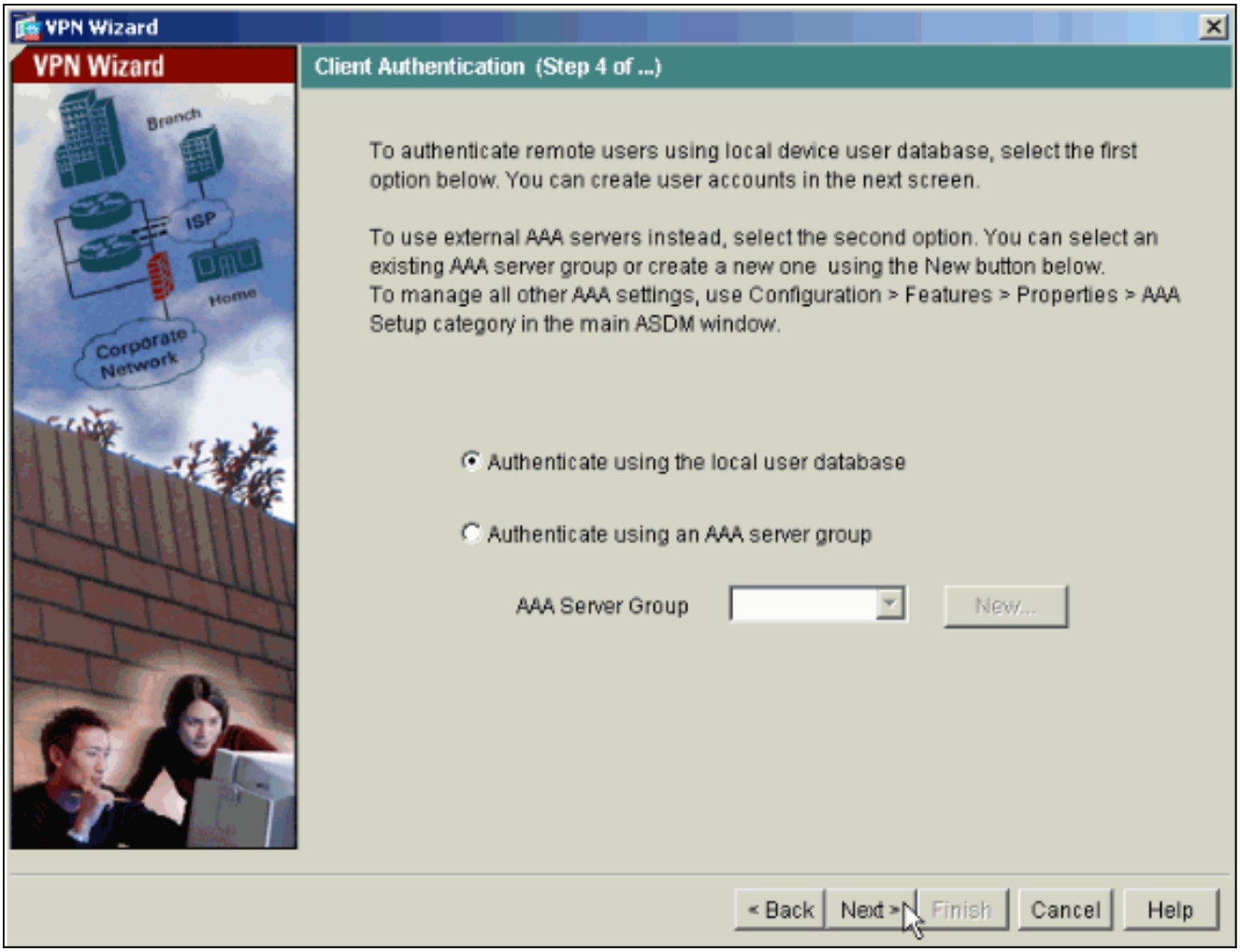


4. أدخل اسما لاسم مجموعة النفق. قم بتوفير معلومات المصادقة لاستخدامها.يتم تحديد **المفتاح المشترك مسبقا** في هذا
المثال.

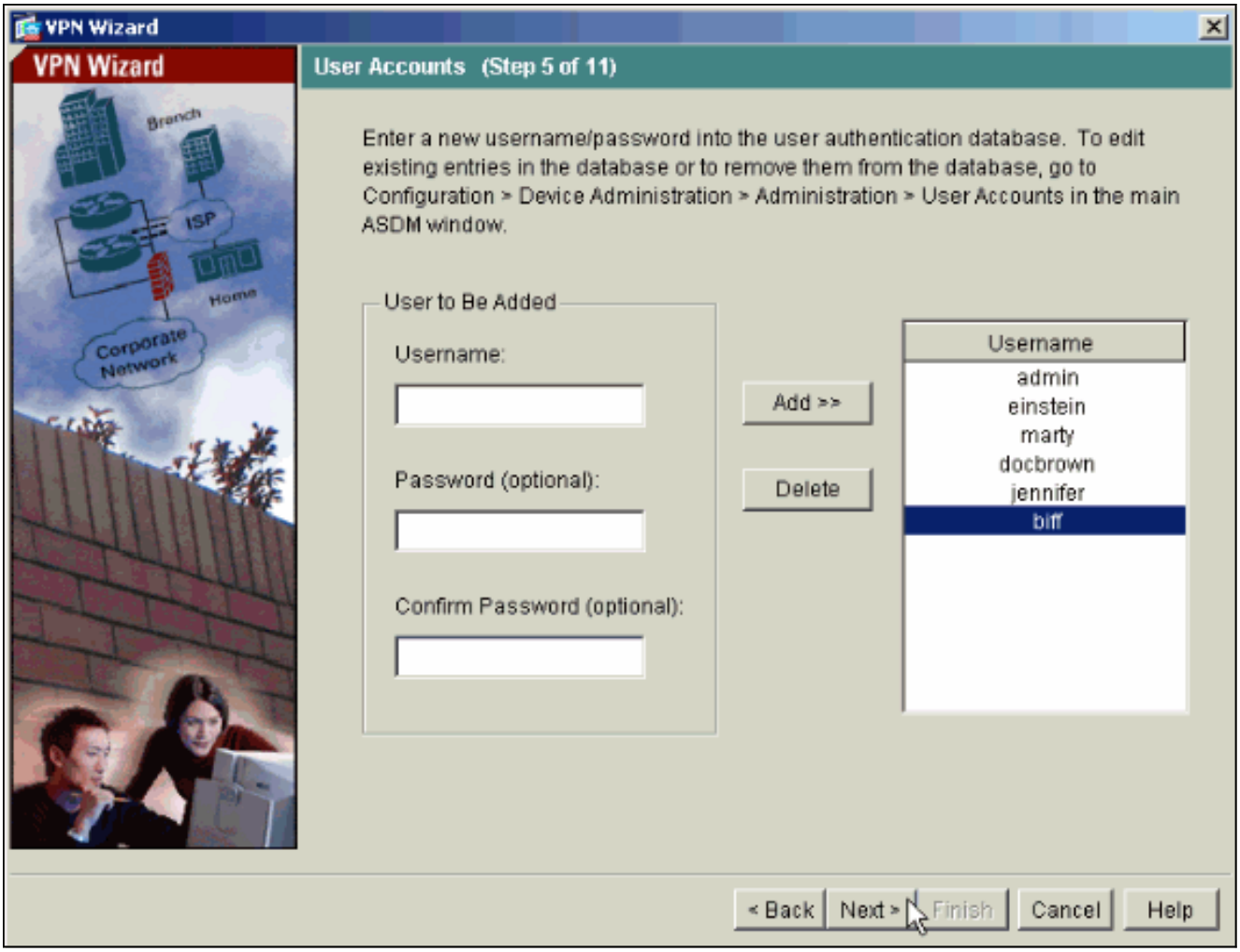


ملاحظة: لا توجد طريقة لإخفاء/تشفير المفتاح المشترك مسبقا على ASDM. السبب هو أنه يجب إستخدام ASDM فقط من قبل الأشخاص الذين يقومون بتكوين ASA أو الأشخاص الذين يساعدون العميل في هذا التكوين.

