ASA/PIX: خادم VPN بعيد مع NAT الوارد لحركة مرور عميل VPN مع CLI ومثال تكوين 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) وبطاقة واجهة الشبكة الخاصة (NAT) الواردة إلى حركة مرور عميل VPN. 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 من خلال عميل Cisco VPN.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM أو CLI بإجراء تغييرات التكوين. كما يفترض أنه تم تكوين ASA ل NAT الصادر. أحلت يسمح داخلي مضيف منفذ إلى شبكة خارجي مع الإستعمالمن ضرب ل كثير معلومة على كيف أن يشكل NAT صادر.

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 Secure Shell (SSH).

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 المُستخدمة 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 للاتصالات المحددة. في حالة عدم تعيين نهج مجموعة معين للمستخدمين، يتم تطبيق نهج المجموعة الافتراضي للاتصال.

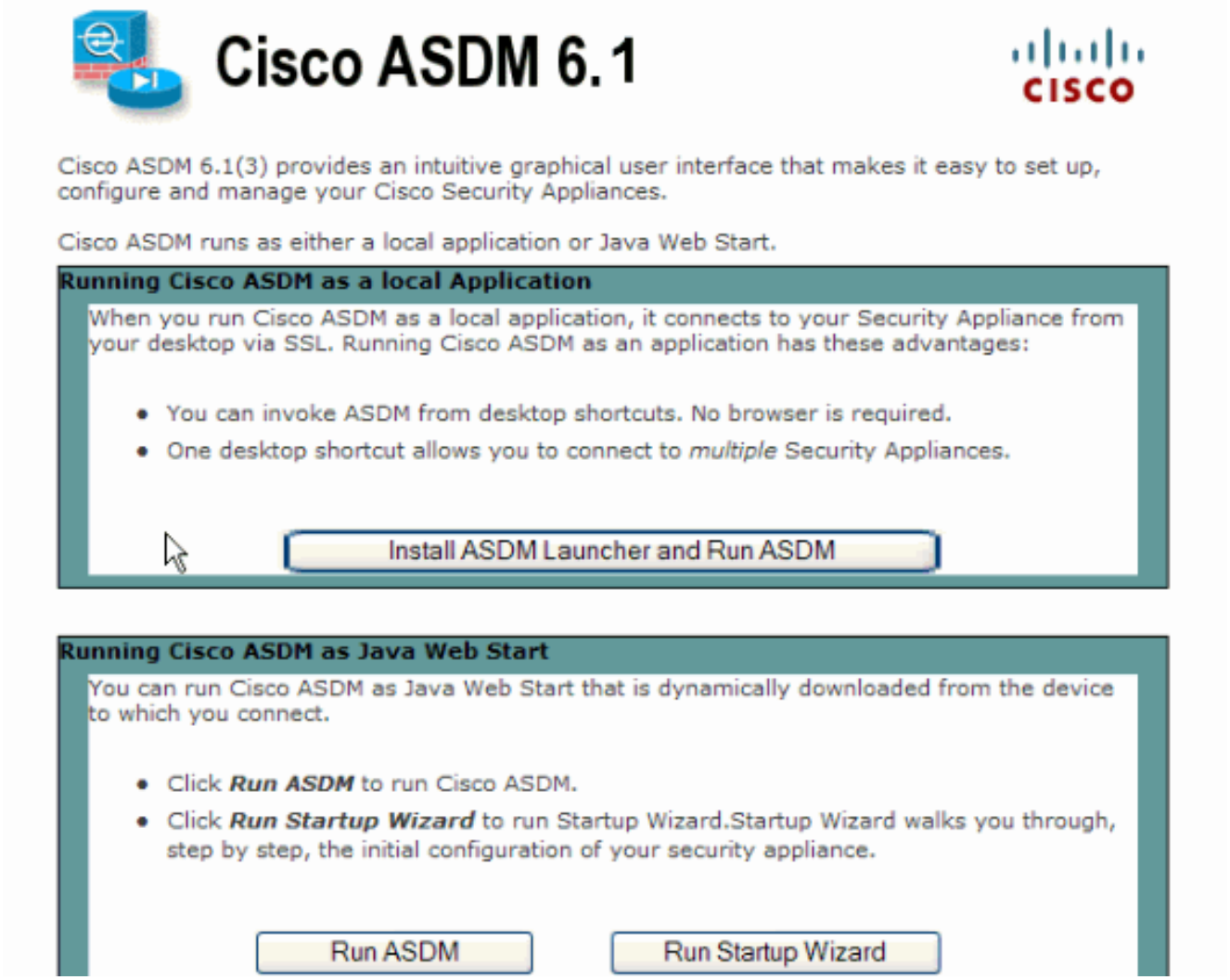
تتكون مجموعة النفق من مجموعة سجلات تحدد نهج اتصال النفق. تحدد هذه السجلات الخوادم التي تتم مصادقة مستخدمي النفق عليها، بالإضافة إلى خوادم المحاسبة، إن وجدت، التي يتم إرسال معلومات الاتصال إليها. كما أنها تحدد نهج مجموعة افتراضي للاتصالات، وهي تحتوي على معلمات اتصال خاصة بالبروتوكول. تتضمن مجموعات الأنفاق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

التكوينات

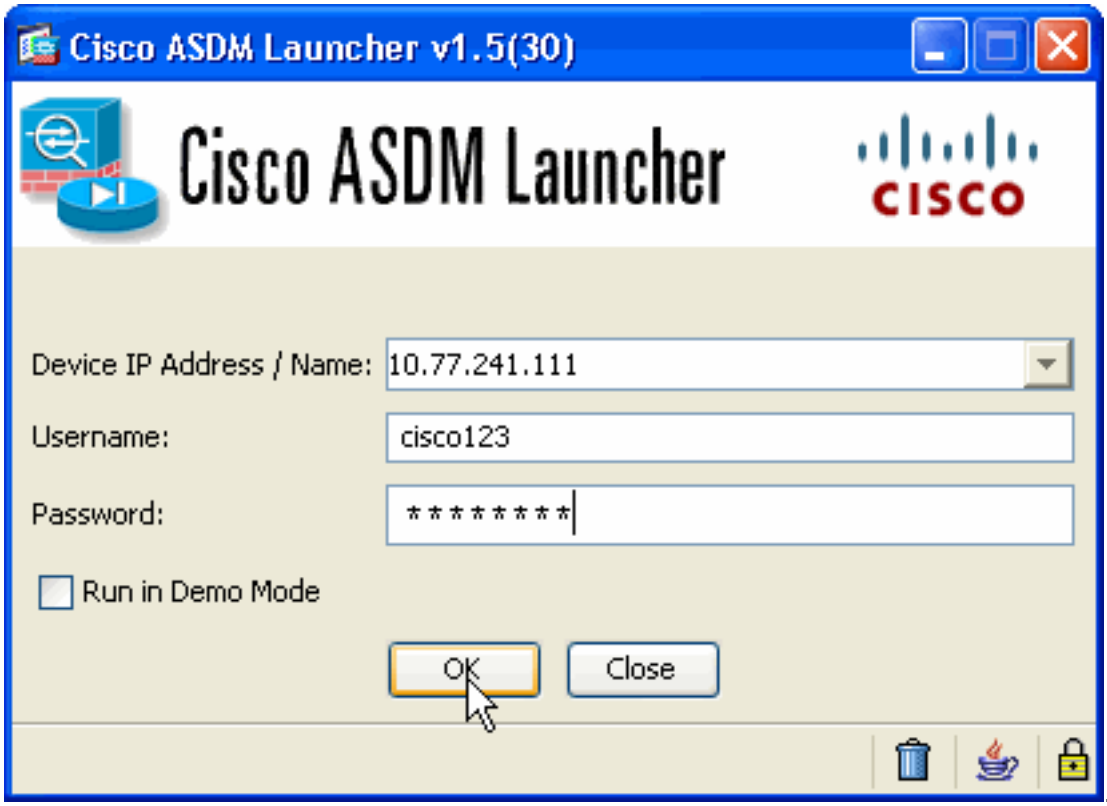
تكوين ASA/PIX كخادم VPN بعيد باستخدام ASDM

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

1. افتح المستعرض وأدخل **https://<IP_Address الخاص بواجهة ASA التي تم تكوينها للوصول إلى ASDM>**للوصول إلى ASDM على ASA.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها صلة بأصالة شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يقدم ASA هذا الإطار للسماح بتنزيل تطبيق ASDM. يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق Java.

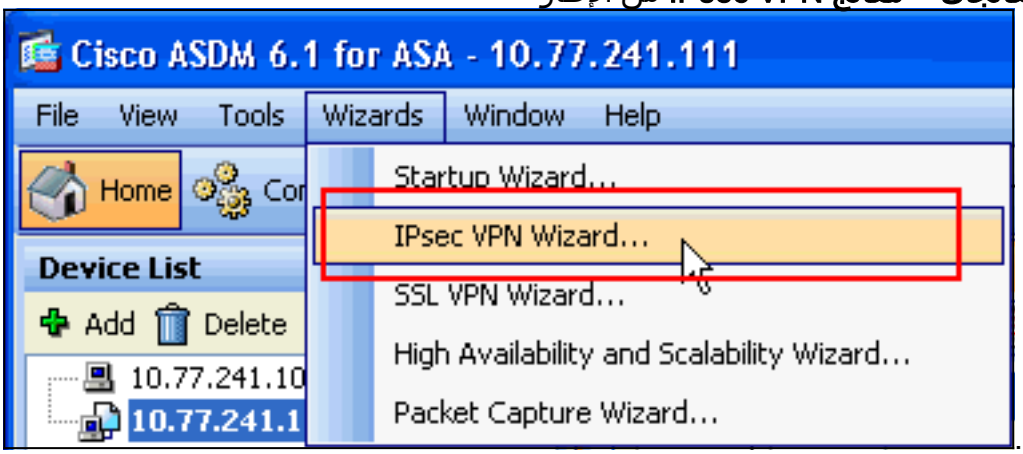


2. انقر على **تنزيل مشغل ASDM وابدأ ASDM** لتنزيل المثبت الخاص بتطبيق ASDM.
3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.
4. دخلت العنوان للقارن أنت تشكل مع **ال http** - أمر، واسم مستخدم وكلمة إن يعين أنت واحد.يستخدم هذا المثال **Cisco123** كاسم مستخدم و**Cisco123** ككلمة



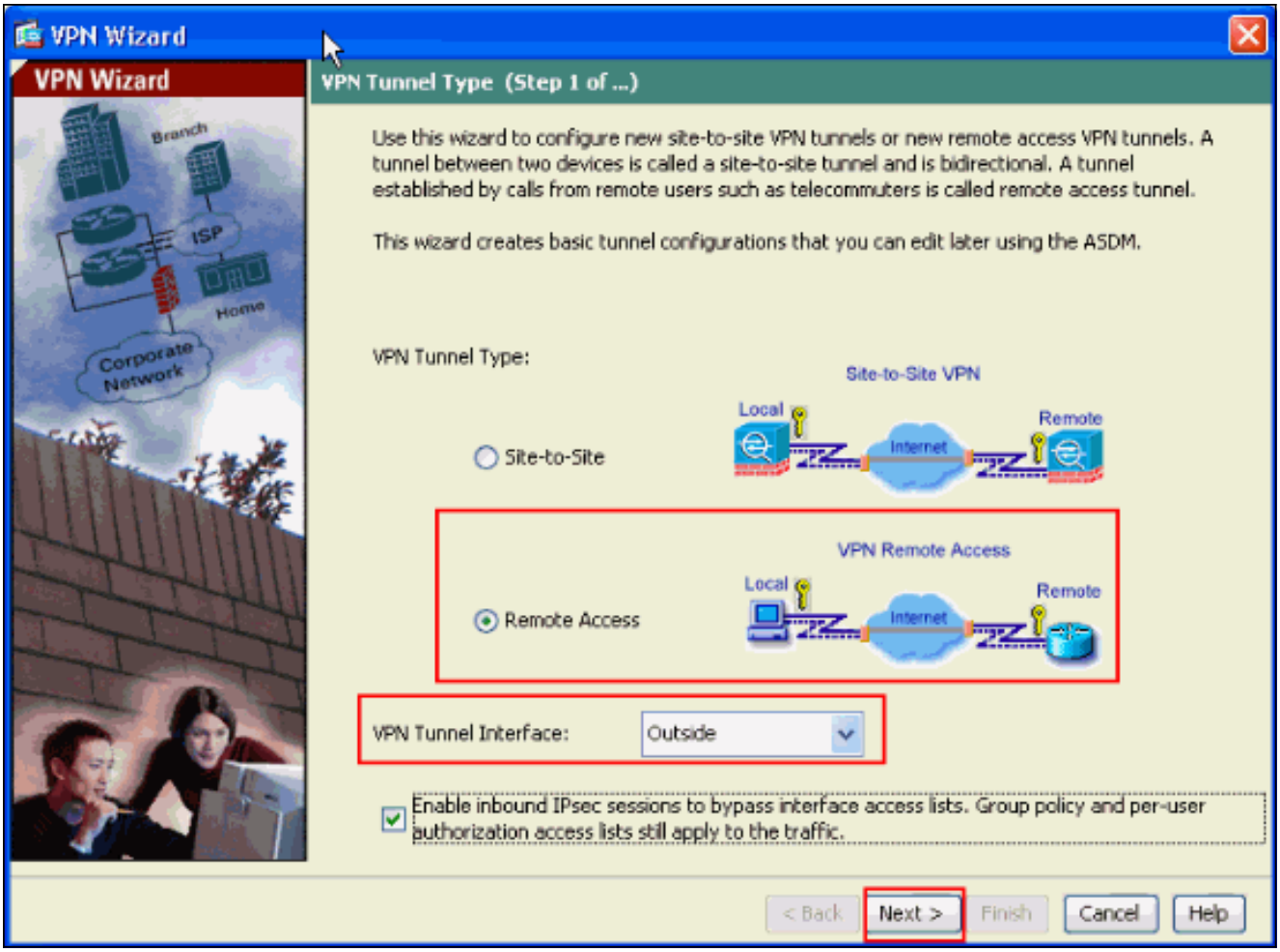
مرور.

