مثال استخدام VPN سهل لخادم Cisco IOS الموجه التكوين الاحترافي

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل cisco ios ® مسحاج تخديد ك VPN سهل (EzVPN) نادل يستعمل cisco تشكيل محترف (cisco cp) وال CLI. تتيح ميزة خادم VPN السهل للمستخدم النهائي البعيد إمكانية الاتصال باستخدام أمان IP (IPsec) مع أي بوابة للشبكة الخاصة الظاهرية (VPN) بنظام Cisco IOS. يتم "دفع" سياسات IPsec المدارة مركزيا إلى جهاز العميل بواسطة الخادم، مما يقلل من التكوين بواسطة المستخدم النهائي.

لمزيد من المعلومات حول خادم Easy VPN، ارجع إلى قسم خادم VPN السهل من مكتبة دليل تكوين الاتصال الآمن، Cisco IOS، الإصدار 12.4T.

المتطلبات الأساسية

المكونات المستخدمة

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

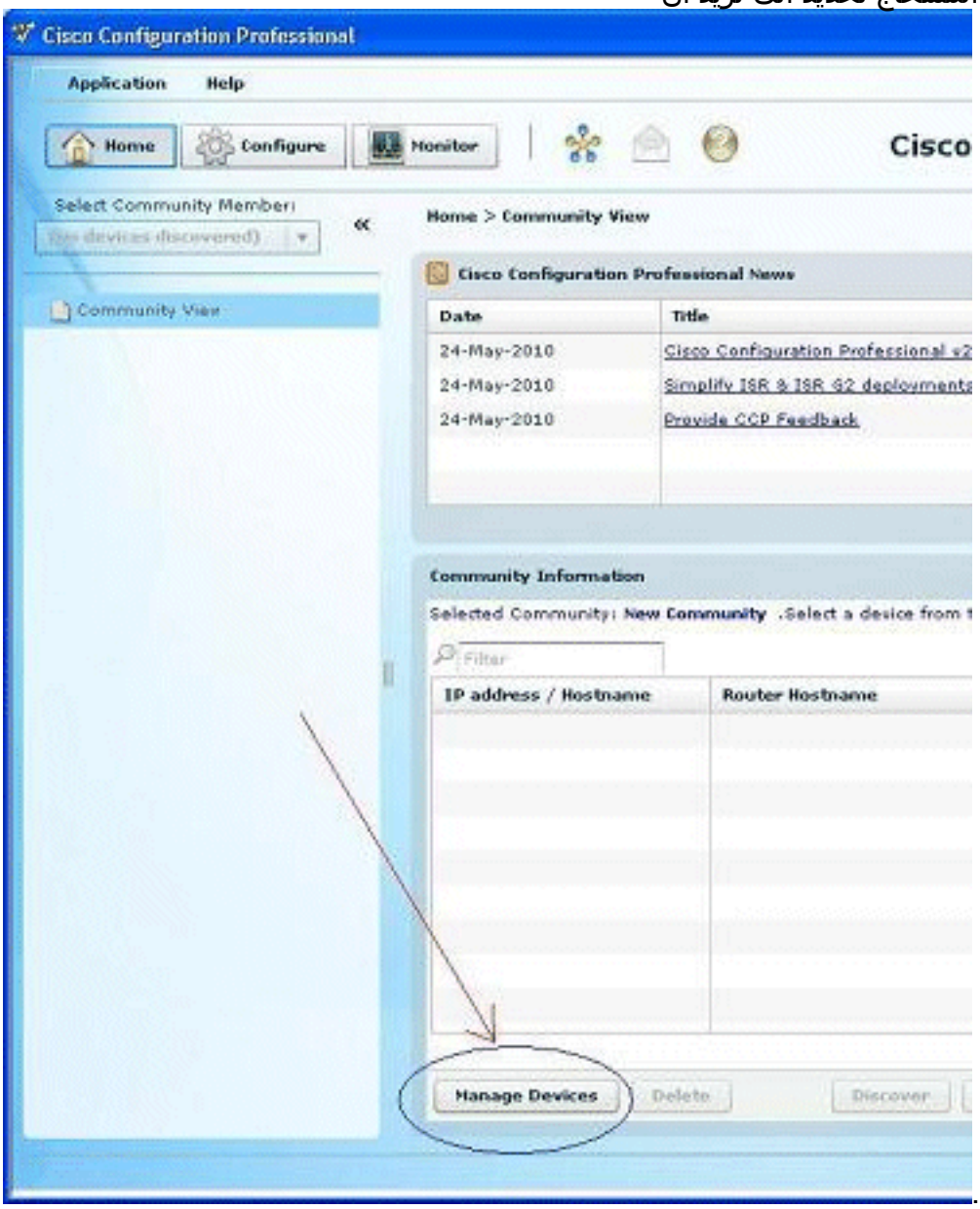
- cisco 1841 مسحاج تخديد مع cisco ios برمجية إطلاق 12.4(15T)
- Cisco CP الإصدار 2.1

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.

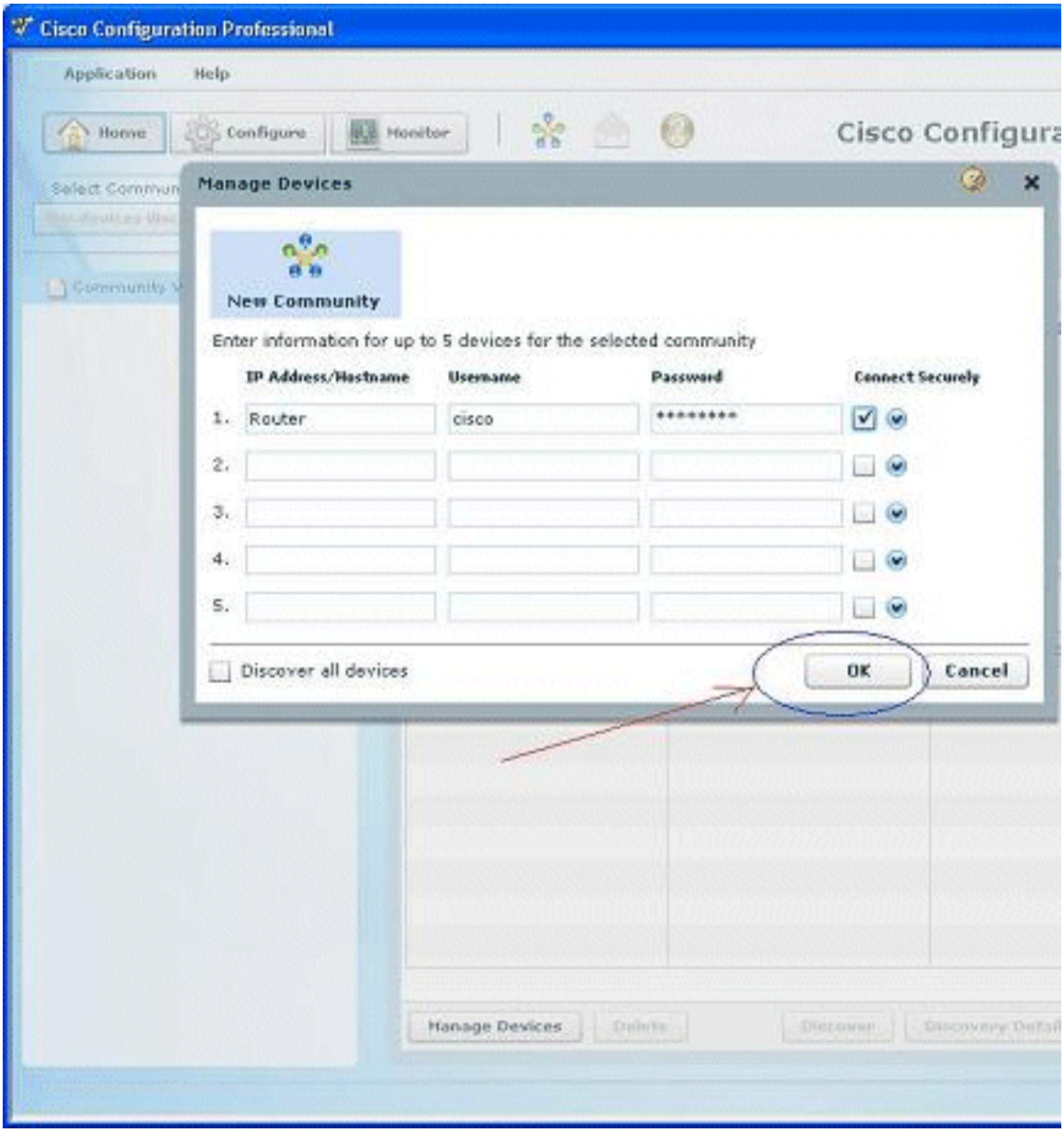
ركبت cisco cp

أنجزت هذا steps in order to ركبت cisco cp:

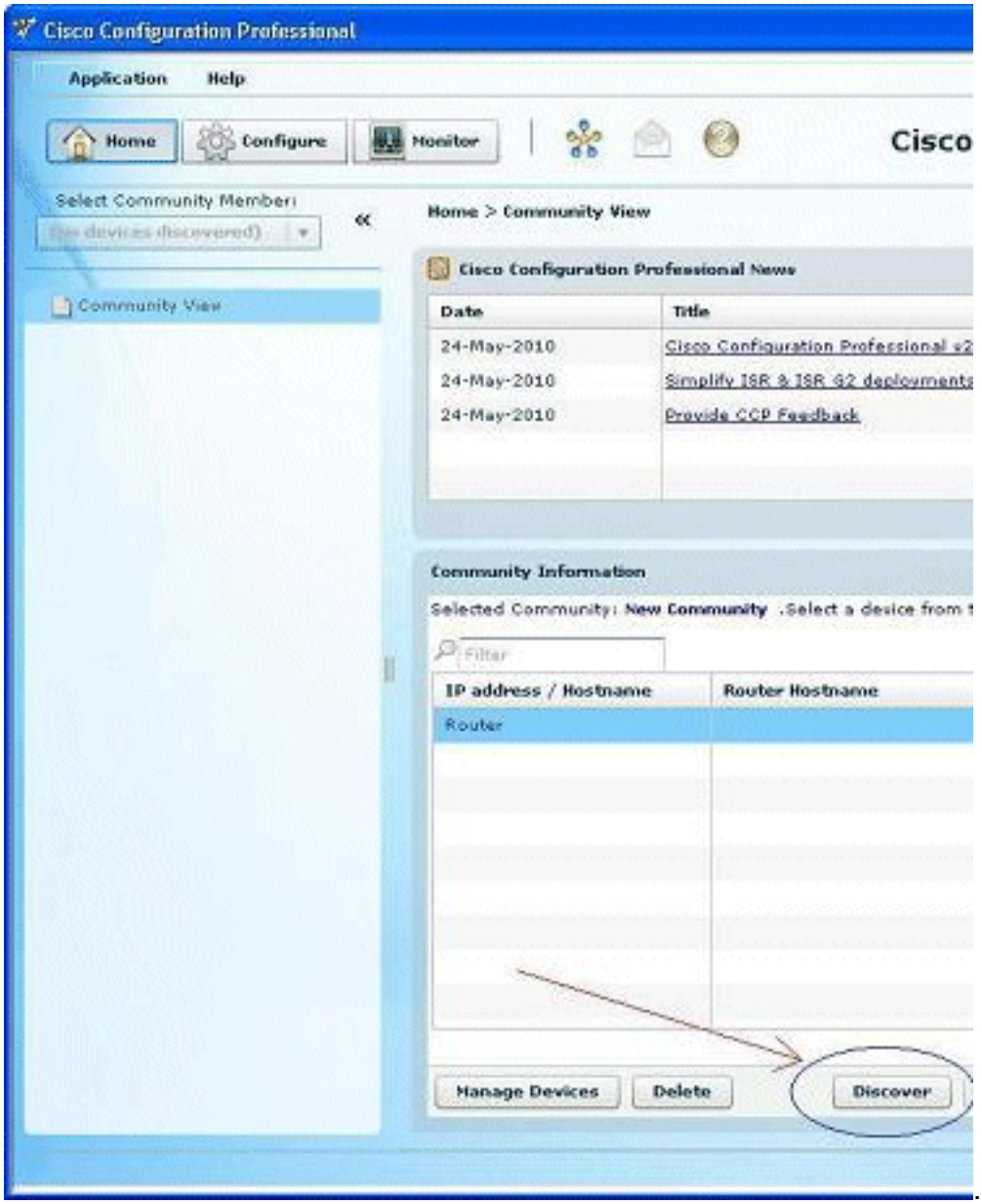
1. جلبت cisco cp V2.1 من ال cisco برمجية مركز (يسجل زبون فقط) وركبت هو على pc ك محلي.الأحدث نسخة ال cisco cp يستطيع كنت أسست في ال cisco cp موقع.
2. أطلقت cisco cp من pc ك محلي من خلال **بداية>برنامج>cisco تشكيل محترف (CCP)** واخترت **الجماعة** أي يتلقى المسحاج تخديد أنت تريد أن



يشكل.



