SDM: شبكة VPN من موقع إلى موقع بين موجه IOS ومثال تكوين ASA/PIX

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل ل ال LAN إلى LAN (موقع إلى موقع) IPsec نفق بين cisco أمن أجهزة (ASA/PIX) و cisco ios مسحاج تخديد. يتم استخدام المسارات الثابتة للتبسيط.

ارجع إلى جهاز الأمان PIX/ASA 7.x إلى مثال تكوين نفق IPsec لموجه IOS إلى شبكة LAN من أجل معرفة المزيد حول نفس السيناريو حيث يقوم جهاز أمان PIX/ASA بتشغيل الإصدار *7.x* Software.

المتطلبات الأساسية

المتطلبات

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

- يجب إنشاء اتصال IP الشامل قبل بدء هذا التكوين.
- يجب تمكين ترخيص جهاز الأمان لتشفير معيار تشفير البيانات (DES) (على أدنى مستوى تشفير).

المكونات المستخدمة

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

- أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA) مع الإصدار x.8 والإصدارات الأحدث
- ASDM الإصدار x.6.والإصدارات الأحدث
- cisco 1812 مسحاج تخديد مع cisco ios ® برمجية إطلاق 12.3
- Cisco Security Device Manager (SDM)، الإصدار 2.5

ملاحظة: ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.

ملاحظة: ارجع إلى تكوين الموجه الأساسي باستخدام SDM للسماح بتكوين الموجه بواسطة SDM.

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.

ملاحظة: ارجع إلى محترف التكوين: الشبكة الخاصة الظاهرية (VPN) لبروتوكول IPsec من موقع إلى موقع بين ASA/PIX ومثال تكوين موجه IOS لتكوين مماثل باستخدام محترف تكوين Cisco على الموجه.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX 500 Series Security Appliance، والذي يشغل الإصدار x.7 والإصدارات الأحدث.

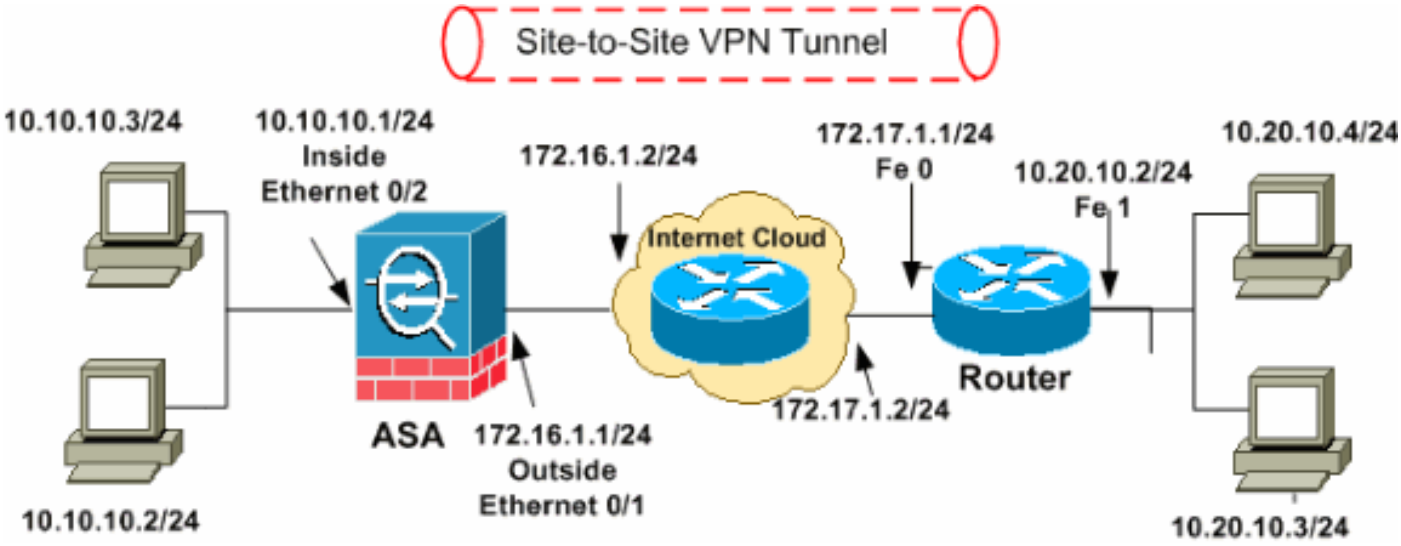
الاصطلاحات

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

التكوين

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



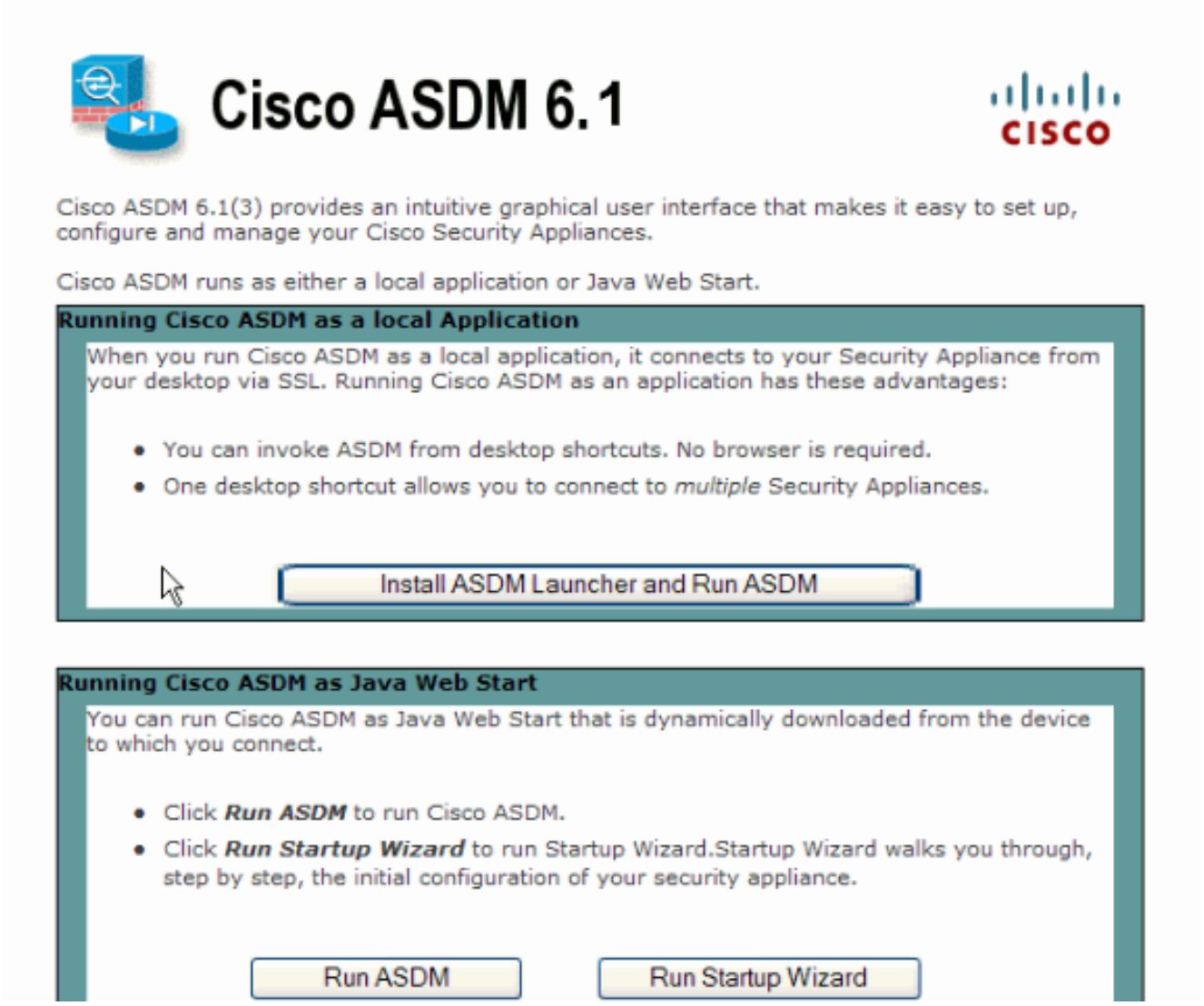
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

- تكوين ASDM لنفق VPN
- تكوين SDM للموجه
- تكوين ASA CLI
- تكوين CLI للموجه

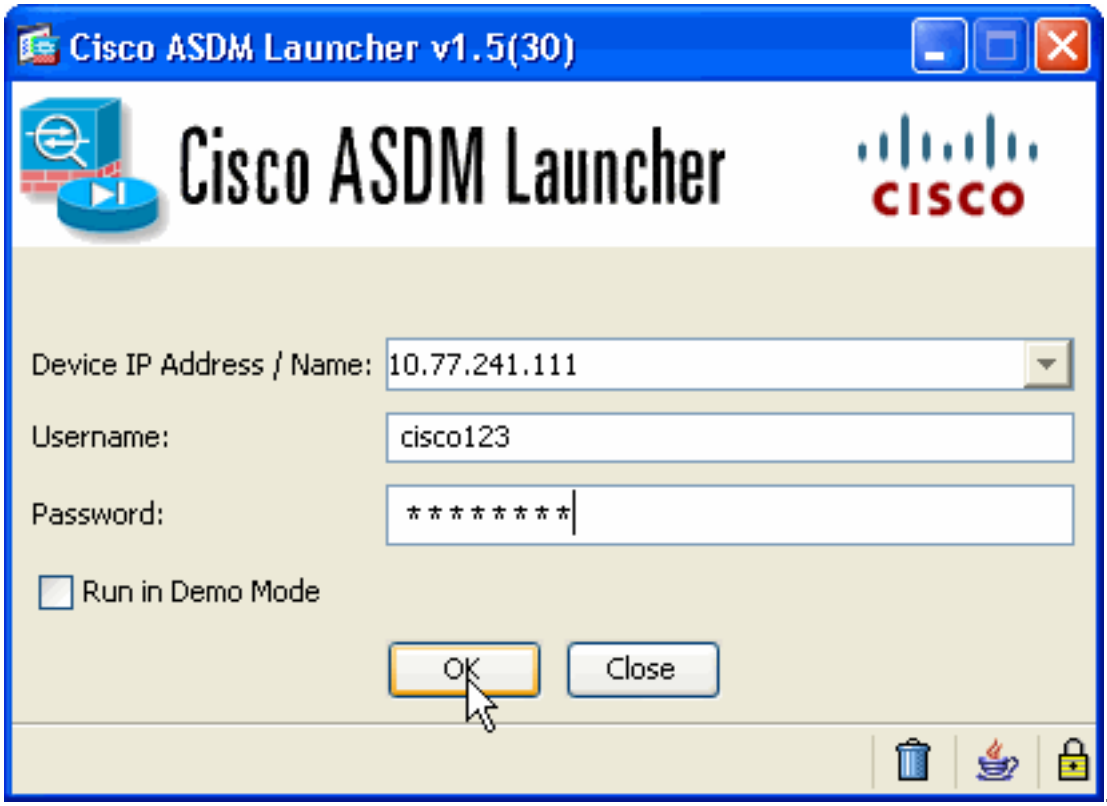
تكوين ASDM لنفق VPN

أتمت هذا steps in order to خلقت ال VPN نفق:

1. افتح المستعرض الخاص بك وأدخل **https://<IP_Address الخاص بواجهة ASA التي تم تكوينها للوصول إلى ASDM** Access>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.

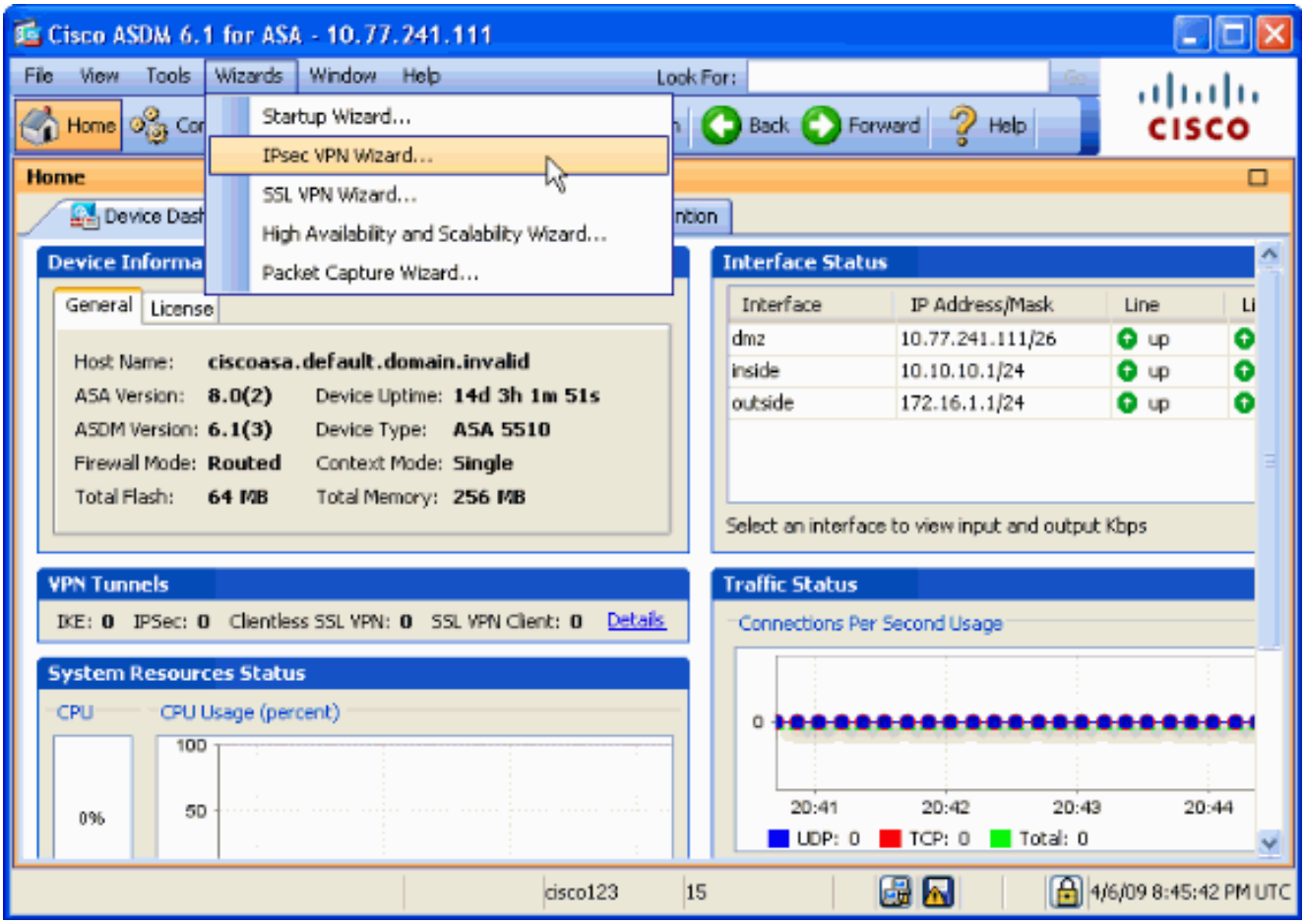


2. انقر على **تنزيل مشغل ASDM وابدأ ASDM** لتنزيل المثبت الخاص بتطبيق ASDM.
3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.
4. دخلت العنوان للقارن أنت تشكل مع **ال http** - أمر، واسم مستخدم وكلمة إن يعين أنت واحد.يستعمل هذا مثال **Cisco123**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

