لاثم عم IOS ىلع SSL VPN Client (SVC) نيوكت SDM

المحتويات

المقدمة

يوفر SSL VPN Client (SVC) نفق كامل للاتصالات الآمنة إلى الشبكة الداخلية للشركة. يمكنك تكوين الوصول على مستخدم حسب المستخدم، أو يمكنك إنشاء سياقات WebVPN مختلفة يمكنك وضع مستخدم واحد أو أكثر فيها.

يتم دعم تقنية SSL VPN أو WebVPN على الأنظمة الأساسية لموجهات IOS التالية:

- 870 و 1811 و 1841 و 2801 و 2811 و 2821 و 2851
- 3725 و 3745 و 3825 و 3845 و 7200 و 7301

يمكنك تكوين تقنية SSL VPN في هذه الأوضاع:

- **SSL VPN (WebVPN) بدون عملاء**—يوفر عميل بعيد يتطلب مستعرض ويب يدعم SSL للوصول إلى خوادم الويب HTTP أو HTTPS على شبكة منطقة محلية (LAN) للشركات. بالإضافة إلى ذلك، توفر الشبكة الخاصة الظاهرية (VPN) الخاصة ببروتوكول نظام ملفات الإنترنت العام (CIFS) وصولا إلى إستعراض ملفات Windows. يعد Outlook Web Access (OWA) مثالا للوصول إلى HTTP.ارجع إلى SSL VPN (WebVPN)

بدون عملاء على Cisco IOS مع مثال تكوين SDM لمعرفة المزيد حول ClientLess SSL VPN.

- **Thin-Client SSL VPN (إعادة توجيه المنفذ)**—يوفر عميلا عن بعد يقوم بتنزيل تطبيق صغير قائم على Java ويسمح بالوصول الآمن لتطبيقات بروتوكول التحكم في الإرسال (TCP) التي تستخدم أرقام منافذ ثابتة. نقطة التواجد (POP3) وبروتوكول نقل البريد البسيط (SMTP) وبروتوكول الوصول إلى رسائل الإنترنت (IMAP) وبروتوكول طبقة الأمان (SSH) وبروتوكول Telnet هي أمثلة للوصول الآمن. نظرا لتغيير الملفات الموجودة على الجهاز المحلي، يجب أن يكون لدى المستخدمين امتيازات إدارية محلية لاستخدام هذه الطريقة. لا تعمل هذه الطريقة ل SSL VPN مع التطبيقات التي تستخدم تعيينات المنافذ الديناميكية، مثل بعض تطبيقات بروتوكول نقل الملفات (FTP).ارجع إلى مثال تكوين IOS الخاص ب WebVPN (Thin-Client SSL VPN) مع SDM لمعرفة المزيد حول Thin-Client SSL VPN.**ملاحظة:** بروتوكول مخطط بيانات المستخدم (UDP) غير مدعوم.
- **عميل SSL VPN (وضع النفق الكامل SVC)**—تنزيل عميل صغير إلى محطة العمل البعيدة والسماح بالوصول الآمن الكامل إلى الموارد على شبكة شركة داخلية. يمكنك تنزيل SVC إلى محطة عمل بعيدة بشكل دائم، أو يمكنك إزالة العميل بمجرد إغلاق جلسة العمل الآمنة.

يوضح هذا المستند تكوين موجه Cisco IOS للاستخدام بواسطة عميل SSL VPN.

المتطلبات الأساسية

المتطلبات

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

- Microsoft Windows 2000 أو XP
- متصفح ويب مزود ب Sun JRE 1. 4 أو إصدار أحدث أو متصفح ActiveX يتم التحكم فيه
- امتيازات إدارية محلية على العميل
- أحد الموجهات المدرجة في المقدمة مع صورة أمان متقدمة (12.4(6)T أو أحدث)
- Cisco Security Device Manager (SDM)، الإصدار 2.3إذا لم يتم تحميل إدارة قاعدة بيانات المحول (SDM) من Cisco بالفعل على الموجه الخاص بك، فيمكنك الحصول على نسخة مجانية من البرنامج من تنزيل البرامج (للعملاء المسجلين فقط). أنت ينبغي يتلقى حساب CCO مع عقد خدمة. لمزيد من المعلومات التفصيلية حول تثبيت إدارة قاعدة بيانات المحول (SDM) وتكوينها، ارجع إلى مدير أجهزة الأمان والموجه من Cisco.
- شهادة رقمية على الموجهيمكنك إستخدام شهادة موقعة ذاتيا ثابتة أو مرجع تصديق خارجي (CA) لتلبية هذا المتطلب. لمزيد من المعلومات عن الشهادات الدائمة ذاتية التوقيع، راجع الشهادات الدائمة ذاتية التوقيع.