5. حدد **المعالجات > معالج IPsec VPN** من الإطار

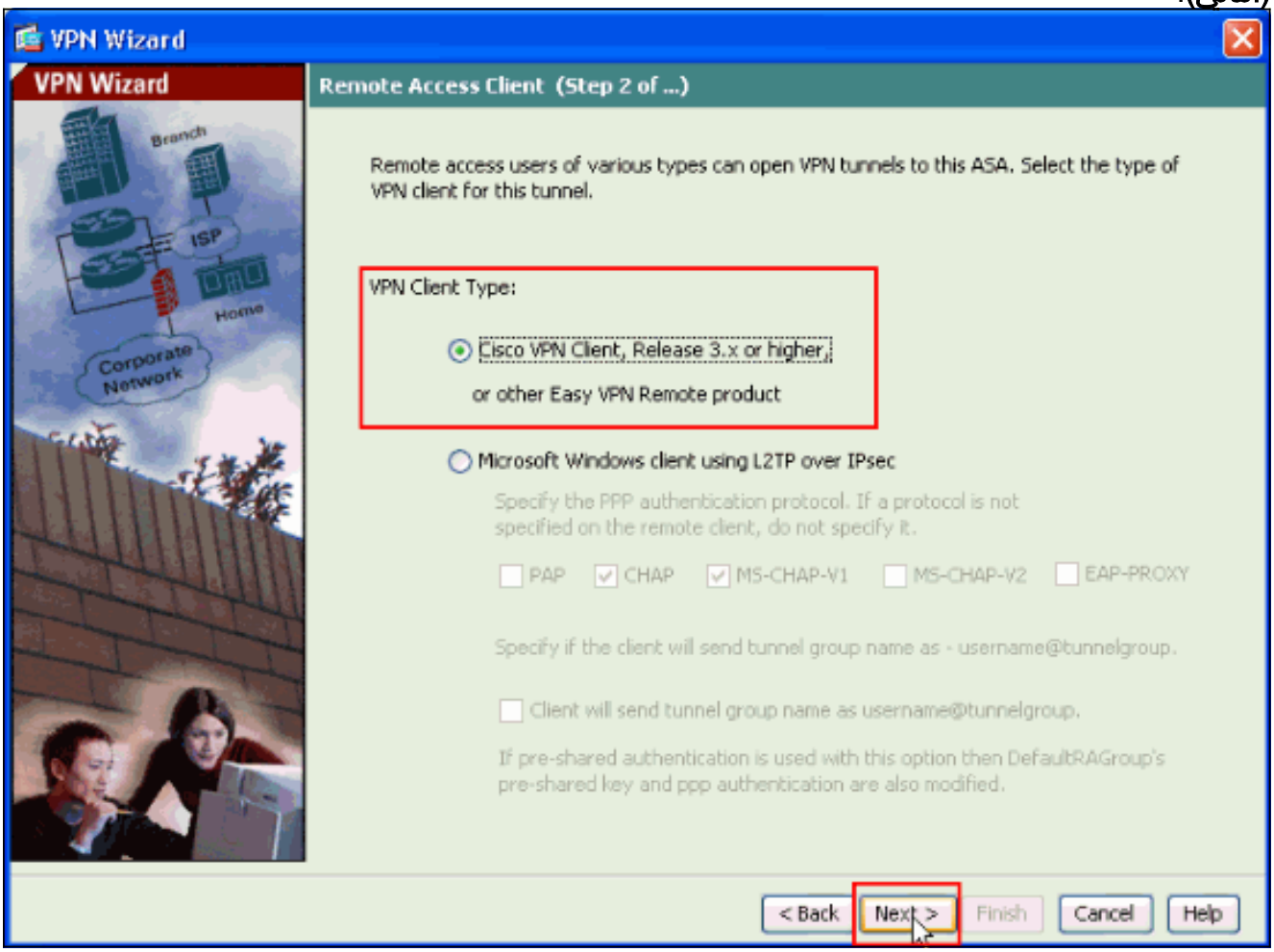


الرئيسي.

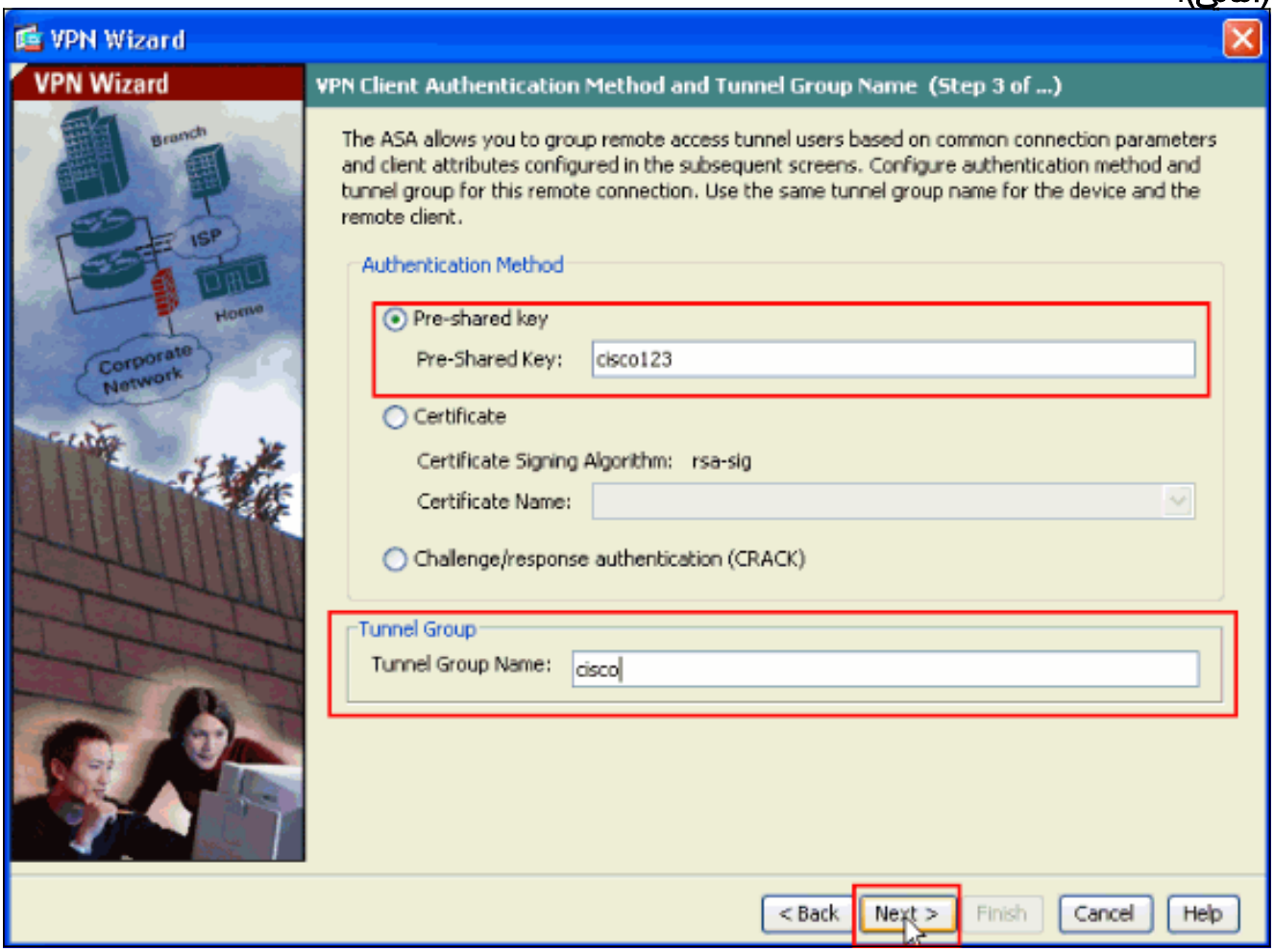
6. حدد نوع نفق VPN **للوصول عن بعد** وتأكد من تعيين واجهة نفق VPN على النحو المطلوب، وانقر فوق **التالي** كما هو موضح
هنا.



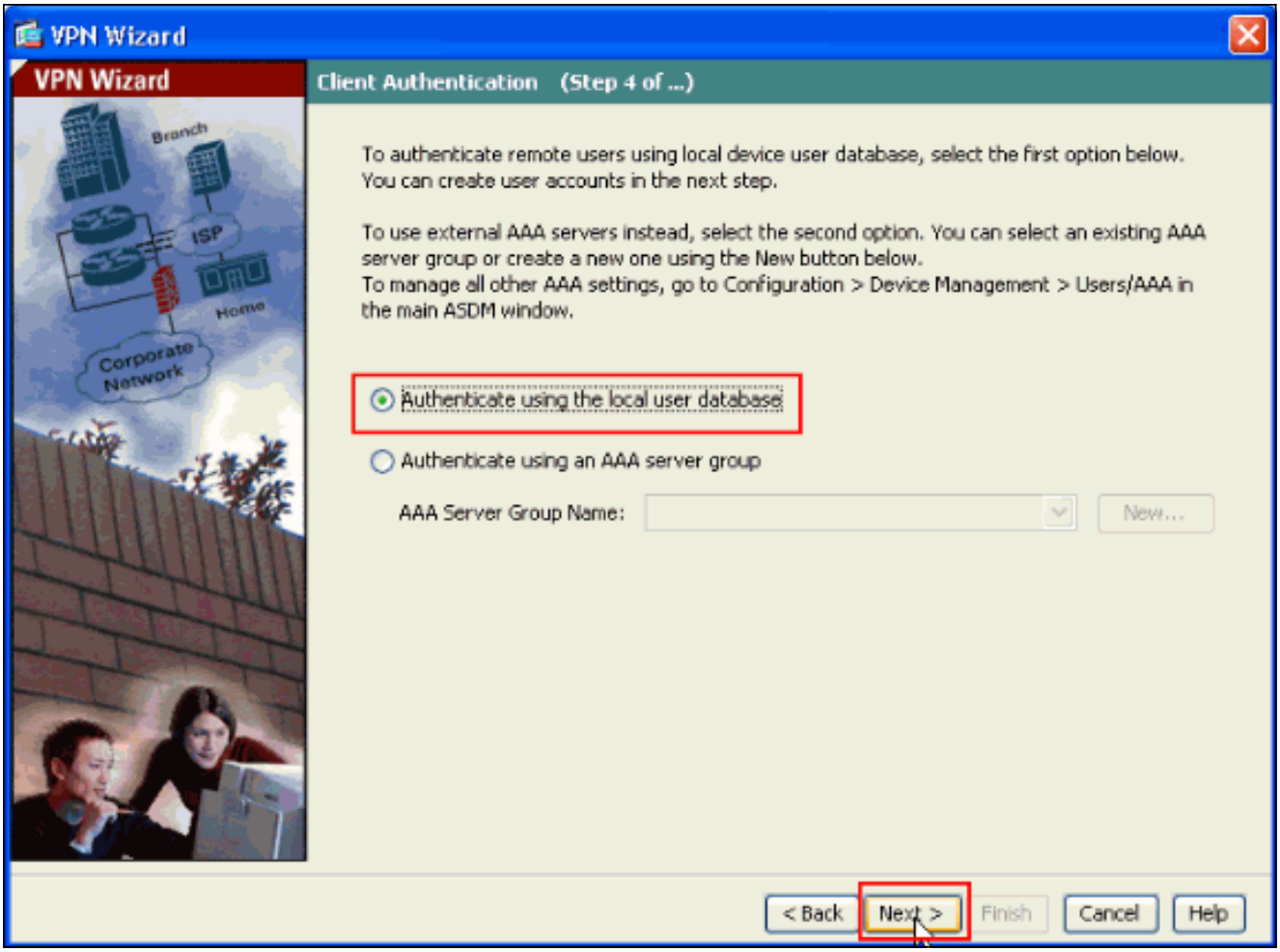
7. يتم إختيار نوع عميل شبكة VPN، كما هو موضح. يتم إختيار **عميل شبكة VPN من Cisco** هنا. انقر فوق **Next (التالي)**.