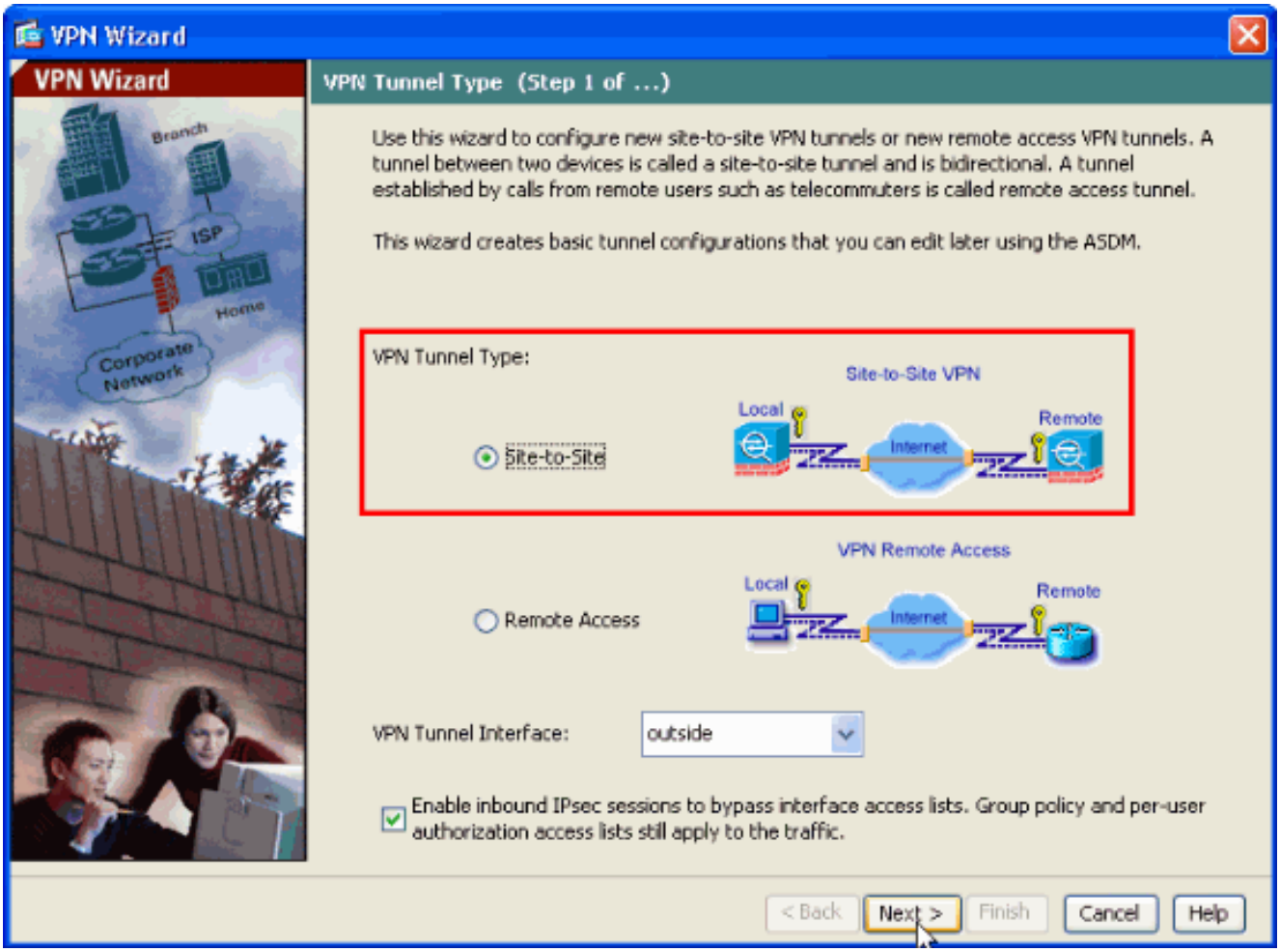


كالكلمة.

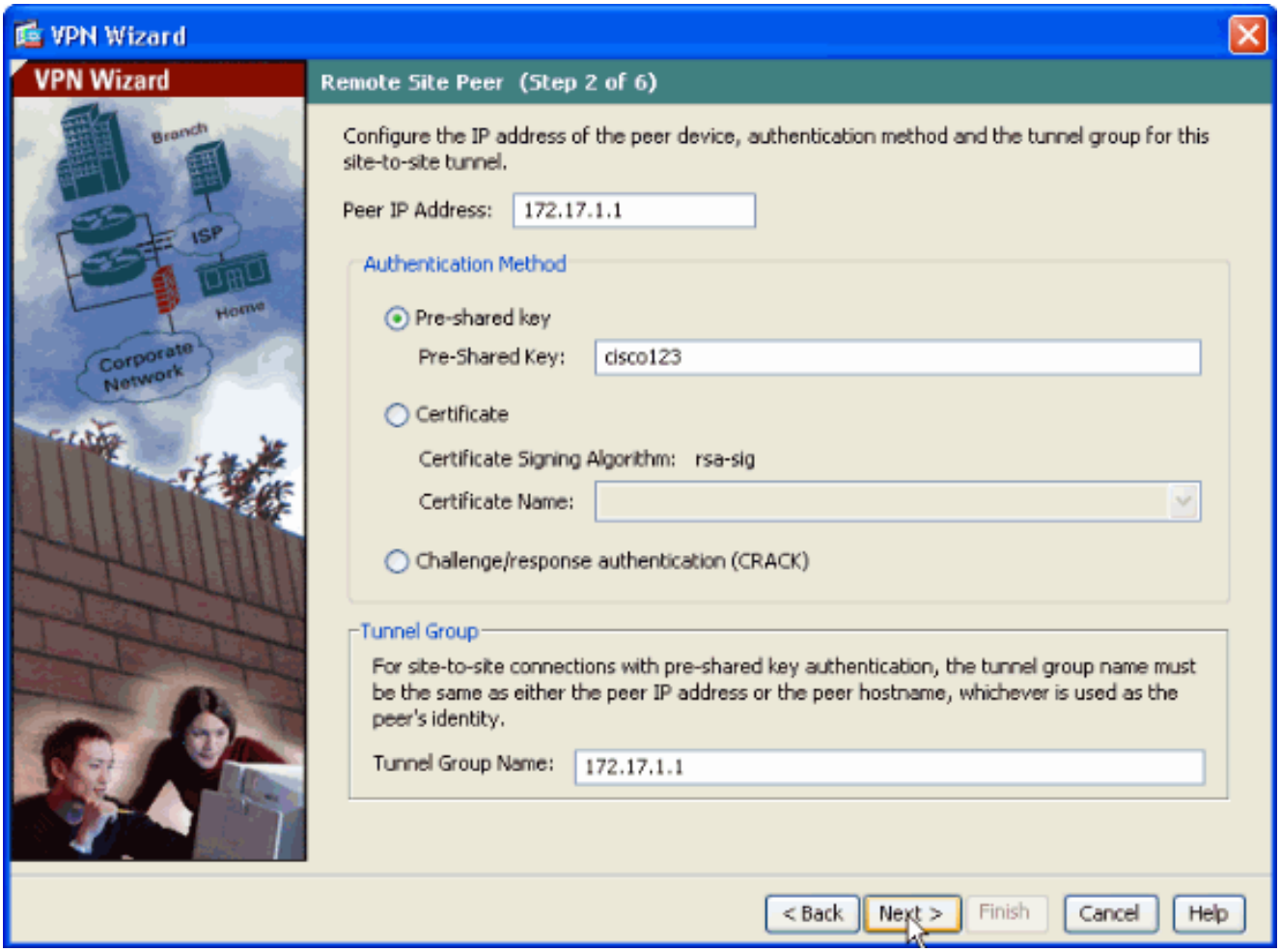
5. قم بتشغيل **معالج IPsec VPN** بمجرد اتصال تطبيق ASDM ب ASA.



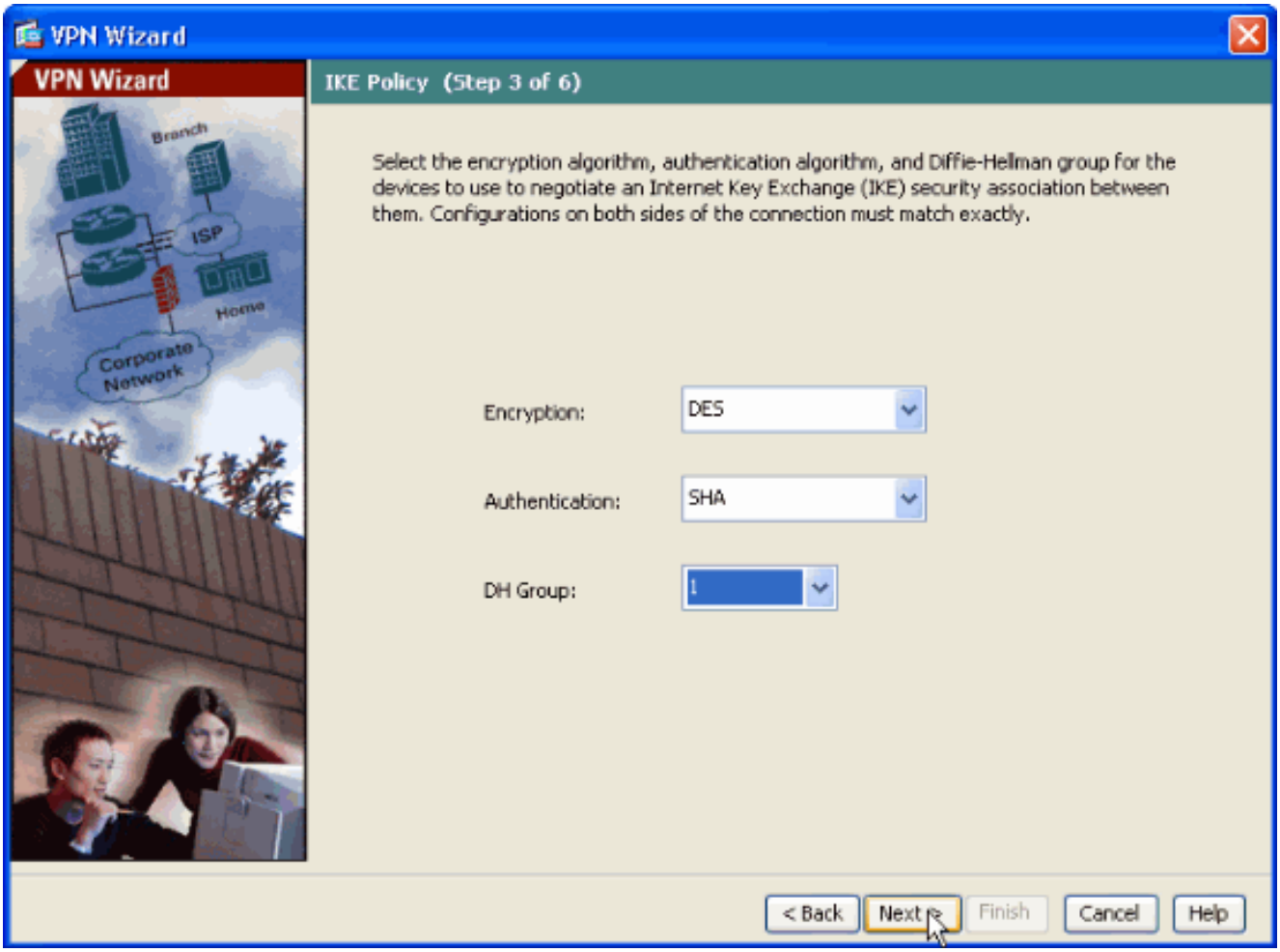
6. أخترت **الموقع إلى موقع** IPsec VPN نفق نوع وطقطقة **بعد ذلك** كما هو موضح هنا.



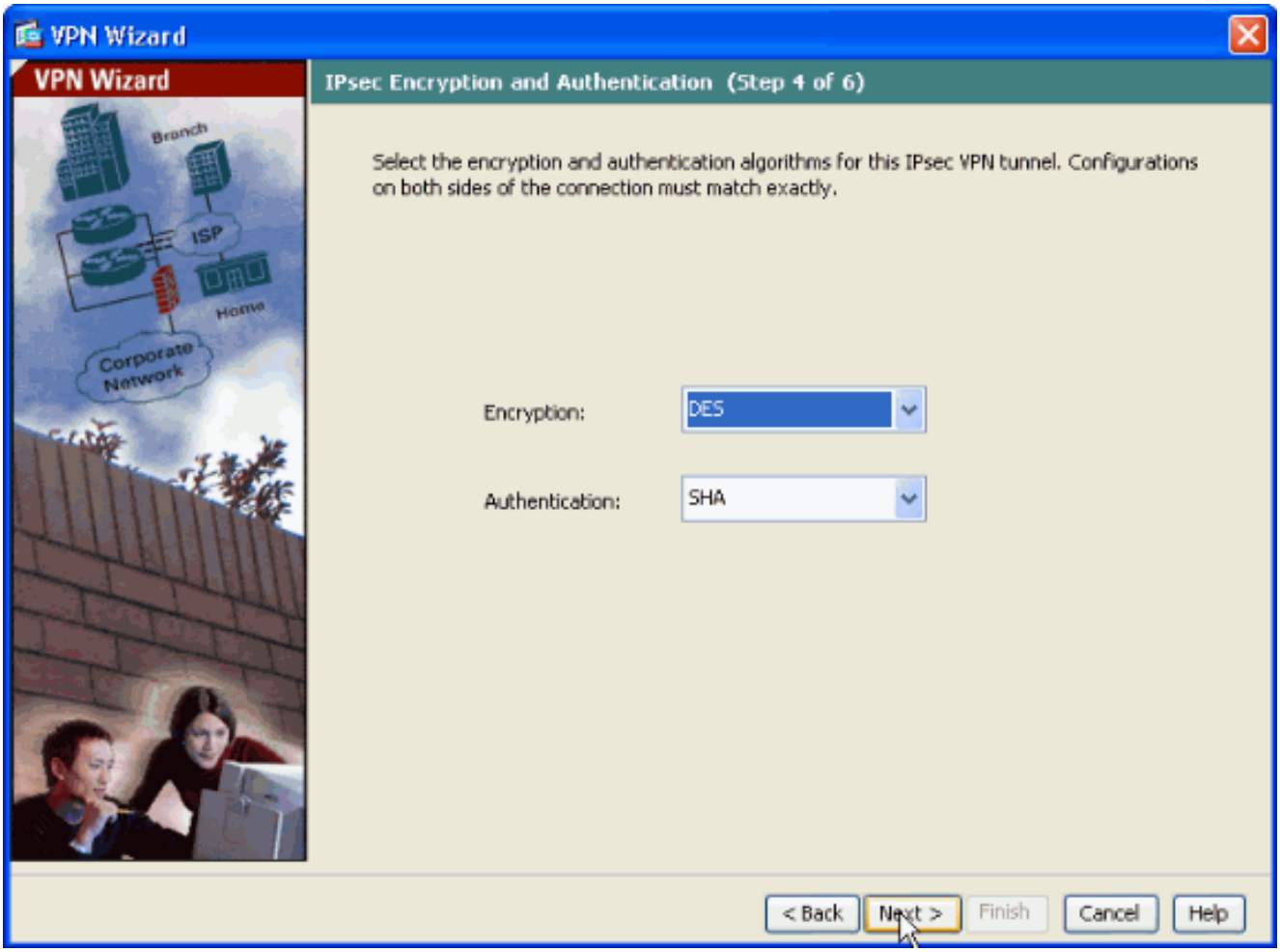
7. حدد عنوان IP الخارجي للنظير البعيد. أدخل معلومات المصادقة المراد إستخدامها، وهو المفتاح المشترك مسبقا في هذا المثال. المفتاح المشترك مسبقا المستخدم في هذا المثال هو **Cisco123**. **النفق مجموعة إسم** يكون ك خارجي عنوان افتراضيا إن يشكل أنت I2L VPN. انقر فوق **Next (التالي)**.



