ASA 8.x: توجيه حركة مرور SSL VPN من خلال مثال تكوين العبارة الافتراضية النفقي

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) لتوجيه حركة مرور SSL VPN من خلال البوابة الافتراضية التي يتم إنشاء قنوات لها (TDG). عندما يخلق أنت تقصير ممر مع ال tunneled خيار، كل حركة مرور من نفق ينتهي على ال ASA أن يستطيع لا يكون وجهت يستعمل يعلم أو ساكن إستاتيكي أرسلت إلى هذا طريق. بالنسبة لحركة المرور الناشئة من نفق، يتجاوز هذا المسار أي مسارات افتراضية مكونة أو متعلمة أخرى.

المتطلبات الأساسية

المتطلبات

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

- ASA الذي يعمل على الإصدار 8.x
- Cisco SSL VPN Client (SVC) 1.x**ملاحظة:** قم بتنزيل حزمة عميل SSL VPN (sslclient-win*.pkg) من تنزيل برامج Cisco (للعملاء المسجلين فقط). انسخ SVC إلى ذاكرة Flash (الذاكرة المؤقتة) على ASA. يجب تنزيل SVC إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA.

المكونات المستخدمة

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

- Cisco 5500 Series ASA أن يركض برمجية صيغة 8.x

- إصدار عميل Cisco SSL VPN ل Windows 1.1.4.179
- كمبيوتر يعمل بنظام التشغيل Windows 2000 Professional أو Windows XP
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 6.1(5)

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.

الاصطلاحات

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

معلومات أساسية

ال SSL VPN Client (SVC) هو تقنية VPN tunneling التي تمنح المستخدمين البعيدين فوائد IPSec VPN Client دون الحاجة إلى مسؤولي الشبكة لتثبيت وتكوين عملاء IPSec VPN على أجهزة الكمبيوتر البعيدة. يستخدم SVC تشفير SSL الموجود بالفعل على الكمبيوتر البعيد بالإضافة إلى تسجيل دخول WebVPN ومصادقة جهاز الأمان.

في السيناريو الحالي، هناك عميل SSL VPN يتصل بالموارد الداخلية خلف ASA من خلال نفق SSL VPN. لم يتم تمكين النفق المنقسم. عند اتصال عميل SSL VPN ب ASA، سيتم إنشاء قنوات لجميع البيانات. إلى جانب الوصول إلى الموارد الداخلية، فإن المعيار الرئيسي هو توجيه حركة المرور النفقي هذه من خلال البوابة النفقي الافتراضية (DTG).

يمكنك تحديد مسار افتراضي منفصل لحركة المرور النفقي عبر المسار الافتراضي القياسي. يتم توجيه حركة المرور غير المشفرة التي يتم استقبالها بواسطة ASA، والتي لا يوجد لها مسار ثابت أو متعلم، عبر المسار الافتراضي القياسي. سيتم تمرير حركة المرور المشفرة التي يتم استقبالها بواسطة ASA، والتي لا يوجد لها مسار ثابت أو متعلم، إلى DTG المحدد من خلال المسار الافتراضي النفقي.

استعملت in order to عينت نفق تقصير ممر، هذا أمر:

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

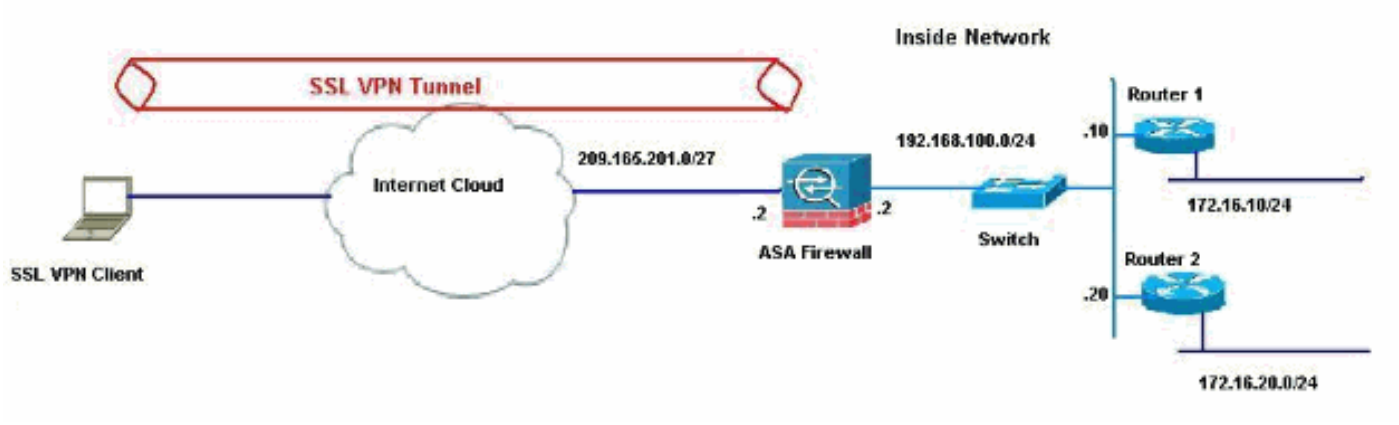
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



في هذا المثال، يصل عميل SSL VPN إلى الشبكة الداخلية من ASA من خلال النفق. كما يتم إنشاء قنوات لحركة المرور المخصصة لوجهات أخرى غير الشبكة الداخلية، حيث لا يوجد تقسيم نفق تم تكوينه، ويتم توجيهها عبر TDG (192.168.100.20).

بعد توجيه الحزم إلى TDG، وهو الموجه 2 في هذه الحالة، فإنه يقوم بتنفيذ ترجمة العنوان لتوجيه هذه الحزم للأمام إلى الإنترنت. لمزيد من المعلومات حول تكوين موجه كبوابة إنترنت، ارجع إلى كيفية تكوين موجه Cisco خلف مودم كبل غير Cisco.