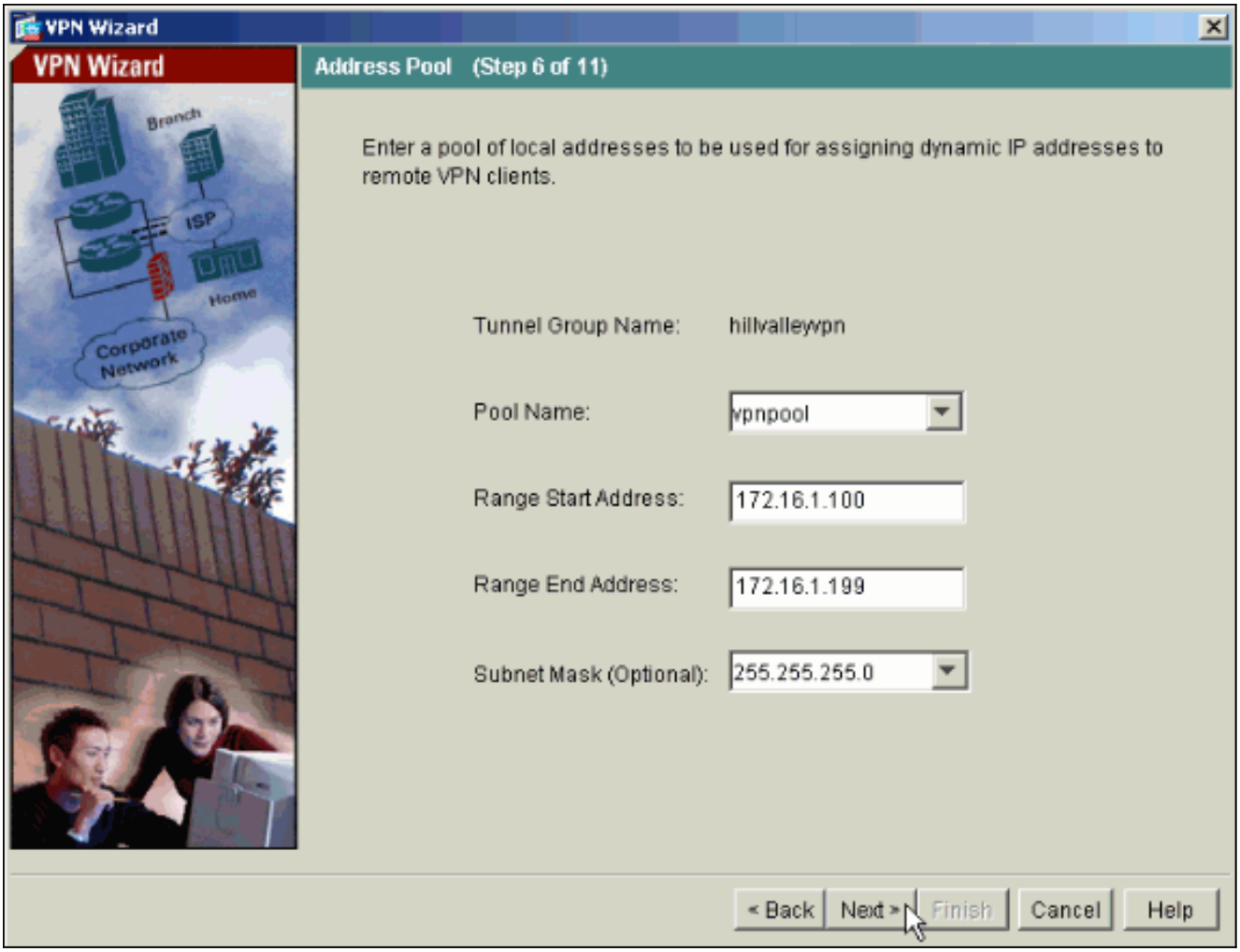
5. أختر ما إذا كنت تريد مصادقة المستخدمين عن بعد إلى قاعدة بيانات المستخدم المحلية أو إلى مجموعة خوادم AAA خارجية.**ملاحظة:** يمكنك إضافة مستخدمين إلى قاعدة بيانات المستخدم المحلية في الخطوة 6.**ملاحظة:** ارجع إلى مجموعات خوادم المصادقة والتفويض الخاصة ب PIX/ASA 7.x لمستخدمي VPN عبر مثال تكوين ASDM للحصول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



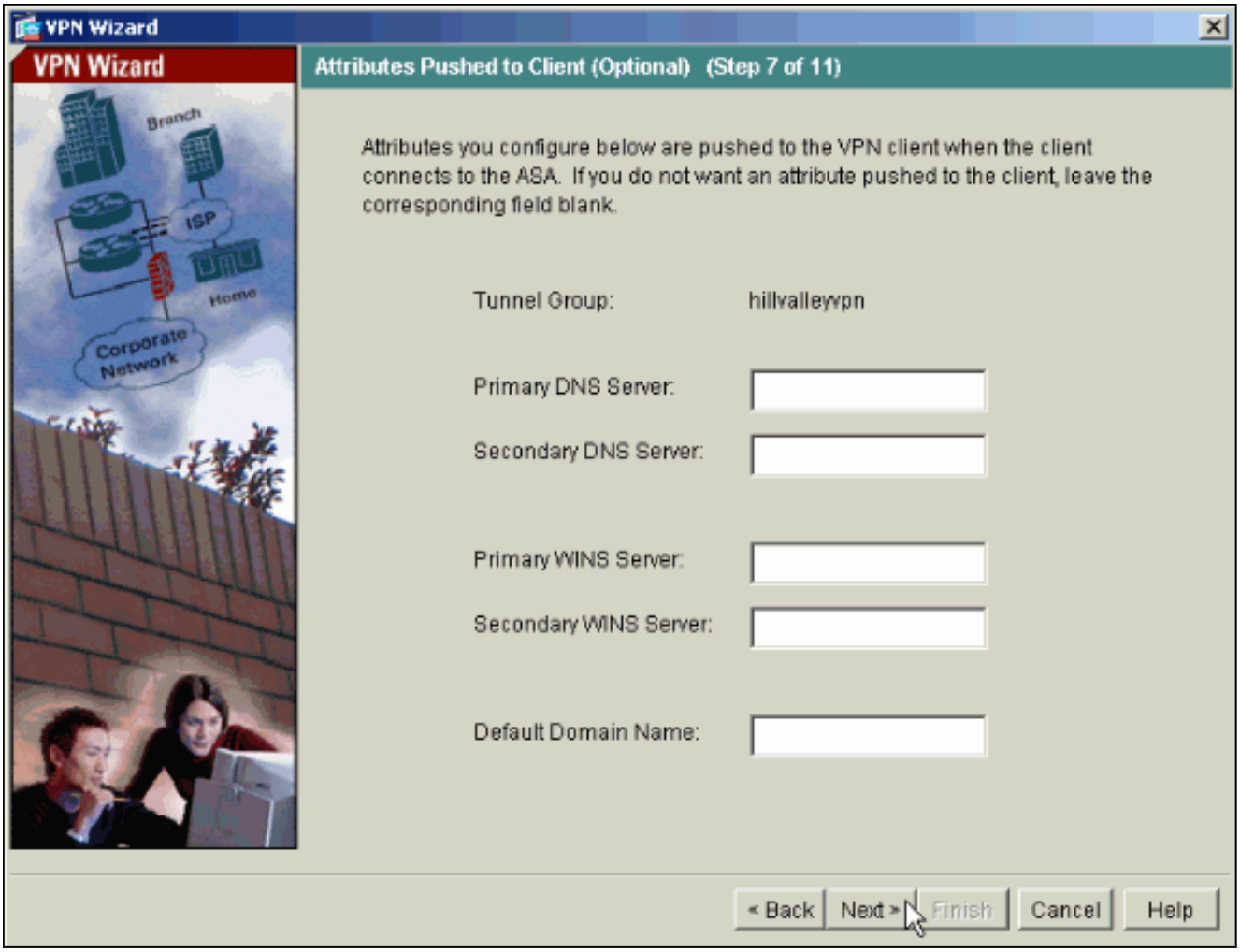
6. قم بإضافة مستخدمين إلى قاعدة البيانات المحلية إذا لزم الأمر.**ملاحظة:** لا تقم بإزالة المستخدمين الحاليين من هذا الإطار. حدد **تكوين > إدارة الأجهزة > إدارة > حسابات المستخدمين في نافذة ASDM الرئيسية** لتحرير الإدخالات الموجودة في قاعدة البيانات أو إزالتها من قاعدة البيانات.