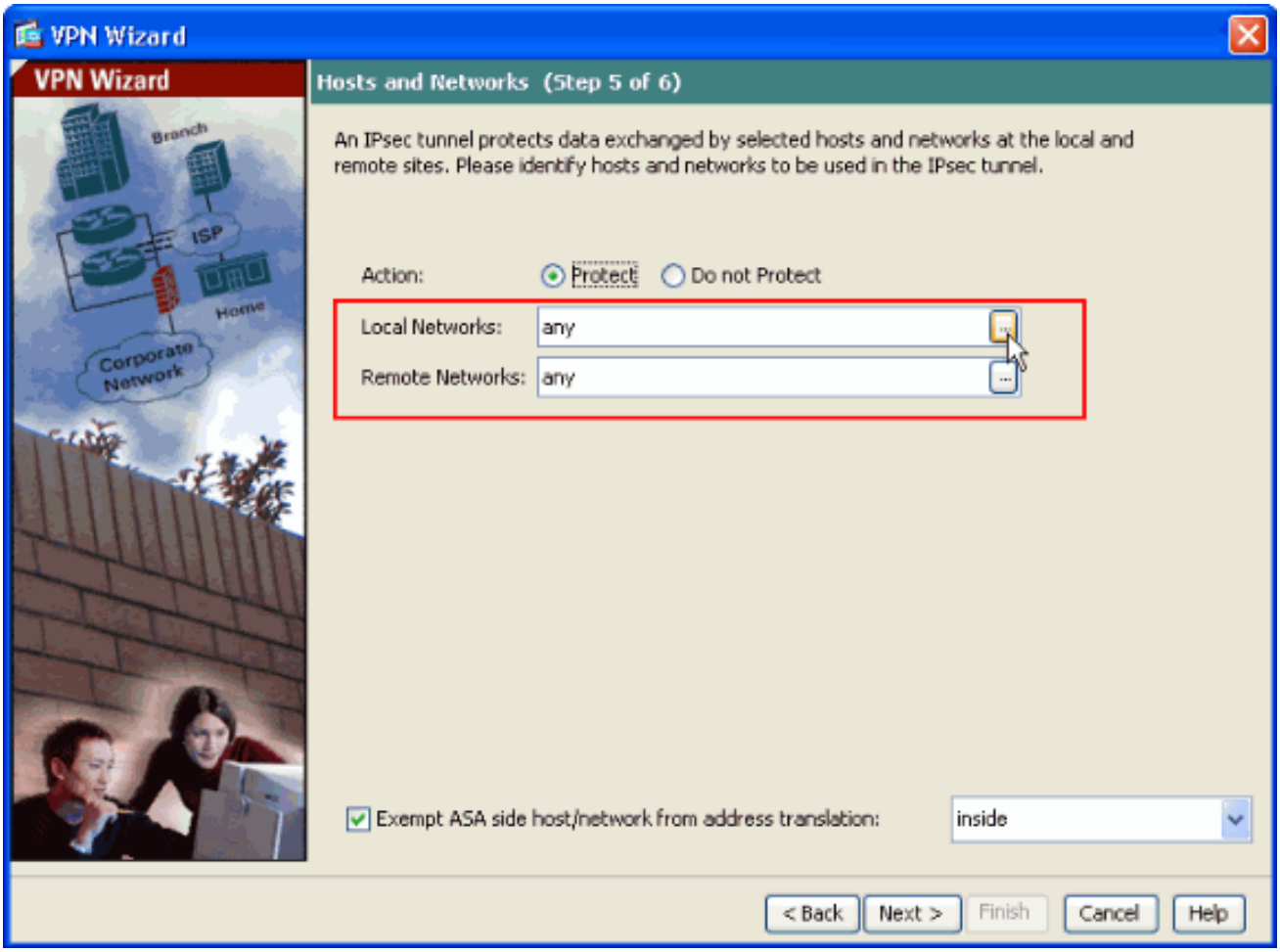
8. حدد السمات التي سيتم إستخدامها ل IKE، والمعروفة أيضا بالطور 1. يجب أن تكون هذه السمات هي نفسها على كل من ASA وموجه IOS. انقر فوق **Next (التالي)**.



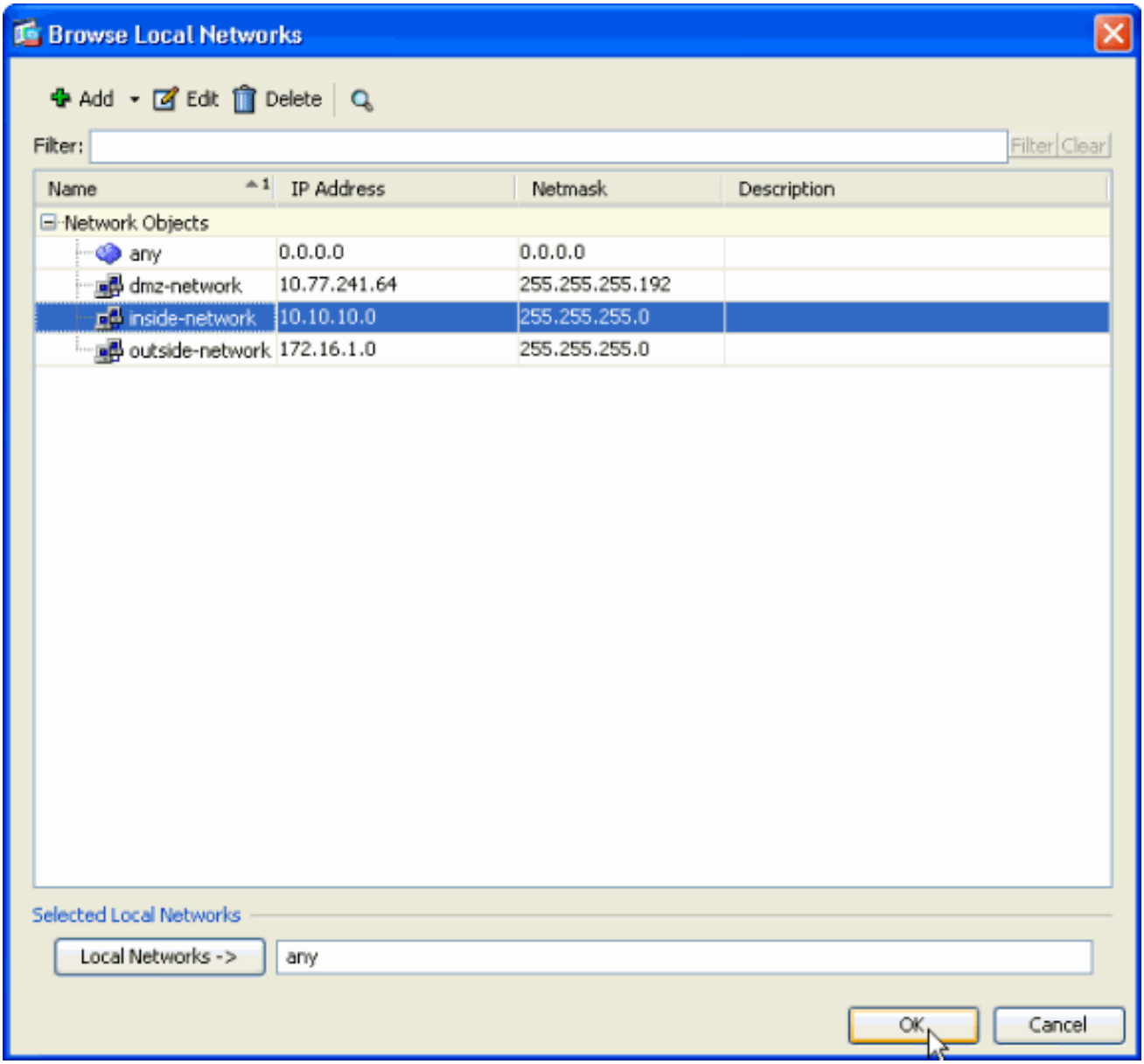
9. حدد السمات التي سيتم إستخدامها ل IPsec، المعروفة أيضا بالطور 2. يجب أن تتطابق هذه السمات على كل من ASA وموجه IOS. انقر فوق **Next (التالي)**.



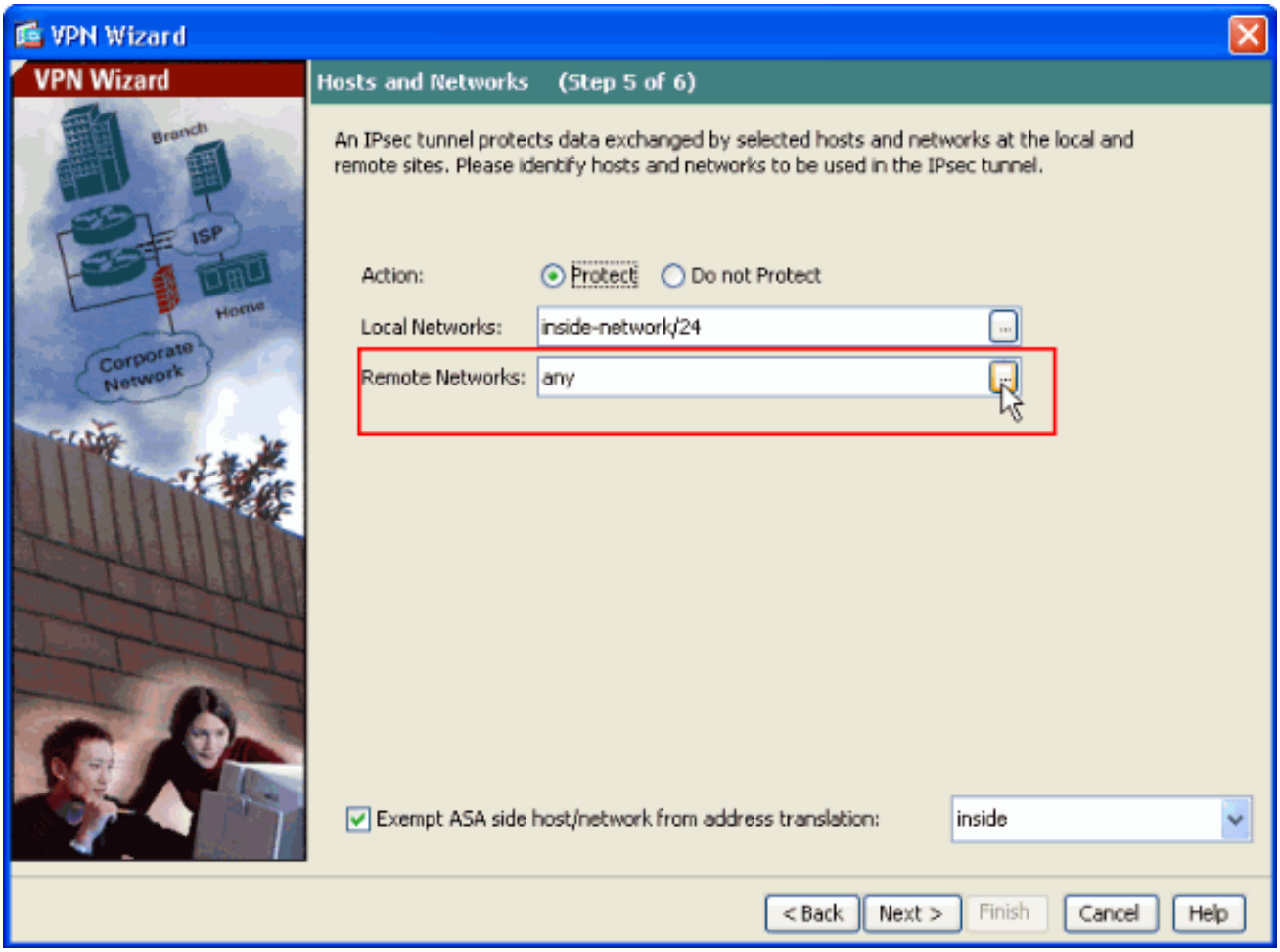
10. حدد البيئات المضيفة التي يجب السماح لحركة مرور البيانات الخاصة بها بالمرور من خلال نفق VPN. في هذه الخطوة، يجب عليك توفير **الشبكات المحلية** والبعيدة لنفق الشبكة الخاصة الظاهرية (VPN). انقر فوق الزر الموجود بجوار **الشبكات المحلية** كما هو موضح هنا لاختيار عنوان الشبكة المحلية من القائمة المنسدلة.



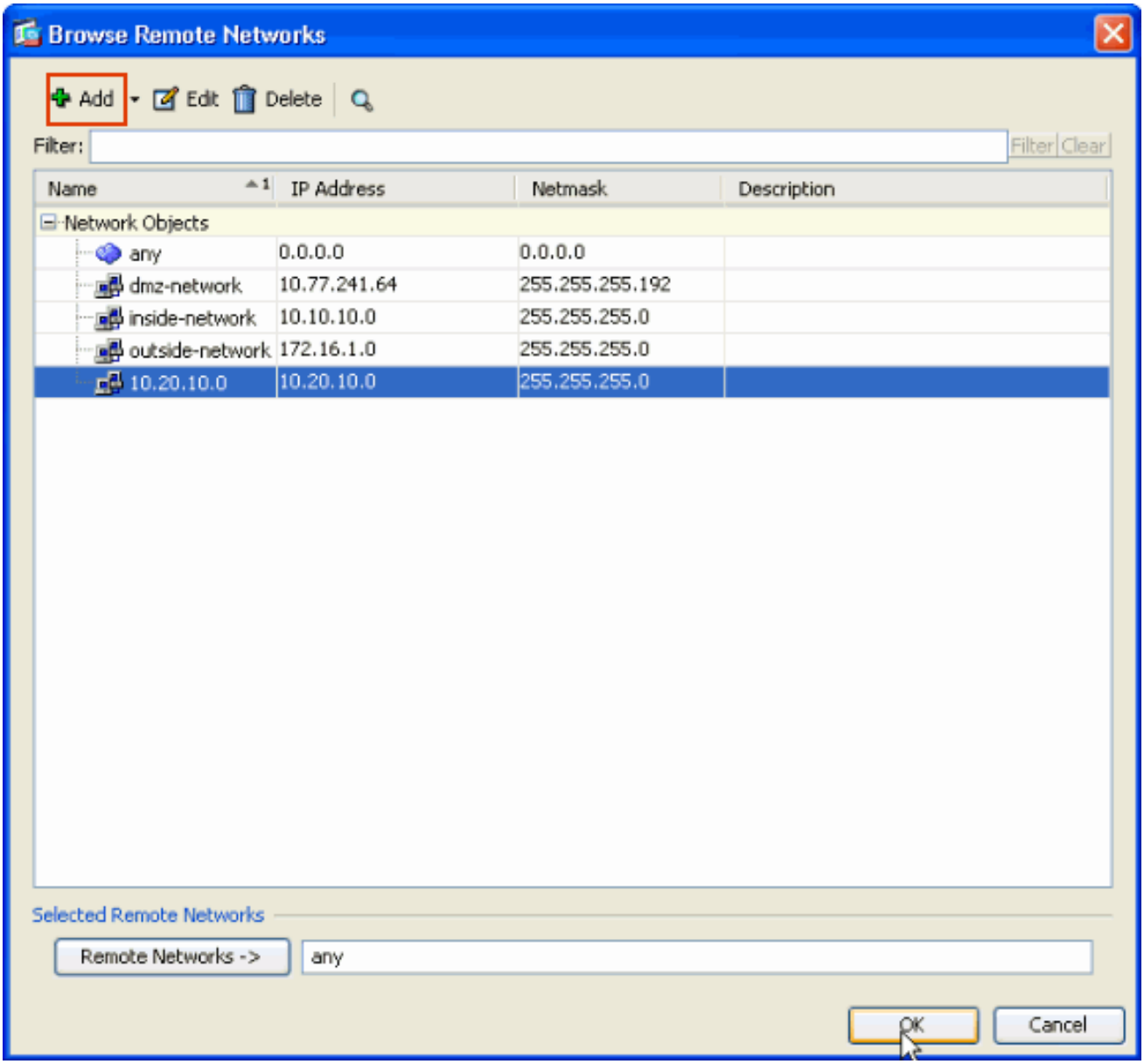
11. أختر عنوان **الشبكة المحلية**، ثم انقر على **موافق** كما هو موضح هنا.