3. ركزت in order to اكتشفت الأداة أنت تريد أن يشكل، المسحاج تخديد وطقطقة



يكتشف.

ملاحظة: أحلت لمعلومة على ال cisco مسحاج تخديد نموذج و ios إطلاق أن يكون متوافق إلى cisco cp V2.1، المتوافق cisco ios إطلاق قسم.

ملاحظة: أحلت لمعلومة على ال pc متطلب أن يركض cisco cp V2.1، النظام متطلب قسم.

تكوين الموجّه لتشغيل Cisco CP

قم بتنفيذ خطوات التكوين التالية لتشغيل Cisco CP على موجّه Cisco:

1. اتصل بالموجّه باستخدام Telnet أو SSH أو من خلال وحدة التحكم.ادخل وضع التكوين العام باستخدام هذا الأمر:

```
Router(config)#enable
#(Router(config
```

2. إذا تم تمكين HTTP وHTTPS وتكوينهما لاستخدام أرقام منافذ غير قياسية، فيمكن تخطي هذه الخطوة واستخدام رقم المنفذ المكون بالفعل.قم بتمكين خادم HTTP أو HTTPS باستخدام الأوامر التالية باستخدام برامج Cisco IOS Software:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

3. إنشاء مستخدم بامتيازات المستوى 15:

```
Router(config)# username privilege 15 password 0
```

ملاحظة: استبدلت *<username>* و *<password>* مع ال username وكلمة أن أنت تريد أن يشكل.

4. شكلت SSH و telnet لمحلي login وامتياز مستوى 15.

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

5. (اختياري) قم بتمكين التسجيل المحلي لدعم وظيفة مراقبة السجل:

```
Router(config)# logging buffered 51200 warning
```

المتطلبات

يفترض هذا وثيقة أن ال cisco مسحاج تخديد يكون كليا عمليت وشكلت أن يسمح cisco cp أن يجعل تشكيل تغير.

أحلت لمعلومات كاملة على كيف أن يبدأ يستعمل cisco cp، يحصل يبدأ مع cisco تشكيل محترف.

الاصطلاحات

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

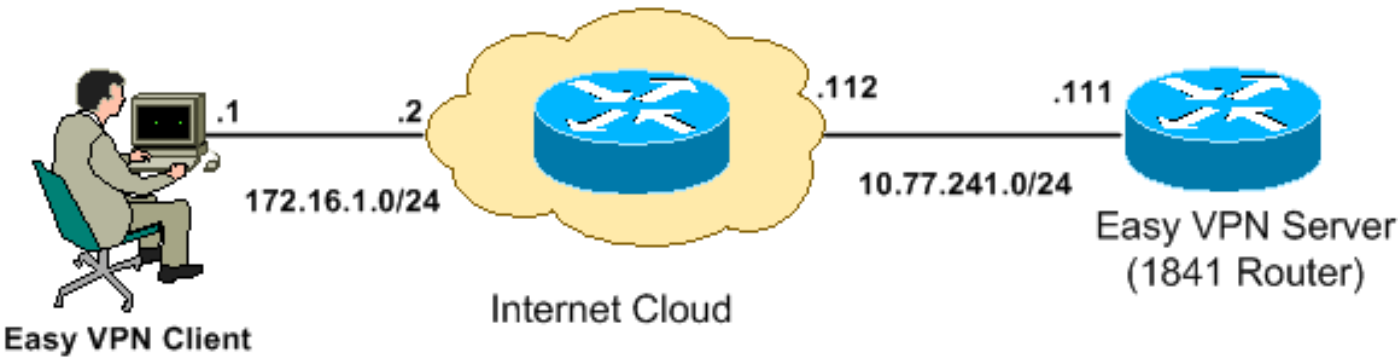
التكوين

في هذا القسم، تُعرض لك معلومات تكوين الإعدادات الأساسية لأي موجّه في الشبكة.

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:

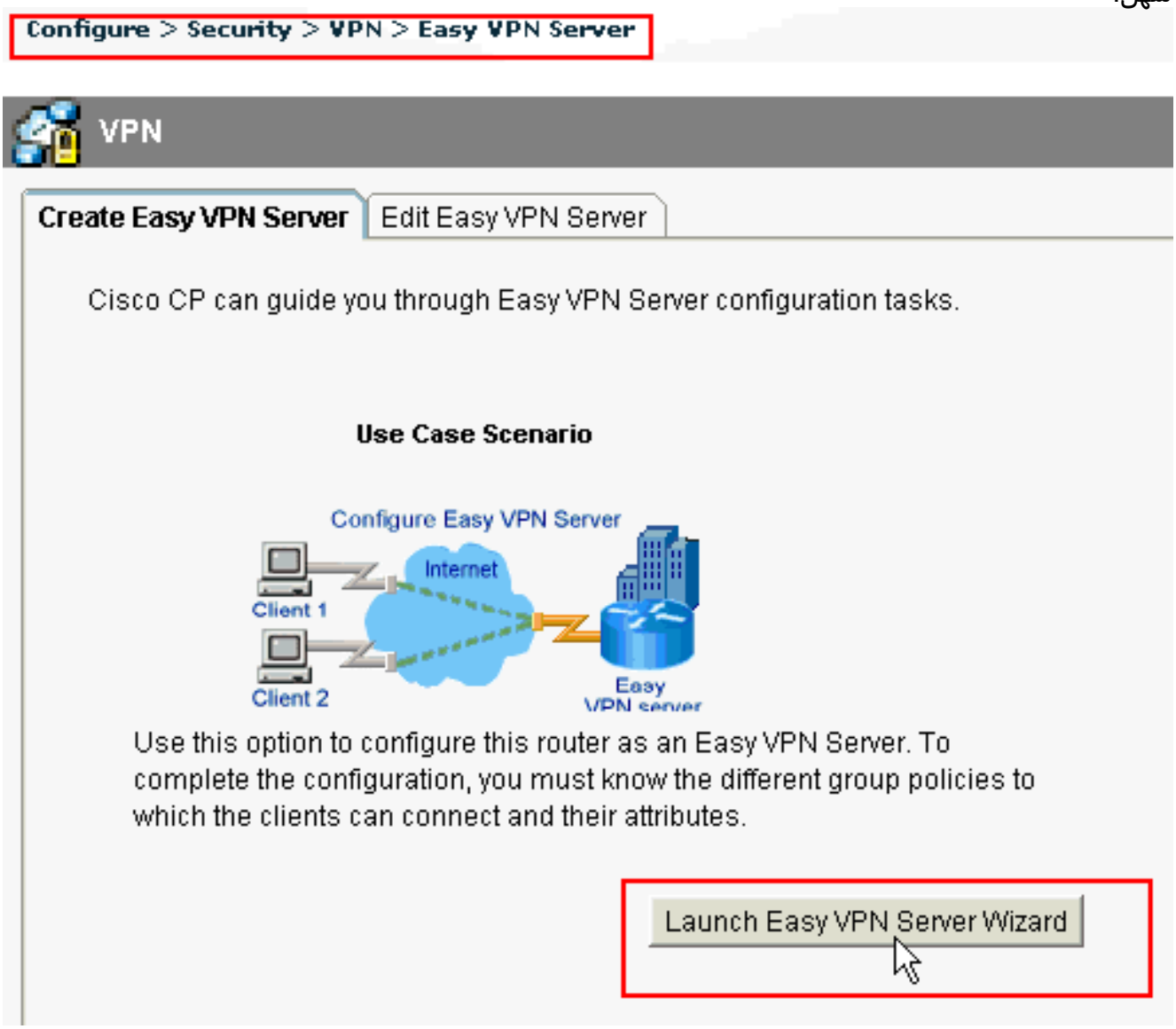


ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

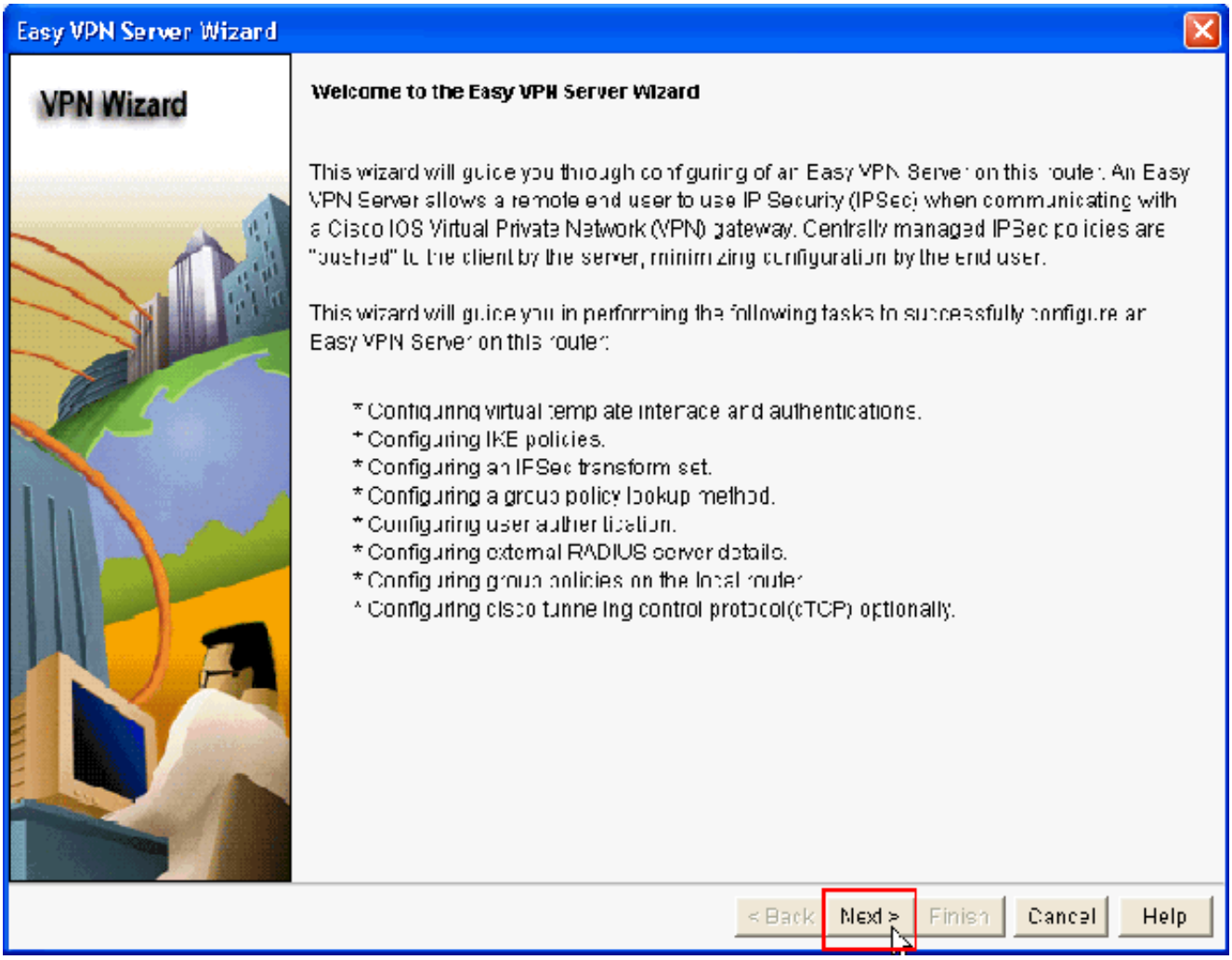
cisco cp - سهل VPN نادل تشكيل

أنجزت هذا steps in order to شكلت ال cisco ios مسحاج تخديد كسهل VPN نادل:

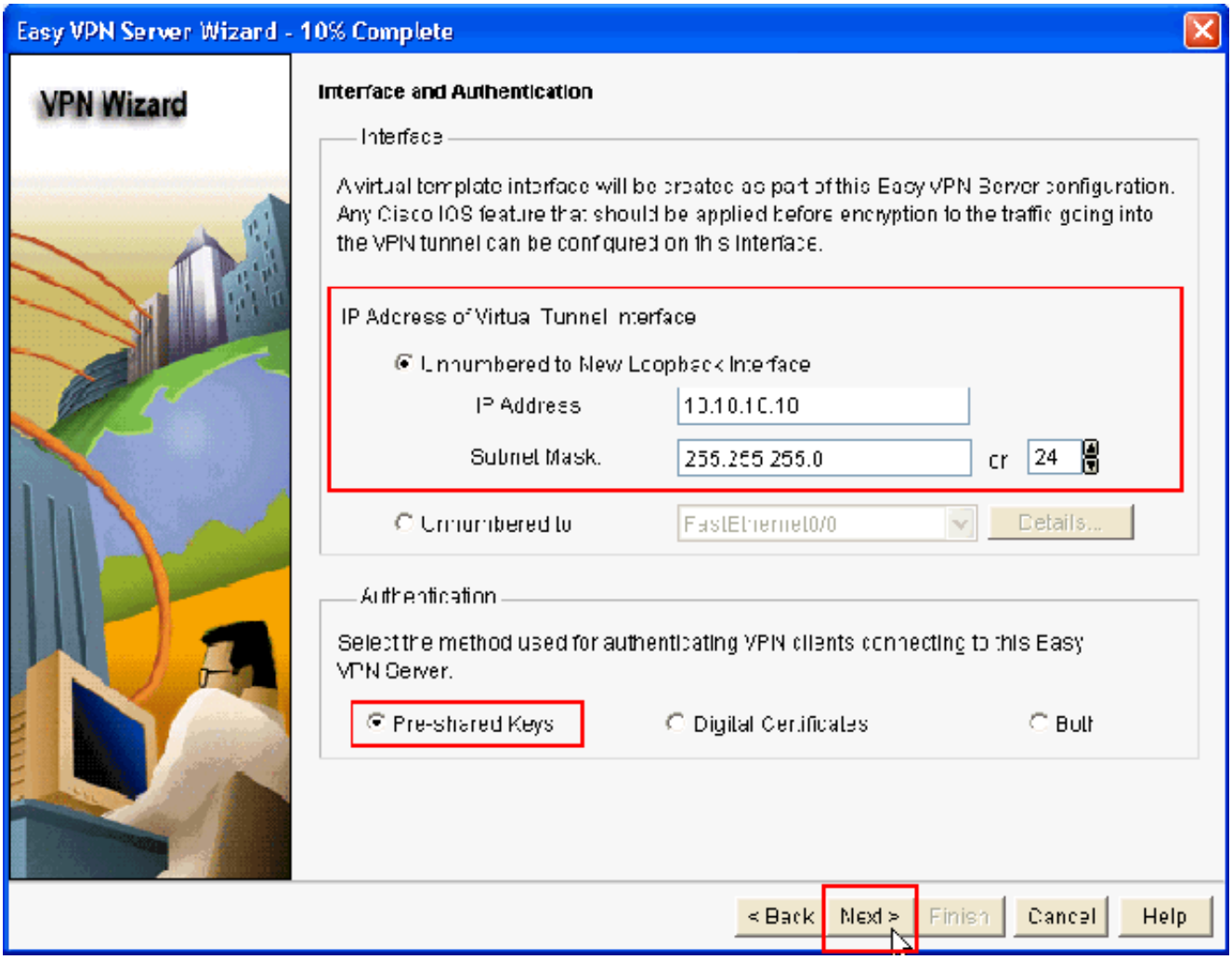
1. أخترت يشكل>أمن>VPN>**ييسر VPN نادل>يخلق VPN نادل سهل** وطقطقة إطلاق easy VPN نادل مرشد in order to شكلت ال cisco ios مسحاج تخديد كخادم VPN سهل:



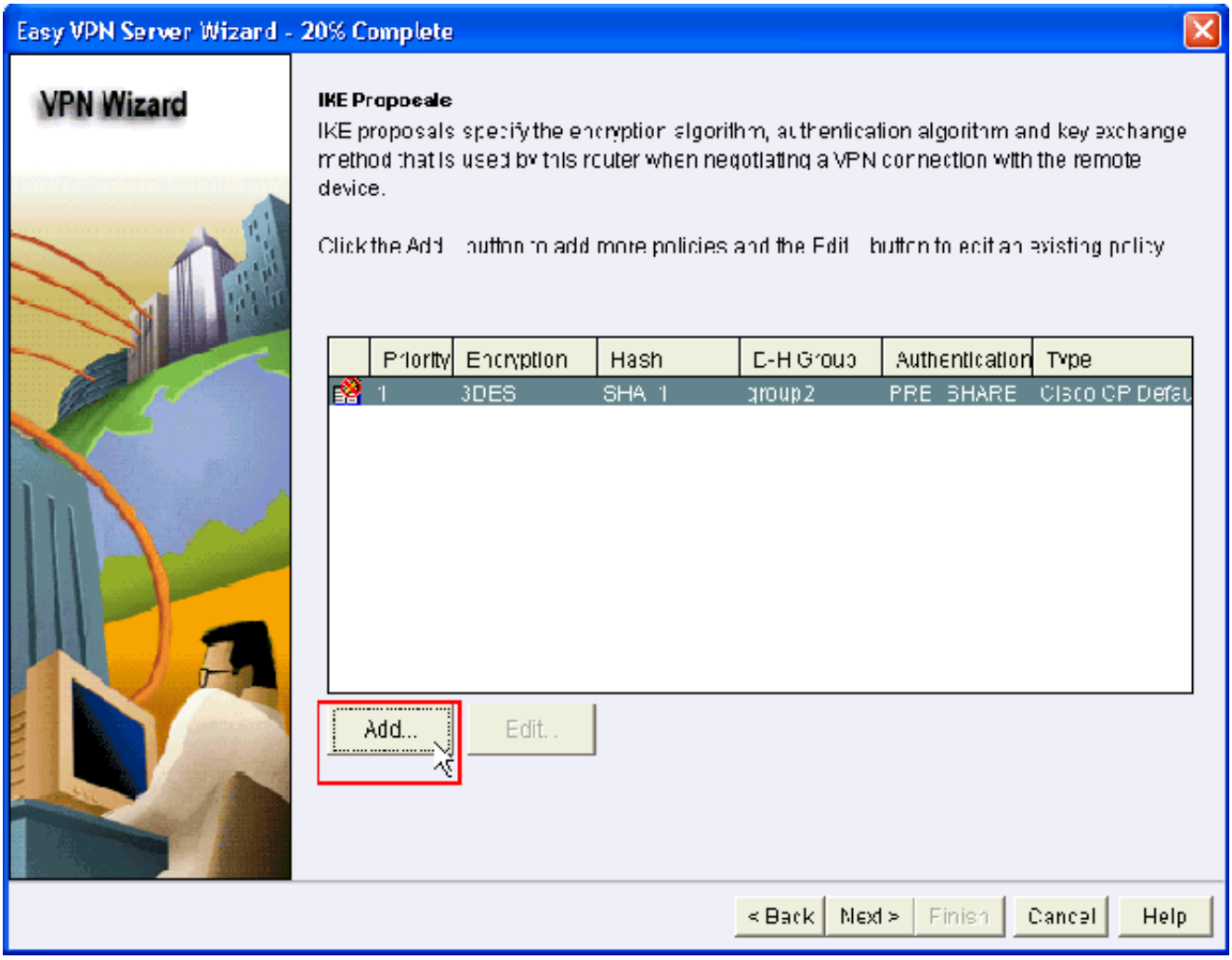
2. طقطقت **بعد ذلك** in order to باشرت مع **السهل VPN نادل** تشكيل.



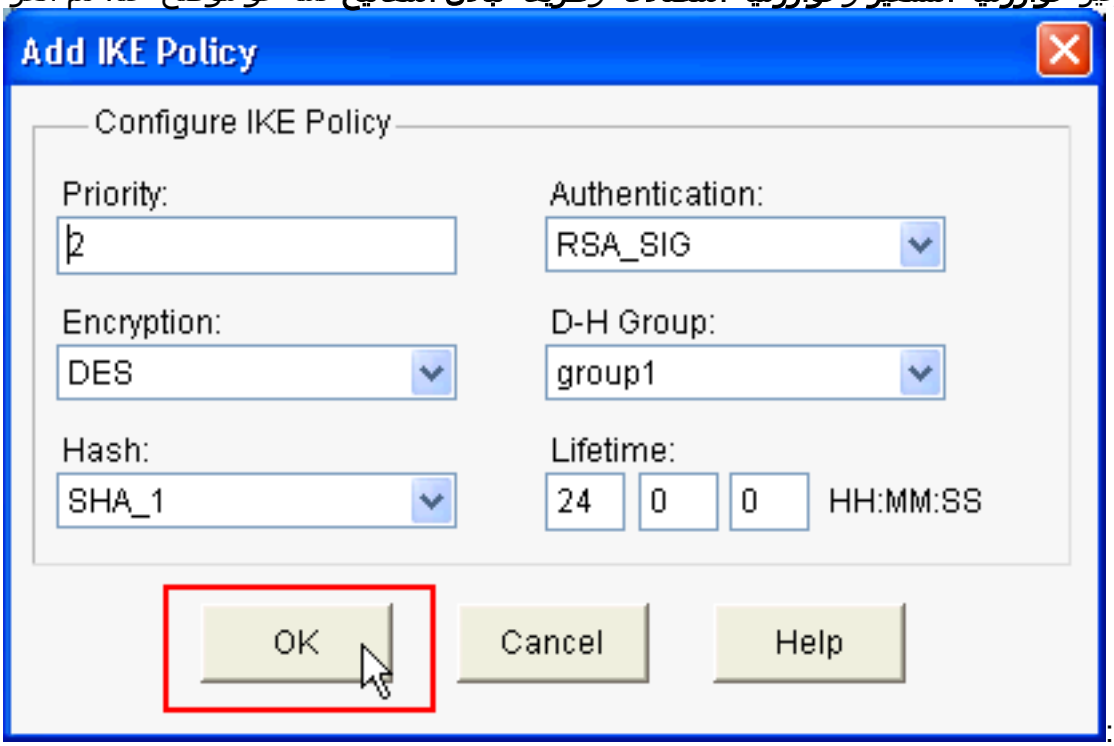
3. في الإطار الناتج، سيتم تكوين **واجهة افتراضية** كجزء من تكوين خادم VPN السهل. قم بتوفير **عنوان IP الخاص بواجهة النفق الظاهري** واختر أيضا **طريقة المصادقة** المستخدمة لمصادقة عملاء VPN. هنا، طريقة المصادقة المستخدمة هي **المفاتيح المشتركة مسبقا**. طقطقت **بعد ذلك**:



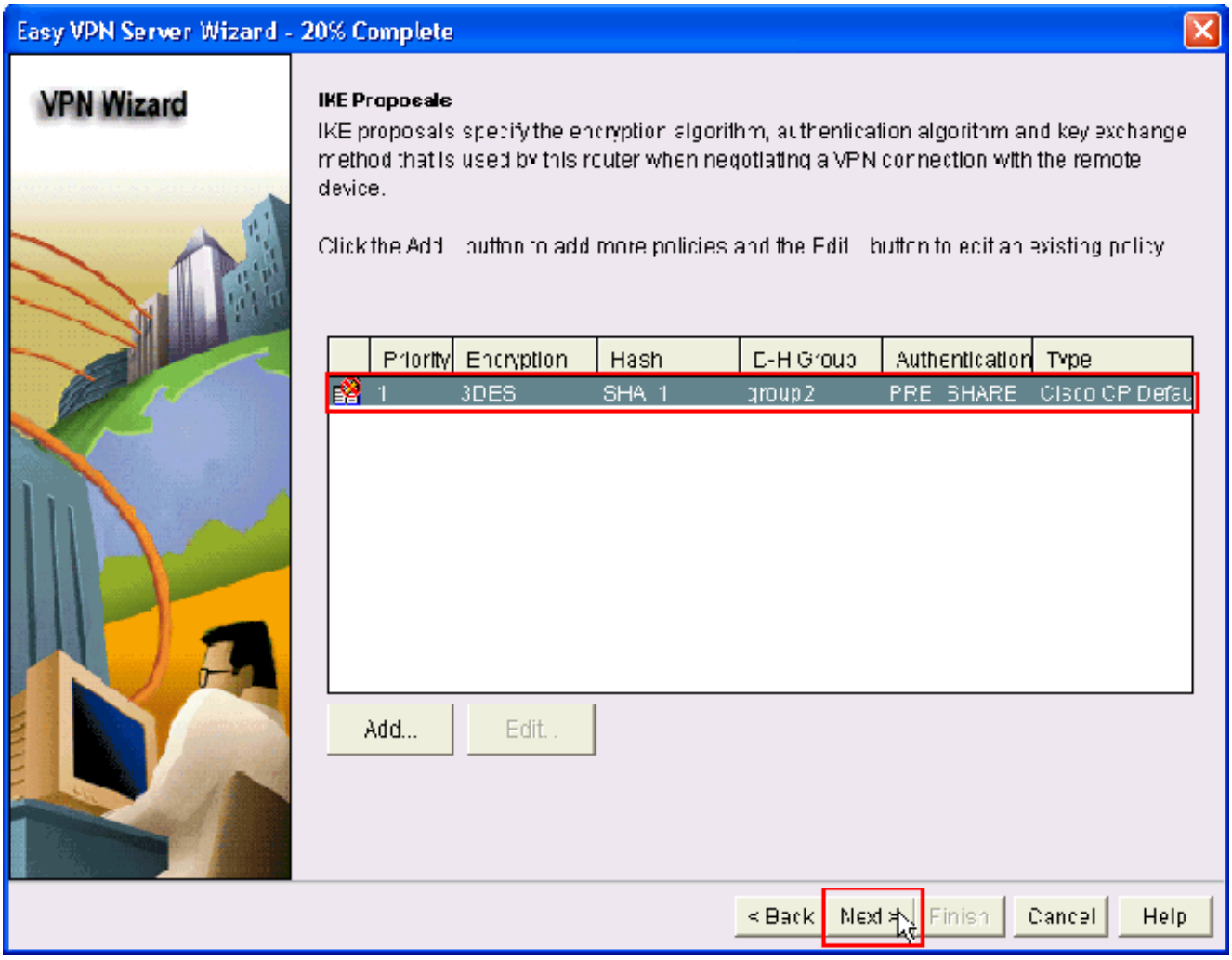
4. حدد **خوارزمية التشفير وخوارزمية المصادقة وطريقة تبادل المفاتيح** التي يجب إستخدامها من قبل هذا الموجه عند التفاوض مع الجهاز البعيد. يوجد نهج IKE افتراضي على الموجه يمكن إستخدامه إذا لزم الأمر. إذا أردت إضافة نهج IKE جديد، انقر فوق
إضافة.



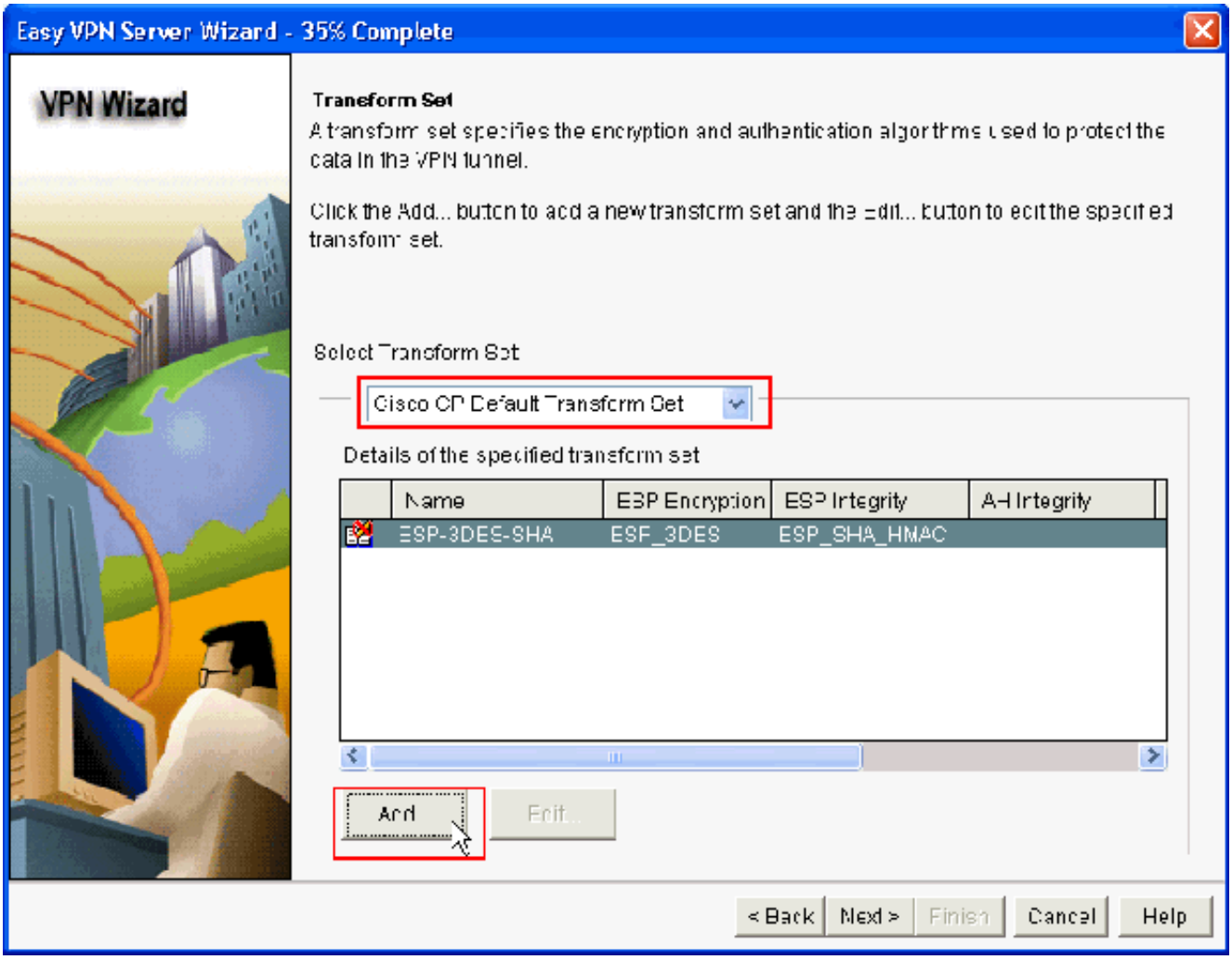
5. قم بتوفير **خوارزمية التشفير** و**خوارزمية المصادقة** و**طريقة تبادل المفاتيح** كما هو موضح هنا، ثم انقر فوق **موافق**.



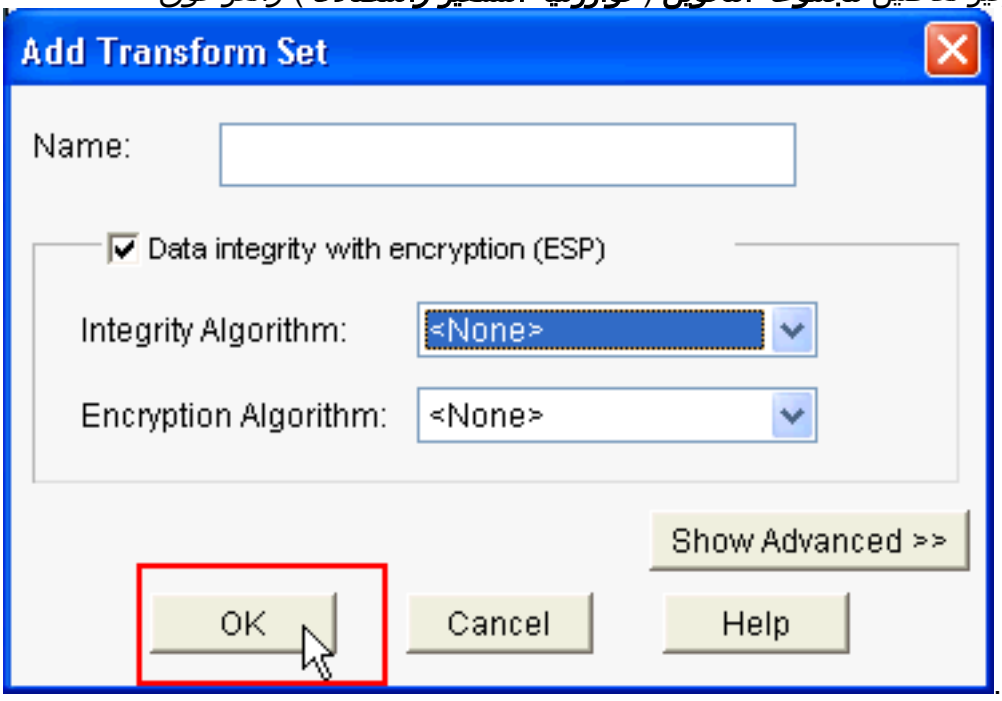
6. يتم إستخدام **نهج IKE الافتراضي** في هذا المثال. ونتيجة لذلك، أختر نهج IKE الافتراضي وانقر فوق **التالي**.



7. في النافذة الجديدة، يجب توفير تفاصيل **مجموعة التحويل**. تحدد مجموعة التحويل خوارزميات **التشفير** و**المصادقة** المستخدمة لحماية **البيانات في نفق VPN**. انقر فوق **إضافة** لتوفير هذه التفاصيل. يمكنك إضافة أي عدد من مجموعات التحويل حسب الحاجة عند النقر فوق **إضافة** وتوفير التفاصيل.**ملاحظة:** تكون **مجموعة تحويل CP الافتراضي** موجودة بشكل افتراضي على الموجه عند تكوينها باستخدام Cisco CP.