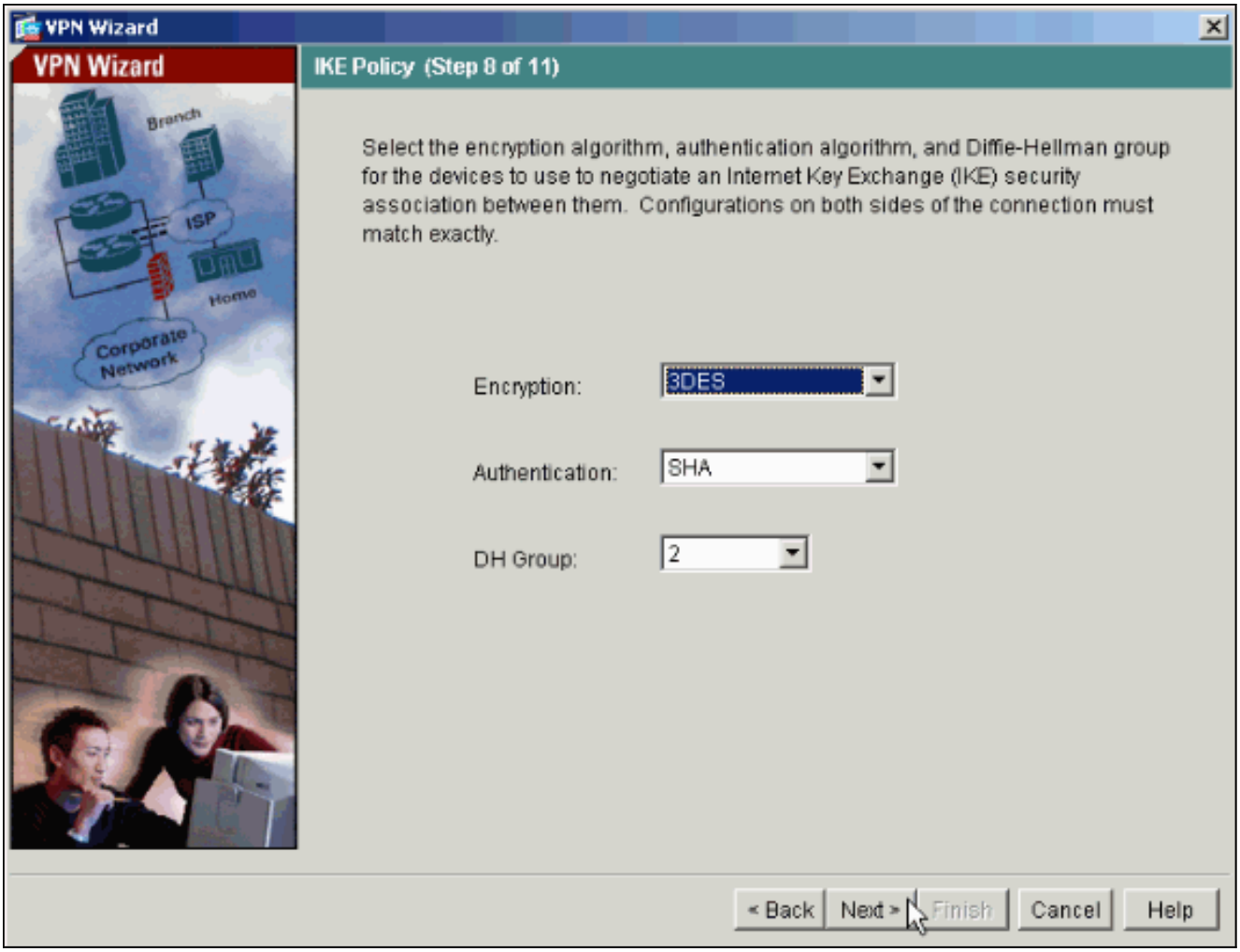
7. حدد مجموعة من العناوين المحلية ليتم تعيينها ديناميكيا لعملاء شبكات VPN البعيدة عند إتصالها.



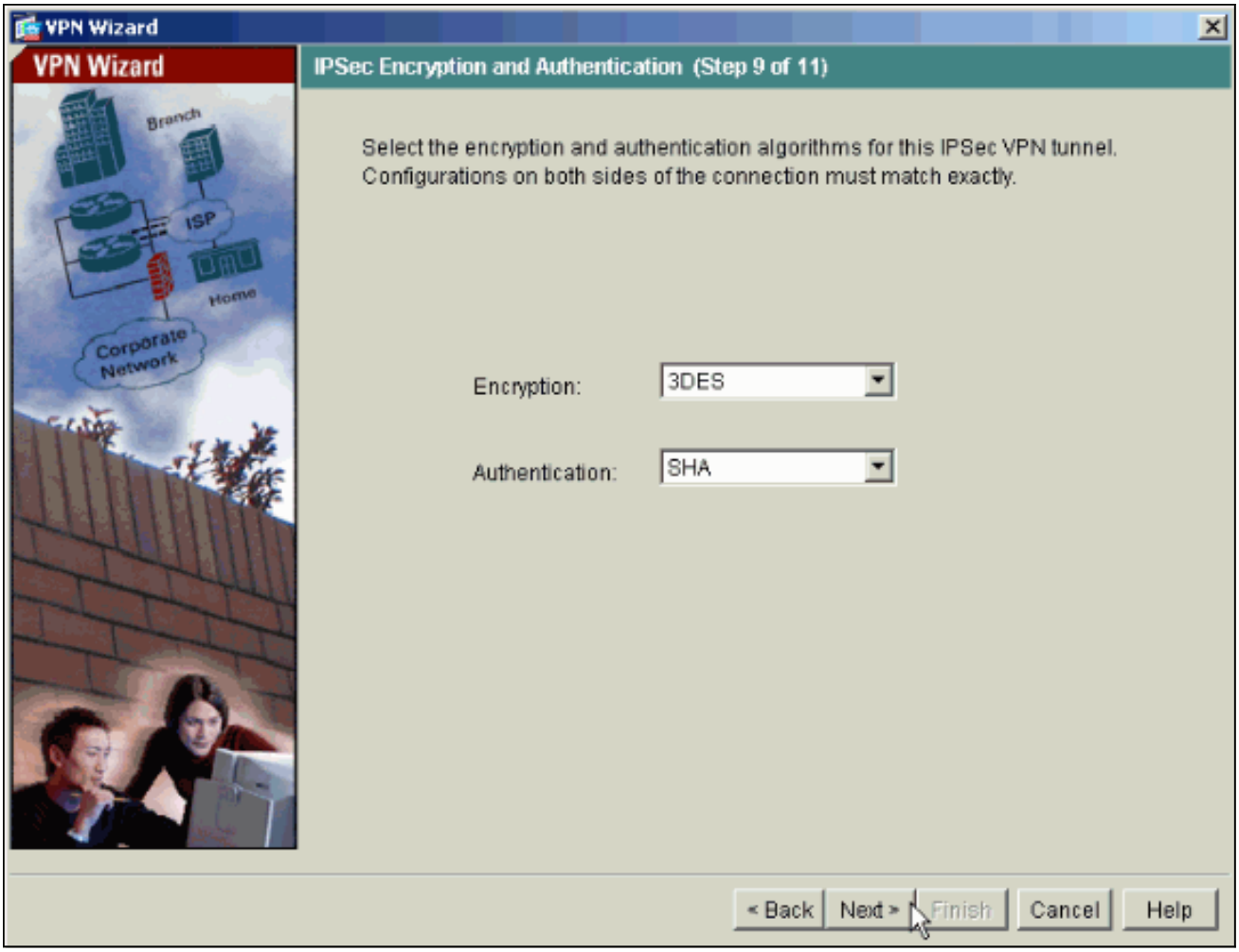
8. *إختياري:* حدد معلومات خادم DNS و WINS واسم مجال افتراضي ليتم دفعه إلى عملاء VPN البعيدة.