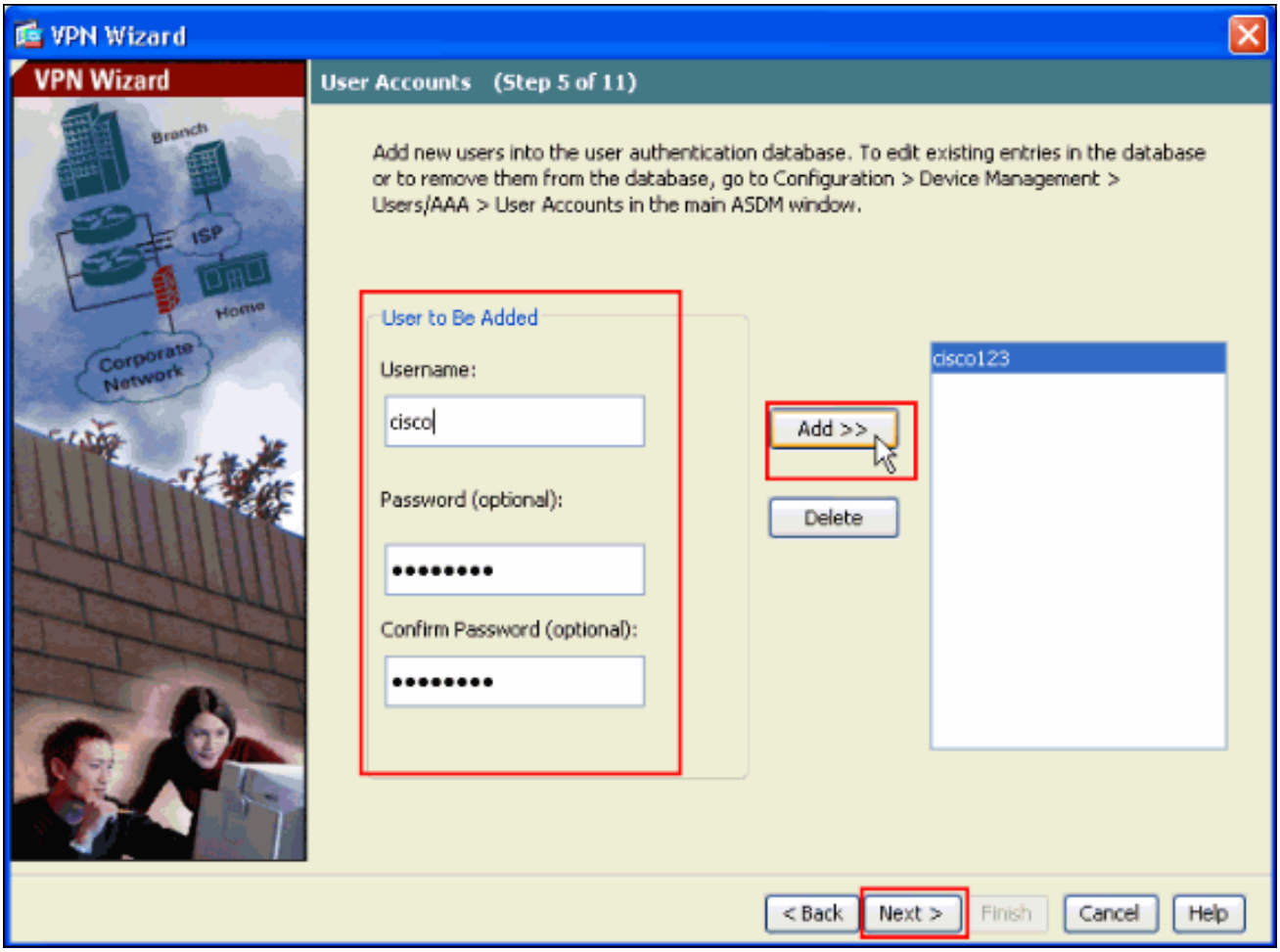
8. أدخل اسما **لاسم مجموعة النفق**. أدخل معلومات المصادقة التي سيتم إستخدامها، وهي **المفتاح المشترك مسبقا** في هذا المثال. المفتاح المشترك مسبقا المستخدم في هذا المثال هو **Cisco123**. اسم مجموعة النفق المستخدم في هذا المثال هو **Cisco**. انقر فوق **Next (التالي)**.



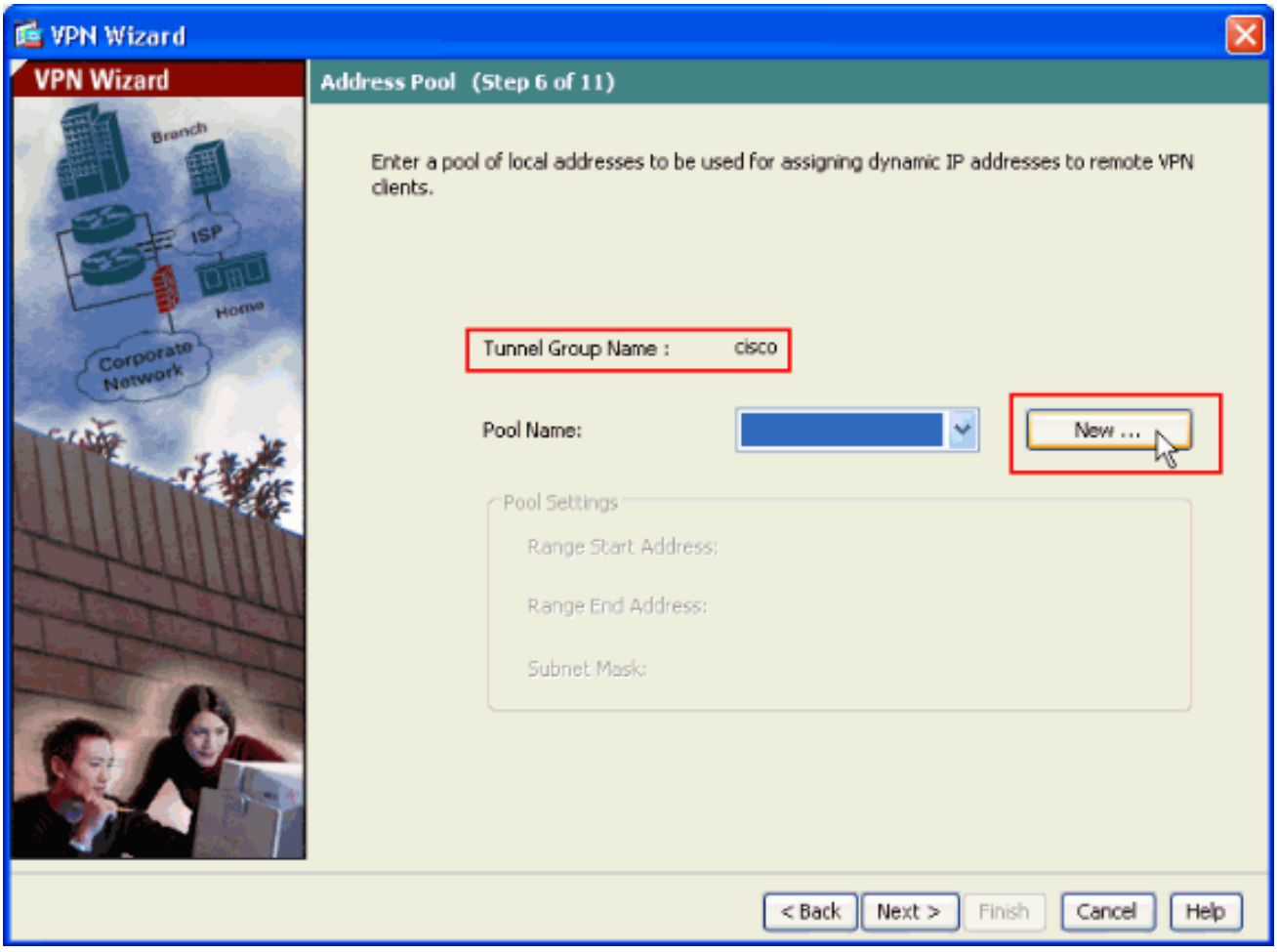
9. أختر ما إذا كنت تريد مصادقة المستخدمين عن بعد إلى قاعدة بيانات المستخدم المحلية أو إلى مجموعة خوادم AAA خارجية.**ملاحظة:** يمكنك إضافة مستخدمين إلى قاعدة بيانات المستخدم المحلية في الخطوة 10.**ملاحظة:** ارجع إلى مجموعات خوادم المصادقة والتفويض الخاصة ب PIX/ASA 7.x لمستخدمي VPN عبر مثال تكوين ASDM للحصول على معلومات حول كيفية تكوين مجموعة خوادم AAA الخارجية مع ASDM.



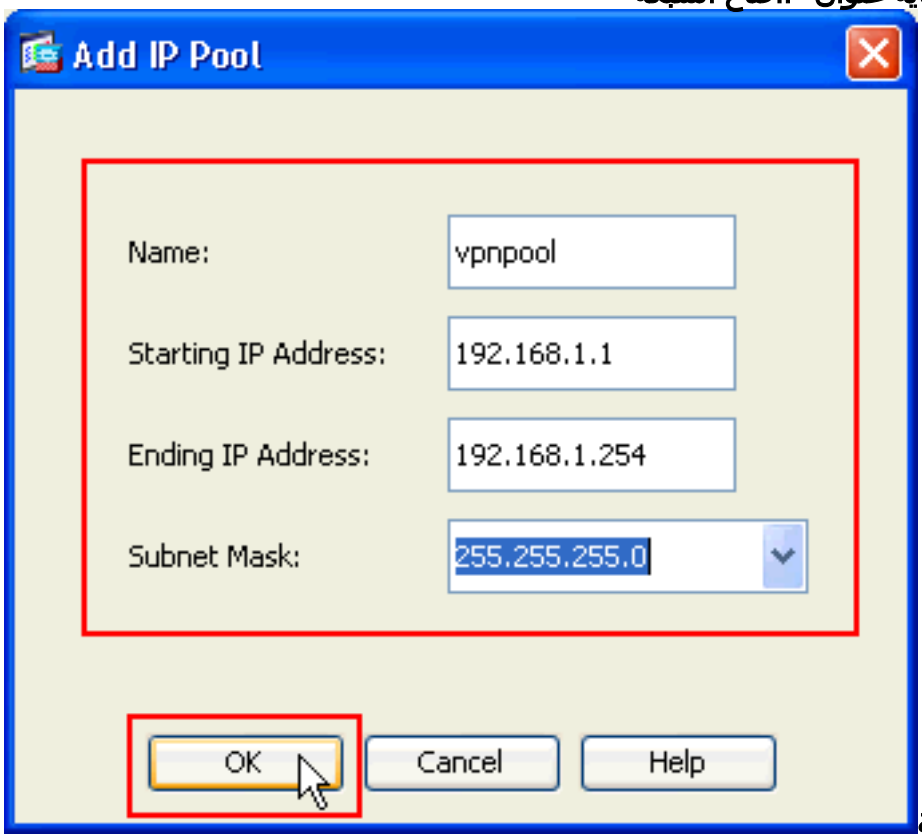
10. توفر **اسم مستخدم** و**كلمة مرور** إختيارية وانقر فوق **إضافة** لإضافة مستخدمين جدد إلى قاعدة بيانات مصادقة المستخدم. انقر فوق **Next (التالي)**.**ملاحظة:** لا تقم بإزالة المستخدمين الحاليين من هذا الإطار. حدد **تكوين > إدارة الأجهزة > Users/AAA > حسابات المستخدمين** في نافذة ASDM الرئيسية لتحرير الإدخالات الموجودة في قاعدة البيانات أو إزالتها من قاعدة البيانات.



11. طقطقت in order to عينت بركة من محلي أن يكون عينت ديناميكيا إلى VPN زبون بعيد، **جديد** أن يخلق جديد **IP**
بركة.

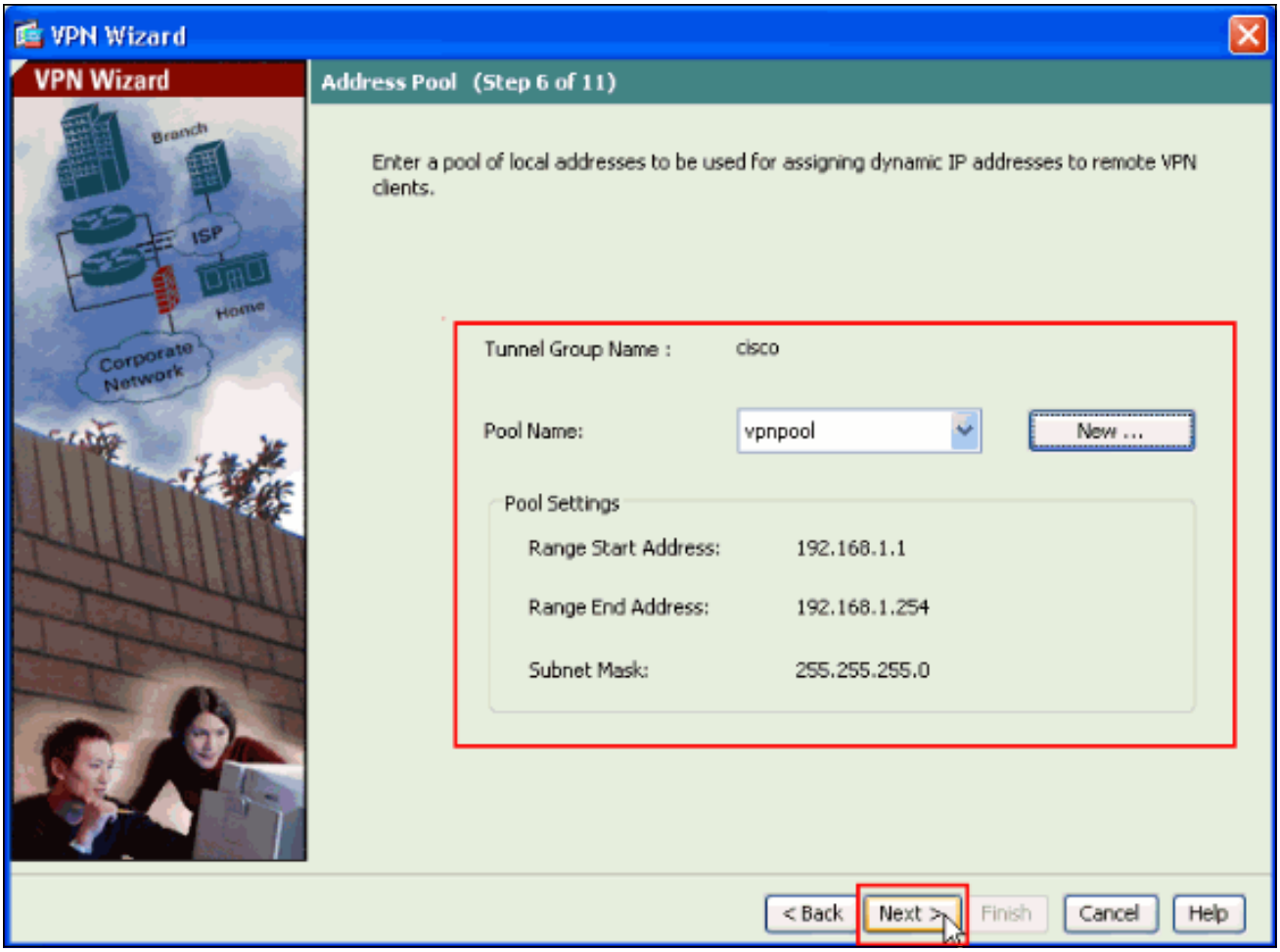


12. في الإطار الجديد بعنوان **إضافة تجمع IP** وفر هذه المعلومات، وانقر **موافق**.**اسم تجمع IP**عنوان IP **الأولينهاية عنوان IP**قناع الشبكة