تكوين ASA باستخدام ASDM 6.1(5)

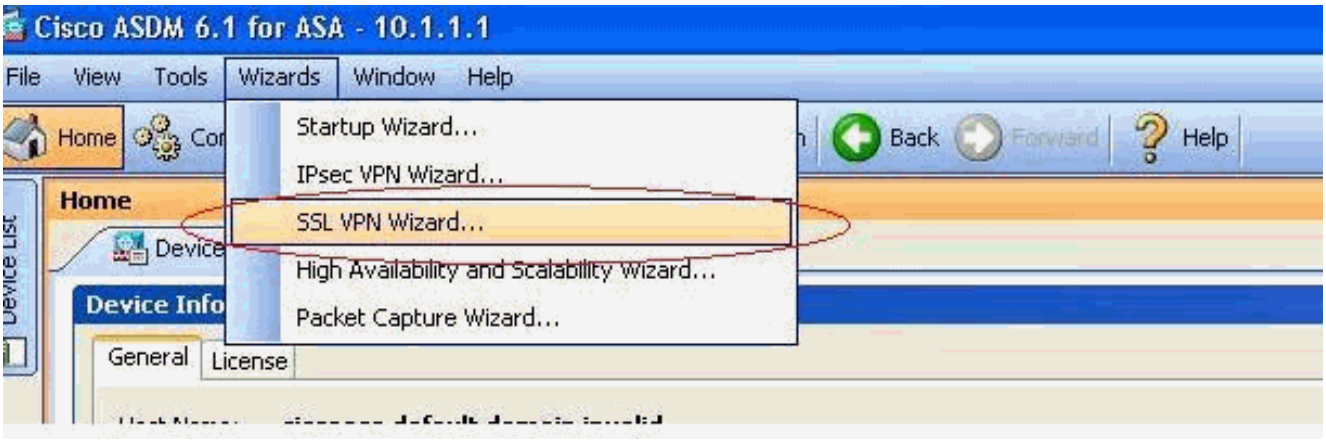
يفترض هذا المستند أن التكوينات الأساسية، مثل تكوين الواجهة، مكتملة وتعمل بشكل صحيح.

ملاحظة: راجع السماح بوصول HTTPS لـ ASDM للحصول على معلومات حول كيفية السماح بتكوين ASA بواسطة ASDM.

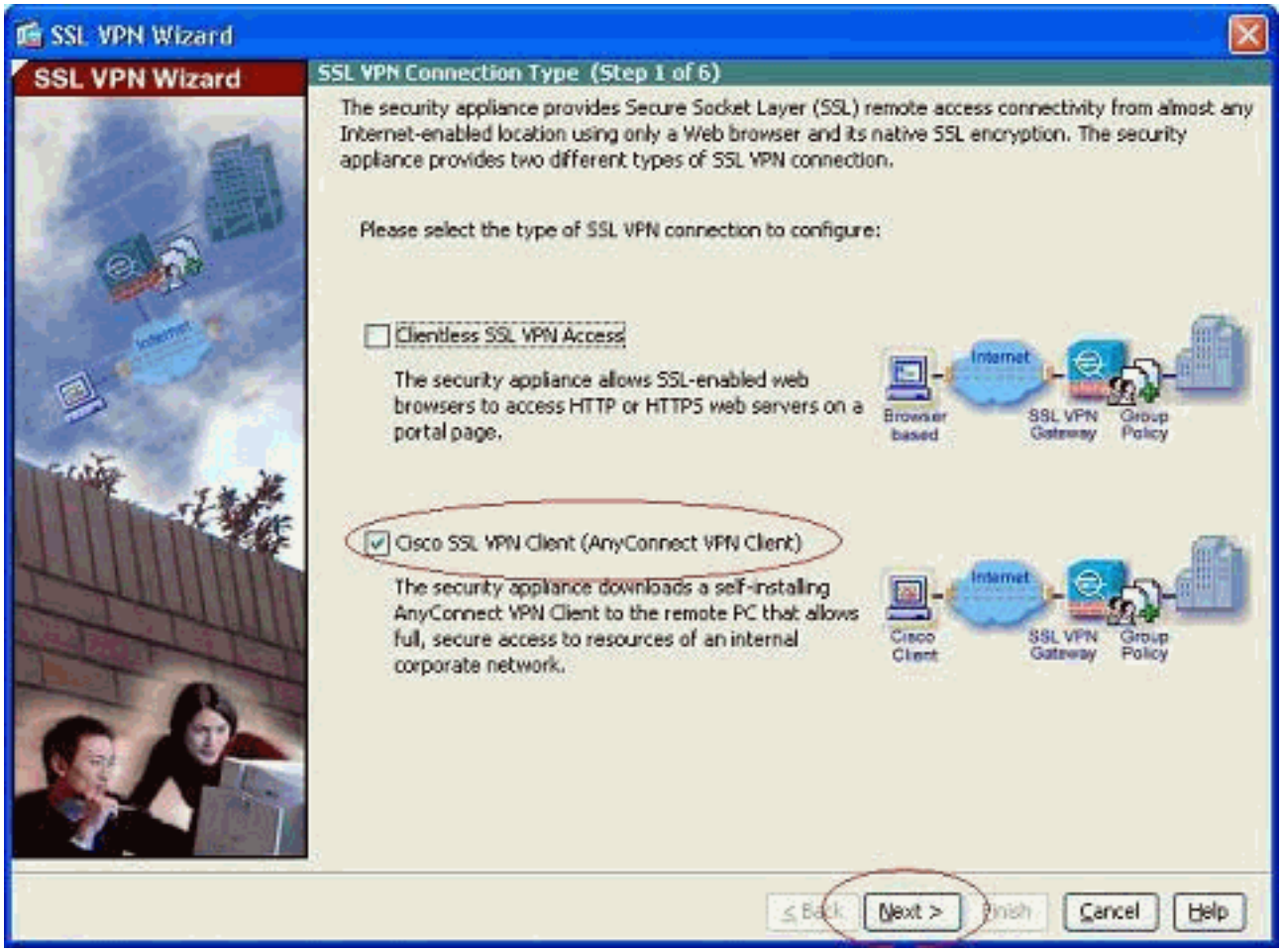
ملاحظة: لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. راجع ASDM و WebVPN الذي تم تمكينه على نفس واجهة ASA للحصول على مزيد من المعلومات.

أكمل هذه الخطوات لتكوين SSL VPN باستخدام معالج SSL VPN.