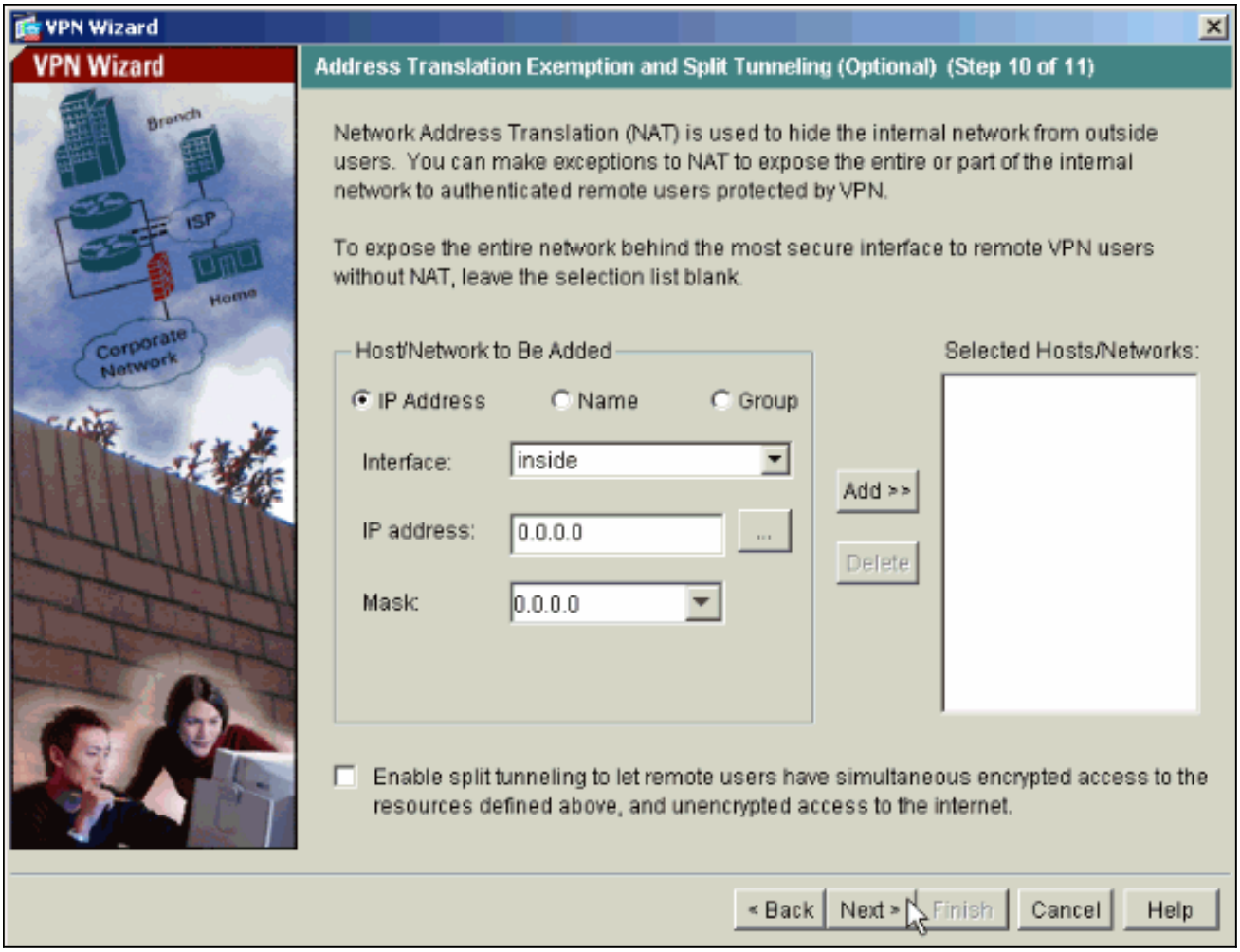
9. حدد معلمات IKE، المعروفة أيضا بالمرحلة 1 من IKE.يجب أن تتطابق التكوينات الموجودة على كلا جانبي النفق تماما. ومع ذلك، يحدد عميل شبكة VPN من Cisco التكوين المناسب تلقائيا لنفسه. لذلك، لا يلزم تكوين IKE على جهاز الكمبيوتر
العميل.