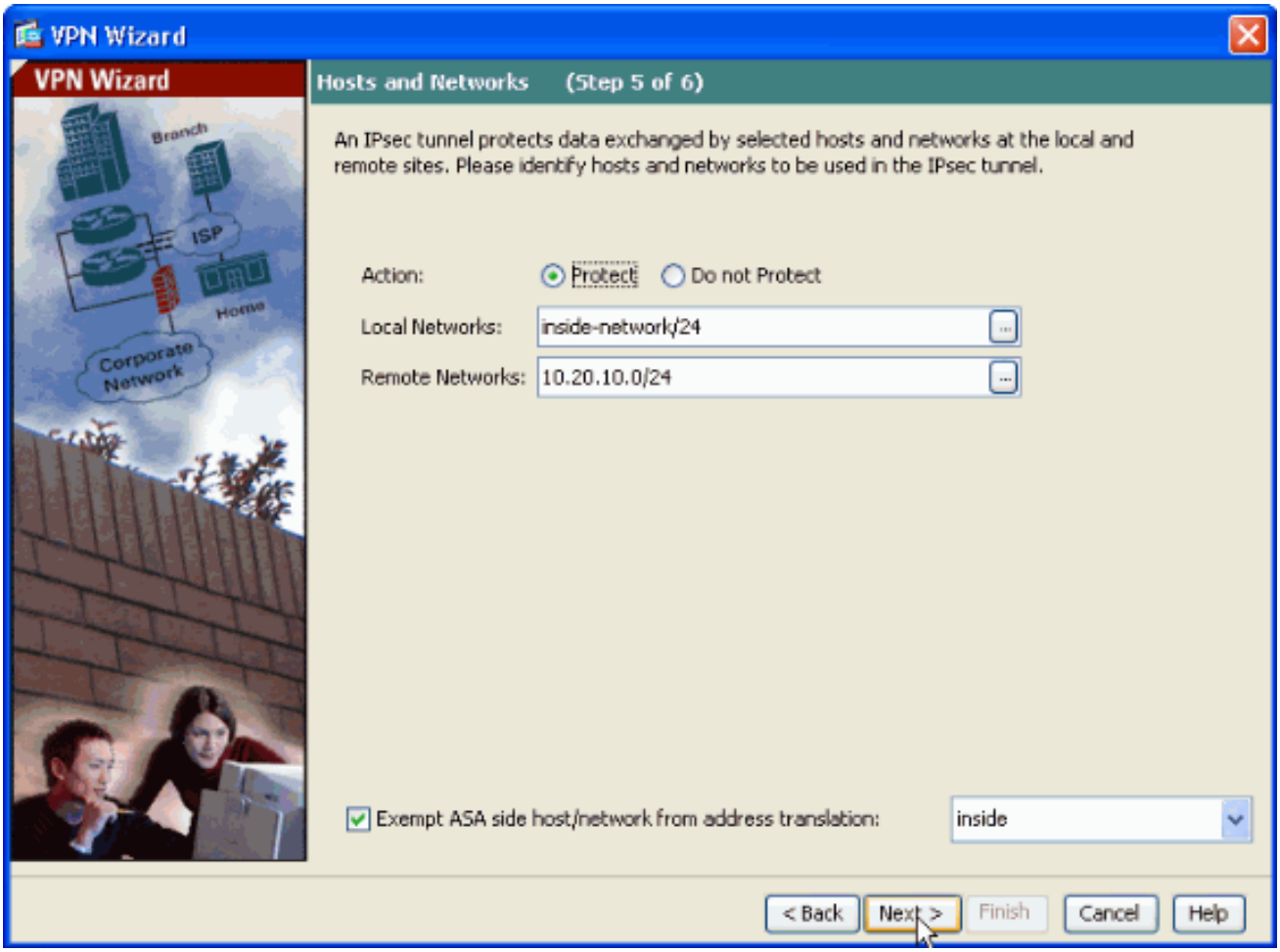
12. انقر فوق الزر الموجود بجوار **الشبكات البعيدة** كما هو موضح هنا لاختيار عنوان الشبكة البعيدة من القائمة المنسدلة.



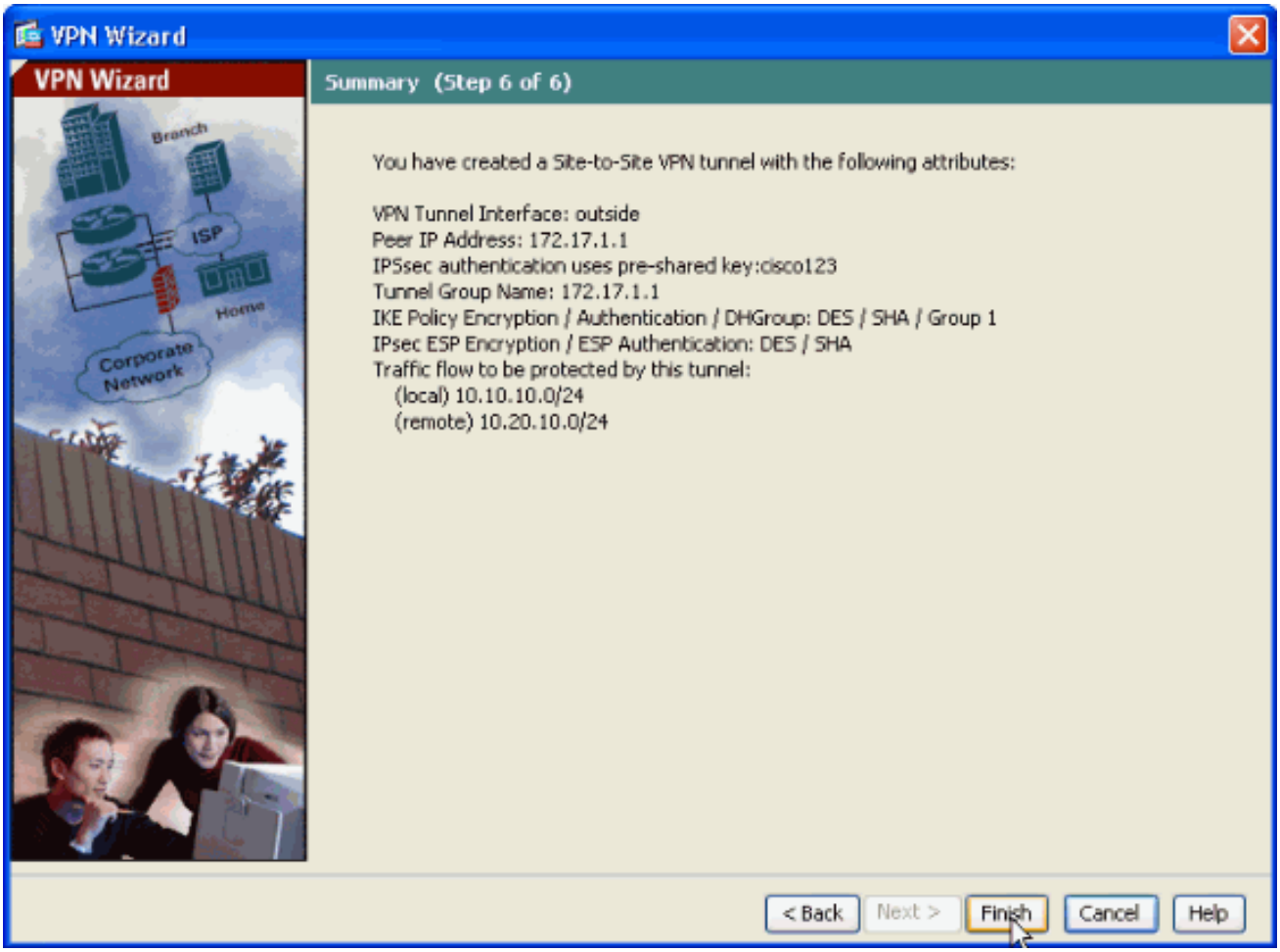
13. أختر عنوان **الشبكة البعيدة**، ثم انقر على **موافق** كما هو موضح هنا.**ملاحظة:** إذا لم يكن لديك الشبكة البعيدة في القائمة، فيجب إضافة الشبكة إلى القائمة عن طريق النقر فوق **إضافة**.



14. حدد خانة الاختيار **Exception ASA Side Host/Network من ترجمة العنوان** لمنع حركة مرور النفق من الخضوع **لترجمة عنوان الشبكة**. ثم انقر فوق **التالي**.



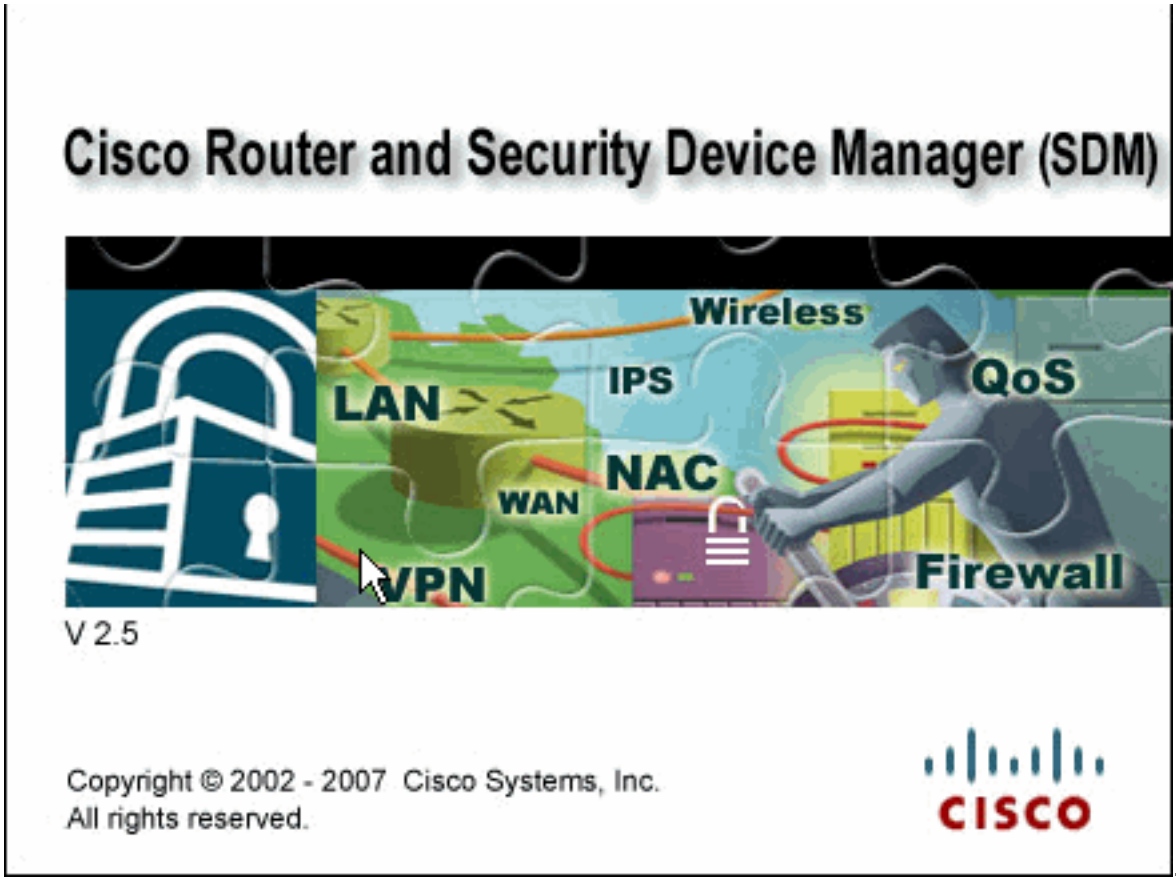
15. يتم عرض السمات التي تم تعريفها بواسطة معالج الشبكة الخاصة الظاهرية (VPN) في هذا الملخص. تحقق مرة أخرى من التكوين وانقر فوق **إنهاء** عندما ترضى بأن الإعدادات صحيحة.