المكونات المستخدمة

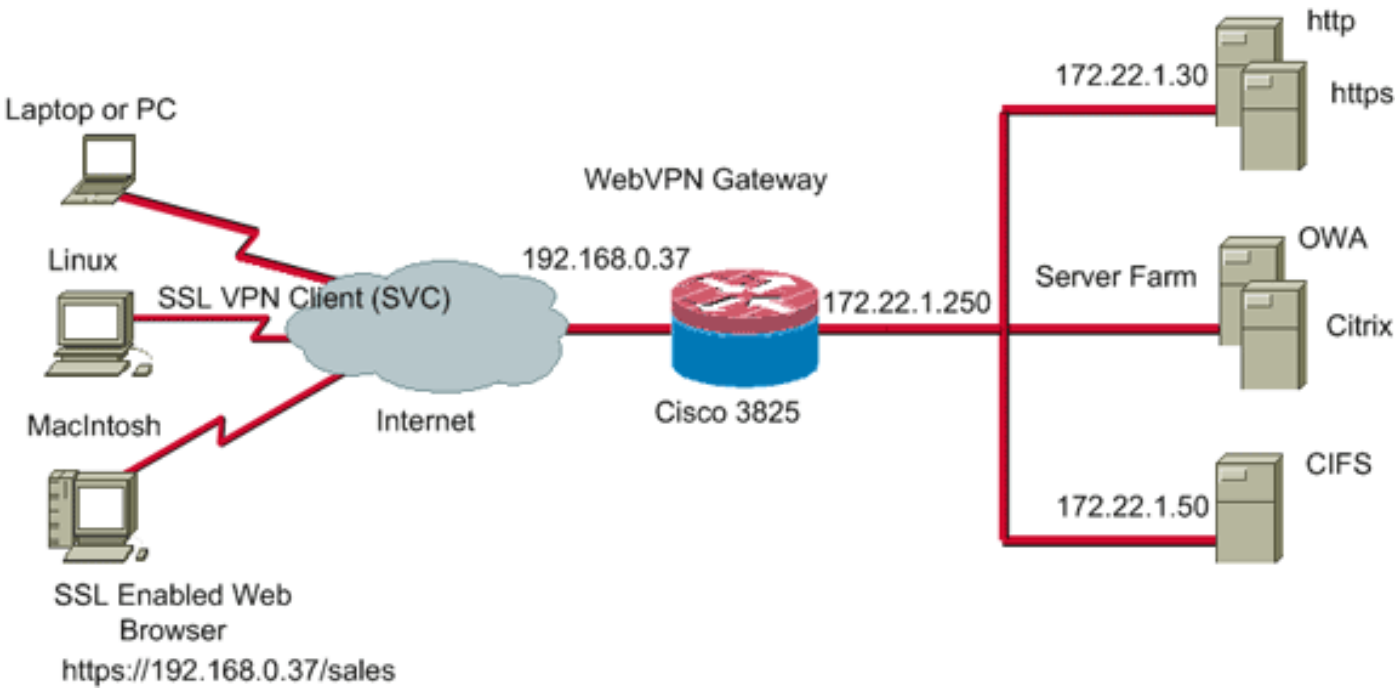
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- سلسلة موجه IOS 3825 من Cisco مع 12.4(9)T
- Security Device Manager (SDM)، الإصدار 2.3.1

ملاحظة: 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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



مهام ما قبل التكوين

1. تكوين الموجه لإدارة قاعدة بيانات المحول (SDM) (إختياري)تحتوي الموجهات التي تحتوي على ترخيص حزمة الأمان المناسب بالفعل على تطبيق إدارة قاعدة بيانات المحول (SDM) الذي تم تحميله في ذاكرة الفلاش. ارجع إلى تنزيل موجه Cisco ومدير أجهزة الأمان (SDM) وتشبته للحصول على البرنامج وتكوينه.
2. قم بتنزيل نسخة من SVC إلى كمبيوتر الإدارة الخاص بك.يمكنك الحصول على نسخة من ملف حزمة SVC من تنزيل البرامج: Cisco SSL VPN Client (للعملاء المسجلين فقط). أنت ينبغي يتلقى شرعي CCO حساب مع خدمة عقد.
3. قم بتعيين التاريخ والوقت والمنطقة الزمنية الصحيحة، ثم قم بتكوين شهادة رقمية على الموجه.