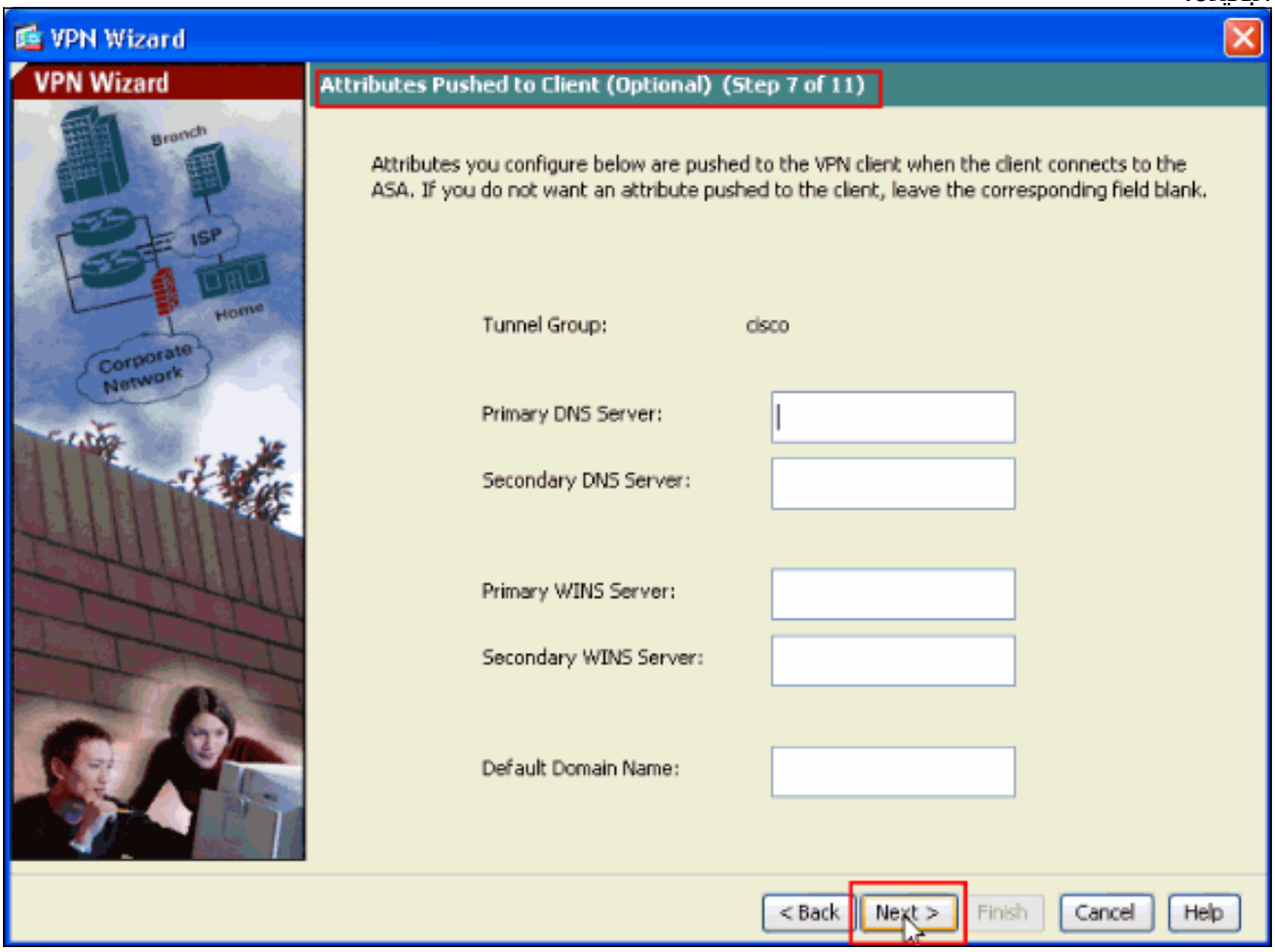


الفرعية

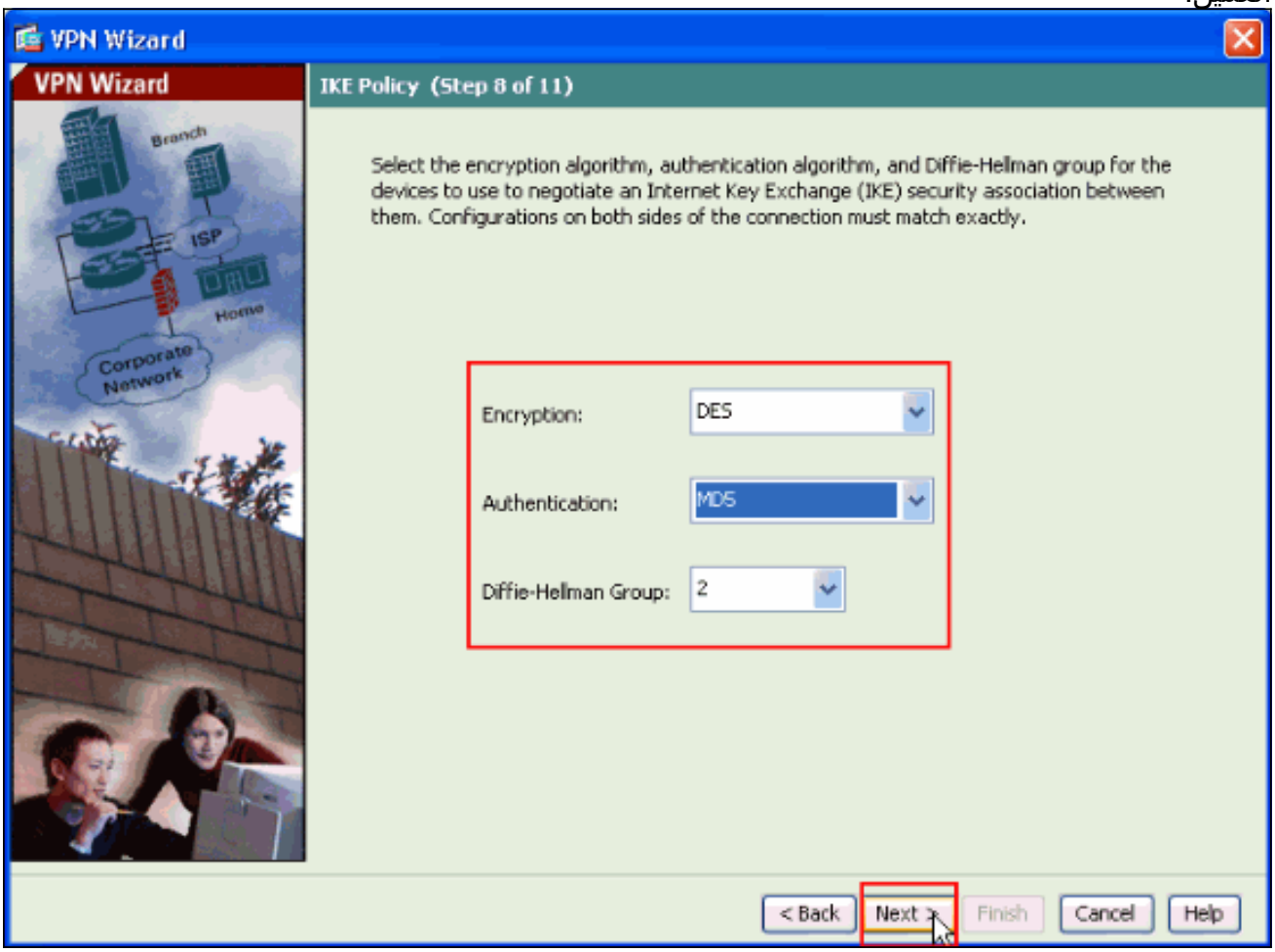
13. بعد تحديد تجمع العناوين المحلية التي سيتم تعيينها ديناميكيا لعملاء VPN البعيدة عند إتصالهم، انقر فوق **التالي**.



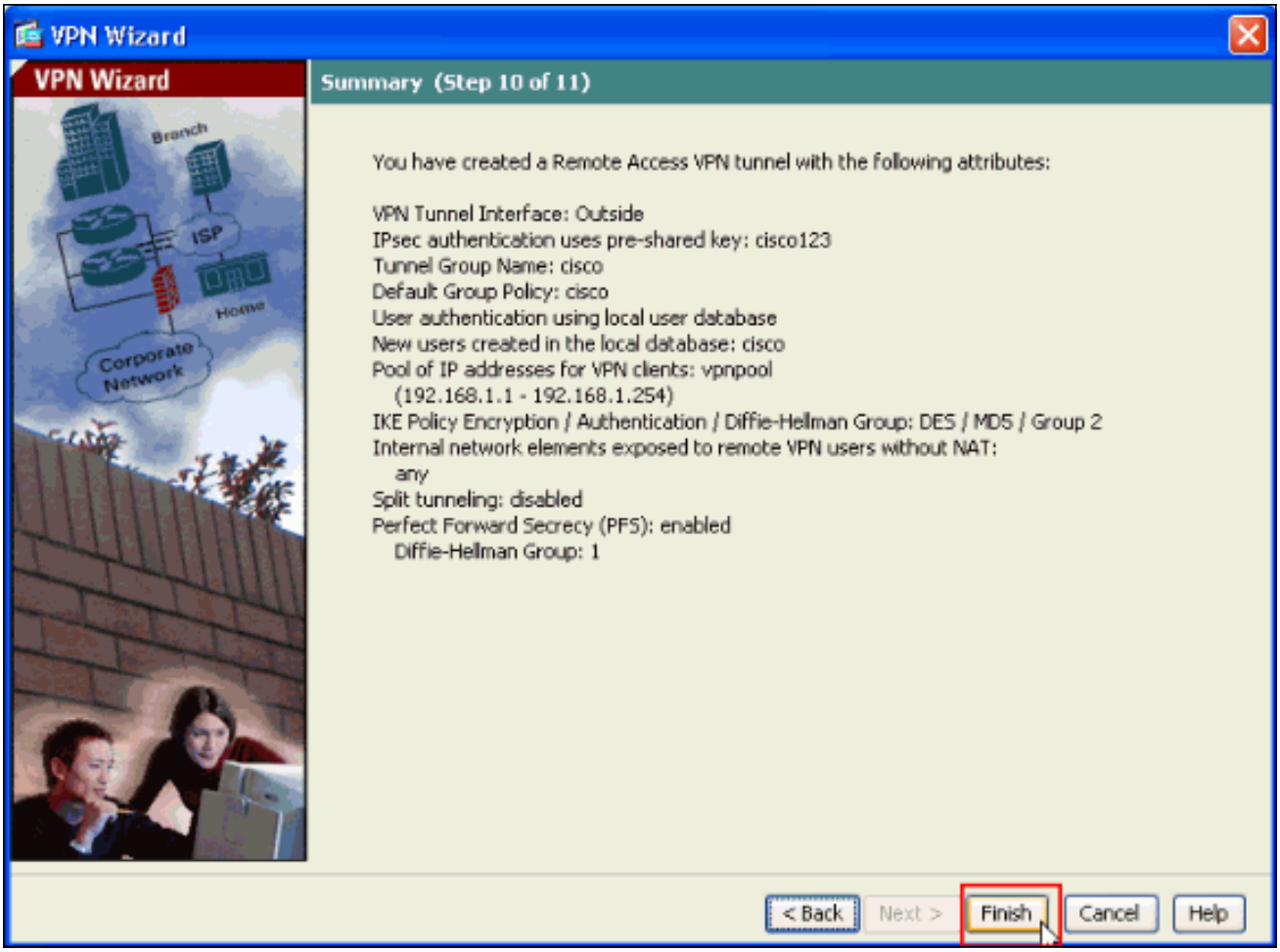
14. *إختياري*: حدد معلومات خادم DNS و WINS واسم مجال افتراضي ليتم دفعه إلى عملاء VPN البعيدة.



15. 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.



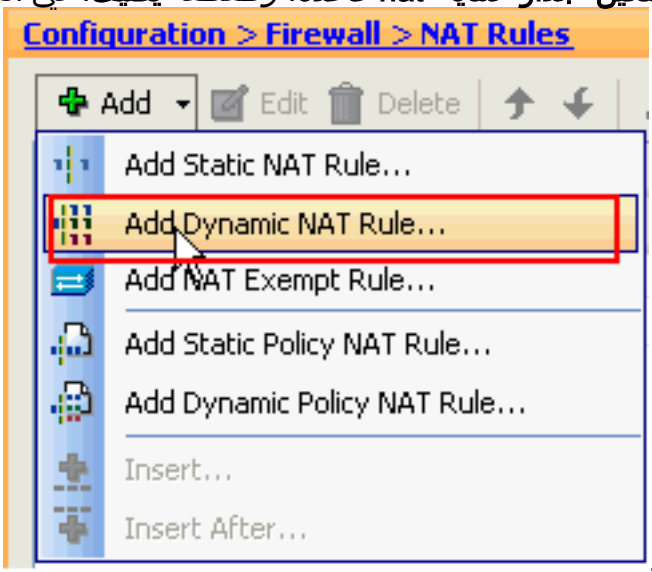
16. تعرض هذه النافذة ملخصا للإجراءات التي اتخذتها. انقر فوق **إنهاء** إذا كنت راضيا عن التكوين الخاص بك.