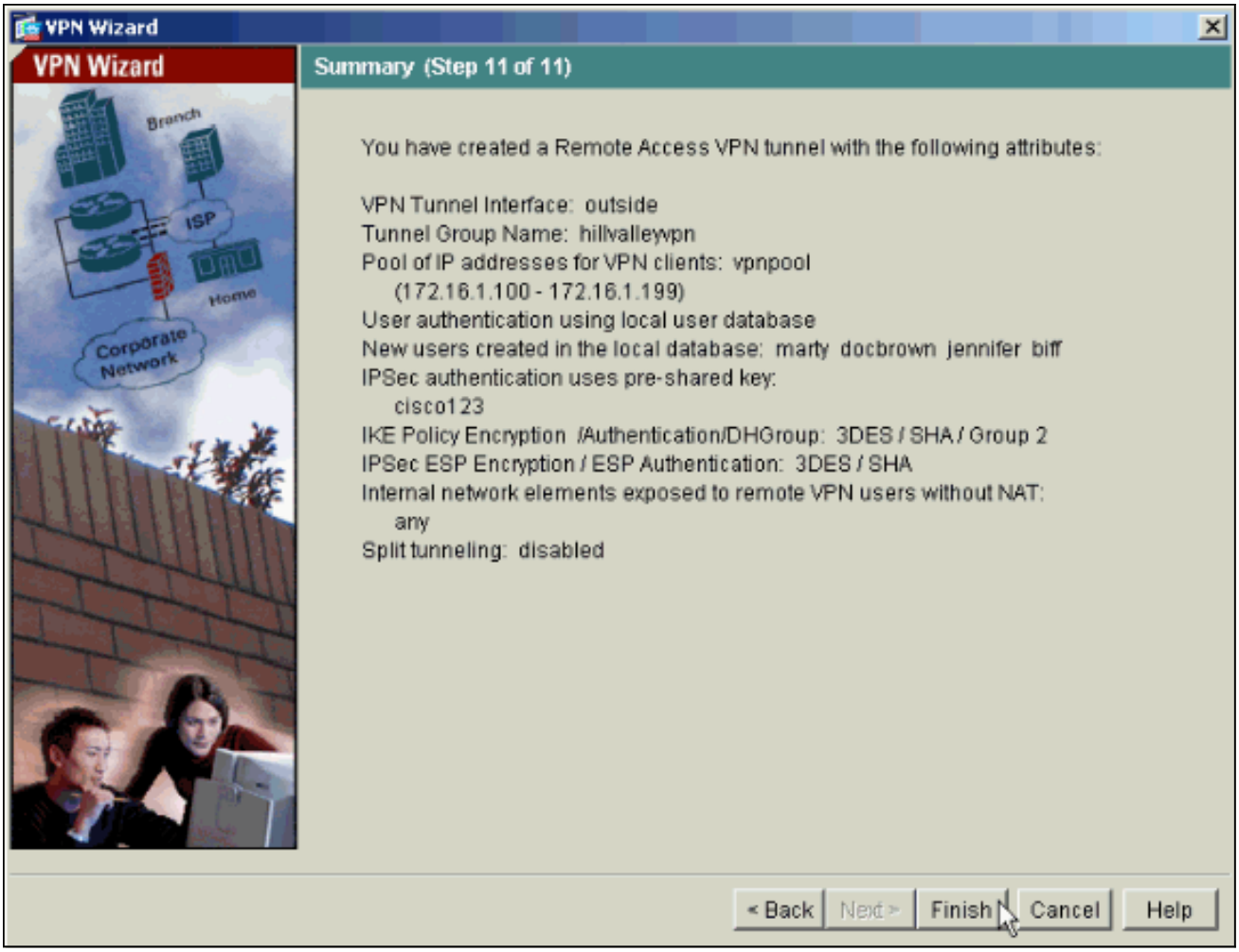
10. حدد معلمات IPSec، المعروفة أيضا باسم المرحلة 2 من IKE.يجب أن تتطابق التكوينات الموجودة على كلا جانبي النفق تماما. ومع ذلك، يحدد عميل شبكة VPN من Cisco التكوين المناسب تلقائيا لنفسه. لذلك، لا يلزم تكوين IKE على جهاز الكمبيوتر
العميل.



11. حدد أي البيئات المضيفة الداخلية أو الشبكات، إن وجدت، يجب أن يتم تعريفها 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.



تكوين ASA/PIX كخادم VPN بعيد باستخدام CLI (واجهة سطر الأوامر)

أتمت هذا steps in order to شكلت بعيد VPN منفذ نادل من الأمر خط. ارجع إلى تكوين شبكات VPN للوصول عن بعد أو مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances للحصول على مزيد من المعلومات حول كل أمر يتم إستخدامه.

1. دخلت **ال ip محلي بركة** أمر في شامل config أسلوب in order to شكلت عنوان بركة أن يستعمل ل VPN بعيد منفذ نفق. لحذف تجمعات العناوين، أدخل الصيغة no من هذا الأمر.يستخدم جهاز الأمان تجمعات العناوين استنادا إلى مجموعة الأنفاق للاتصال. إذا قمت بتكوين أكثر من تجمع عناوين واحد لمجموعة نفق، فإن جهاز الأمان يستخدمهم بالترتيب الذي تم تكوينهم به. أصدرت هذا أمر in order to خلقت بركة من عنوان محلي أن يستطيع كنت استعملت أن يعين عنوان حركي إلى وصول عن بعد VPN زبون:

```
ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
                    255.255.255.0
```

2. قم بإصدار هذا الأمر:

```
ASA-AIP-CLI(config)#username marty password 12345678
```

3. أصدرت هذا مجموعة الأمر in order to شكلت النفق خاص:**1 policy isakmp#**(config-AIP-CLI-ASA **صحة**
هوية قبل مشاركة-ASA-AIP-CLI(config)#**isakmp policy 1 encryption 3des**ASA-AIP-CLI(config)#**isakmp** **سياسة 1 hash**ASA-AIP-CLI(config)#**isakmp** **سياسة 1 مجموعة** -ASA-AIP-**2**
CLI(config)#**isakmp** **سياسة 1 مدى الحياة 43200**ASA-AIP-CLI(config)#**isakmp** **يمكن خارج**-ASA-AIP-CLI(config)#**crypto ipSec transform-set ESP-3DES-SHA ESP-3des esp-sha-hmac**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set reverse-route**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set security-association life**

seconds 288000ASA-AIP-CLI(config)#**crypto map outside_map 10 ipsSec-isakmp dynamic outside_dyn_map**ASA-AIP-CLI(config)#**crypto map outside_map interface** خارجي-ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**

4. *إختياري:* إذا كنت تريد أن يتجاوز الاتصال قائمة الوصول التي يتم تطبيقها على الواجهة، فعليك إصدار هذا الأمر:
ASA-AIP-CLI(config)#**sysopt connection permit-ipsec**

ملاحظة: يعمل هذا الأمر على الصور x.7 قبل 7.2(2). إذا كنت تستخدم الصورة 7.2(2)، فعليك إصدار الأمر ASA-AIP-CLI(config)#sysopt connection allowed-vpn.

5. قم بإصدار هذا الأمر:
ASA-AIP-CLI(config)#**group-policy hillvalleyvpn internal**

6. أصدرت هذا أمر in order to شكلت زبون توصيل عملية إعداد:سمات ASA-AIP-CLI(config)#**group-policy hillvalleyvpn**ASA-AIP-CLI(config)#(config-group-policy)#**dns-server value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**

7. قم بإصدار هذا الأمر:
ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**

8. قم بإصدار هذا الأمر:
ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**

9. قم بإصدار هذا الأمر:
ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**

10. قم بإصدار هذا الأمر:
ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**

11. أصدرت هذا أمر in order to أحلت المستعمل قاعدة معطيات محلي للمصادقة.
ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**

12. إقران نهج المجموعة بمجموعة النفق
ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**

13. قم بإصدار هذا الأمر أثناء وجوده في وضع السمات العامة لمجموعة نفق Hillvalleyvpn من أجل تعيين VPNpool الذي تم إنشاؤه في الخطوة 1 إلى مجموعة Hillvalleyvpn.
ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