الاصطلاحات

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

معلومات أساسية

يتم تحميل SVC في البداية على موجه عبارة WebVPN. في كل مرة يتصل فيها العميل، يتم تنزيل نسخة من SVC بشكل ديناميكي على الكمبيوتر الشخصي. لتغيير هذا السلوك، قم بتكوين الموجه لتمكين البرنامج من البقاء بشكل دائم على كمبيوتر العميل.

تكوين SVC على IOS

في هذا القسم، تقدم لك الخطوات اللازمة لتكوين الميزات الموضحة في هذا المستند. يستخدم مثال التكوين هذا معالج إدارة قاعدة بيانات المحول (SDM) لتمكين عملية تشغيل SVC على موجه IOS.

أتمت هذا steps in order to شكلت SVC على ال ios مسحاج تخديد:

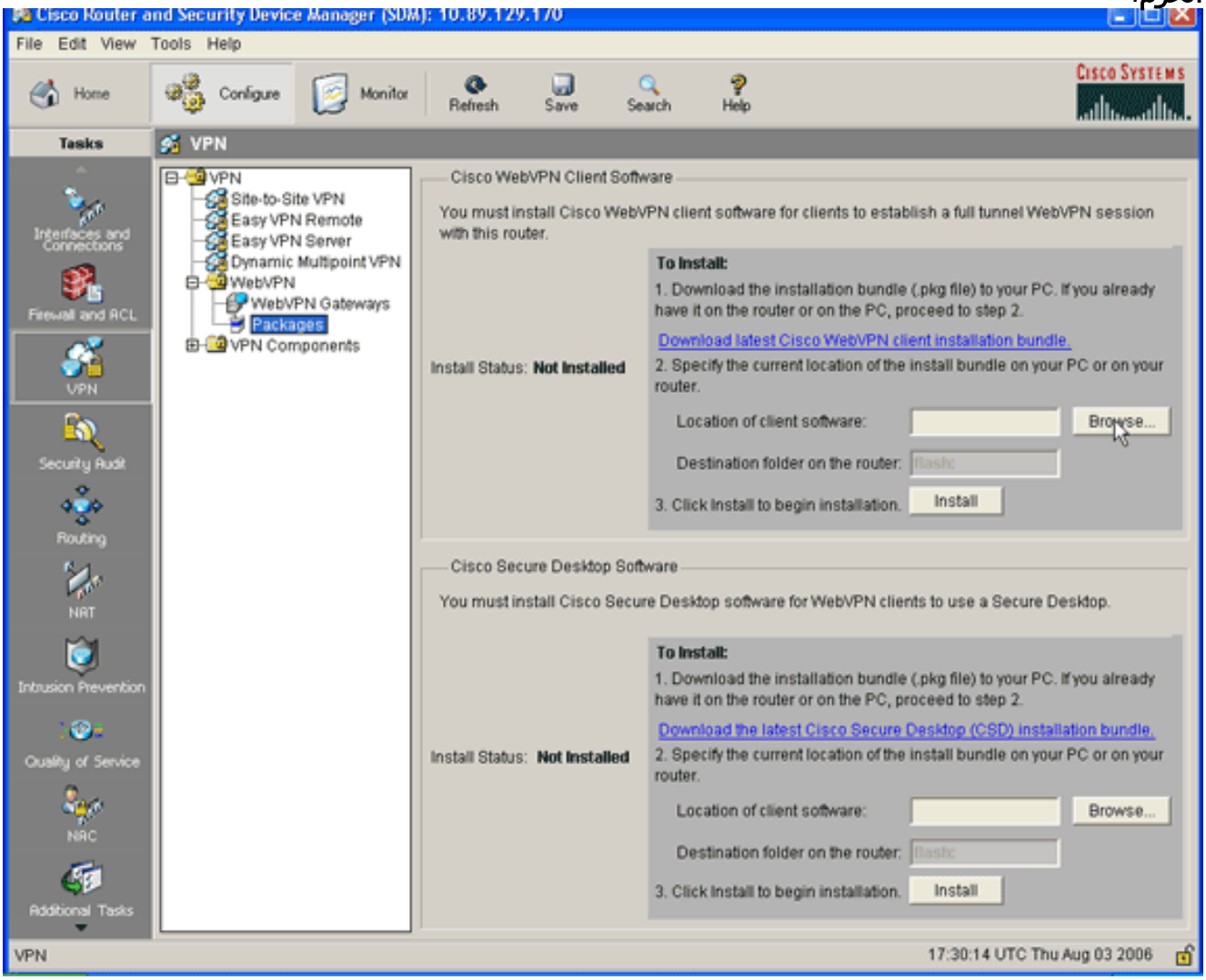
1. تثبيت برنامج SVC وتمكينه على موجه IOS
2. تكوين سياق WebVPN وبوابة WebVPN باستخدام معالج إدارة قاعدة بيانات المحول (SDM)
3. تكوين قاعدة بيانات المستخدم لمستخدمي SVC