تكوين حركة مرور عميل VPN الواردة ل ASA/PIX إلى NAT باستخدام ASDM

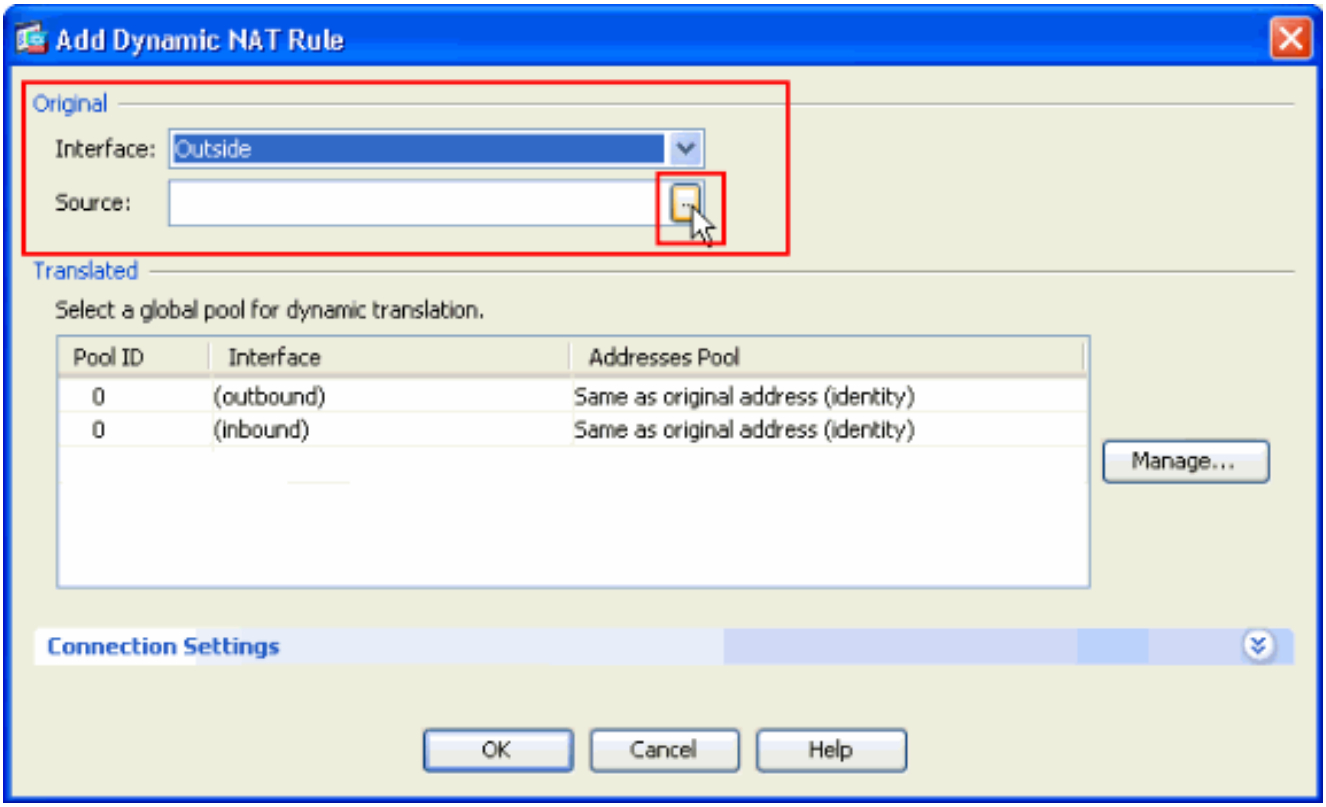
أتمت هذا steps in order to شكلت ال cisco ASA أن nat داخل VPN زبون حركة مرور مع ASDM:

1. أخترت **تشكيل>جدار حماية>nat قاعدة**، وطقطقة **يضيف**. في القائمة المنسدلة، حدد **إضافة قاعدة NAT**

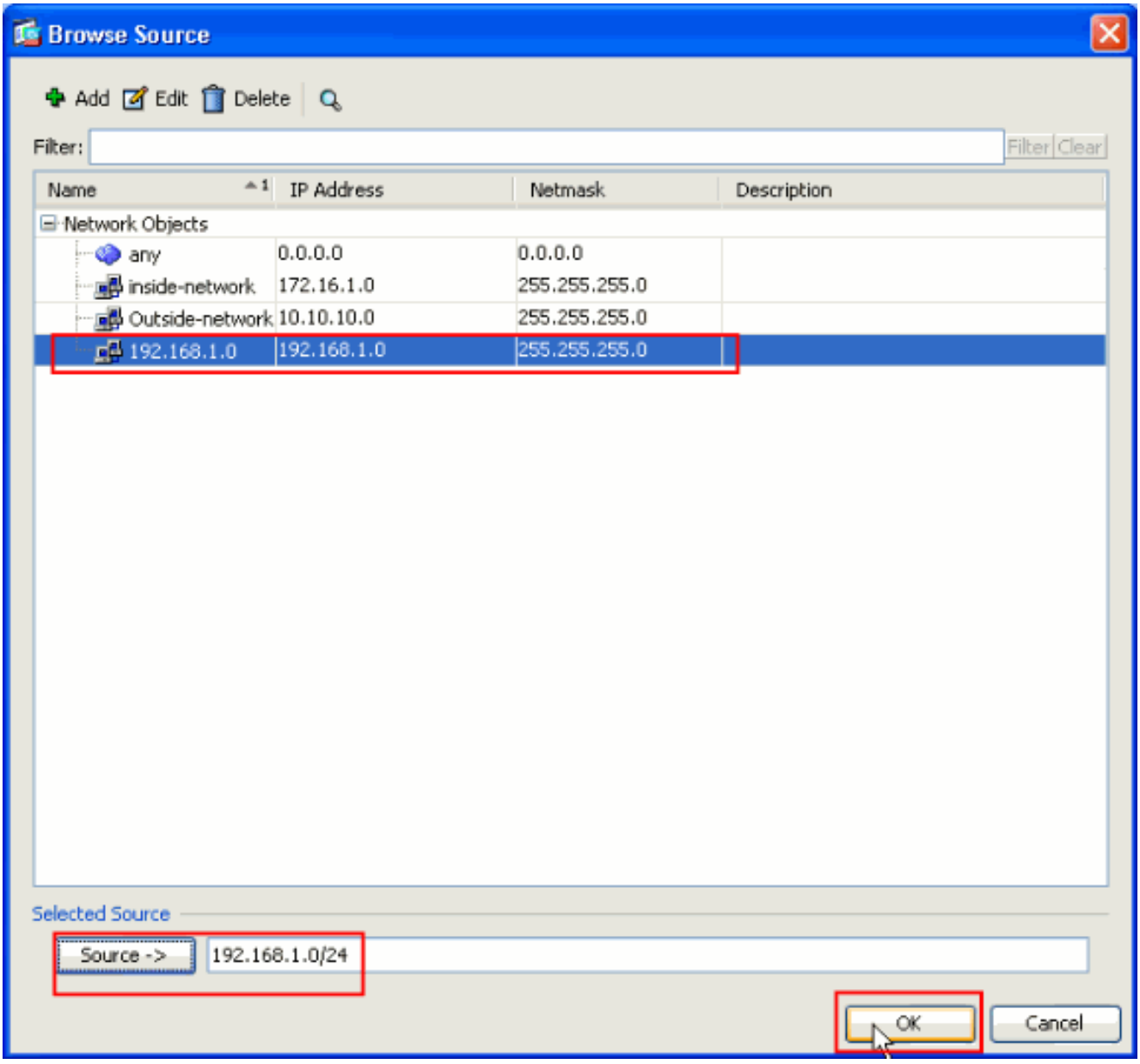


ديناميكية.

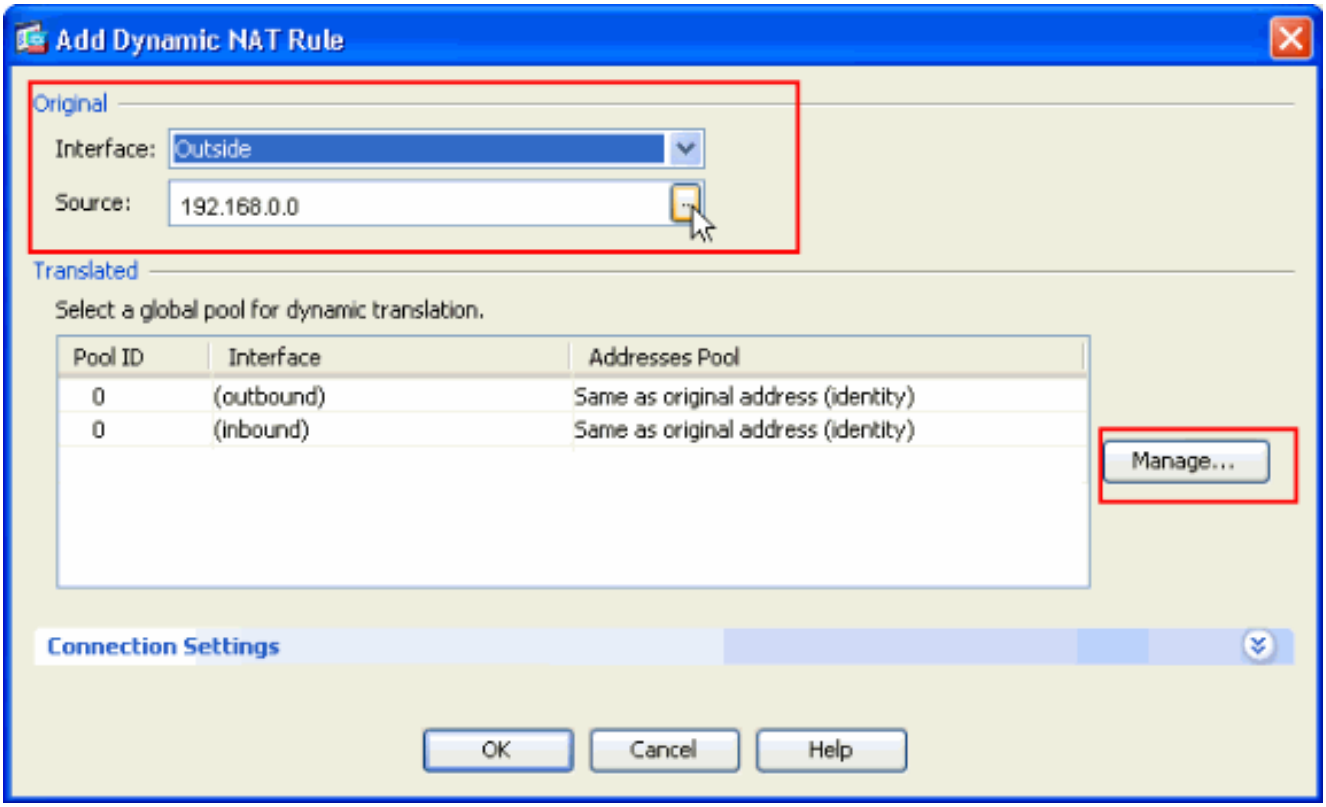
2. في نافذة **قاعدة إضافة شبكة (NAT) الديناميكية**، أختر **خارجي** كواجهة، وانقر زر الاستعراض الموجود بجوار المربع **المصدر**.



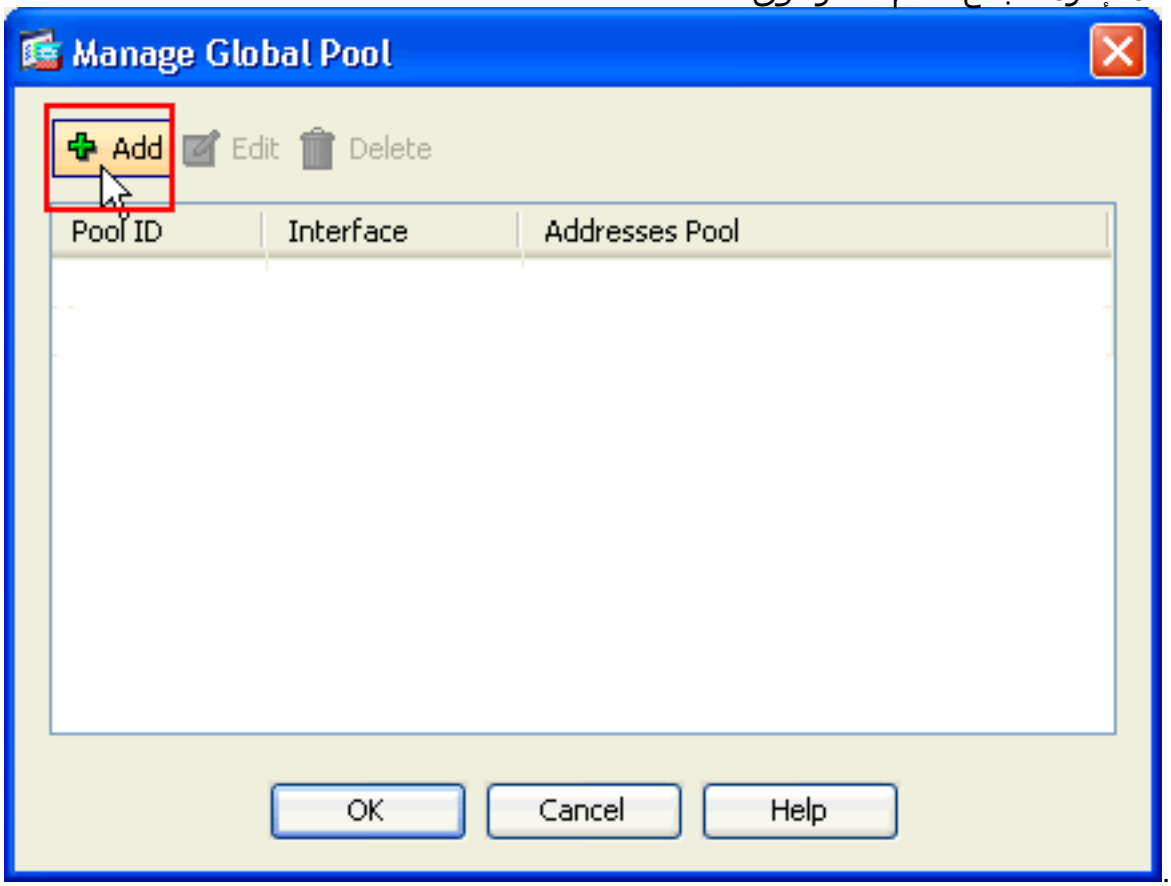
3. في نافذة تصفح المصدر، حدد كائنات الشبكة المناسبة واختر أيضا **المصدر** تحت قسم المصدر المحدد، وانقر **موافق**. هنا يتم إختيار كائن الشبكة 192.168.1.0.