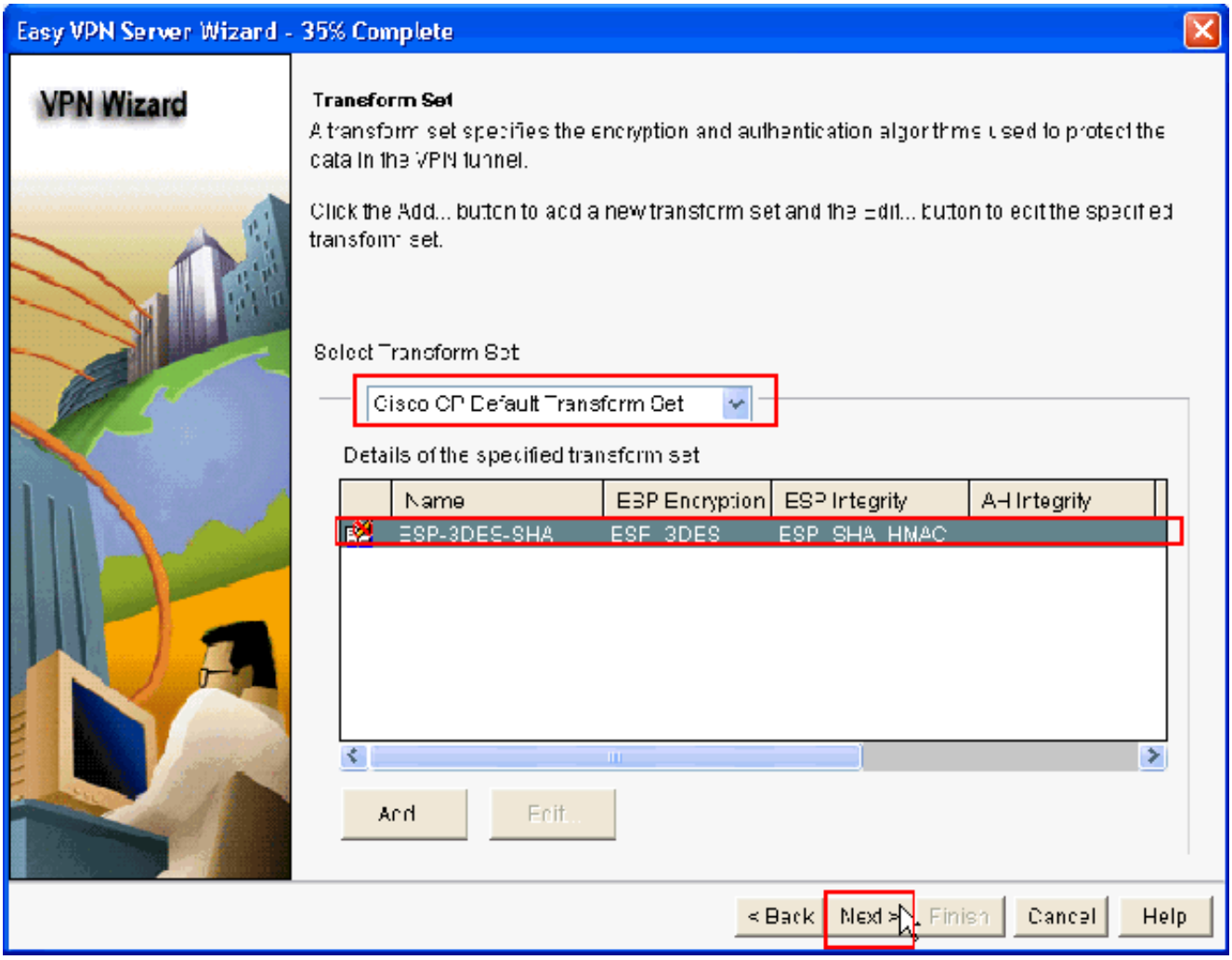


8. قم بتوفير تفاصيل **مجموعة التحويل** (**خوارزمية التشفير والمصادقة**) وانقر فوق

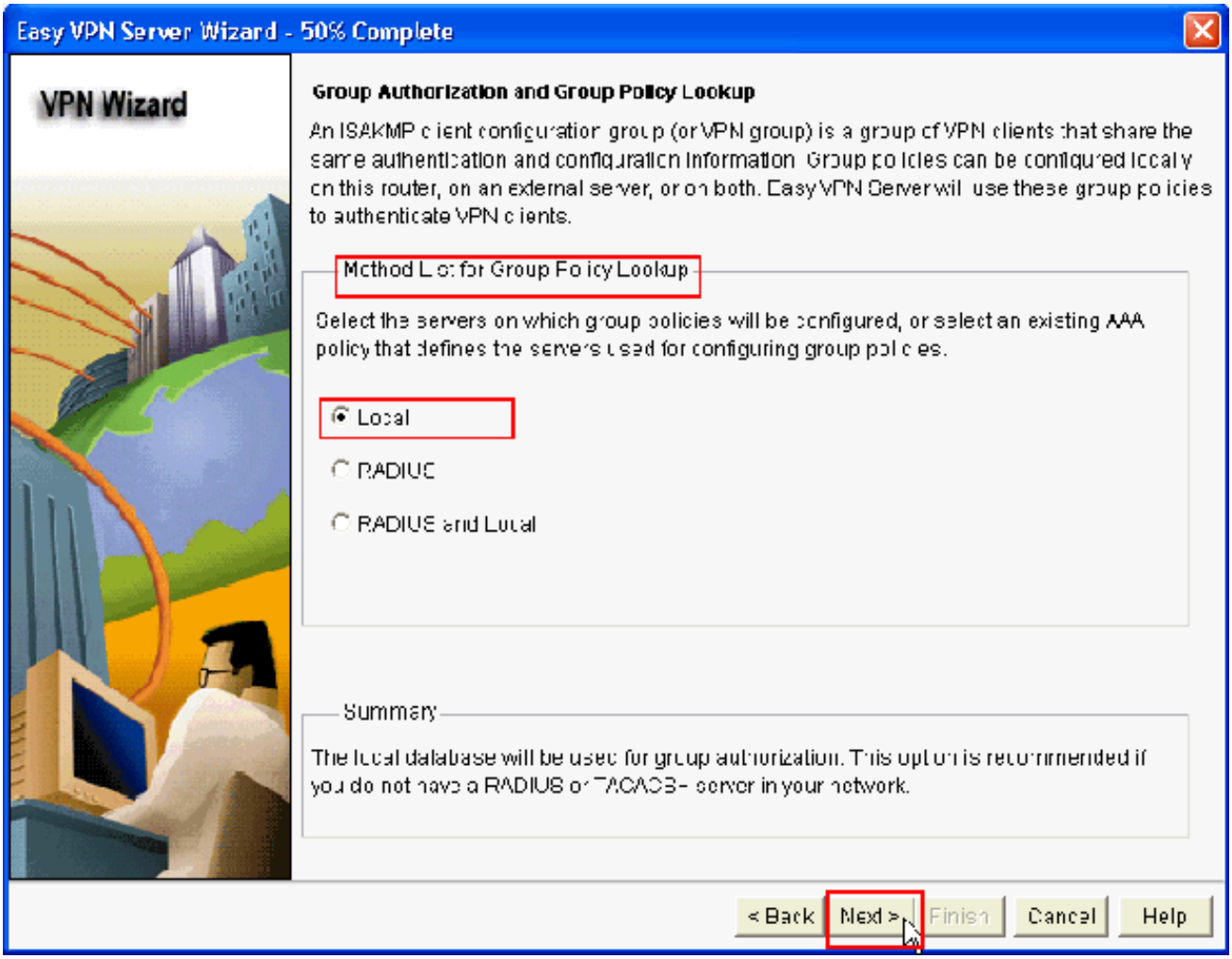


موافق.

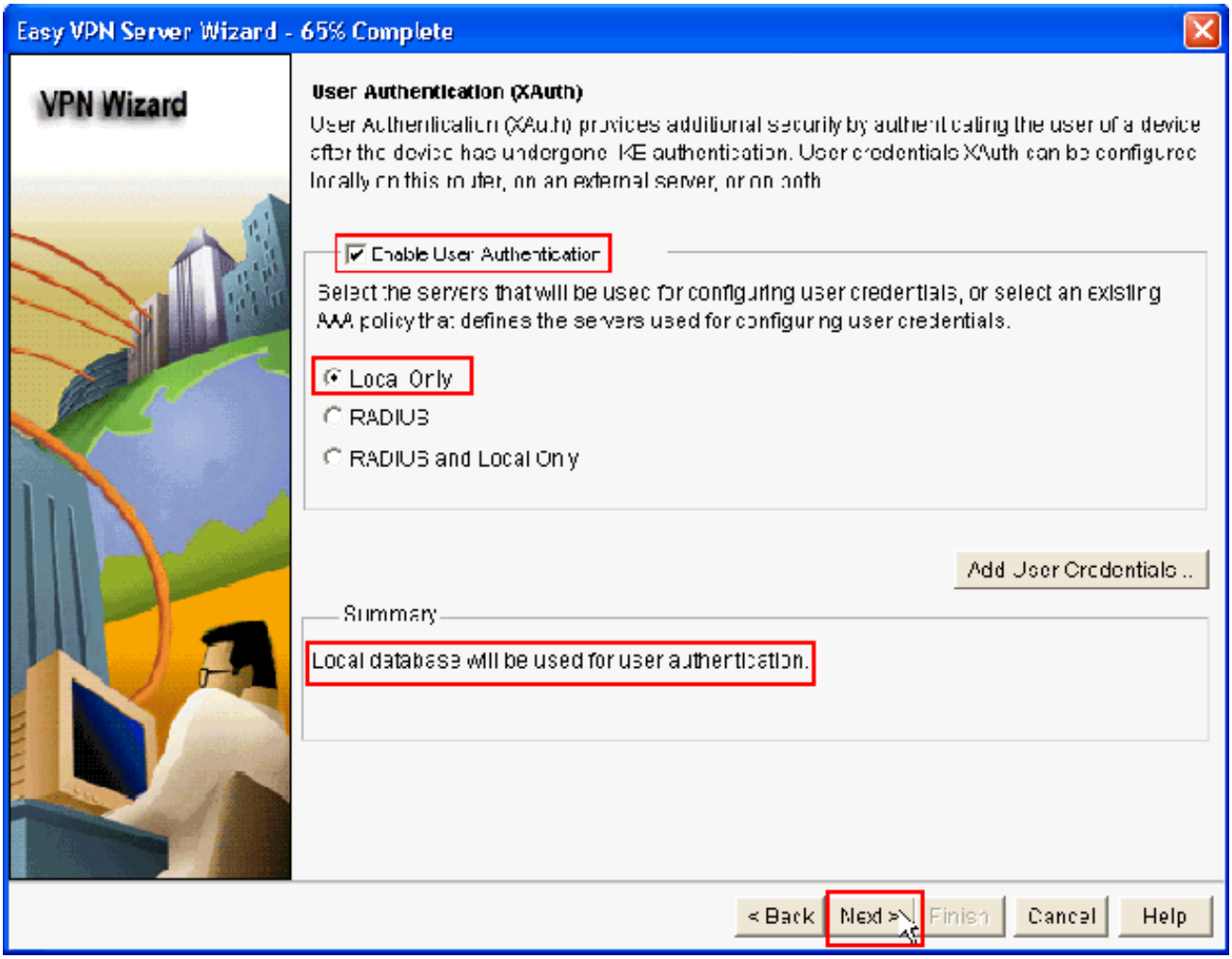
9. **التقصير تحويل مجموعة** يعين **cp تقصير تحويل مجموعة** استعملت في هذا مثال. بالنتيجة، أختر مجموعة التحويل الافتراضية وانقر
التالي.