تشغيل التكوين على جهاز ASA

```
ASA-AIP-CLI(config)#show running-config
(ASA Version 7.2(2
!
hostname ASAwAIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.10.10.2 255.255.255.0
!
interface Ethernet0/1
```

```
                                                nameif inside
                                              security-level 100
                                    ip address 172.16.1.2 255.255.255.0
                                                             !
                                             interface Ethernet0/2
                                                       shutdown
                                                      no nameif
                                                 no security-level
                                                     no ip address
                                                             !
                                             interface Ethernet0/3
                                                       shutdown
                                                      no nameif
                                                 no security-level
                                                     no ip address
                                                             !
                                           interface Management0/0
                                                       shutdown
                                                      no nameif
                                                 no security-level
                                                     no ip address
                                                             !
                                        passwd 2KFQnbNIdI.2KYOU encrypted
                                                   ftp mode passive
                                          dns server-group DefaultDNS
                                                domain-name corp.com
                                                   pager lines 24
                                                mtu outside 1500
                                                 mtu inside 1500
    ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
                                                   255.255.255.0
                                                    no failover
                    icmp unreachable rate-limit 1 burst-size 1
                                         no asdm history enable
                                              arp timeout 14400
                                          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
                        group-policy hillvalleyvpn1 internal
                     group-policy hillvalleyvpn1 attributes
                              dns-server value 172.16.1.11
                                 vpn-tunnel-protocol IPSec
                             default-domain value test.com
      username marty password 6XmYwQOO9tiYnUDN encrypted
                                    no snmp-server location
                                     no snmp-server contact
     snmp-server enable traps snmp authentication linkup
                                          linkdown coldstart
   crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
                                                   sha-hmac
 crypto dynamic-map outside_dyn_map 10 set transform-set
                                                ESP-3DES-SHA
     crypto dynamic-map outside_dyn_map 10 set security-
                          association lifetime seconds 288000
          crypto map outside_map 10 ipsec-isakmp dynamic
                                          outside_dyn_map
                 crypto map outside_map interface outside
                                crypto isakmp enable outside
                                     crypto isakmp policy 10
```

```
                                authentication pre-share
                                encryption 3des
                                hash sha
                                group 2
                                lifetime 86400
                        crypto isakmp nat-traversal  20
                    tunnel-group hillvalleyvpn type ipsec-ra
                tunnel-group hillvalleyvpn general-attributes
                                address-pool vpnpool
                        default-group-policy hillvalleyvpn
                tunnel-group hillvalleyvpn ipsec-attributes
                                * pre-shared-key
                                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:0f78ee7ef3c196a683ae7a4804ce1192
                                                end :
                                #(ASA-AIP-CLI(config
```

تكوين تخزين كلمة مرور عميل شبكة VPN من Cisco

إن يتلقى أنت كثير cisco VPN زبون، هو صعب جدا أن يتذكر all the VPN زبون اسم وكلمة. لتخزين كلمات المرور في جهاز عميل شبكة VPN، قم بتكوين ASA/PIX وعميل شبكة VPN كما يوضح هذا القسم.

ASA/PIX

أستخدم الأمر **group-policy attributes** في وضع التكوين العام:

```
group-policy VPNusers attributes
      password-storage enable
```

عميل شبكة VPN من Cisco

حرر .pcf **مبرد** وعدل هذا معلم:

```
SaveUserPassword=1
=UserPassword
```

تعطيل المصادقة الموسعة

في وضع مجموعة النفق، أدخل هذا الأمر لتعطيل المصادقة الموسعة، والتي يتم تمكينها بشكل افتراضي، على PIX/ASA 7.x:

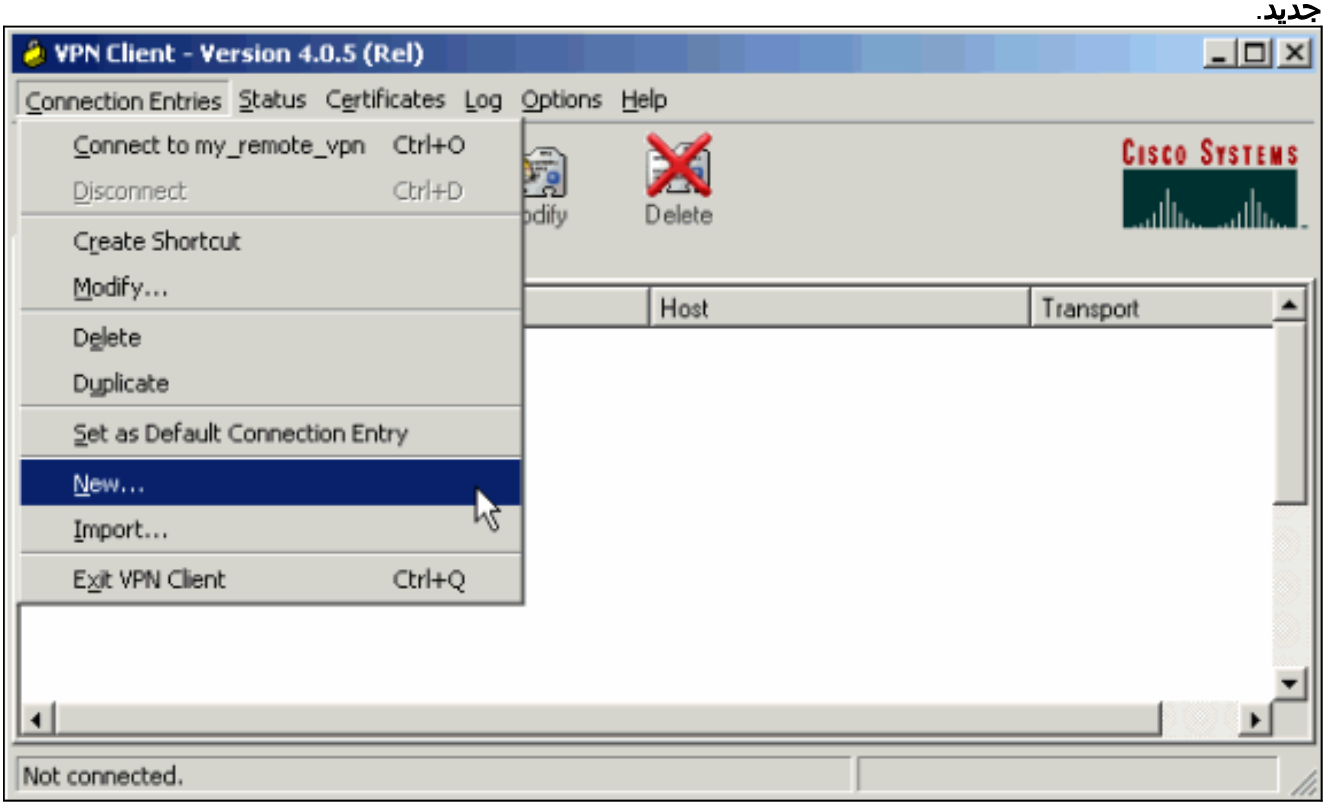
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

بعد تعطيل المصادقة الموسعة، لا يقوم عملاء VPN بإنشاء اسم مستخدم/كلمة مرور لمصادقة (Xauth). لذلك، لا يتطلب ال ASA/PIX ال username وكلمة تشكيل أن يصدق ال VPN زبون.