4. انقر فوق
إدارة.

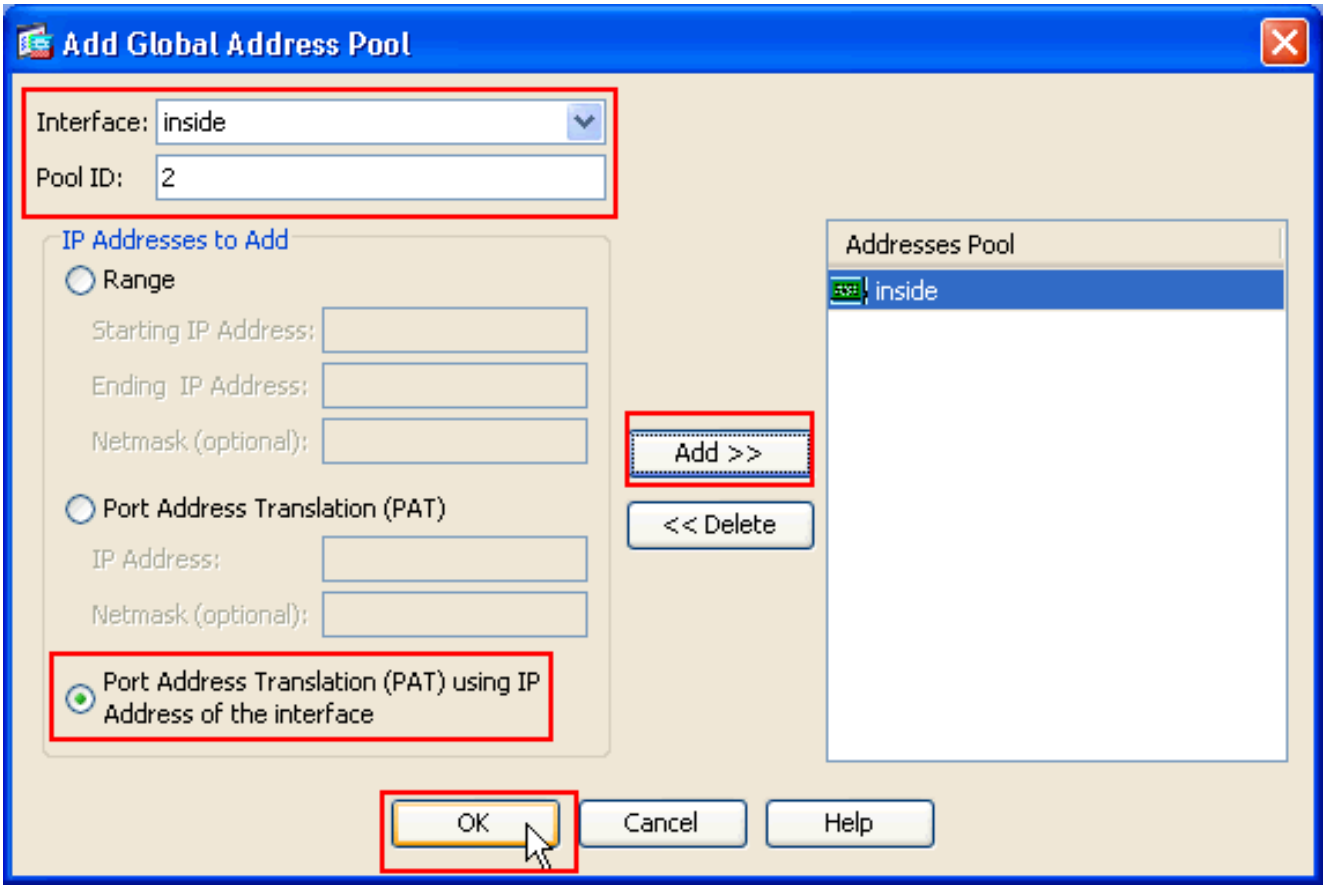


5. في نافذة "إدارة التجمع العام"، انقر فوق

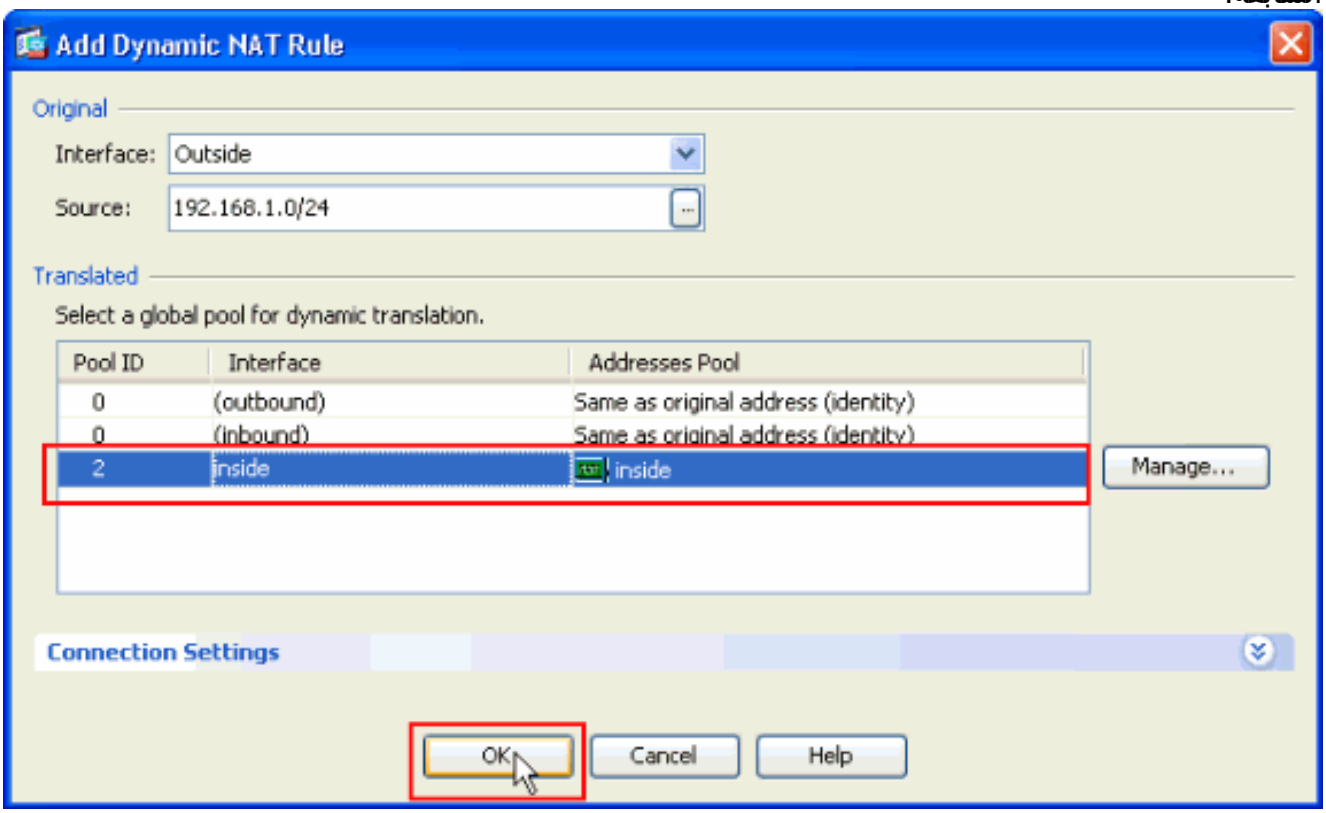


إضافة.

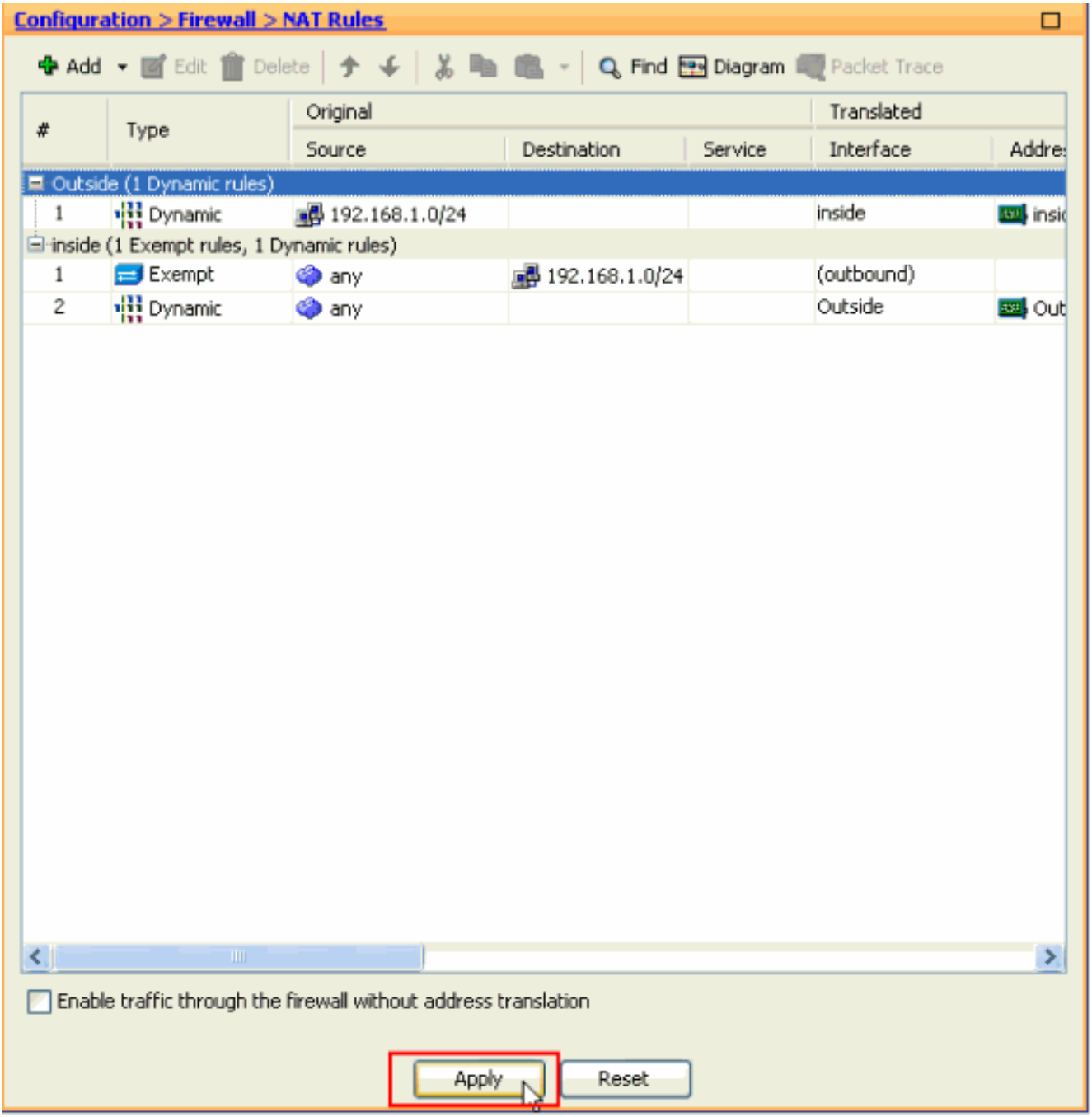
6. في نافذة "إضافة تجمع عناوين عمومي"، أختر **Inside** كواجهة و**2** كمعرف **التجمع**. تأكدت أيضا أن **انتقيت** زر لاسلكي بجوار **ضرب يستعمل عنوان من القارن**. طقطقة **يضيف>**، وبعد ذلك يطقطق **ok**.



7. انقر فوق **موافق** بعد تحديد التجمع العام باستخدام **معرف التجمع 2** الذي تم تكوينه في الخطوة السابقة.



8. انقر الآن فوق **تطبيق** حتى يتم تطبيق التكوين على ASA.يؤدي هذا إلى اكتمال التكوين.