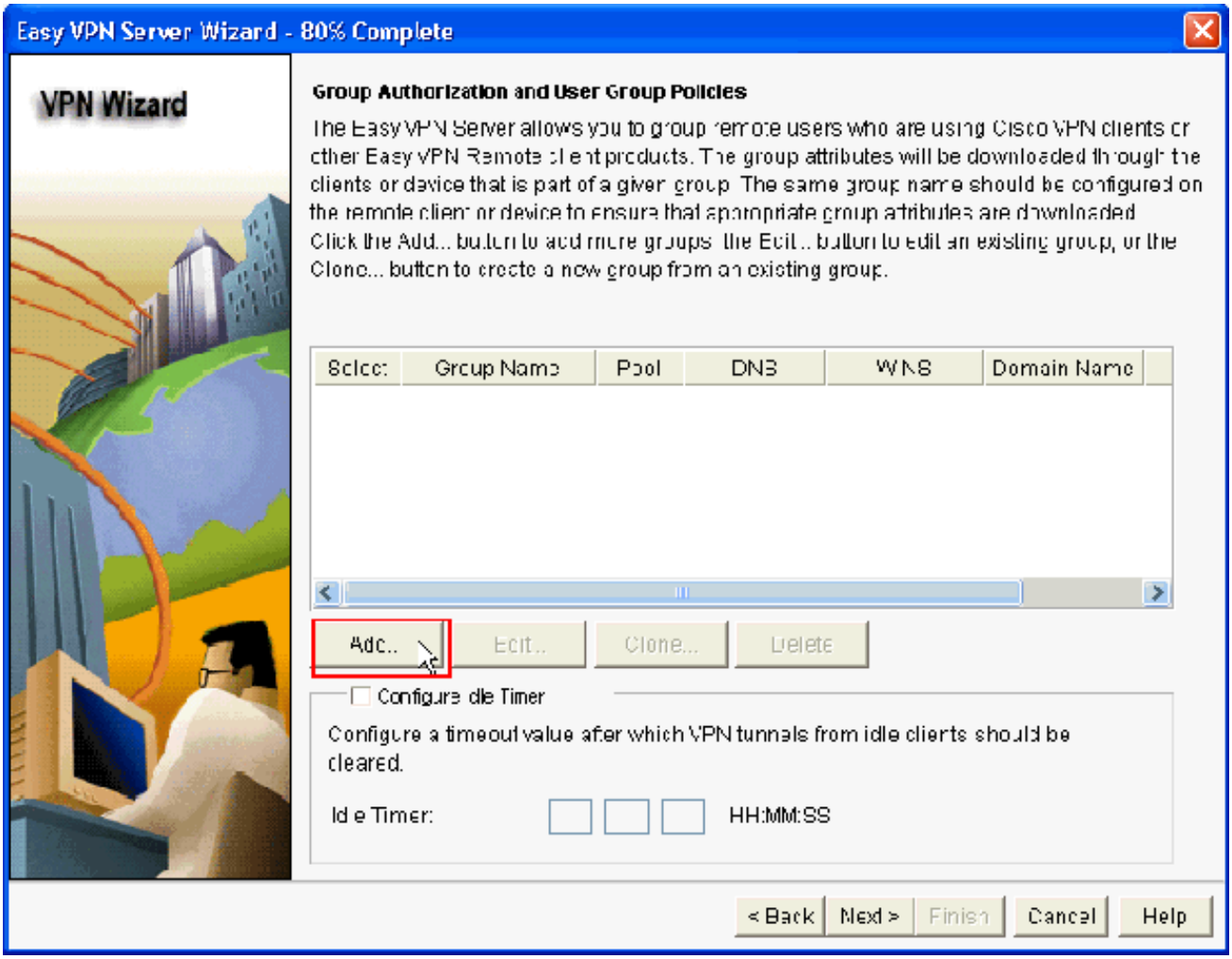
10. في النافذة الجديدة، أختر الخادم الذي سيتم تكوين سياسات المجموعة عليه والذي يمكن أن يكون إما **محلي** أو **RADIUS** أو كلا النوعين **محلي و RADIUS**. في هذا المثال، نستخدم **الخادم المحلي** لتكوين سياسات المجموعة. أخترت **محلي** وطقطقة **بعد ذلك**.



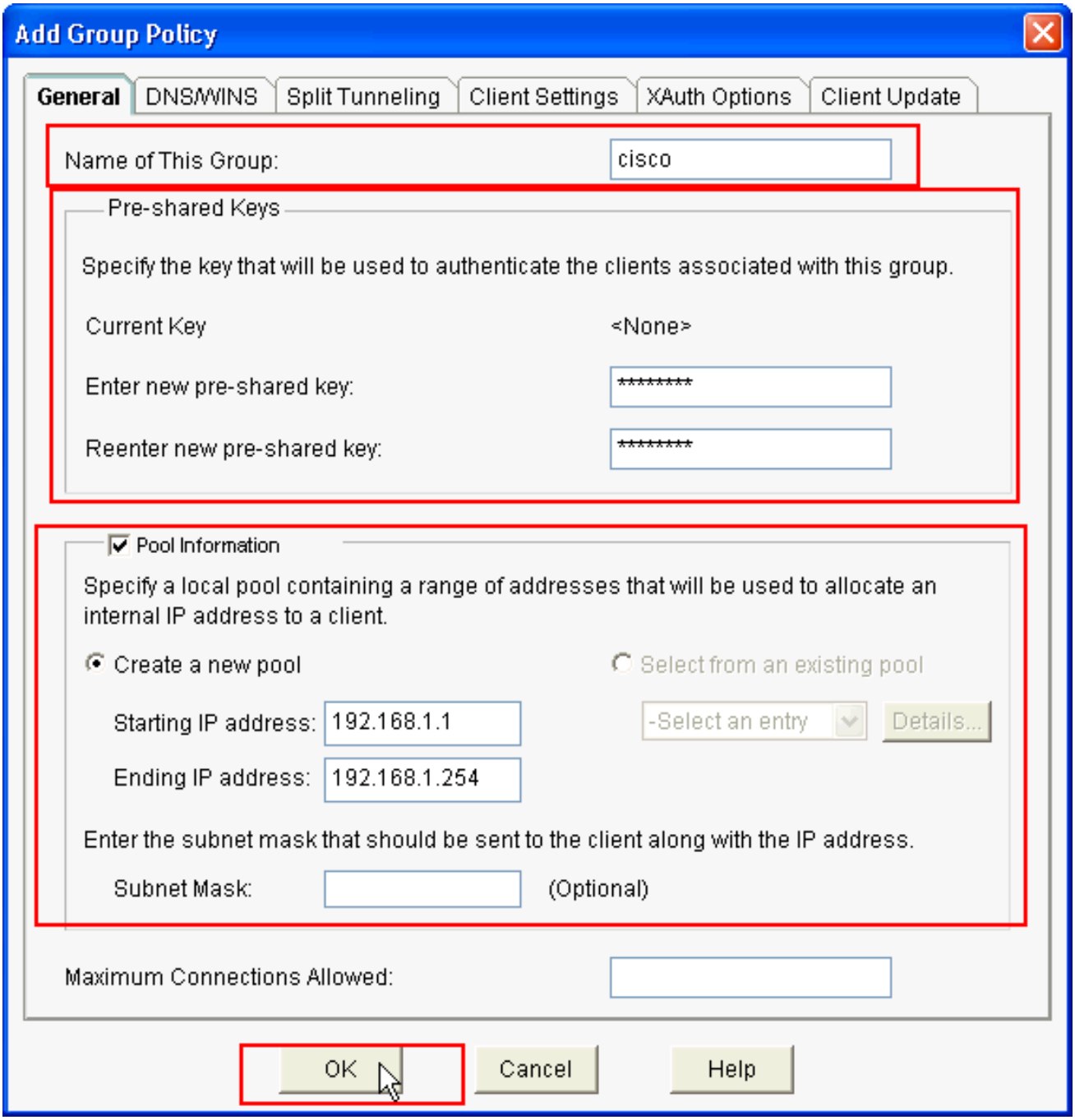
11. أخترت الخادم أن يكون استعملت لمصادقة مستعمل في هذا نافذة جديد أي يستطيع كنت **محلي فقط** أو **RADIUS** أو كلا **محلي فقط و RADIUS**. في هذا المثال، نستخدم **الخادم المحلي** لتكوين مسوغات المستخدم للمصادقة. تأكد من تحديد خانة الاختيار المجاورة **لتمكين مصادقة المستخدم**. أخترت **محلي فقط** وطقطقة **بعد ذلك**.



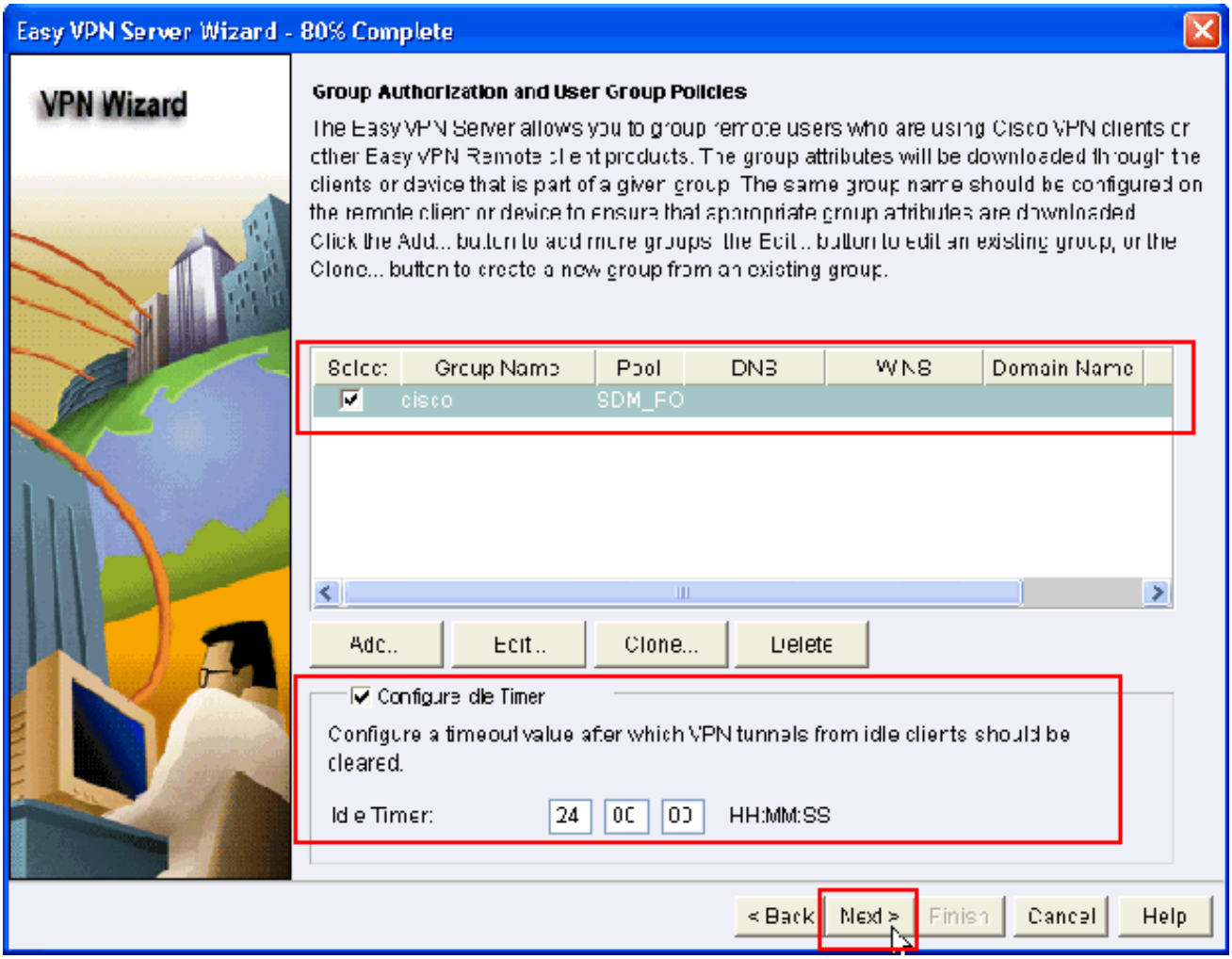
12. انقر فوق **إضافة** لإنشاء نهج مجموعة جديد ولإضافة المستخدمين عن بعد في هذه المجموعة.