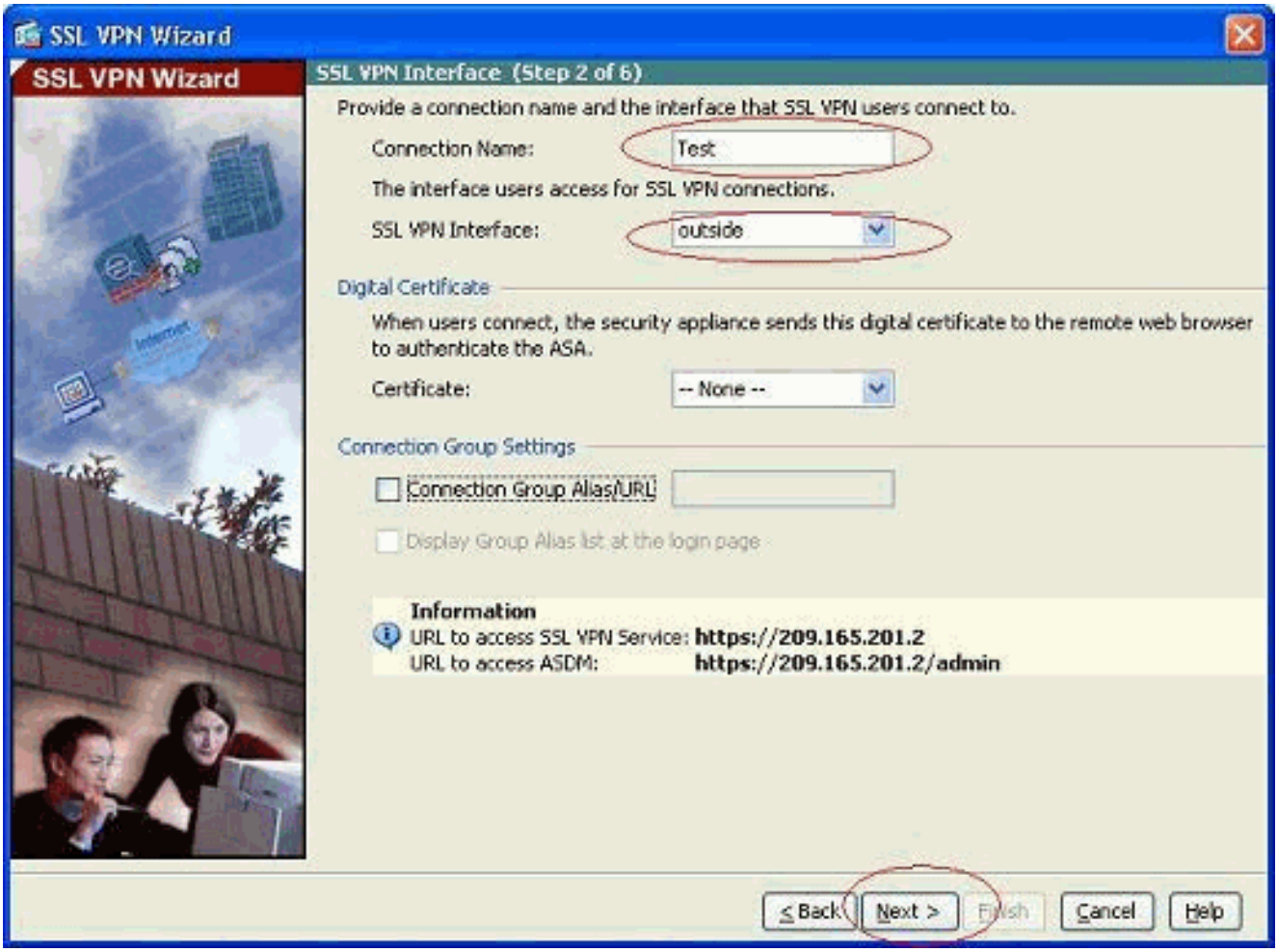
1. من قائمة المعالجات، أختر **معالج SSL VPN**.



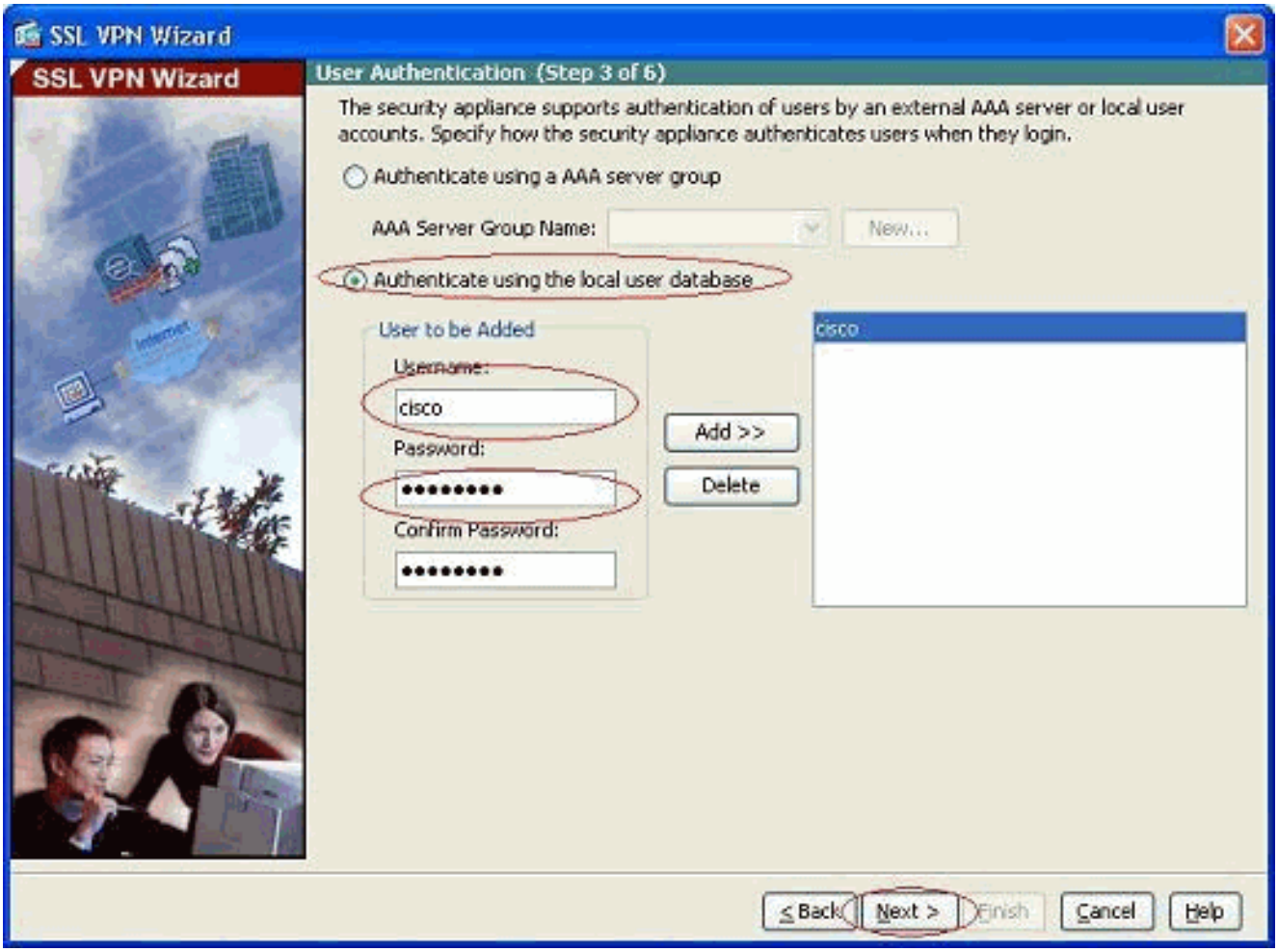
2. انقر فوق خانة الاختيار **Cisco SSL VPN Client**، ثم انقر فوق **التالي**.