شكلت ال ASA/PIX كنادل VPN بعيد و ل inbound NAT مع ال CLI

تشغيل التكوين على جهاز ASA
ciscoasa#**show running-config** Saved : (ASA Version 8.0(3 ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 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
                                                             !
                                                             !
                                     passwd 2KFQnbNIdI.2KYOU encrypted
                                      boot system disk0:/asa803-k8.bin
                                                   ftp mode passive
 access-list inside_nat0_outbound extended permit ip any
                                          192.168.1.0 255.255.255
                                                             0
                                                pager lines 24
                                                logging enable
                                              mtu Outside 1500
                                               mtu inside 1500
    ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
                                                 255.255.255.0
                                                 no failover
                    icmp unreachable rate-limit 1 burst-size 1
                                 asdm image disk0:/asdm-615.bin
                                           asdm history enable
                                             arp timeout 14400
                                                   nat-control
                                 global (Outside) 1 interface
                                  global (inside) 2 interface
       nat (Outside) 2 192.168.1.0 255.255.255.0 outside
         nat (inside) 0 access-list inside_nat0_outbound
                                 nat (inside) 1 0.0.0.0 0.0.0.0
                    route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1
                                          timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                                   icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
                                       0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                        sip-disconnect 0:02:00
                                timeout uauth 0:05:00 absolute
          dynamic-access-policy-record DfltAccessPolicy
                                            http server enable
                                       no snmp-server location
                                        no snmp-server contact

 Configuration for IPsec policies. !--- Enables the ---!
 crypto transform configuration mode, !--- where you can
 specify the transform sets that are used !--- during an
  IPsec negotiation. crypto ipsec transform-set ESP-DES-
                                          SHA esp-des esp-sha-hmac
 crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-
                                                        hmac
  crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
                                                  pfs group1
  crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
                                          transform-set ESP-DES-SH
                                                ESP-DES-MD5
       crypto map Outside_map 65535 ipsec-isakmp dynamic
                                       SYSTEM_DEFAULT_CRYPTO_MAP
                  crypto map Outside_map interface Outside
                                  crypto isakmp enable Outside

    Configuration for IKE policies. !--- Enables the ---!
    IKE policy configuration (config-isakmp) !--- command
 mode, where you can specify the parameters that !--- are
      used during an IKE negotiation. Encryption and !---
      Policy details are hidden as the default values are
```

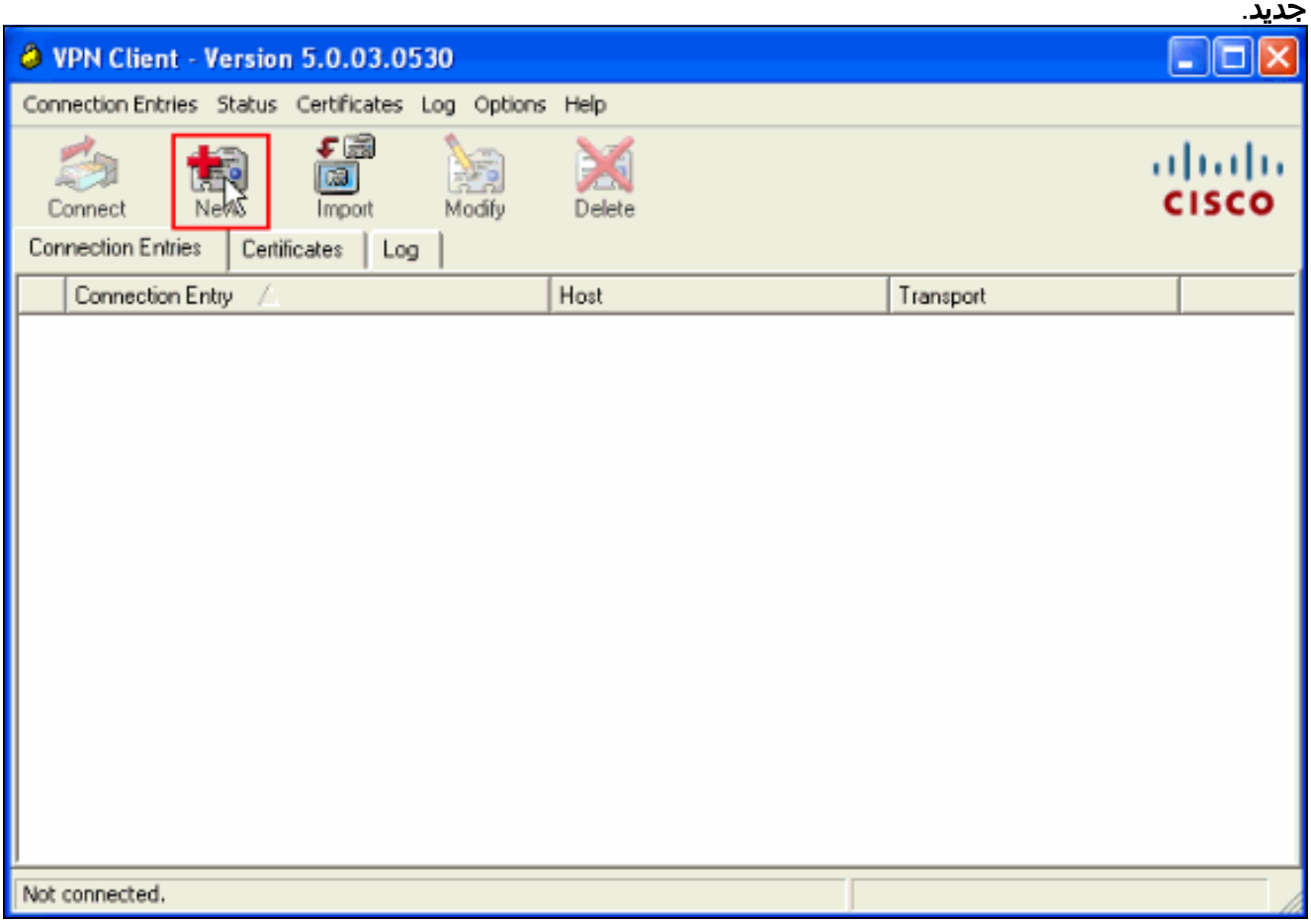
```
chosen. crypto isakmp policy 10
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400
crypto isakmp policy 30
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
telnet timeout 5
ssh timeout 60
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
group-policy cisco internal
group-policy cisco attributes
vpn-tunnel-protocol IPSec

Specifies the username and password with their !--- ---!
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 0

username cisco attributes
vpn-group-policy cisco
tunnel-group cisco type remote-access
tunnel-group cisco general-attributes
address-pool vpnpool
default-group-policy cisco