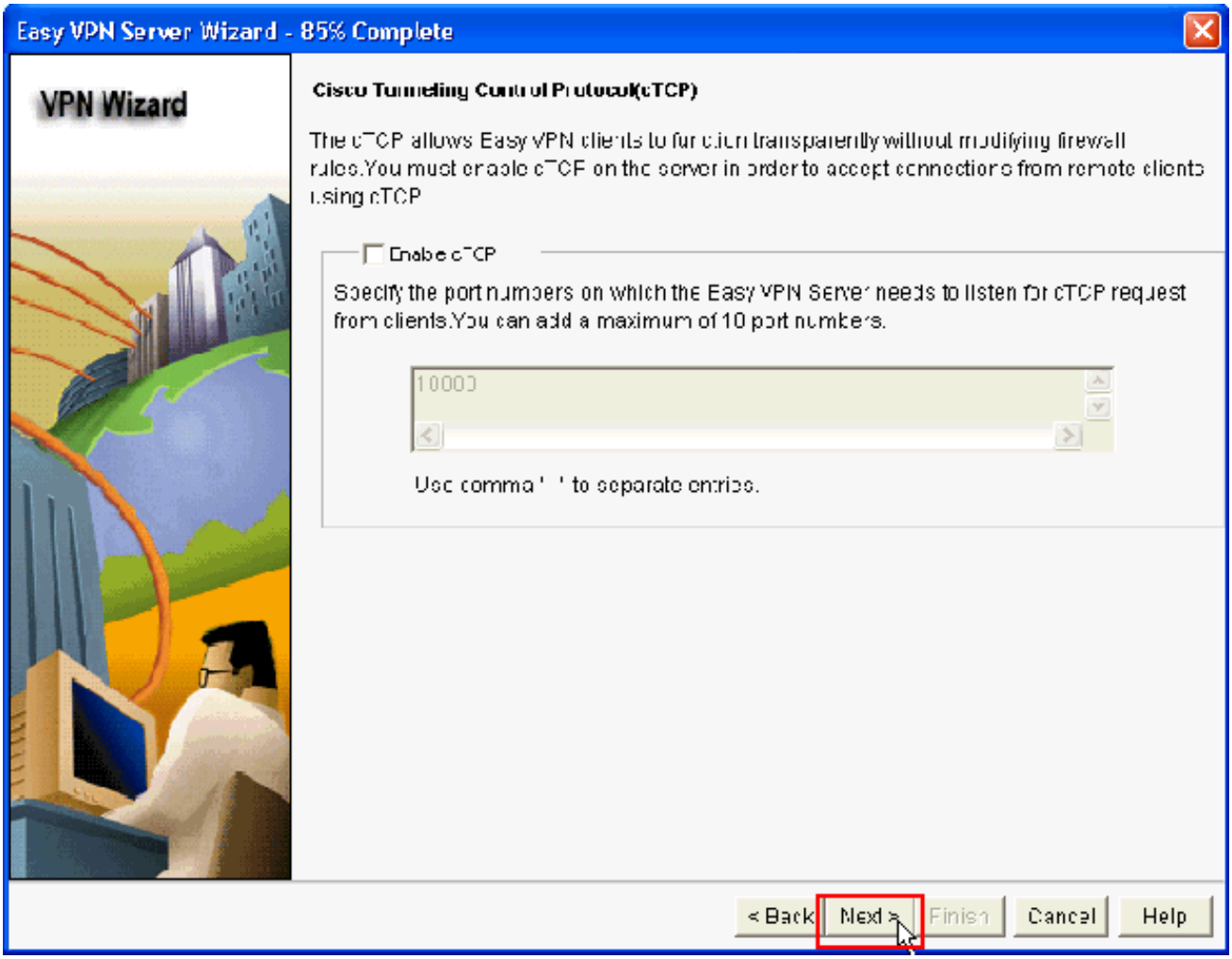
13. في نافذة إضافة نهج المجموعة، قم بتوفير اسم المجموعة في المساحة لاسم هذه المجموعة (Cisco في هذا المثال) مع مفتاح مشترك مسبقا، وتجمع IP (عنوان IP الأولي وعنوان IP الختامي) المعلومات كما هو موضح وانقر فوق موافق.**ملاحظة:** يمكنك إنشاء تجمع IP جديد أو إستخدام تجمع IP موجود إذا كان موجودا.



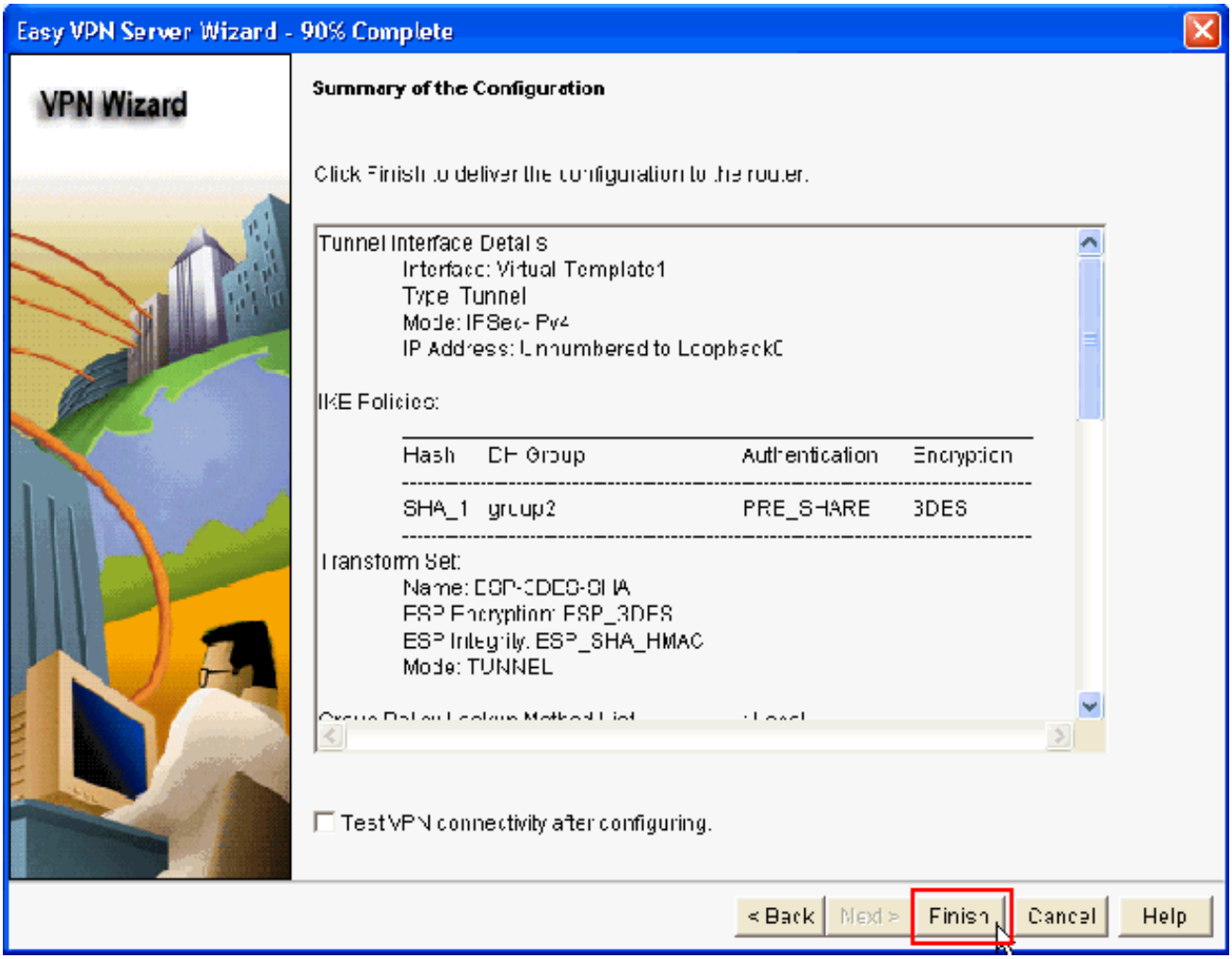
14. أختر الآن **نهج المجموعة** الجديد الذي تم إنشاؤه باسم **Cisco** ثم انقر فوق خانة الاختيار المجاورة ل **تكوين المؤقت الخامل** كما هو مطلوب لتكوين **المؤقت الخامل**. انقر فوق **Next (التالي)**.



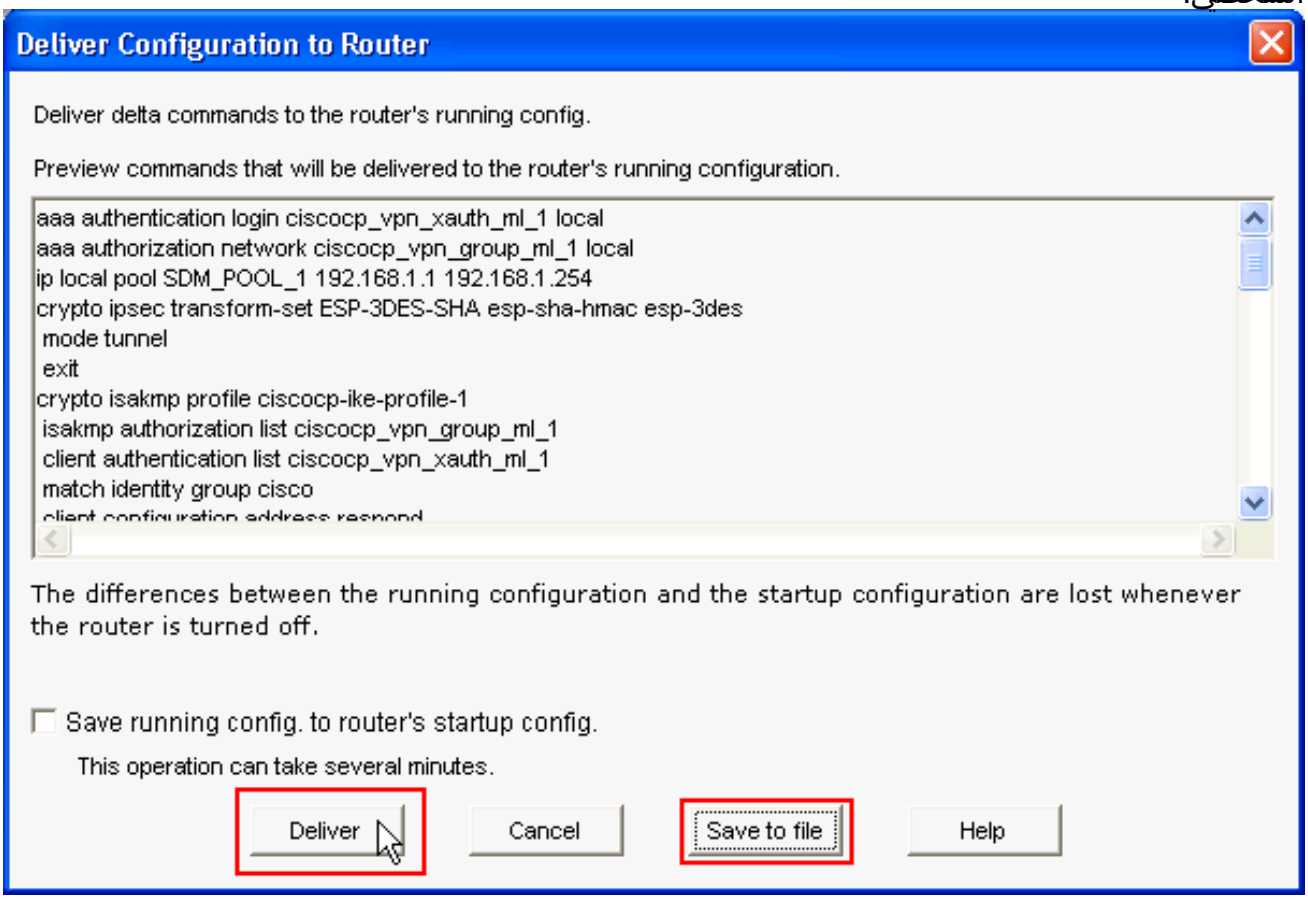
15. مكنت **cisco tunneling تحكم بروتوكول** (cTCP) إن يتطلب. وإلا، انقر **التالي**.