التحقق من الصحة

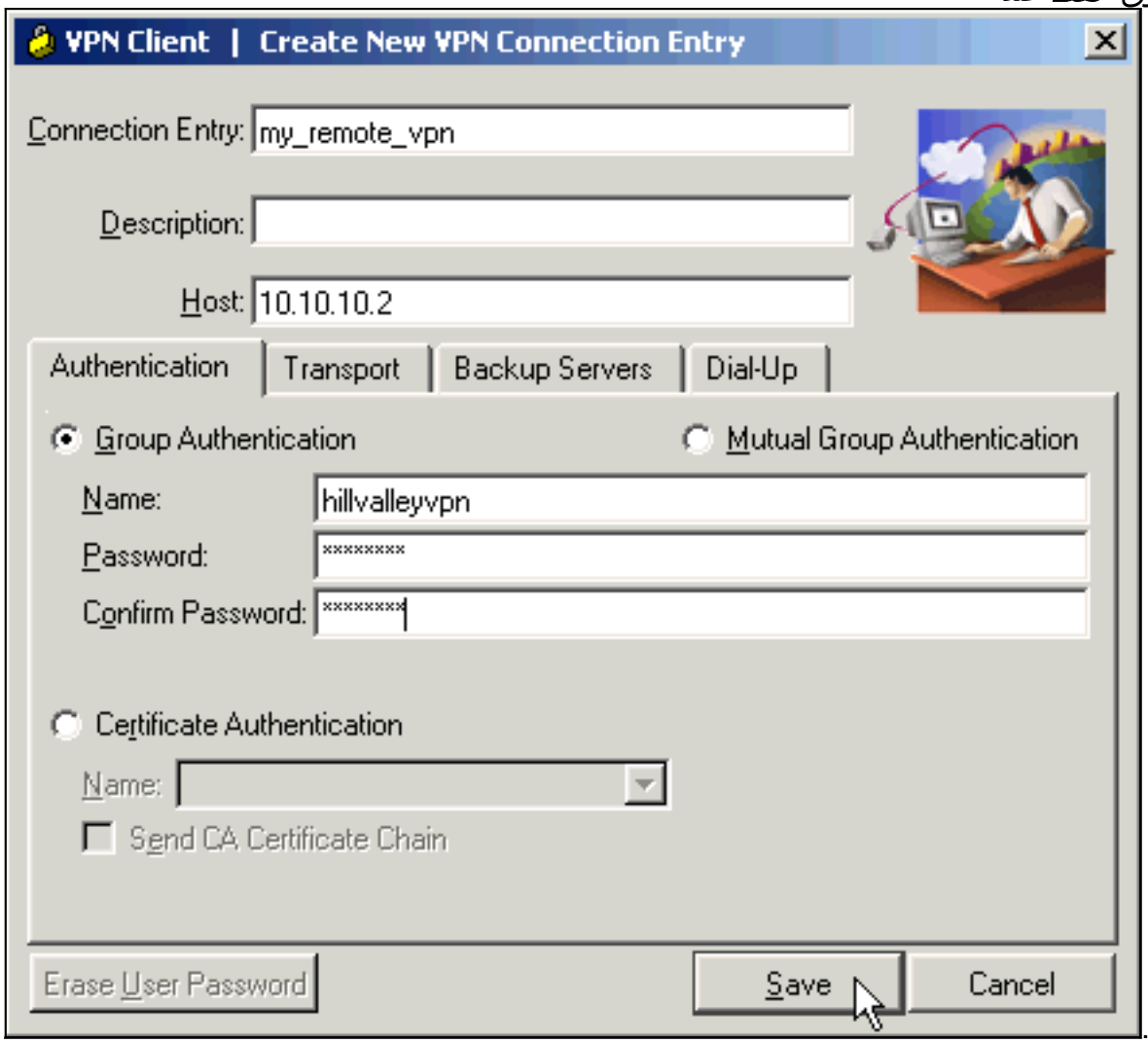
حاول الاتصال ب Cisco ASA باستخدام عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

1. حدد **إدخالات الاتصال > جديد**.



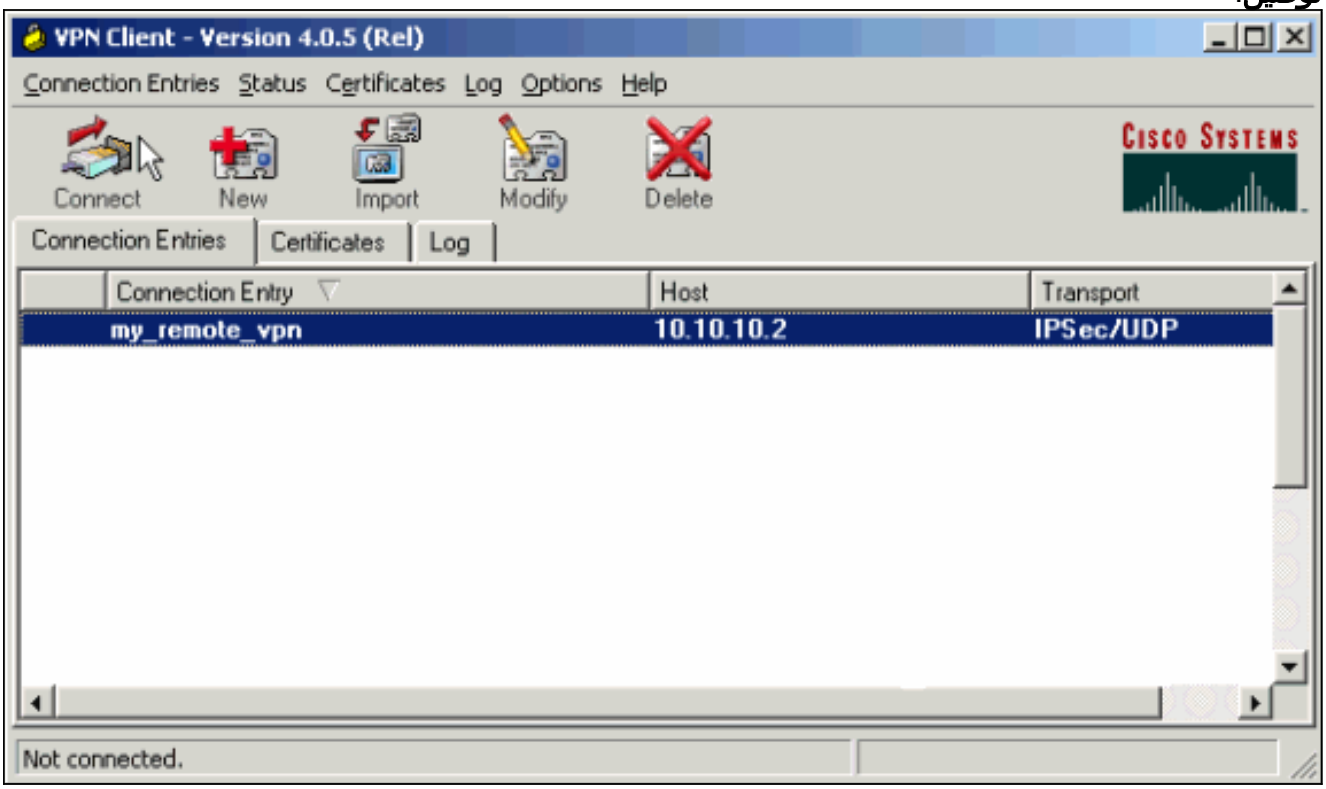
2. املأ تفاصيل إتصالك الجديد.يجب أن يحتوي حقل المضيف على عنوان IP أو اسم المضيف الخاص ب Cisco

ASA الذي تم تكوينه مسبقا. يجب أن تتوافق معلومات مصادقة المجموعة مع تلك المستخدمة في الخطوة 4.
انقر فوق **حفظ** عند



الانتهاء.