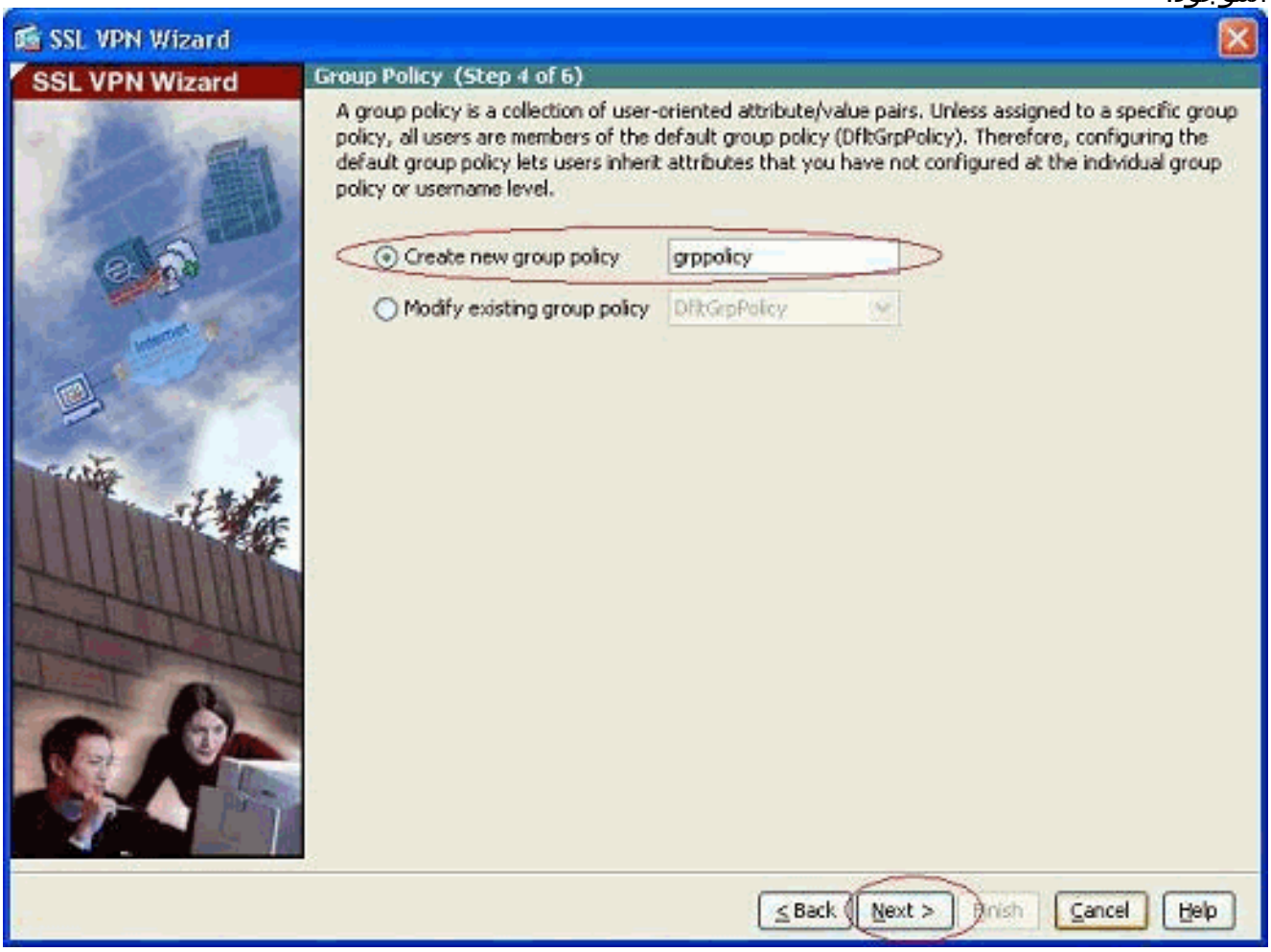
3. أدخل اسما للاتصال في حقل "اسم الاتصال"، ثم أختر الواجهة التي يتم إستخدامها من قبل المستخدم للوصول إلى SSL VPN من القائمة المنسدلة "واجهة VPN الخاصة ب SSL".



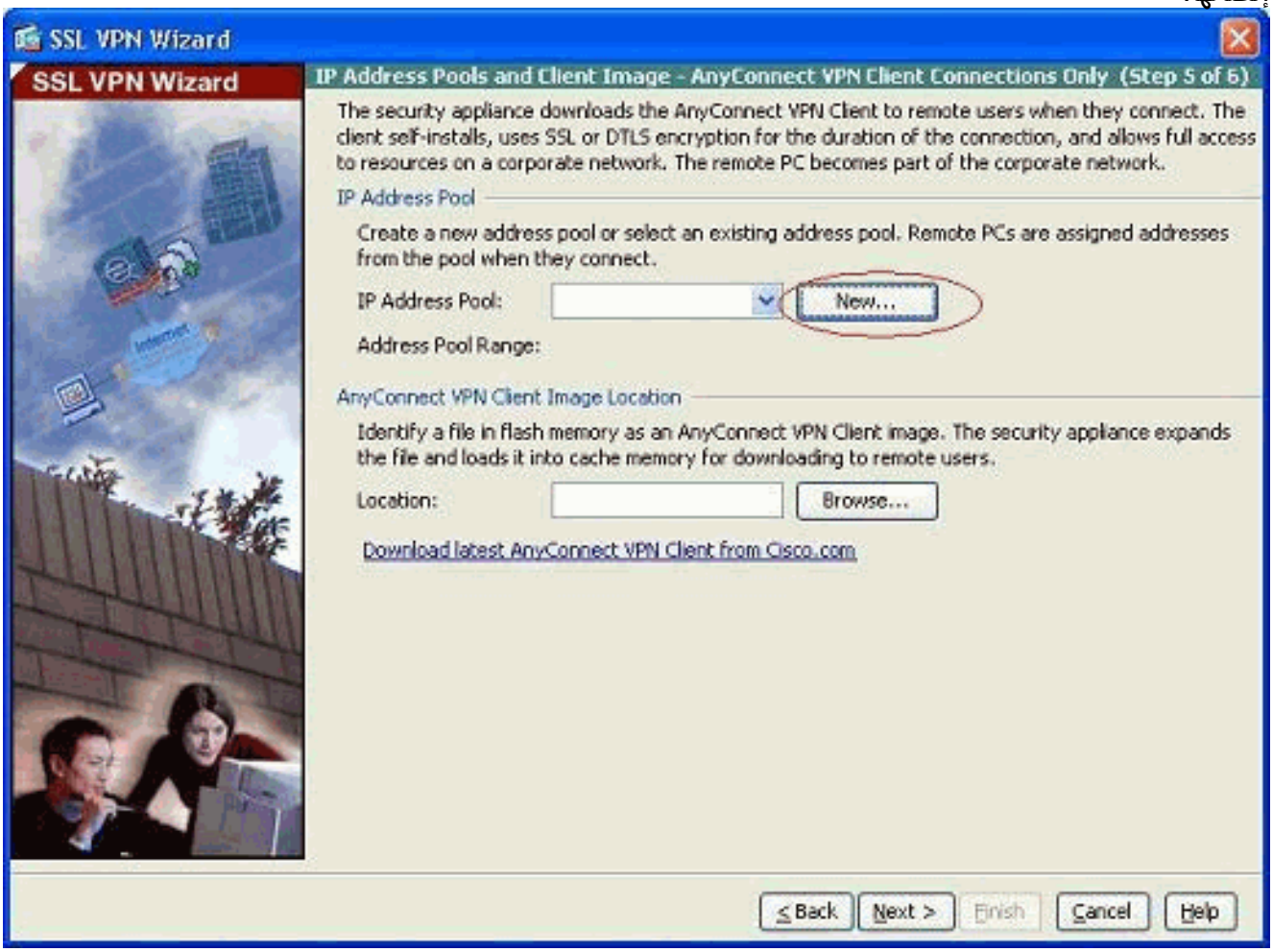
4. انقر فوق **Next (التالي)**.
5. أختر وضع مصادقة، وانقر **التالي**. (يستخدم هذا المثال المصادقة المحلية.)