تكوين SDM للموجه

أكمل هذه الخطوات لتكوين نفق VPN من موقع إلى موقع على موجه Cisco IOS:

1. افتح المستعرض وأدخل **https://<IP_Address الخاص بواجهة الموجه الذي تم تكوينه للوصول إلى إدارة قاعدة بيانات المحول (SDM)>** للوصول إلى إدارة قاعدة بيانات المحول (SDM) على الموجه.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها صلة بأصالة شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يعرض الموجه هذه النافذة للسماح بتنزيل تطبيق إدارة قاعدة بيانات المحول (SDM). يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق



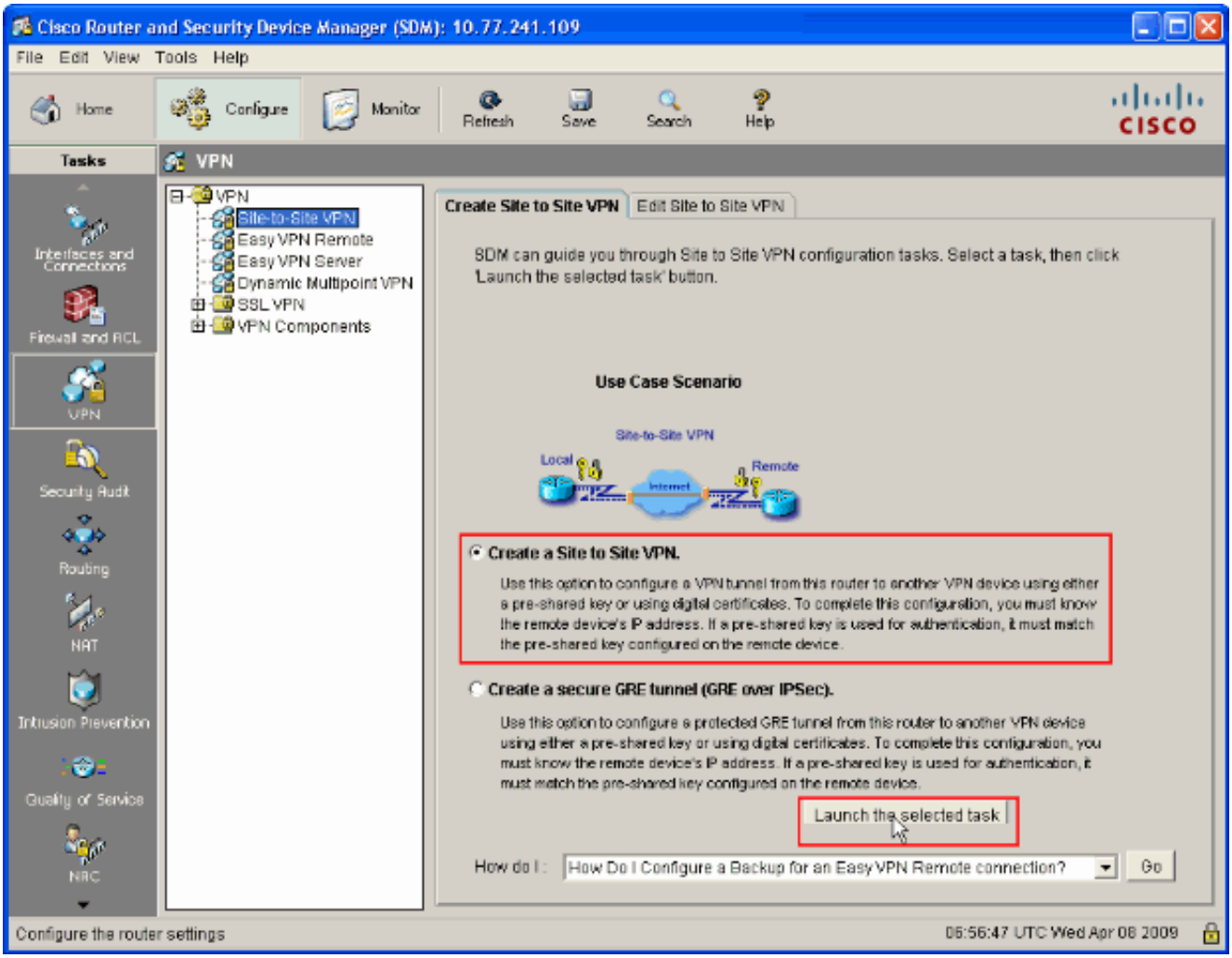
Java.

2. يبدأ تنزيل إدارة قاعدة بيانات المحول (SDM) الآن. بمجرد تنزيل مشغل إدارة قاعدة بيانات المحول (SDM)، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل إدارة قاعدة بيانات المحول (SDM) من Cisco.
3. دخلت **ال username** و **كلمة** إن يعين أنت واحد وطقطقة **ok**.يستخدم هذا المثال **Cisco123** لاسم المستخدم

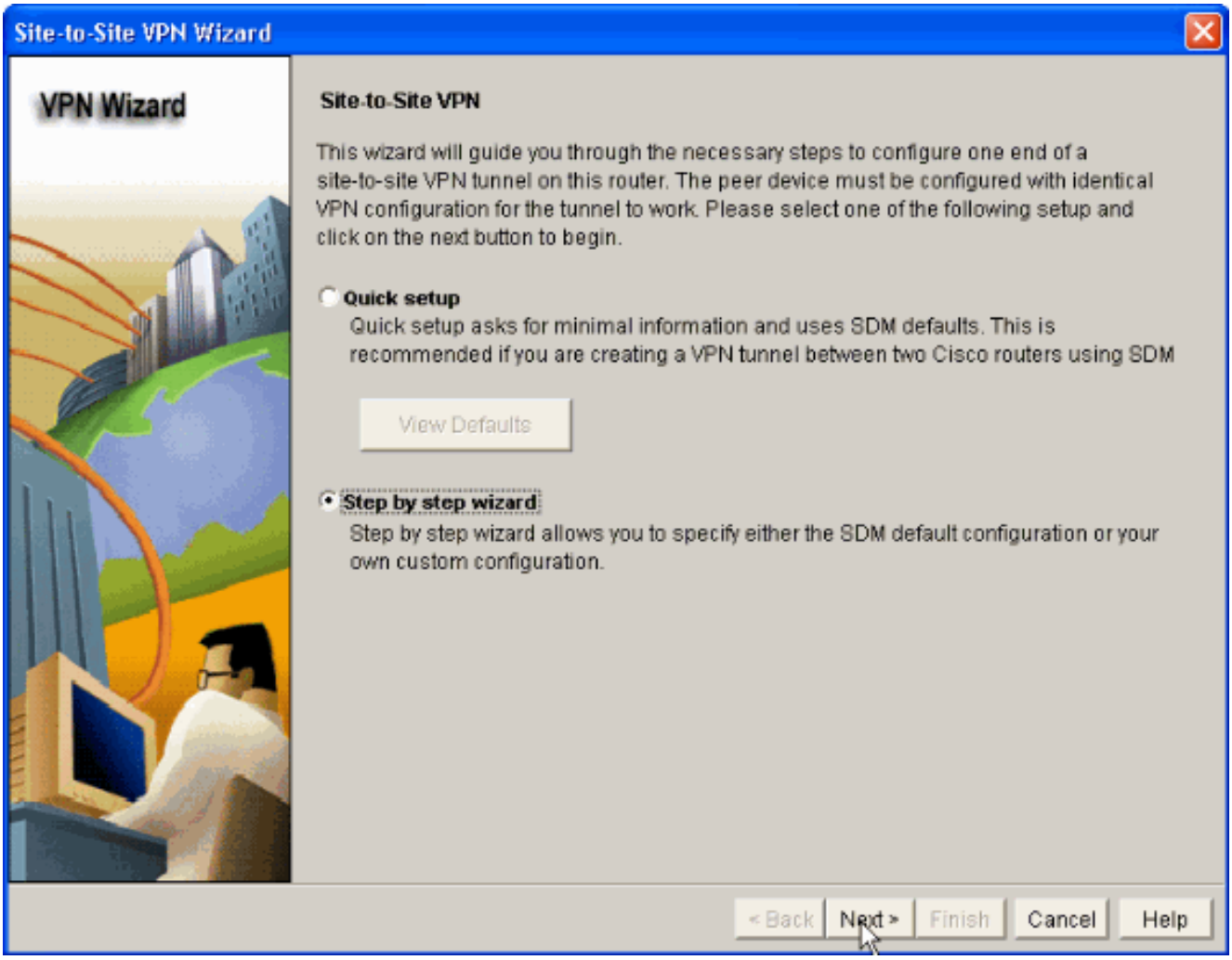
و**Cisco123** ككلمة المرور.

4. أخترت **تشكيل->VPN<موقع إلى موقع VPN** وطقطقت زر لاسلكي next to **خلقت VPN من موقع إلى موقع** على ال SDM صفحة الرئيسية. ثم انقر فوق **تشغيل المهمة المحددة** كما هو موضح

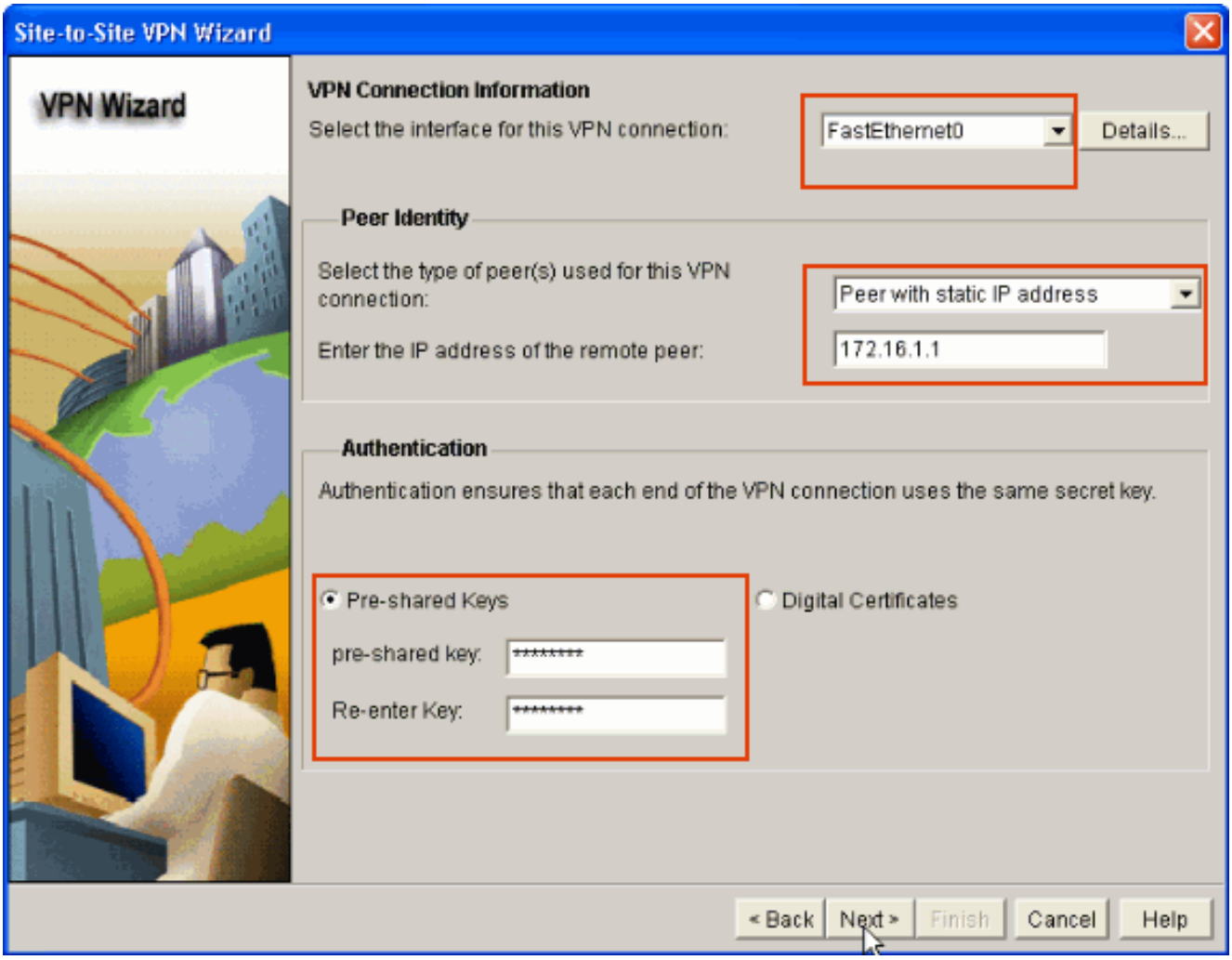
هنا:



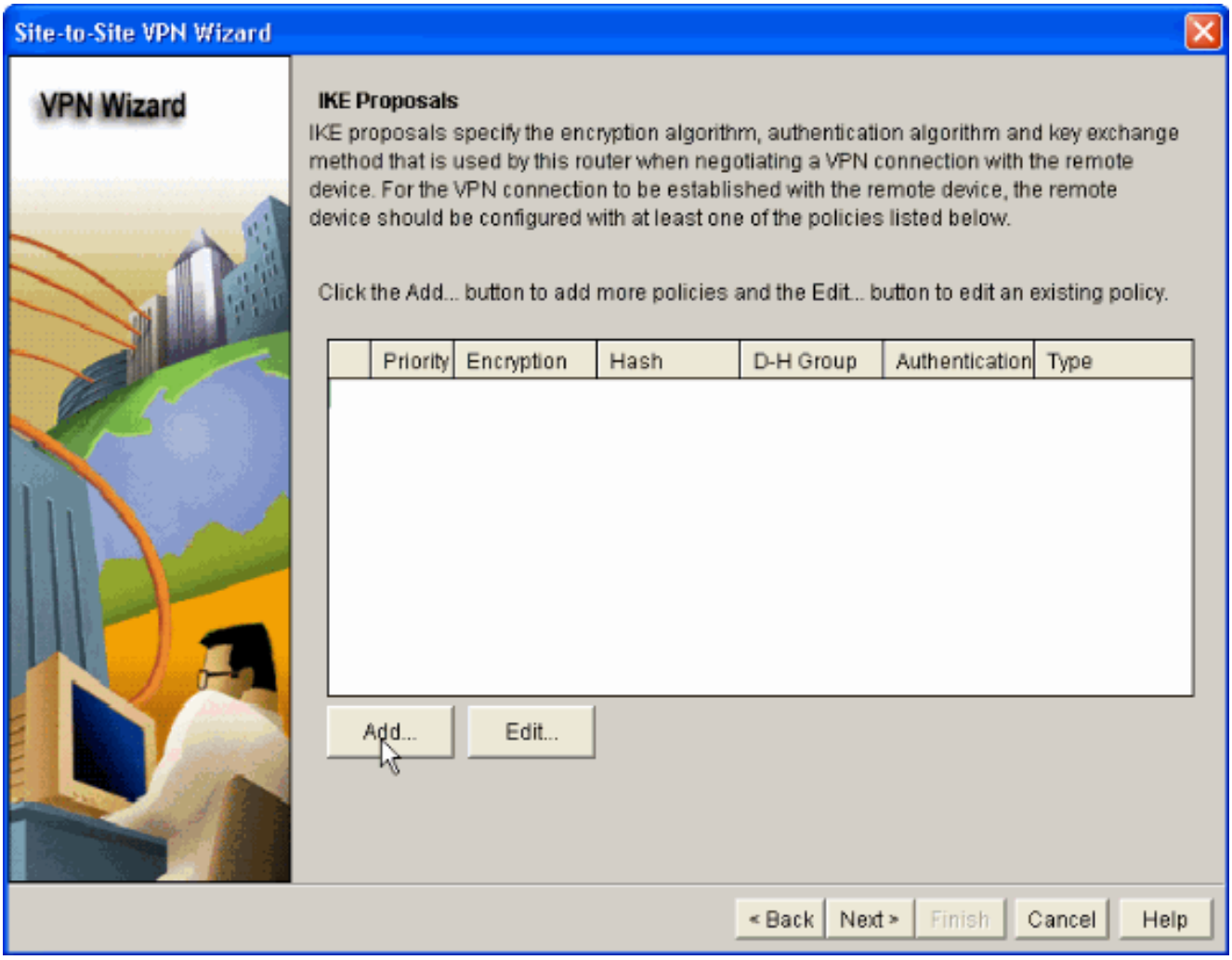
5. أختر **معالج خطوة بخطوة** لمتابعة التكوين:



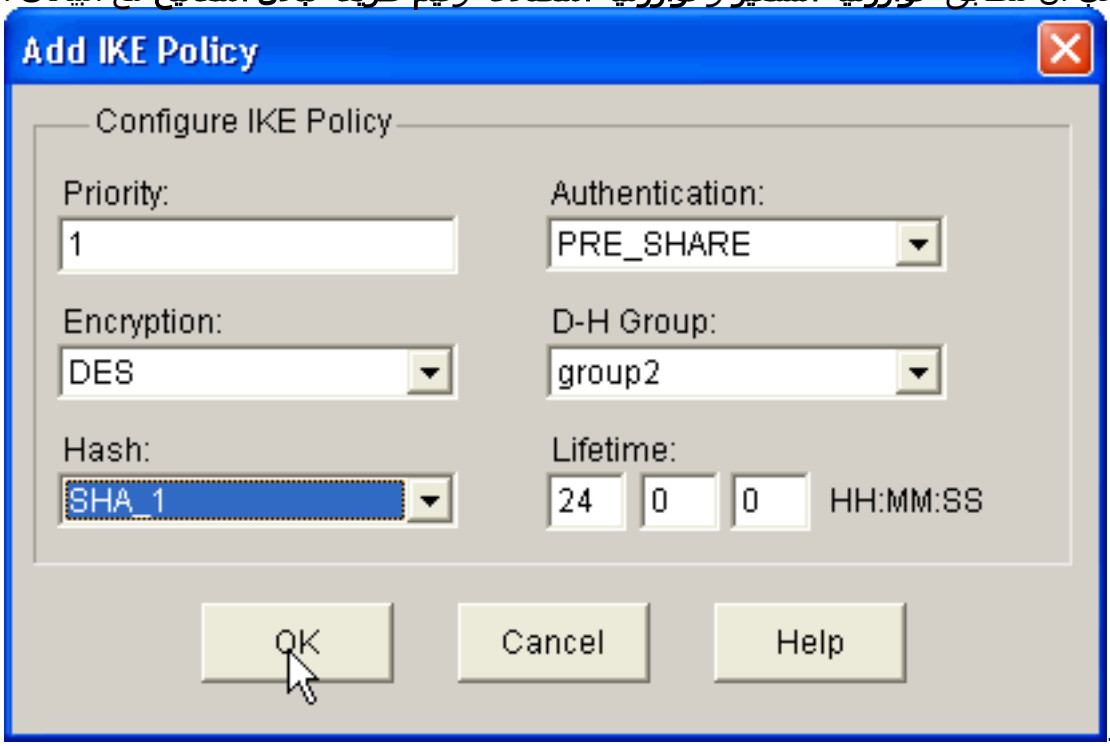
6. في الإطار التالي، توفر **معلومات اتصال VPN** في المساحات المقابلة. حدد واجهة نفق VPN من القائمة المنسدلة. هنا، يتم إختيار FastEthernet0. أخترت في **ال نظير هوية** قسم، **نظير مع ساكن إستاتيكي عنوان** ووفرت النظير بعيد عنوان. بعد ذلك، قم بتوفير **المفتاح المشترك مسبقا** (Cisco123 في هذا المثال) في قسم المصادقة كما هو موضح . ثم انقر فوق **التالي**.



7. انقر فوق **إضافة** لإضافة اقتراحات IKE التي تحدد **خوارزمية التشفير وخوارزمية المصادقة** و**أسلوب تبادل المفاتيح**.

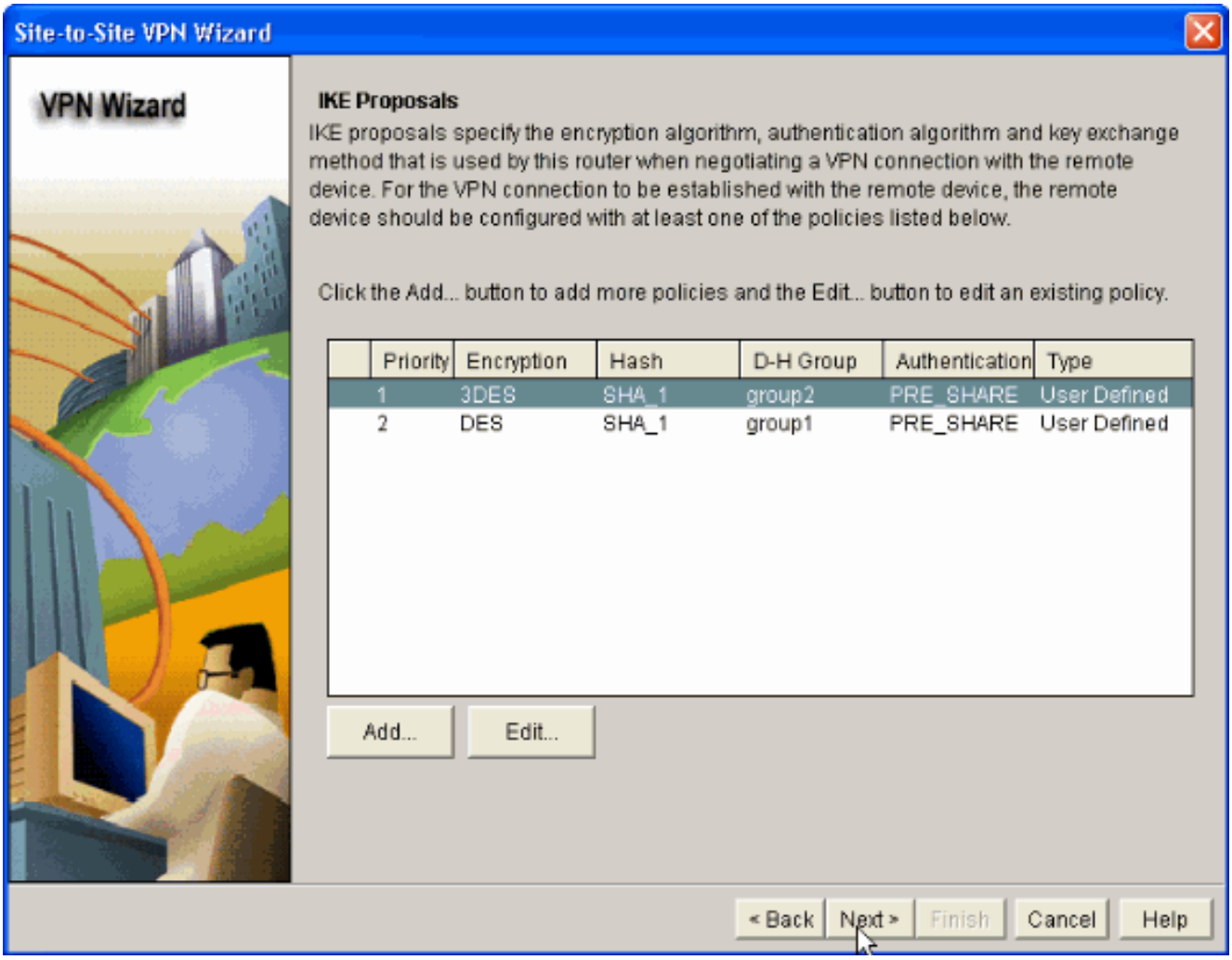


8. قم بتوفير **خوارزمية التشفير** و**خوارزمية المصادقة** و**طريقة تبادل المفاتيح** كما هو موضح هنا، ثم انقر فوق **موافق**. يجب أن تتطابق **خوارزمية التشفير** و**خوارزمية المصادقة** و**قيم طريقة تبادل المفاتيح** مع البيانات المقدمة

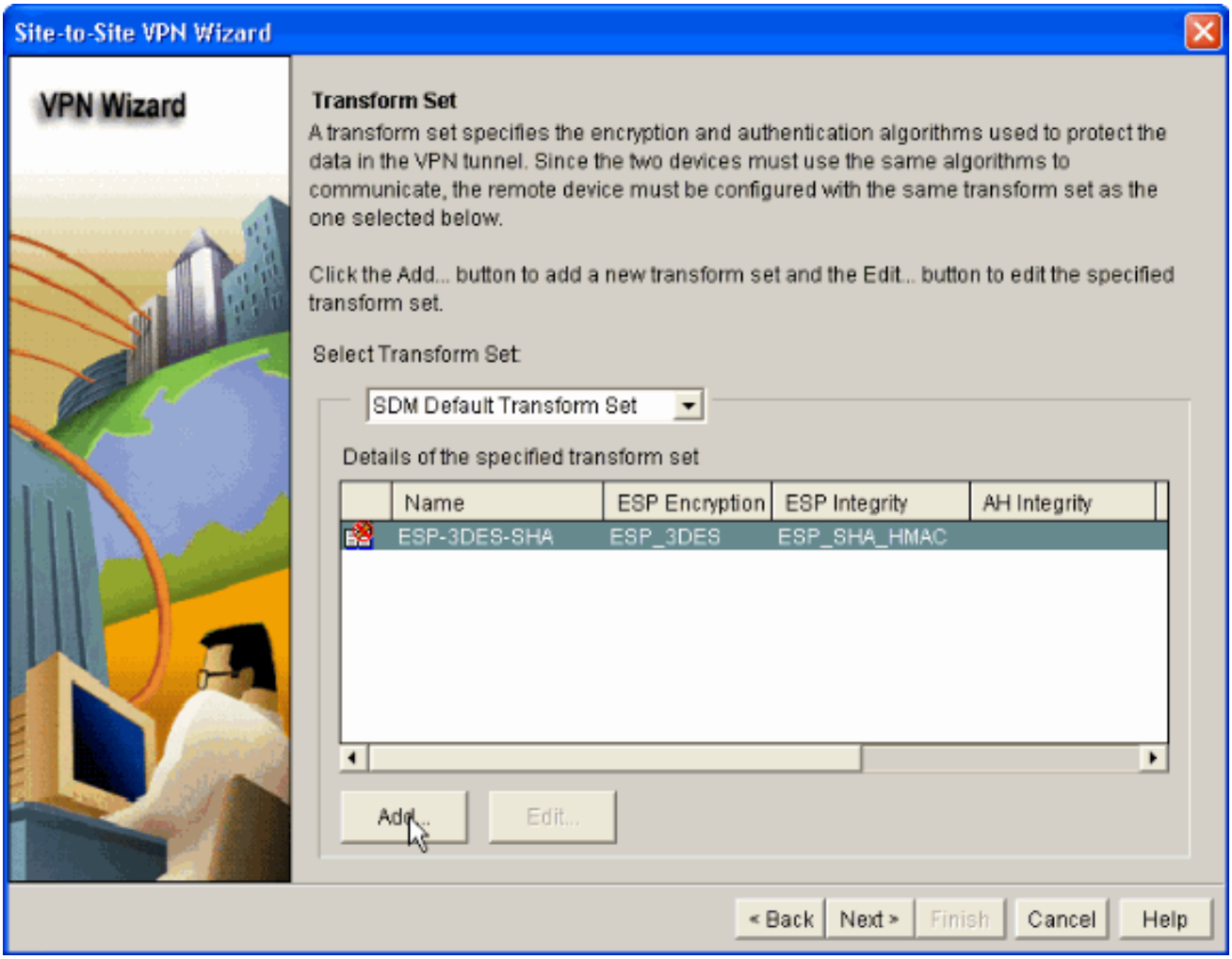


في ASA.

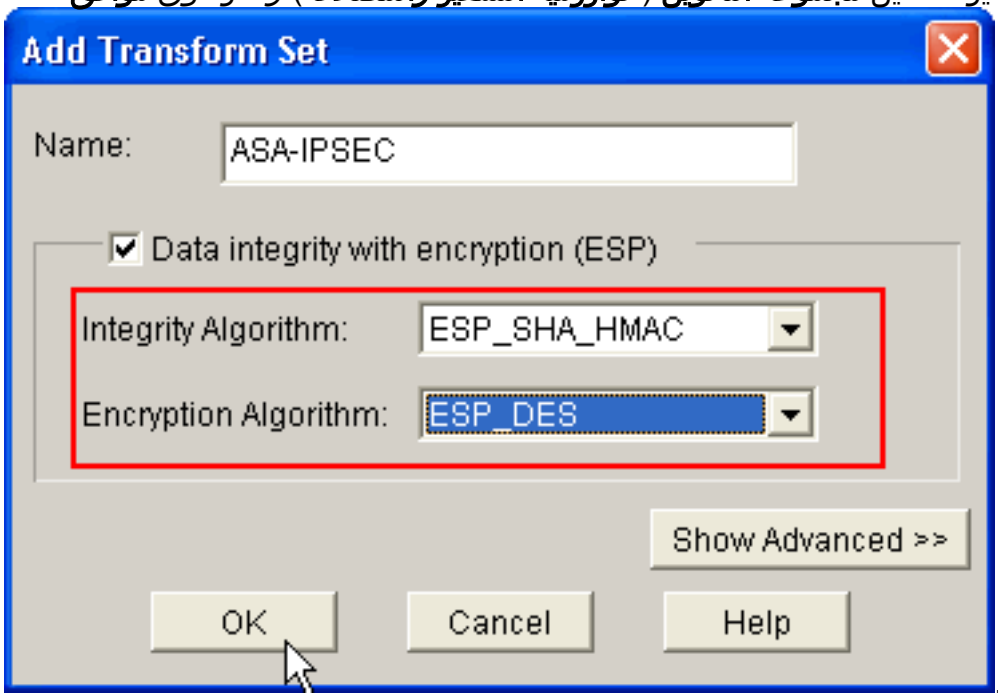
9. طقطقت **بعد ذلك** كما هو موضح هنا.



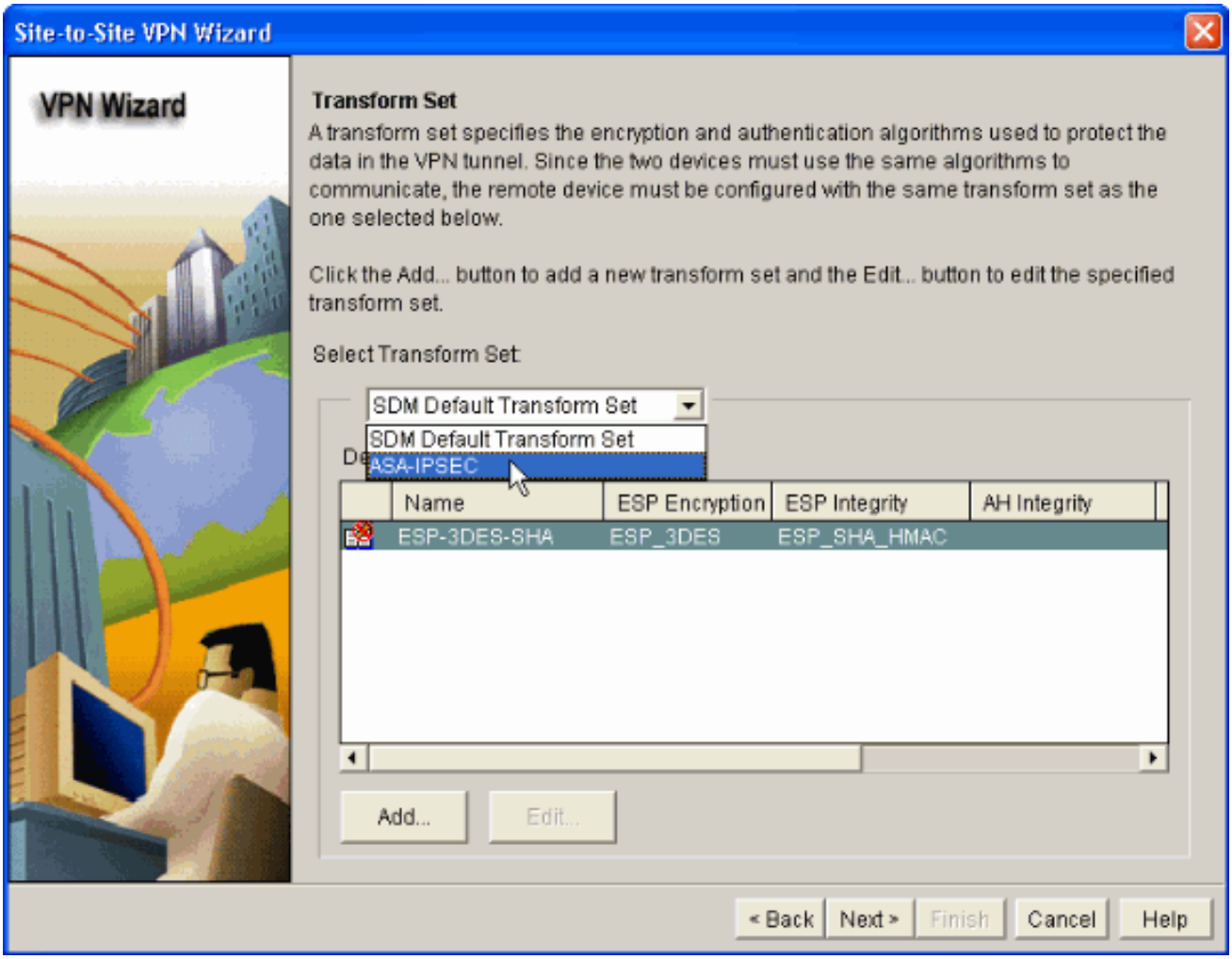
10. في هذه النافذة الجديدة، يجب توفير تفاصيل **مجموعة التحويل**. تحدد مجموعة التحويل خوارزميات **التشفير** و**المصادقة** المستخدمة لحماية **البيانات في نفق VPN**. ثم انقر فوق **إضافة** لتوفير هذه التفاصيل. يمكنك إضافة أي عدد من مجموعات التحويل حسب الحاجة بالنقر فوق **إضافة** وتوفير التفاصيل.