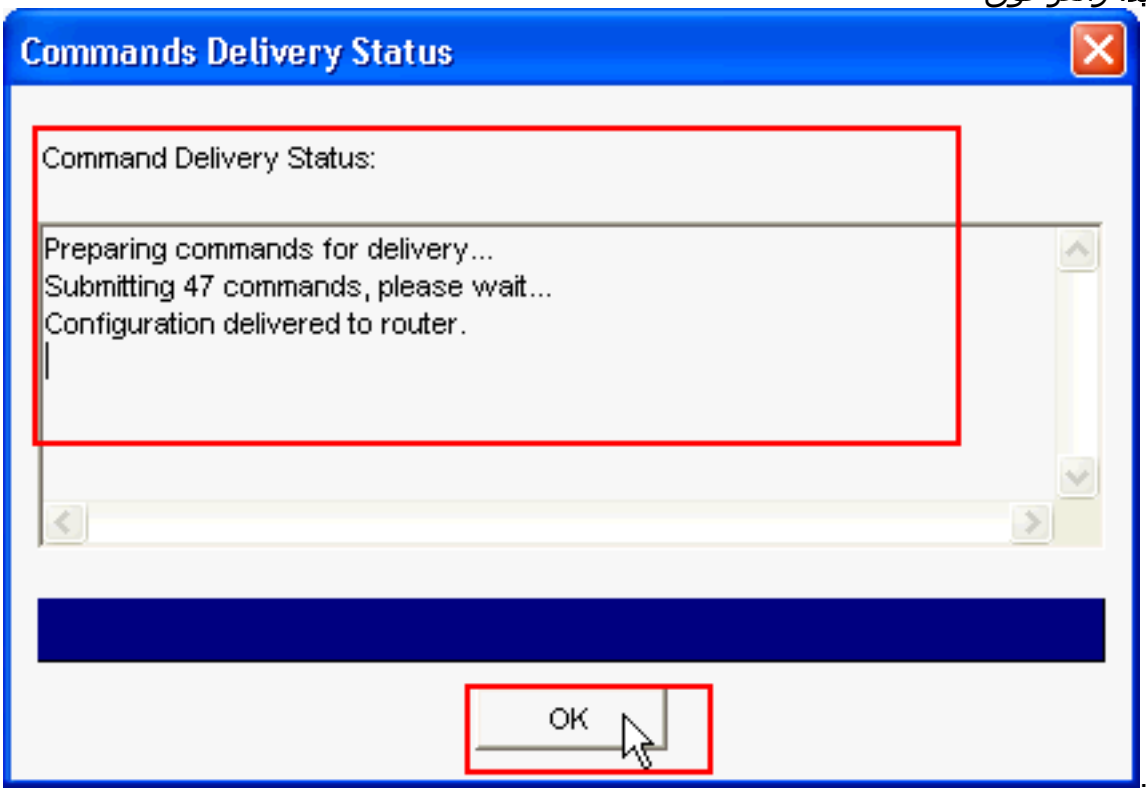
16. راجعت **خلاصة التشكيل**. انقر فوق **إنهاء**.



17. في نافذة **تسليم التكوين إلى الموجه**، انقر فوق **تسليم** لتسليم التكوين إلى الموجه. يمكنك النقر فوق **حفظ إلى ملف** لحفظ التكوين كملف على الكمبيوتر الشخصي.

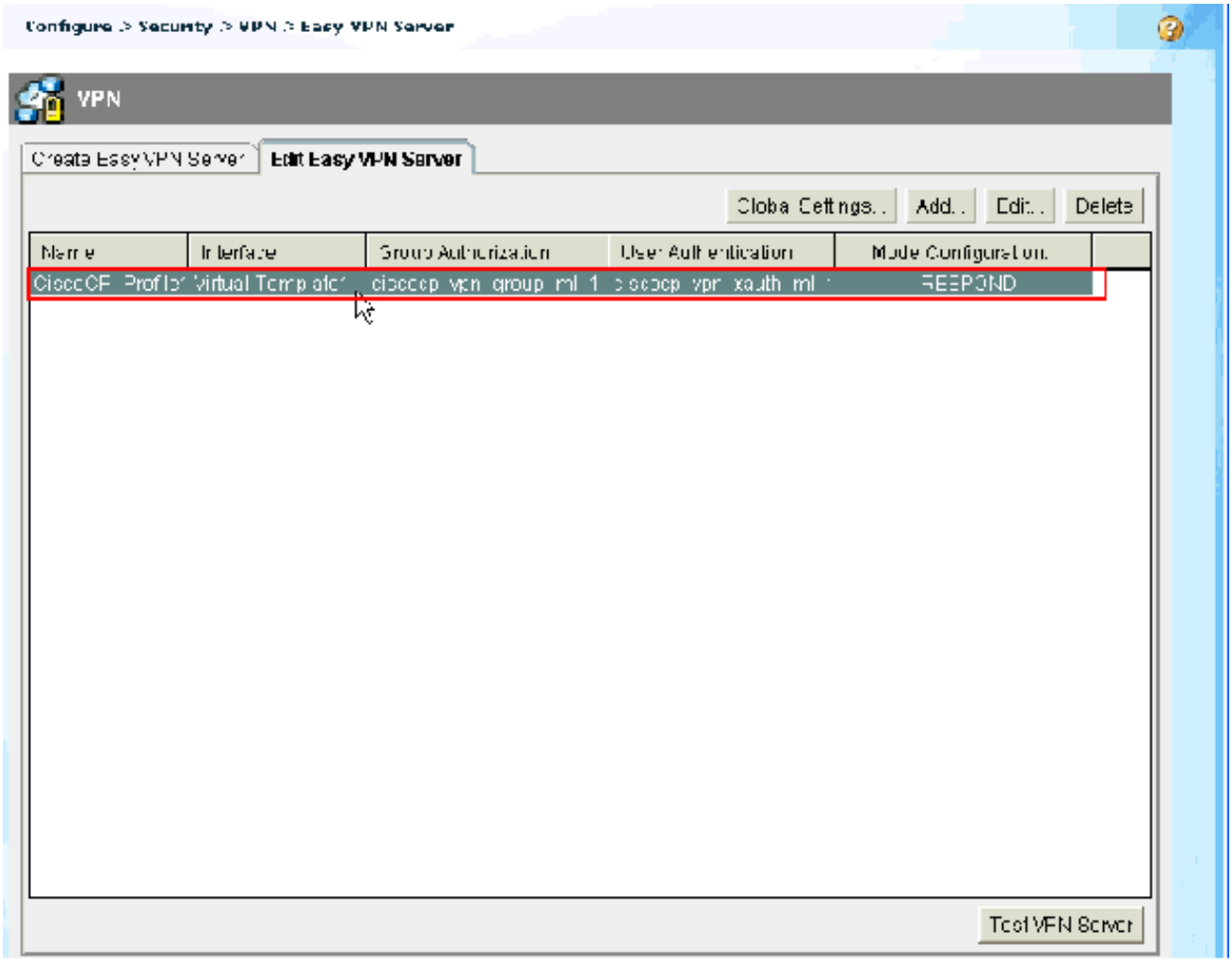


18. يعرض نافذة **حالة تسليم الأوامر** حالة تسليم الأوامر إلى الموجه. يظهر على أنه **تشكيل يسلم إلى مسحاج تخديد**. وانقر فوق



OK.

19. أنت يستطيع رأيت ال newly created easy VPN نادل. يمكنك تحرير الخادم الموجود باختيار **تحرير خادم VPN سهل**. يؤدي هذا إلى اكتمال تكوين خادم VPN السهل على موجه Cisco IOS.



تكوين واجهة سطر الأوامر (CLI)

تكوين الموجّه

```
Router#show run
...Building configuration

Current configuration : 2069 bytes
version 12.4 service timestamps debug datetime msec !
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled---! aaa
new-model
!
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
!
aaa session-id common
ip cef
!
!
!
!
ip domain name cisco.com
!
multilink bundle-name authenticated
!
!
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 1
encr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
key cisco123
pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
match identity group cisco
client authentication list ciscocp_vpn_xauth_ml_1
isakmp authorization list ciscocp_vpn_group_ml_1
client configuration address respond
virtual-template 1
!
!
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-3DES-
SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
set security-association idle-time 86400
```

```
                                    set transform-set ESP-3DES-SHA
                              set isakmp-profile ciscocp-ike-profile-1
                                                                    !
                                                                    !
                                                                    !
RSA certificate generated after you enable the !--- ---!
                                          .ip http secure-server command

                       crypto pki trustpoint TP-self-signed-1742995674
                                                   enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
                                                   revocation-check none
                                 rsakeypair TP-self-signed-1742995674

     Create a user account named cisco123 with all ---!
                                                        .privileges

     username cisco123 privilege 15 password 0 cisco123
                                                          archive
                                                        log config
                                                         hidekeys
                                                                !
                                                                !
Interface configurations are done as shown below--- ---!
            ! interface Loopback0 ip address 10.10.10.10
    255.255.255.0 ! interface FastEthernet0/0 ip address
  10.77.241.111 255.255.255.192 duplex auto speed auto !
   interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
          profile CiscoCP_Profile1 ! !--- VPN pool named
 SDM_POOL_1 has been defined in the below command---! ip
          local pool SDM_POOL_1 192.168.1.1 192.168.1.254

This is where the commands to enable HTTP and HTTPS ---!
   are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
   con 0 line aux 0 !--- Telnet enabled with password as
  cisco. line vty 0 4 password cisco transport input all
                    scheduler allocate 20000 1000 ! ! ! ! end
```

التحقق من الصحة

خادم VPN سهل - إظهار الأوامر

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

```
Router#show crypto isakmp sa

                                                IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
 QM_IDLE           1003    0 ACTIVE     172.16.1.1    10.77.241.111
```

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

```
Router#show crypto ipsec sa
                                    interface: Virtual-Access2
        Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

                                                   (protected vrf: (none
      (local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
```

```
(remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0
                                    current_peer 172.16.1.1 port 1086
                                     {,PERMIT, flags={origin_is_acl
                  pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28#
                  pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36#
                            pkts compressed: 0, #pkts decompressed: 0#
                          pkts not compressed: 0, #pkts compr. failed: 0#
                       pkts not decompressed: 0, #pkts decompress failed: 0#
                                        send errors 0, #recv errors 2#

          local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
                        path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
                                  (current outbound spi: 0x186C05EF(409732591

                                                       :inbound esp sas
                                              (spi: 0x42FC8173(1123844467
                                         transform: esp-3des esp-sha-hmac
```

استكشاف الأخطاء وإصلاحها

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

ملاحظة: أحلت معلومة مهم على Debug أمر قبل أن يضبط أنت إصدار أمر.

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- Cisco Configuration Professional Start Guide
- صفحة دعم منتجات Cisco - موجّهات
- 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).