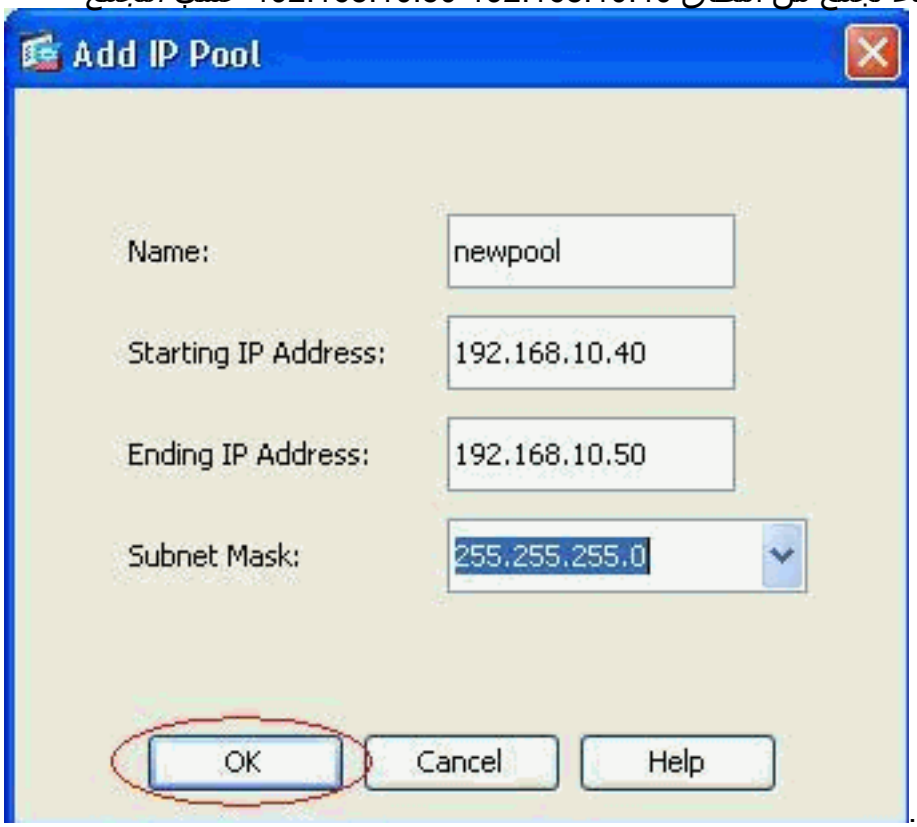
6. إنشاء نهج مجموعة جديد غير نهج المجموعة الافتراضي الموجود.



7. قم بإنشاء مجموعة جديدة من العناوين التي سيتم تعيينها إلى أجهزة كمبيوتر عميل SSL VPN بمجرد إتصالها.