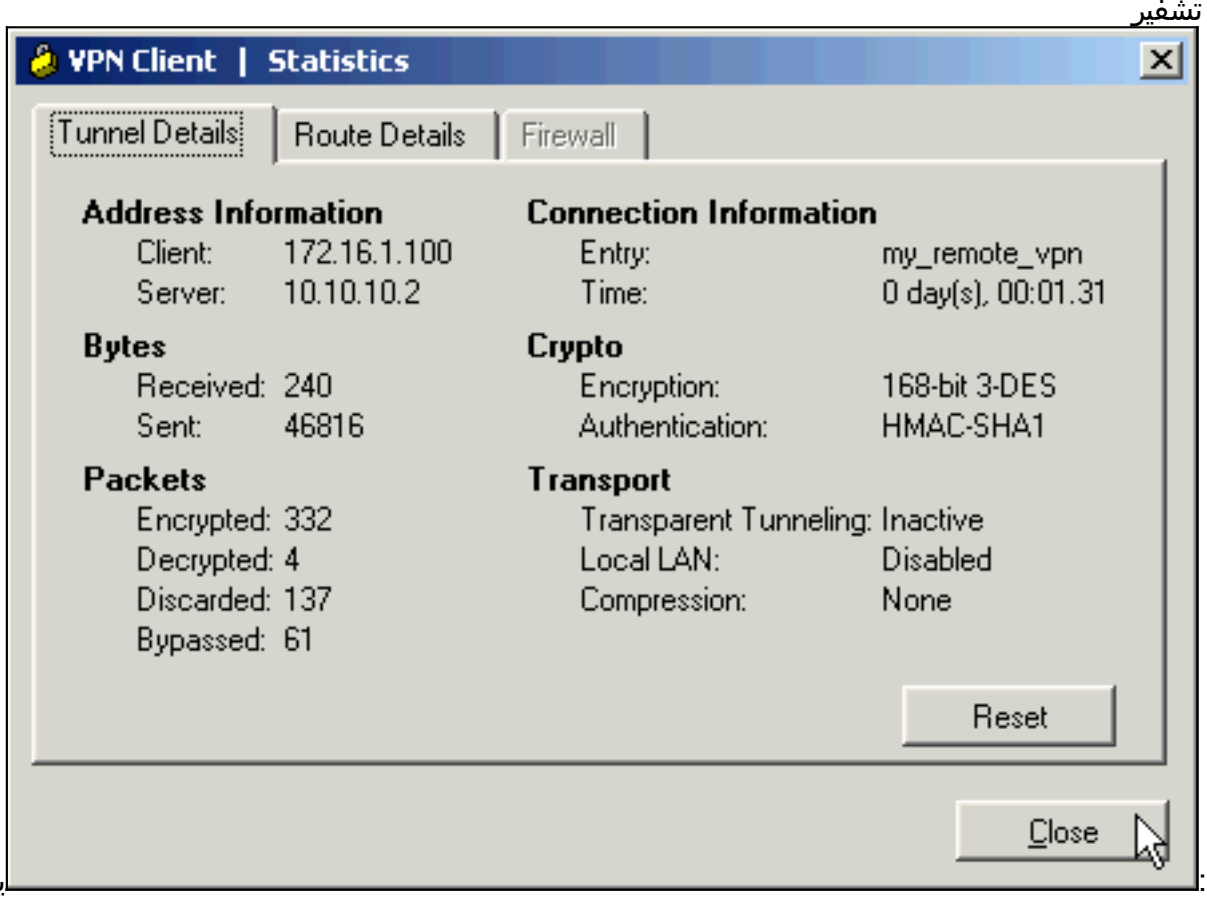
3. حدد الاتصال الذي تم إنشاؤه حديثا، وانقر فوق **توصيل**.



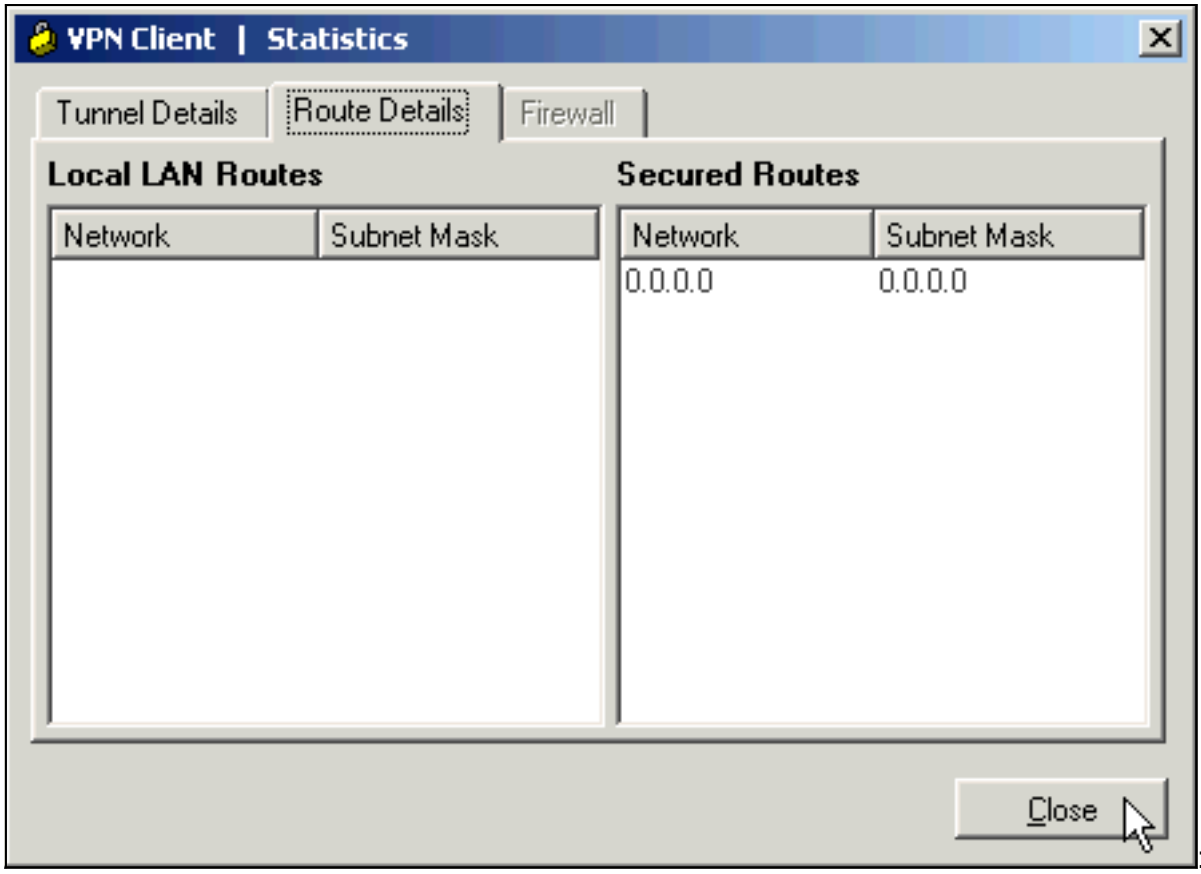
4. أدخل اسم مستخدم وكلمة مرور للمصادقة الموسعة. يجب أن تطابق هذه المعلومات المعلومات المحددة في الخطوتين 5 و

6.

5. بمجرد إنشاء الاتصال بنجاح، حدد **إحصائيات** من قائمة الحالة للتحقق من تفاصيل النفق.يبدي هذا نافذة حركة مرور و تشفير



معلومة:يبد ي هذا نافذة انقسام tunneling



معلومة:

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

قائمة التحكم في الوصول (ACL) للتشفير غير صحيح

يعرف ASDM 5.0(2) بإنشاء قائمة تحكم في الوصول (ACL) تشفير وتطبيقها، والتي يمكن أن تتسبب في مشاكل لعملاء VPN الذين يستخدمون الاتصال النفقي المنقسم، وكذلك لعملاء الأجهزة في وضع امتداد الشبكة. أستخدم الإصدار 5.0(4.3) من ASDM أو إصدار أحدث لتجنب هذه المشكلة. راجع معرف تصحيح الأخطاء من Cisco CSCsc10806 (العملاء المسجلون فقط) للحصول على مزيد من التفاصيل.

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
- أستكشاف أخطاء أجهزة الأمان المعدلة وإصلاحها وتنبيهات سلسلة Cisco ASA 5500
- 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).