4. تكوين الموارد للتعريف للمستخدمين

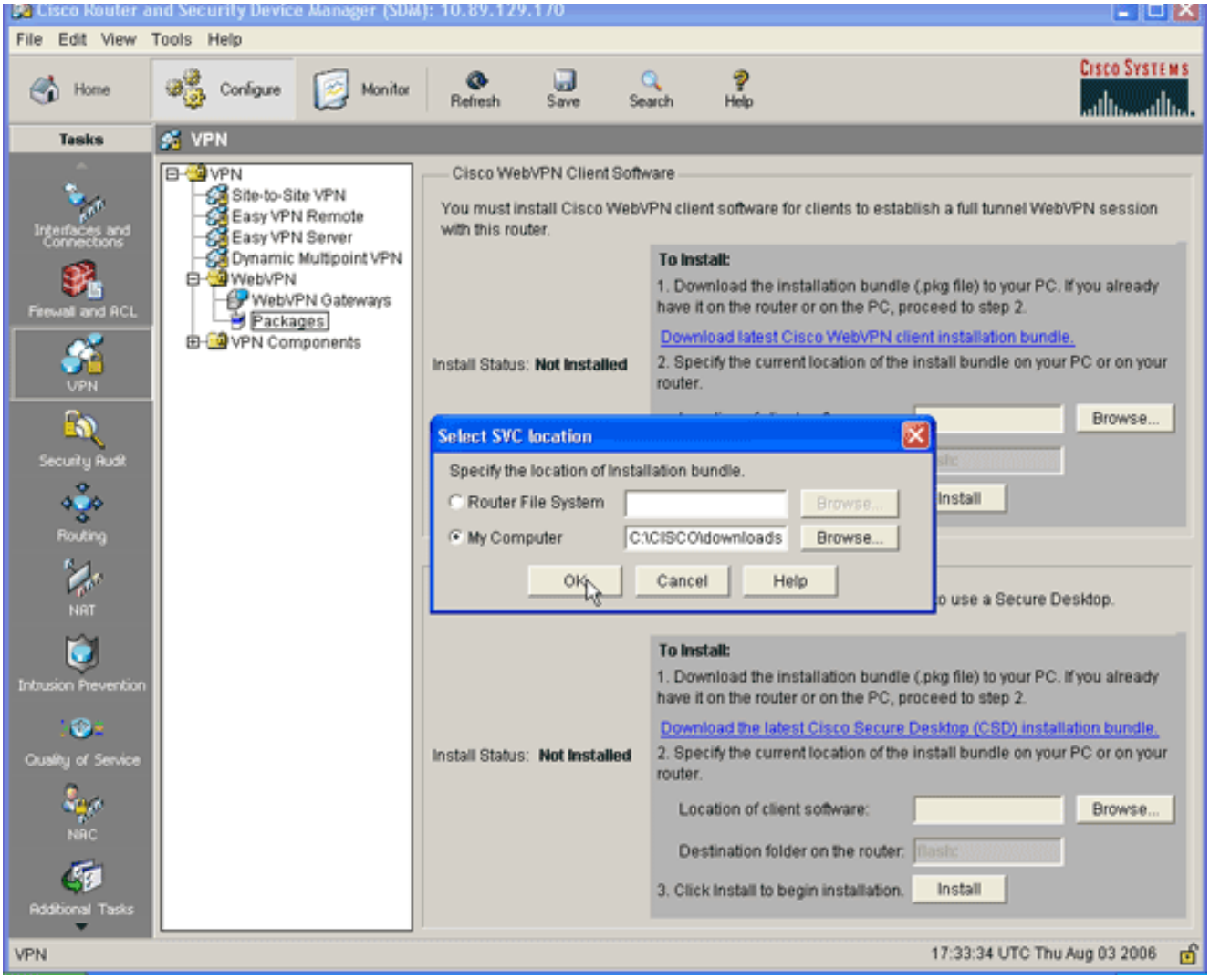
الخطوة 1. تثبيت برنامج SVC وتمكينه على موجه IOS