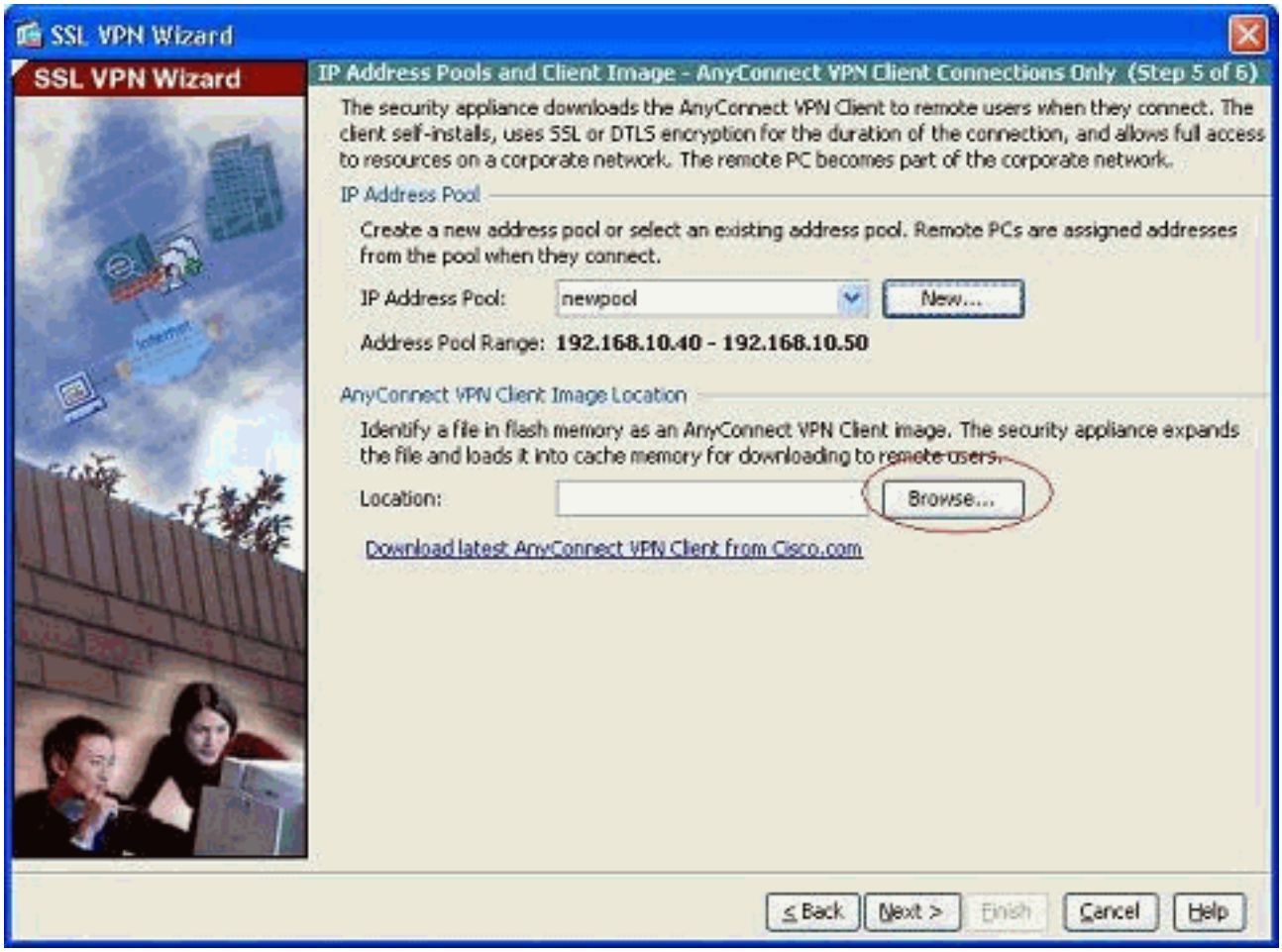


تم إنشاء تجمع من النطاق 192.168.10.40-192.168.10.50 حسب *التجمع*



بالاسم.

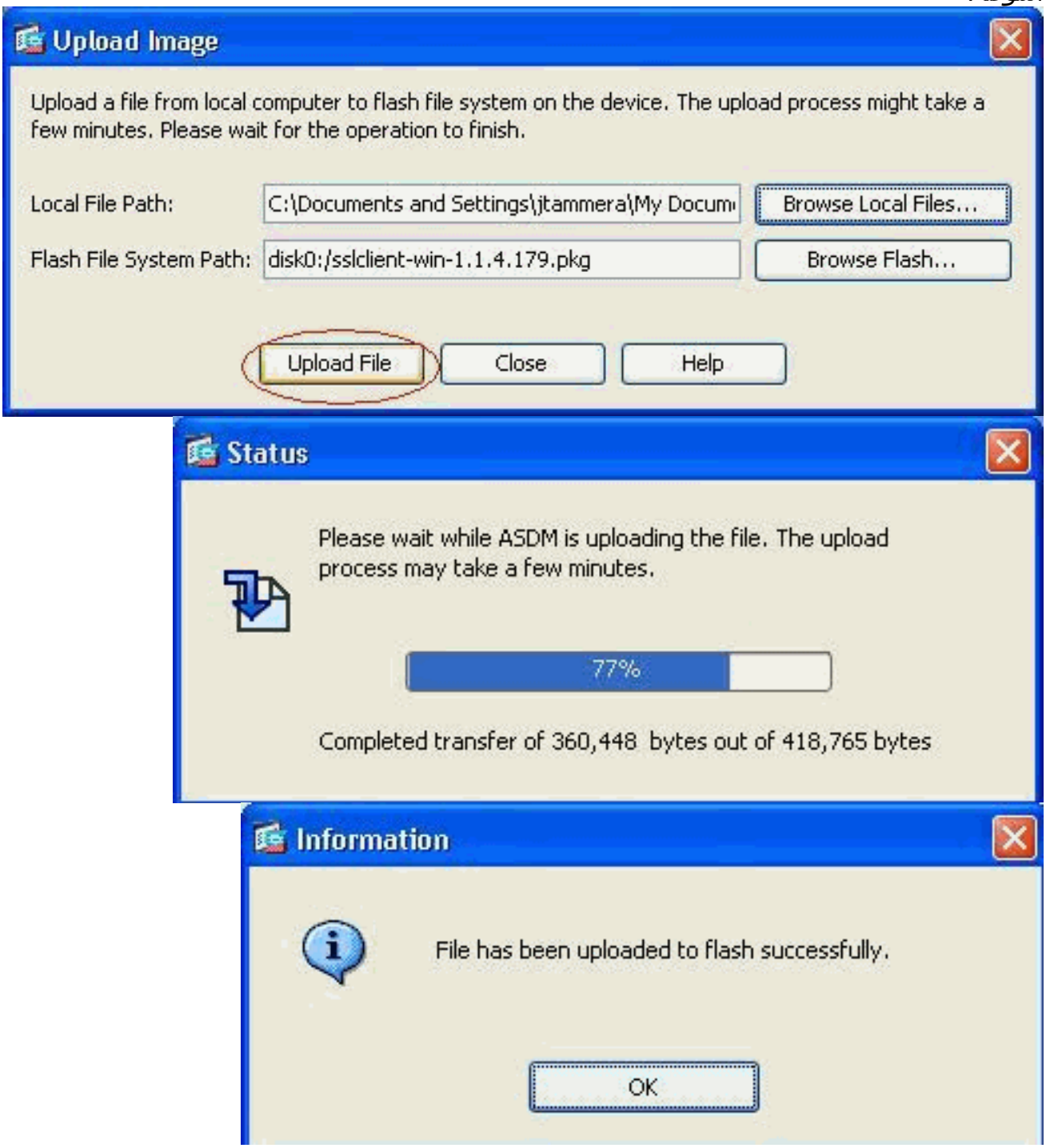
8. انقر فوق **إستعراض** لاختيار صورة عميل SSL VPN وتحميلها إلى ذاكرة Flash (الذاكرة المؤقتة) الخاصة ب ASA.



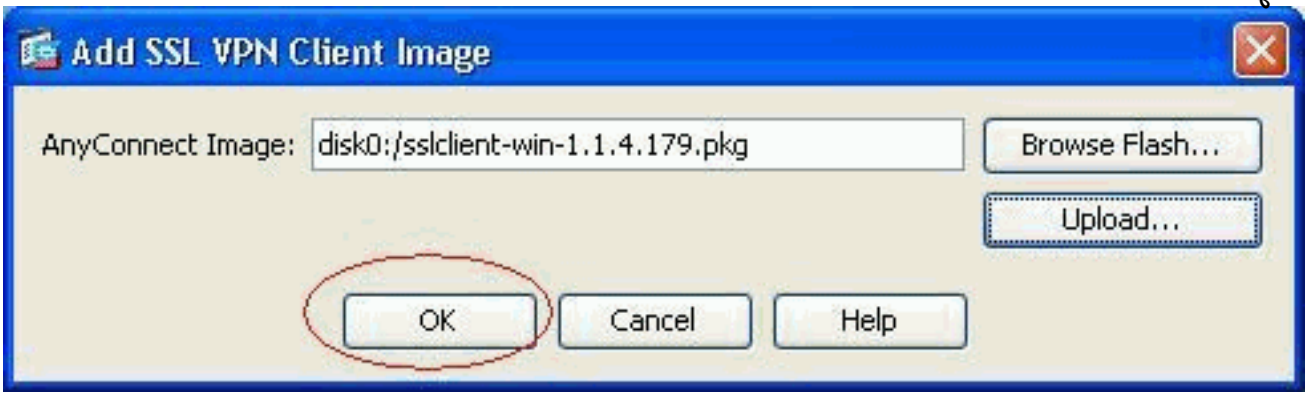
9. انقر فوق **تحميل** لتعيين مسار الملف من الدليل المحلي للجهاز.