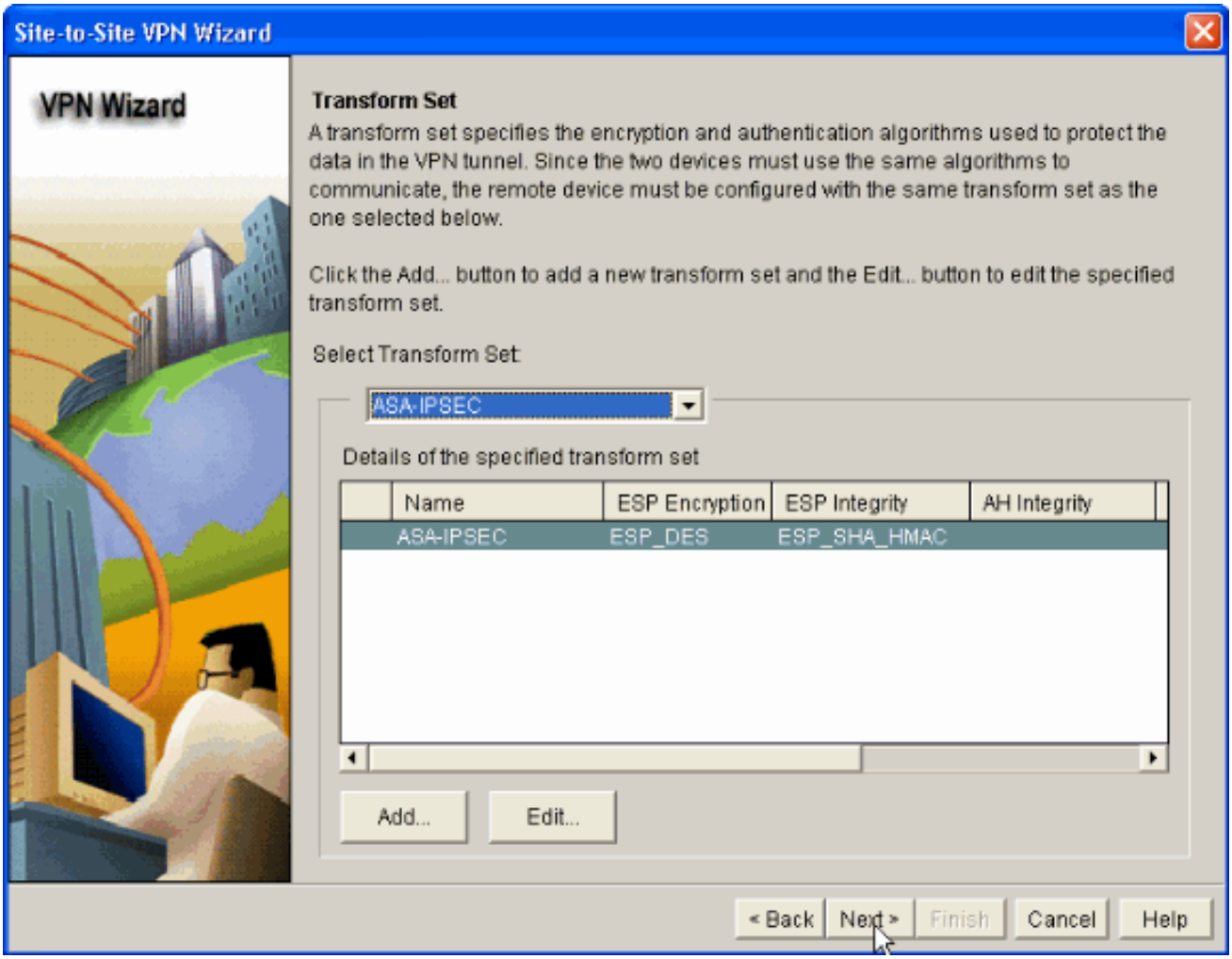
11. قم بتوفير تفاصيل **مجموعة التحويل** (**خوارزمية التشفير والمصادقة**) وانقر فوق **موافق** كما هو موضح.



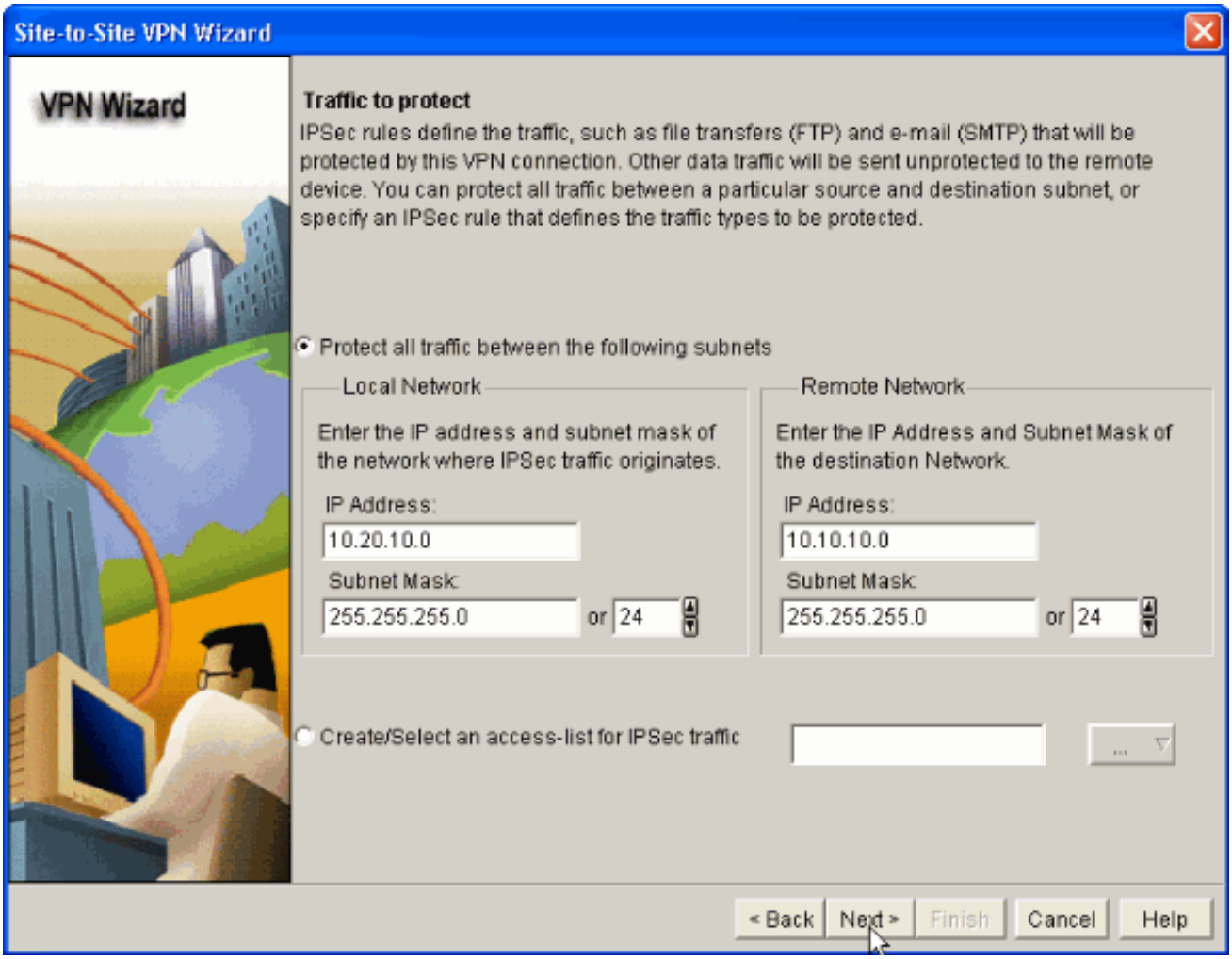
12. أختر **مجموعة التحويل** المطلوبة التي سيتم إستخدامها من القائمة المنسدلة كما هو موضح.



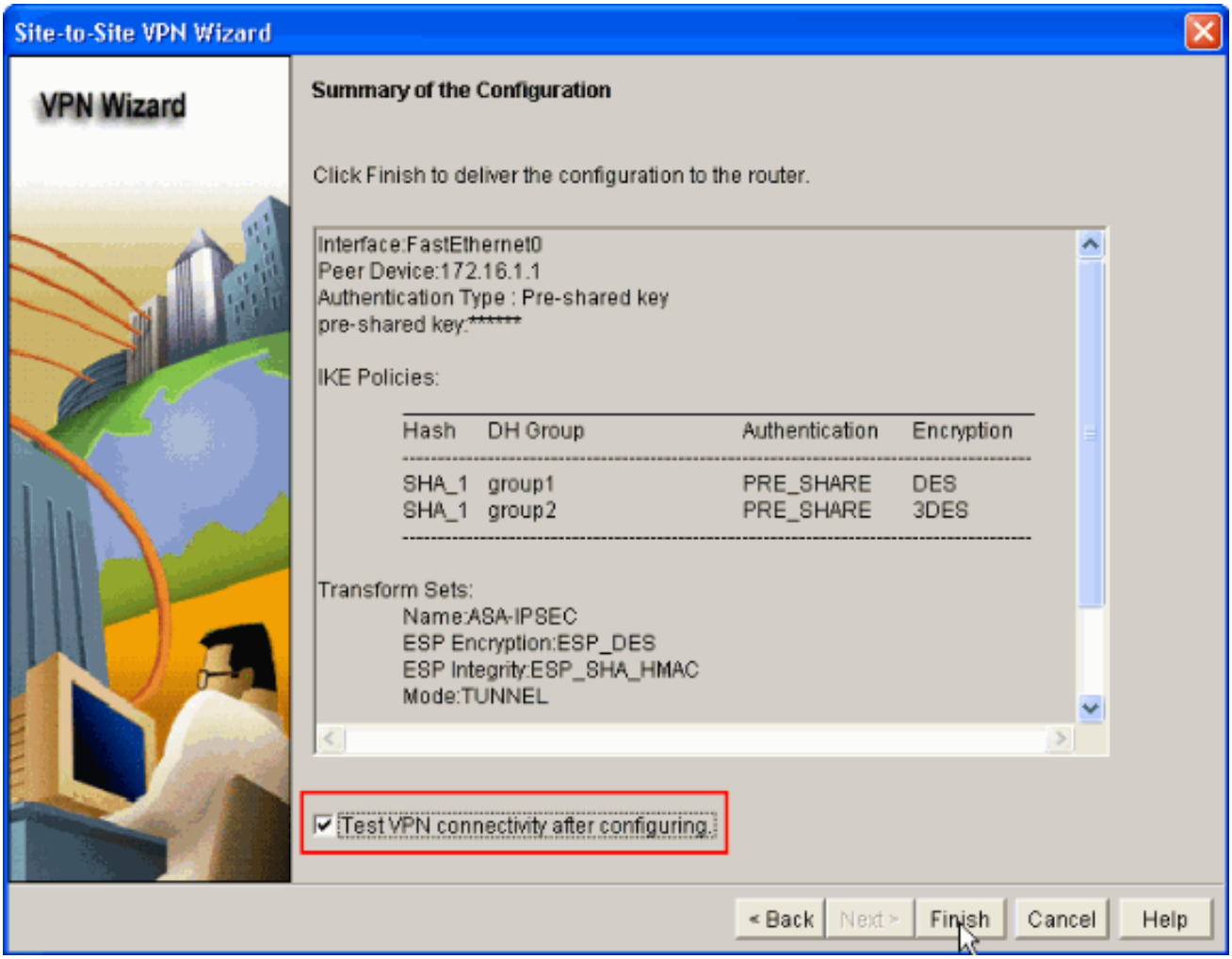
13. انقر فوق **Next** (التالي).