Specifies the pre-shared key "cisco123" which must ---!
!--- be identical at both peers. This is a global !---
configuration mode command. tunnel-group cisco ipsec-
attributes
* pre-shared-key
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
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:f2ad6f9d5bf23810a26f5cb464e1fdf3
end :
#ciscoasa
```

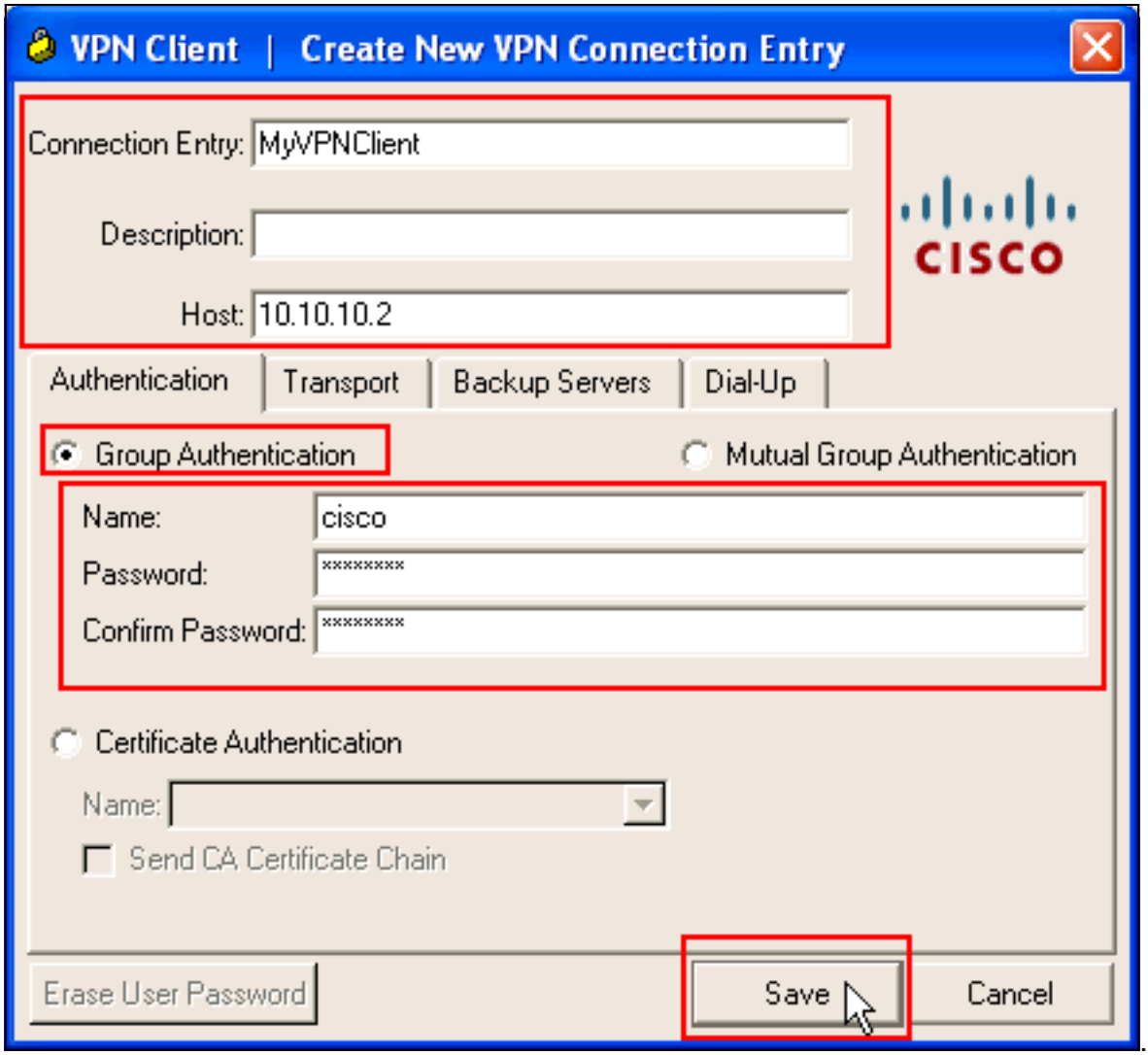
التحقق من الصحة

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

1. طقطقت **جديد**.

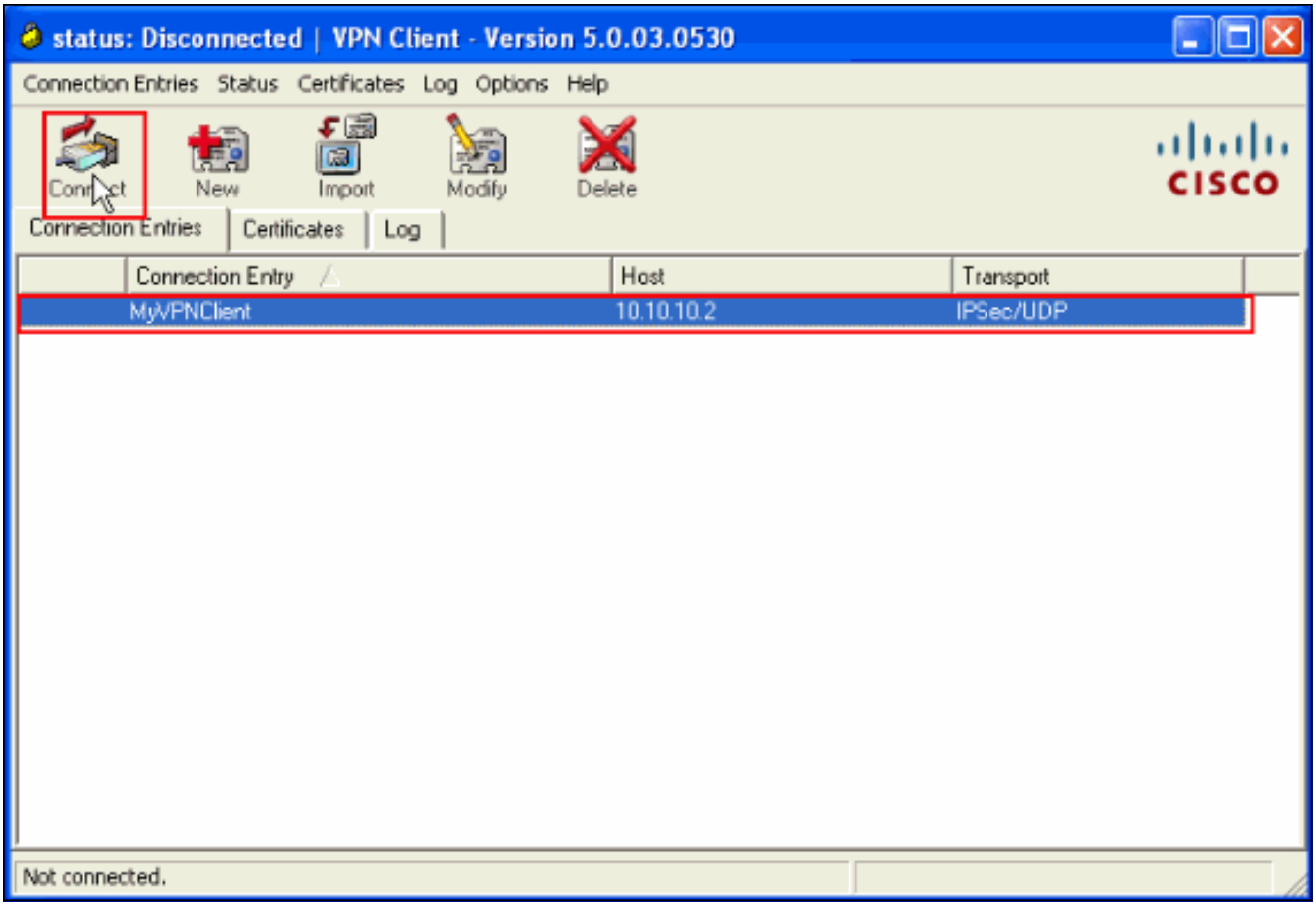


2. املأ تفاصيل إتصالك الجديد.يجب أن يحتوي حقل المضيف على عنوان IP أو اسم المضيف الخاص ب Cisco ASA الذي تم تكوينه مسبقا. يجب أن تتوافق معلومات مصادقة المجموعة مع تلك المستخدمة في **الخطوة 4**. انقر فوق **حفظ** عند



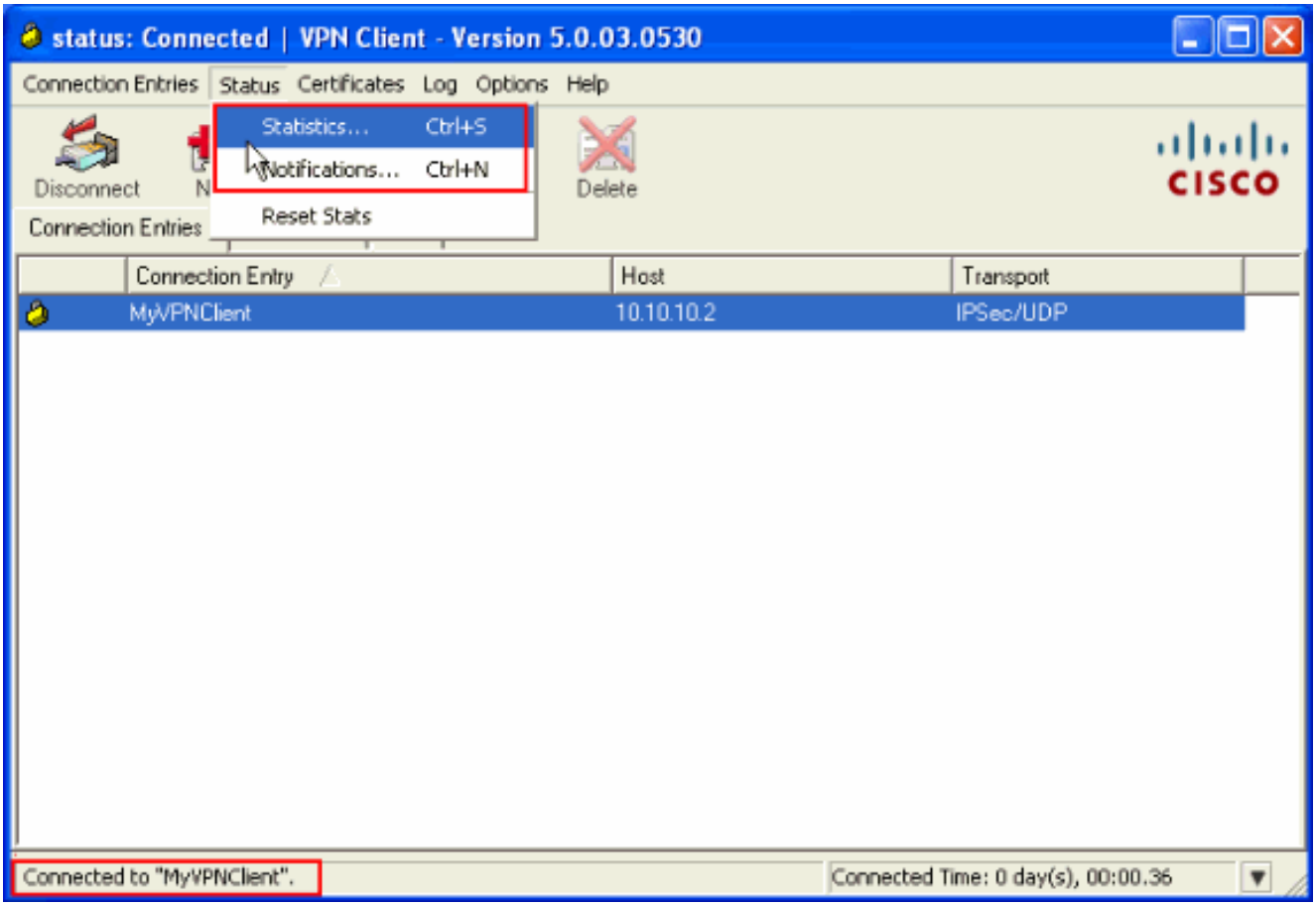
الانتهاء.

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

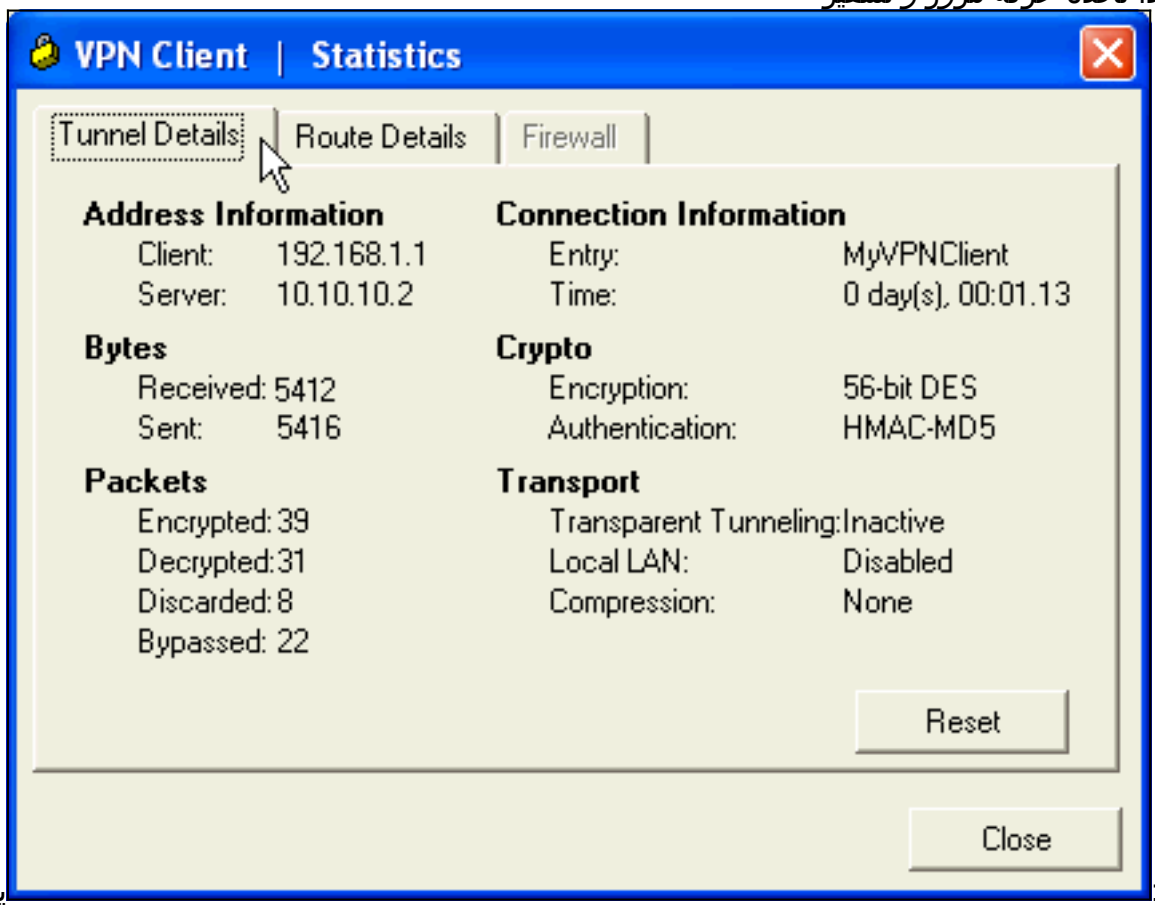


4. أدخل اسم مستخدم وكلمة مرور للمصادقة الموسعة. يجب أن تطابق هذه المعلومات المعلومات المحددة في **الخطوتين 5 و 6**.

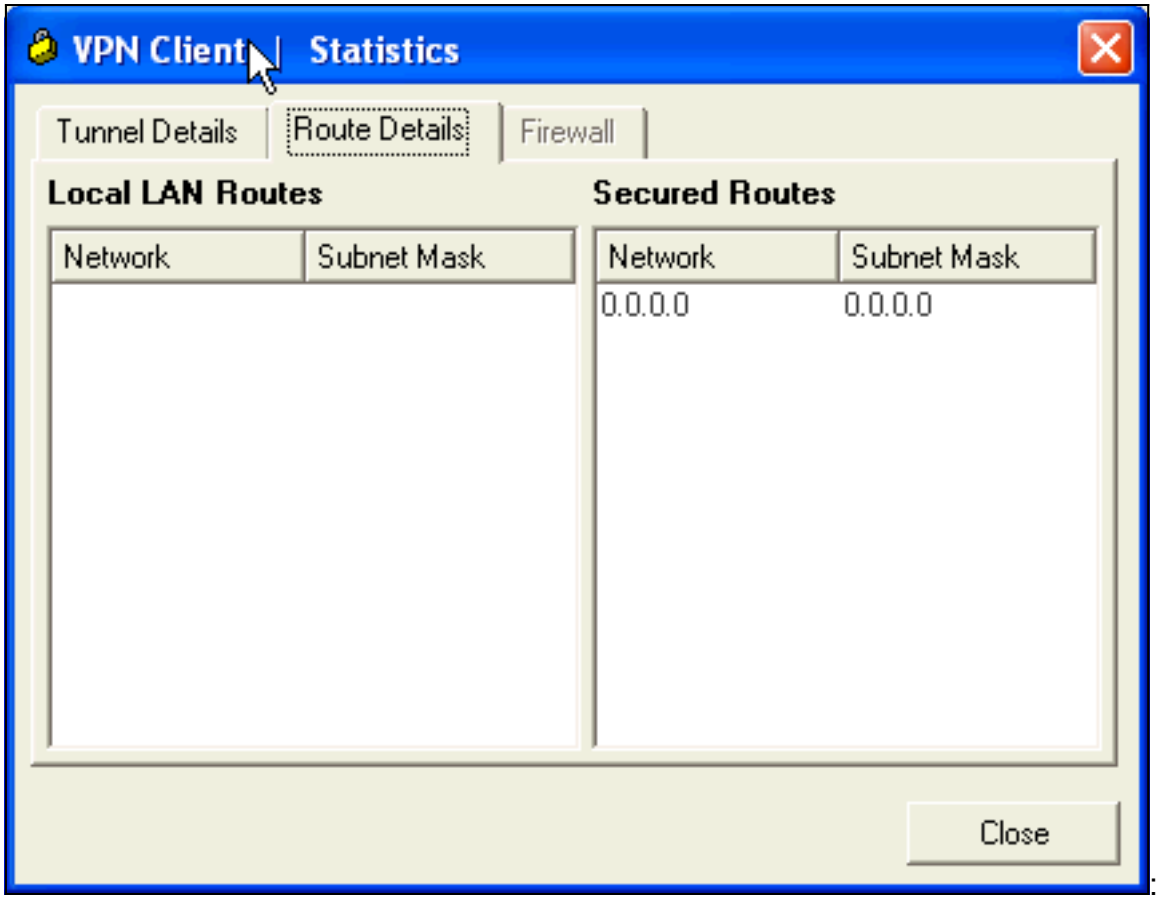
5. بمجرد تأسيس الاتصال بنجاح، أختر **إحصائيات** من قائمة الحالة للتحقق من تفاصيل النفق.



يبدي هذا نافذة حركة مرور و تشفير



معلومة: يبدي هذا نافذة انقسام tunneling



معلومة:

جهاز الأمان ASA/PIX - show commands

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

```
ASA#show crypto isakmp sa

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

                                IKE Peer: 10.10.10.1   1
Type    : user                   Role    : responder
Rekey   : no                     State   : AM_ACTIVE
```

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

```
ASA#show crypto ipsec sa
                                     interface: Outside
Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
                                                                   10.2.

                  (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
          (remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0
                              current_peer: 10.10.10.1, username: cisco123
                                   dynamic allocated peer ip: 192.168.1.1

                    pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20#
                    pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74#
                                pkts compressed: 0, #pkts decompressed: 0#
      pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0#
        pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                        send errors: 0, #recv errors: 0#

            local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
                path mtu 1500, ipsec overhead 58, media mtu 1500
                                current outbound spi: F49F954C

                                                    :inbound esp sas
                                              (spi: 0x3C10F9DD (1007745501
                                    transform: esp-des esp-md5-hmac none
                                         { ,in use settings ={RA, Tunnel
        slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
                        sa timing: remaining key lifetime (sec): 27255
                                                    IV size: 8 bytes
                                        replay detection support: Y
                                                    :outbound esp sas
                                              (spi: 0xF49F954C (4104099148
                                    transform: esp-des esp-md5-hmac none
                                         { ,in use settings ={RA, Tunnel
        slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
                        sa timing: remaining key lifetime (sec): 27255
                                                    IV size: 8 bytes
                                        replay detection support: Y
```

-

```
                                                ciscoasa(config)#debug icmp trace
Inbound Nat Translation is shown below for Outside to Inside ICMP echo request ---!
                                    translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
                                                                                2
 Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply ---!
                                  untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
 ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
                                                                             len=32
    ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
                                                                                2
    ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
         ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
           ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
         ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
           ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
         ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
           ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

ارجع إلى حلول أستكشاف أخطاء IPSec VPN وإصلاحها للمستوىL2 والوصول عن بعد للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء شبكة VPN الخاصة بالموقع وإصلاحها.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- مدير أجهزة حلول الأمان المعدلة من Cisco
- 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).