10. انقر فوق **إستعراض الملفات المحلية** لتحديد الدليل حيث يوجد ملف sslclient.pkg.

11. انقر فوق **تحميل الملف** لتحميل الملف المحدد إلى ذاكرة ASA المؤقتة.

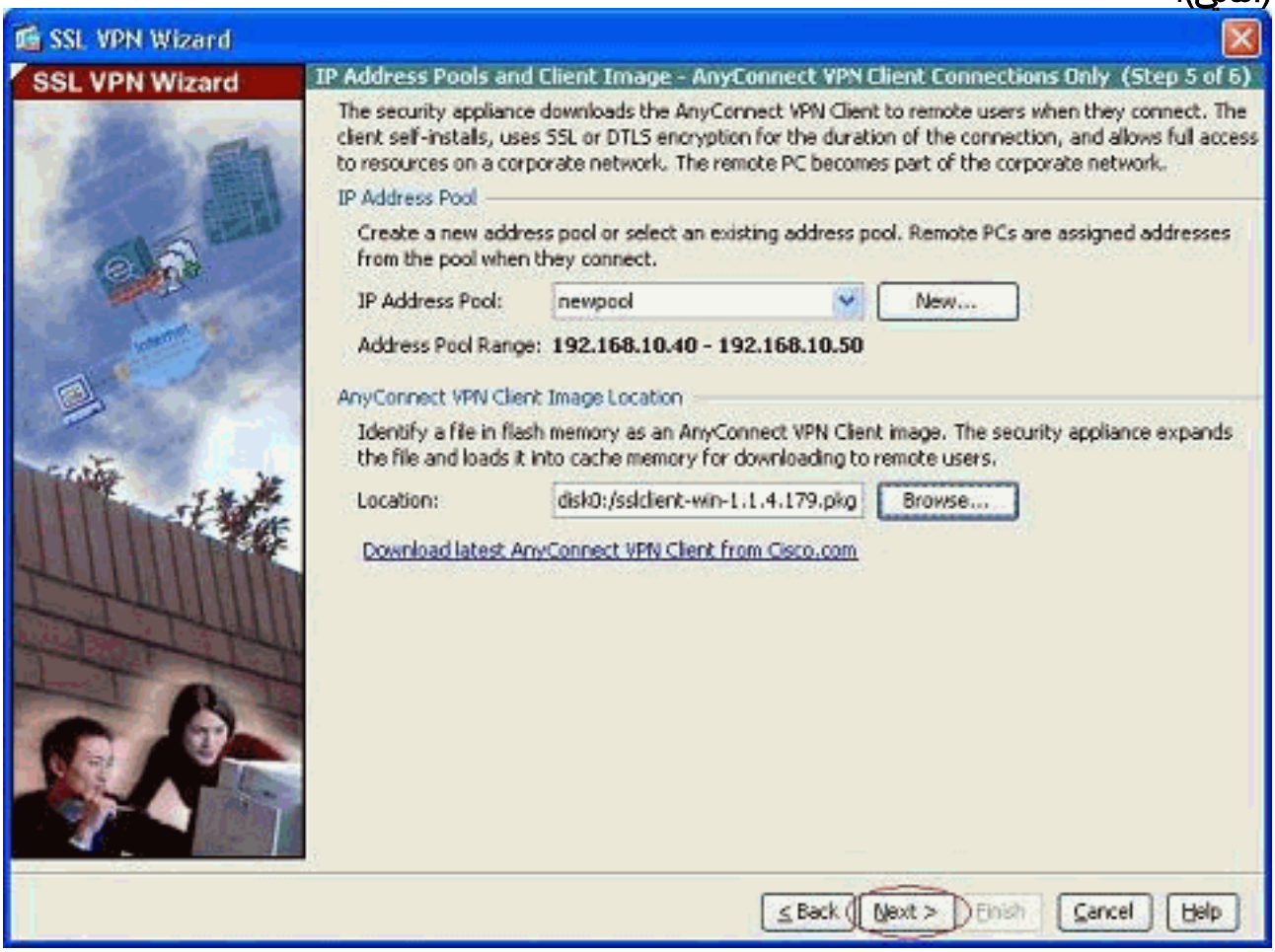


12. بمجرد تحميل الملف على ذاكرة Flash (الذاكرة المؤقتة) ل ASA، انقر فوق **موافق** لإكمال هذه المهمة.