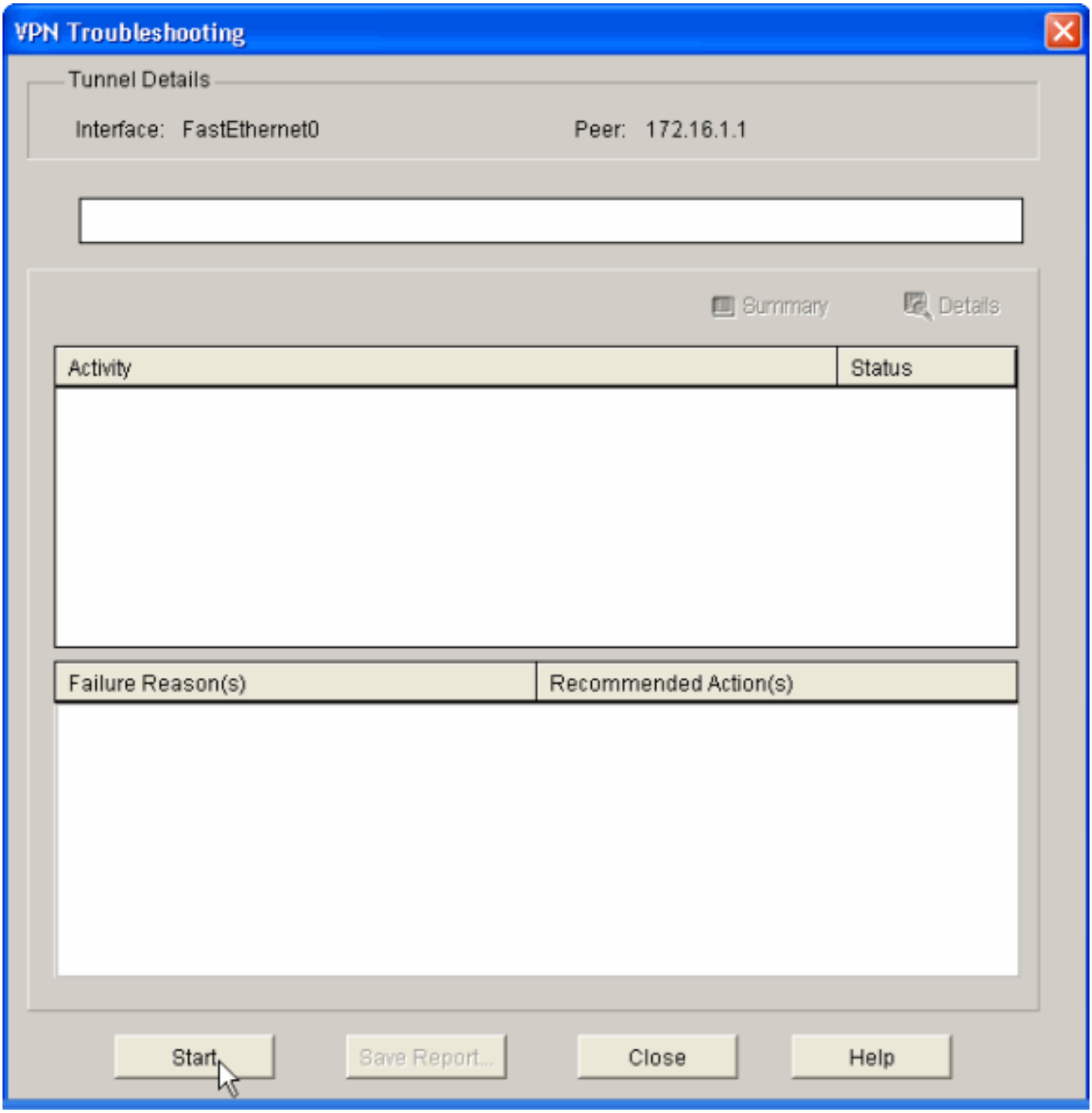
14. في الإطار التالي، يمكنك توفير تفاصيل حول **حركة مرور البيانات التي يجب حمايتها** من خلال نفق الشبكة الخاصة الظاهرية (VPN). وفر **شبكات المصدر والوجهة** لحركة المرور أن يكون محميا بحيث تتم حماية حركة المرور بين شبكات المصدر والوجهة المحددة. في هذا المثال، شبكة المصدر هي 10.20.10.0 وشبكة الوجهة هي 10.10.10.0. ثم انقر فوق
التالي.



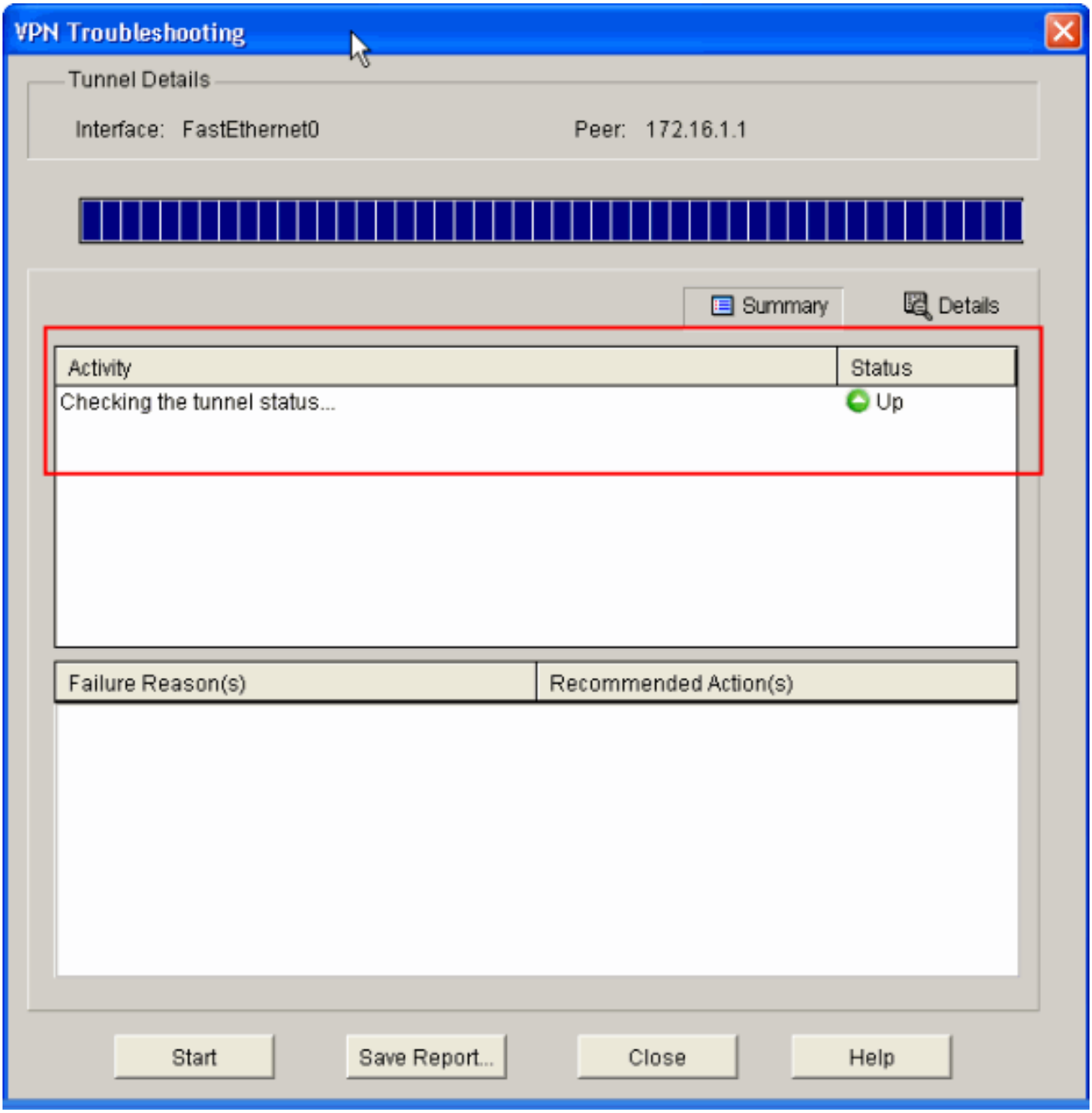
15. يبدي هذا نافذة خلاصة من الموقع إلى موقع VPN تشكيل تم. فحصت **إختبار اتصال VPN بعد تشكيل** خانة الاختيار إن أنت تريد أن إختبار اتصال VPN. هنا، يتم تحديد المربع حيث يلزم التحقق من الاتصال. ثم انقر فوق **إنهاء**.



16. انقر على **بدء** كما هو موضح للتحقق من اتصال VPN.



17. في الإطار التالي يتم توفير نتيجة **إختبار اتصال VPN**. هنا، يمكنك أن ترى ما إذا كان النفق **أعلى** أو **أسفل**. في مثال التكوين هذا، يتم **تشغيل** النفق كما هو موضح بالأخضر.



يؤدي هذا إلى اكتمال التكوين على موجه Cisco IOS.

تكوين ASA CLI

ASA

```
ASA#show run
Saved :
(ASA Version 8.0(2
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
Configure the outside interface. ! interface ---!
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 !--- Configure the inside
interface. ! interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
!-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU
```

```
  encrypted ftp mode passive dns server-group DefaultDNS
      domain-name default.domain.invalid access-list 100
                  extended permit ip any any access-list
       inside_nat0_outbound extended permit ip 10.10.10.0
                                              255.255.255.0
                                  255.255.255.0 10.20.10.0
This access list (inside_nat0_outbound) is used !-- ---!
- with the nat zero command. This prevents traffic which
    !--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
    this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
 -- the same as (outside_1_cryptomap). !--- Two separate
              access lists should always be used in this
                                              .configuration

      access-list outside_1_cryptomap extended permit ip
                                      10.10.10.0 255.255.255.0
                                  255.255.255.0 10.20.10.0
 This access list (outside_cryptomap) is used !--- ---!
 with the crypto map outside_map !--- to determine which
    traffic should be encrypted and sent !--- across the
      tunnel. !--- This ACL is intentionally the same as
 (inside_nat0_outbound). !--- Two separate access lists
           .should always be used in this configuration

                                              pager lines 24
                                            mtu inside 1500
                                           mtu outside 1500
                                                no failover
                                asdm image disk0:/asdm-613.bin
                                            asdm history enable
                                              arp timeout 14400
                                 global (outside) 1 interface
                        nat (inside) 1 10.10.10.0 255.255.255.0

              nat (inside) 0 access-list inside_nat0_outbound
 NAT 0 prevents NAT for networks specified in !--- ---!
                                 .the ACL inside_nat0_outbound


                      access-group 100 in interface outside
                    route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
                                        http server enable
                                     http 0.0.0.0 0.0.0.0 dmz
                                      no snmp-server location
                                       no snmp-server contact

    PHASE 2 CONFIGURATION ---! !--- The encryption ---!
       types for Phase 2 are defined here. crypto ipsec
          transform-set ESP-DES-SHA esp-des esp-sha-hmac
  Define the transform set for Phase 2. crypto map ---!
        outside_map 1 match address outside_1_cryptomap
  Define which traffic should be sent to the IPsec ---!
       peer. crypto map outside_map 1 set peer 172.17.1.1
  Sets the IPsec peer crypto map outside_map 1 set ---!
```

```
transform-set ESP-DES-SHA
Sets the IPsec transform set "ESP-AES-256-SHA" !--- ---!
    to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside
  Specifies the interface to be used with !--- the ---!
   settings defined in this configuration. !--- PHASE 1
 CONFIGURATION ---! !--- This configuration uses isakmp
  policy 10. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. crypto
                                    isakmp enable outside
                                crypto isakmp policy 10
                              authentication pre-share
                                    encryption des
                                        hash sha
                                        group 1
                                    lifetime 86400
                                  telnet timeout 5
                                     ssh timeout 5
                                 console timeout 0
                          threat-detection basic-threat
                  threat-detection statistics access-list
                                                  !




                        tunnel-group 172.17.1.1 type ipsec-l2l
     In order to create and manage the database of ---!
   connection-specific !--- records for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
 in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
                                        .of the IPsec peer




                      tunnel-group 172.17.1.1 ipsec-attributes
                                      * pre-shared-key
 Enter the pre-shared-key in order to configure the ---!
!--- authentication method. telnet timeout 5 ssh timeout
      5 console timeout 0 threat-detection basic-threat
    threat-detection statistics access-list ! class-map
 inspection_default match default-inspection-traffic ! !
      !-- Output suppressed! username cisco123 password
                  ffIRPGpDSOJh9YLq encrypted privilege 15
  Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

تكوين CLI للموجه

الموجّه

```
...Building configuration

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

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 2
authentication pre-share

Specifies the pre-shared key "cisco123" which ---!
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
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 ASA-IPSEC
esp-des esp-sha-hmac
!

Indicates that IKE is used to establish !--- ---! ---!
the IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
description Tunnel to172.16.1.1

Sets the IP address of the remote end. set ---! ---!
peer 172.16.1.1

Configures IPsec to use the transform-set !--- ---! ---!
"ASA-IPSEC" defined earlier in this configuration. set
transform-set ASA-IPSEC

Specifies the interesting traffic to be ---! ---!
encrypted. match address 100
!
!
!
Configures the interface to use the !--- crypto map ---!
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
ip address 10.20.10.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
Configure the access-lists and map them to the ---!
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
This ACL 110 identifies the traffic flows using ---!
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
 line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

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** .

- جهاز أمان PIX - أوامر show
- موجه IOS البعيد - أوامر show

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: 172.17.1.1   1
                    Type    : L2L             Role    : initiator
                    Rekey   : no              State   : MM_ACTIVE
```

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

```
ASA#show crypto ipsec sa
                                          interface: outside
                Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

                 (local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                (remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0
                                          current_peer: 172.17.1.1

                              pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9#
                              pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9#
                                    pkts compressed: 0, #pkts decompressed: 0#
            pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

                              path mtu 1500, ipsec overhead 58, media mtu 1500
                                    current outbound spi: 434C4A7F

                                                    :inbound esp sas
                                      (spi: 0xB7C1948E (3082917006
                                transform: esp-des esp-sha-hmac none
                            { ,in use settings ={L2L, Tunnel, PFS Group 2
                       slot: 0, conn_id: 12288, crypto-map: outside_map
                (sa timing: remaining key lifetime (kB/sec): (4274999/3588
                                                    IV size: 8 bytes
                                        replay detection support: Y
                                                   :outbound esp sas
                                      (spi: 0x434C4A7F (1129073279
                                transform: esp-des esp-sha-hmac none
                            { ,in use settings ={L2L, Tunnel, PFS Group 2
                       slot: 0, conn_id: 12288, crypto-map: outside_map
                (sa timing: remaining key lifetime (kB/sec): (4274999/3588
                                                    IV size: 8 bytes
                                        replay detection support: Y
```

موجه IOS البعيد - إظهار الأوامر

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

```
Router#show crypto isakmp sa

 dst             src             state          conn-id slot status
 QM_IDLE           3    0 ACTIVE      172.16.1.1      172.17.1.1
```

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

```
Router#show crypto ipsec sa
                                    interface: FastEthernet0
                            Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

                                    (protected vrf: (none
      (local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0
      (remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                                    current_peer 172.16.1.1 port 500
                                    {,PERMIT, flags={origin_is_acl
        pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68#
        pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68#
                            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 0#

      local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
                                    path mtu 1500, ip mtu 1500
                            (current outbound spi: 0xB7C1948E(3082917006

                                    :inbound esp sas
                                (spi: 0x434C4A7F(1129073279
                            , transform: esp-des esp-sha-hmac
                                { ,in use settings ={Tunnel
          conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
            (sa timing: remaining key lifetime (k/sec): (4578719/3004
                                    IV size: 8 bytes
                                replay detection support: Y
                                    Status: ACTIVE

                                    :inbound ah sas

                                    :inbound pcp sas

                                    :outbound esp sas
                                (spi: 0xB7C1948E(3082917006
                            , transform: esp-des esp-sha-hmac
                                { ,in use settings ={Tunnel
          conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
            (sa timing: remaining key lifetime (k/sec): (4578719/3002
                                    IV size: 8 bytes
                                replay detection support: Y
                                    Status: ACTIVE

                                    :outbound ah sas

                                    :outbound pcp sas
```

- **show crypto engine connections active**—يعرض الاتصالات والمعلومات الحالية حول الحزم المشفرة وغير المشفرة (الموجه فقط).

```
Router#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
  FastEthernet0        172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0 3
  FastEthernet0        172.17.1.1      set    DES+SHA                   0       59 2001
  FastEthernet0        172.17.1.1      set    DES+SHA                  59        0 2002
```

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** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر تصحيح الأخطاء وأستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها قبل أن تستخدم أوامر **debug**.

- **debug crypto ips 7**—يعرض مفاوضات IPsec للمرحلة 2. **debug crypto isakmp 7**—يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2. **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.

ارجع إلى حلول أستكشاف أخطاء IPSec VPN وإصلاحها الأكثر شيوعا في المستوى2L والوصول عن بعد للحصول على مزيد من المعلومات حول أستكشاف أخطاء موقع VPN وإصلاحها.

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- محترف التكوين: شبكة VPN من موقع إلى موقع بين ASA/PIX ومثال تكوين موجه IOS
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- مدير أجهزة الأمان والموجه من Cisco
- 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).