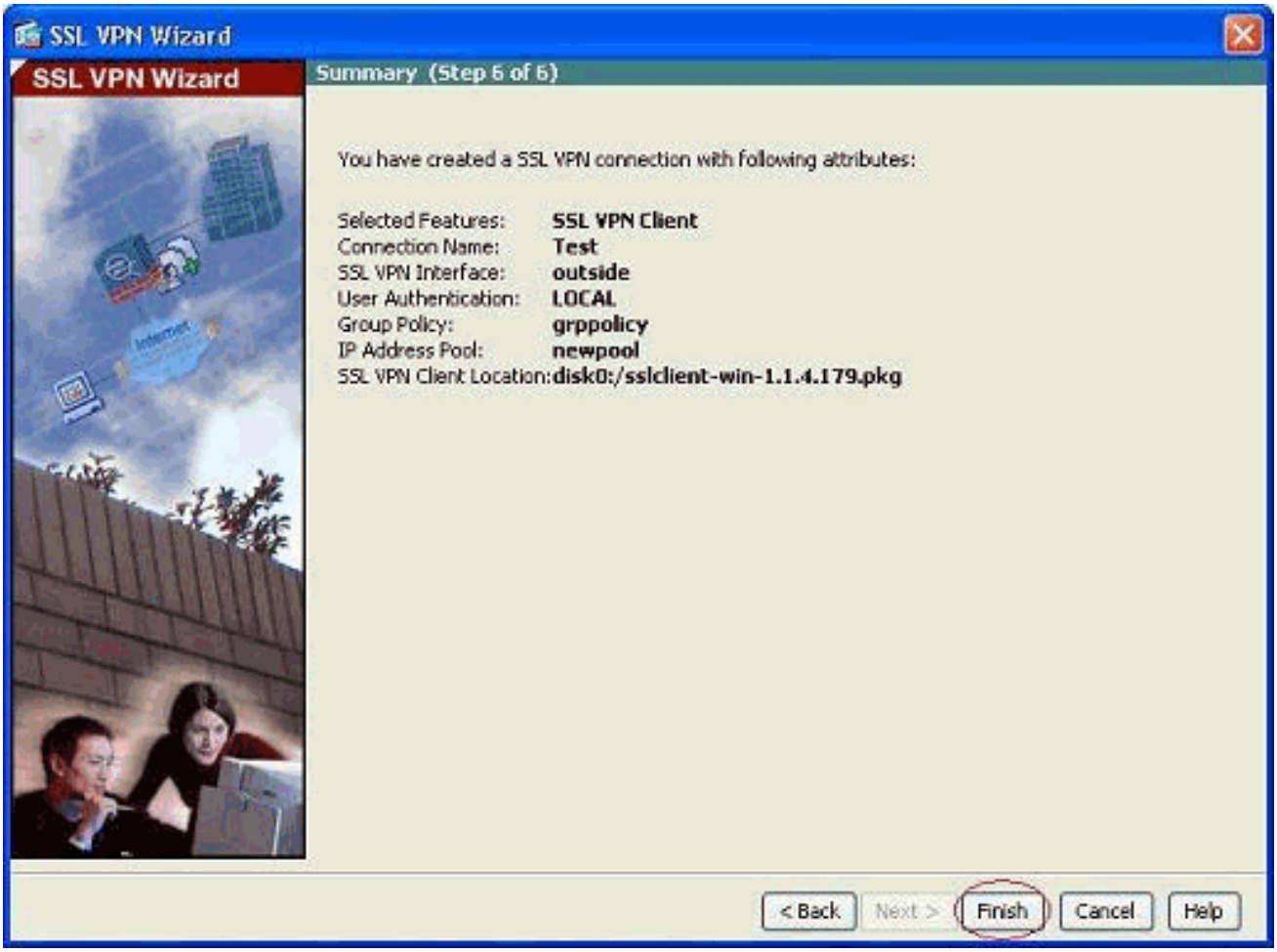


13. الآن هو يعرض أحدث ملف AnyConnect pkg الذي تم تحميله على ذاكرة ASA) Flash). انقر فوق **Next**.

(التالي).



14. يتم عرض ملخص تكوين عميل SSL VPN. انقر فوق **إنهاء**" لإكمال المعالج.



يتعلق التكوين الظاهر في ASDM بشكل رئيسي بتكوين معالج عميل SSL VPN.

في واجهة سطر الأوامر (CLI)، يمكنك ملاحظة بعض التكوين الإضافي. يتم عرض تكوين واجهة سطر الأوامر (CLI) الكامل أدناه وقد تم تمييز الأوامر الهامة.

سيسكوسا

```
ciscoasa#show running-config
Saved :
:
(ASA Version 8.0(4
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.2 255.255.255.0
!
interface Ethernet0/2
nameif manage
security-level 0
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/3
```

```
                                                shutdown
                                              no nameif
                                          no security-level
                                              no ip address
                                                      !
                                          interface Ethernet0/4
                                                shutdown
                                              no nameif
                                          no security-level
                                              no ip address
                                                      !
                                          interface Ethernet0/5
                                                shutdown
                                              no nameif
                                          no security-level
                                              no ip address
                                                      !
                                   passwd 2KFQnbNIdI.2KYOU encrypted
                                                ftp mode passive
                        access-list nonat extended permit ip 192.168.100.0
                                  255.255.255.0 192.168.10.0 255.255.255.0
                         access-list nonat extended permit ip 192.168.10.0
                                  255.255.255.0 192.168.100.0 255.255.255.0
                   ACL to define the traffic to be exempted from NAT. ---!
                    no pager logging enable logging asdm informational mtu
                          outside 1500 mtu inside 1500 mtu manage 1500 !---
                      Creating IP address block to be assigned for the VPN
                              clients ip local pool newpool 192.168.10.40-
                                          192.168.10.50 mask 255.255.255.0
                                                no failover
                               icmp unreachable rate-limit 1 burst-size 1
                                        asdm image disk0:/asdm-615.bin
                                              no asdm history enable
                                                   arp timeout 14400
                                     global (outside) 1 interface
                                  nat (inside) 0 access-list nonat
      The traffic permitted in "nonat" ACL is exempted ---!
       from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
                             route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
          Default route is configured through "inside" ---!
        interface for normal traffic. route inside 0.0.0.0
                                          0.0.0.0 192.168.100.20 tunneled
          Tunneled Default route is configured through ---!
    "inside" interface for encrypted traffic ! 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
      Configuring the ASA as HTTP server. http 10.1.1.0 ---!
                                          255.255.255.0 manage
        Configuring the network to be allowed for ASDM ---!
      access. ! !--- Output is suppressed ! 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
              ! ! 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 ! !--- Output suppressed !
                                                  webvpn
                                          enable outside
   Enable WebVPN on the outside interface svc image ---!
                          disk0:/sslclient-win-1.1.4.179.pkg 1
   Assign the AnyConnect SSL VPN Client image to be ---!
                                              used svc enable
    Enable the ASA to download SVC images to remote ---!
                    computers group-policy grppolicy internal
 Create an internal group policy "grppolicy" group- ---!
                                  policy grppolicy attributes
                                    VPN-tunnel-protocol svc
Specify SSL as a permitted VPN tunneling protocol ! ---!
      username cisco password ffIRPGpDSOJh9YLq encrypted
                                                 privilege 15
    Create a user account "cisco" tunnel-group Test ---!
                                          type remote-access
   Create a tunnel group "Test" with type as remote ---!
                    access tunnel-group Test general-attributes
                                          address-pool newpool
Associate the address pool vpnpool created default- ---!
                                       group-policy grppolicy
   Associate the group policy "clientgroup" created ---!
                                    prompt hostname context
   Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
                                                  #ciscoasa
```

التحقق من الصحة

يمكن إستخدام الأوامر المقدمة في هذا القسم للتحقق من هذا التكوين.

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

- **show webVPN svc**— يعرض صور SVC المخزنة في ذاكرة ASA المؤقتة.
- **show vpn-sessiondb svc**— يعرض المعلومات حول إتصالات SSL الحالية.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- دعم جهاز الأمان القابل للتكيف سلسلة Cisco 5500
- عميل PIX/ASA و VPN لشبكة VPN العامة على مثال تكوين العصا
- SSL VPN Client (SVC) على ASA مع مثال تكوين ASDM
- 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).