أكمل الخطوات التالية لتثبيت برنامج SVC وتمكينه على موجه IOS:

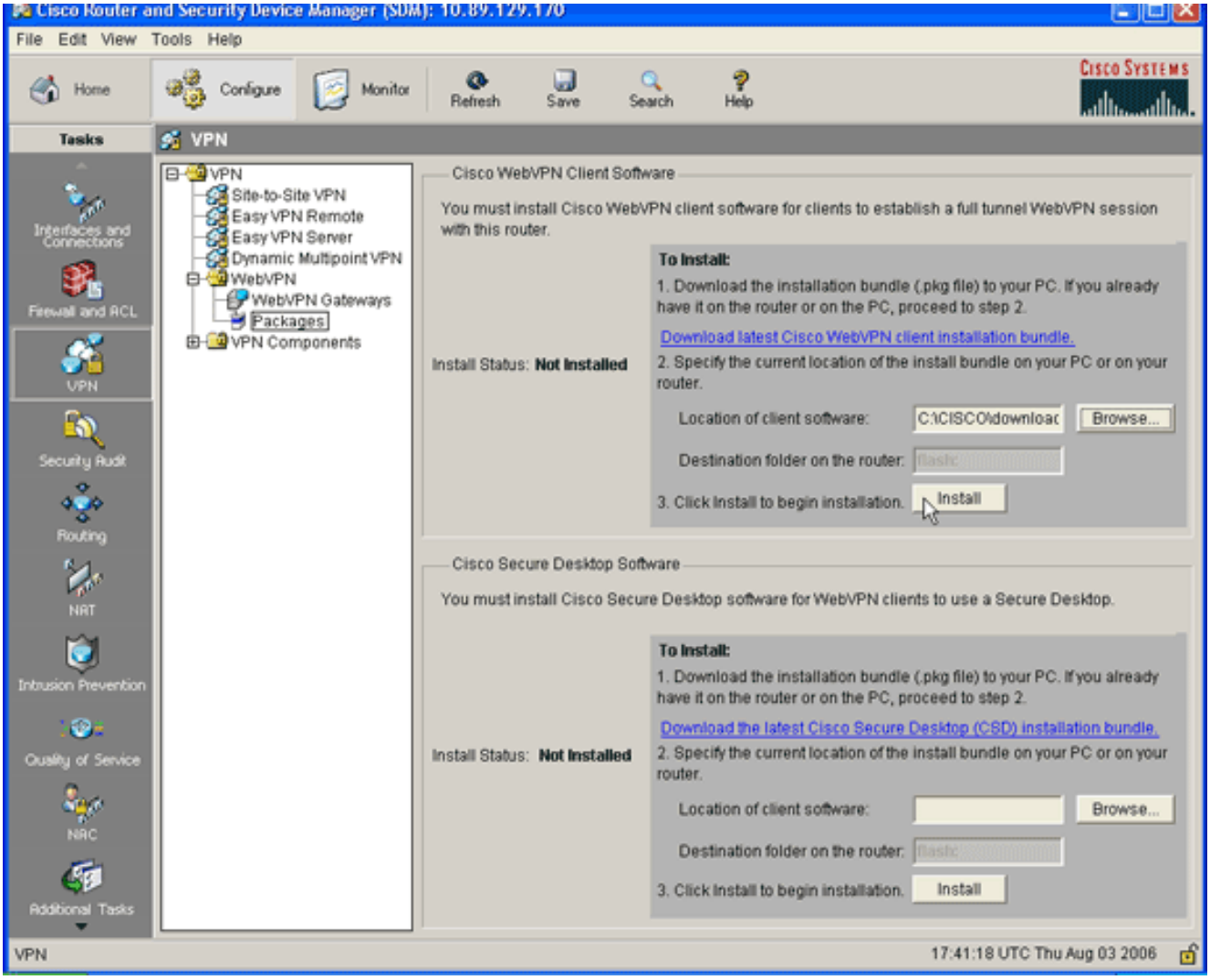
1. افتح تطبيق إدارة قاعدة بيانات المحول (SDM)، وانقر فوق **تكوين**، ثم انقر فوق **VPN**.
2. قم بتوسيع **WebVPN**، واختر **الحزم**.



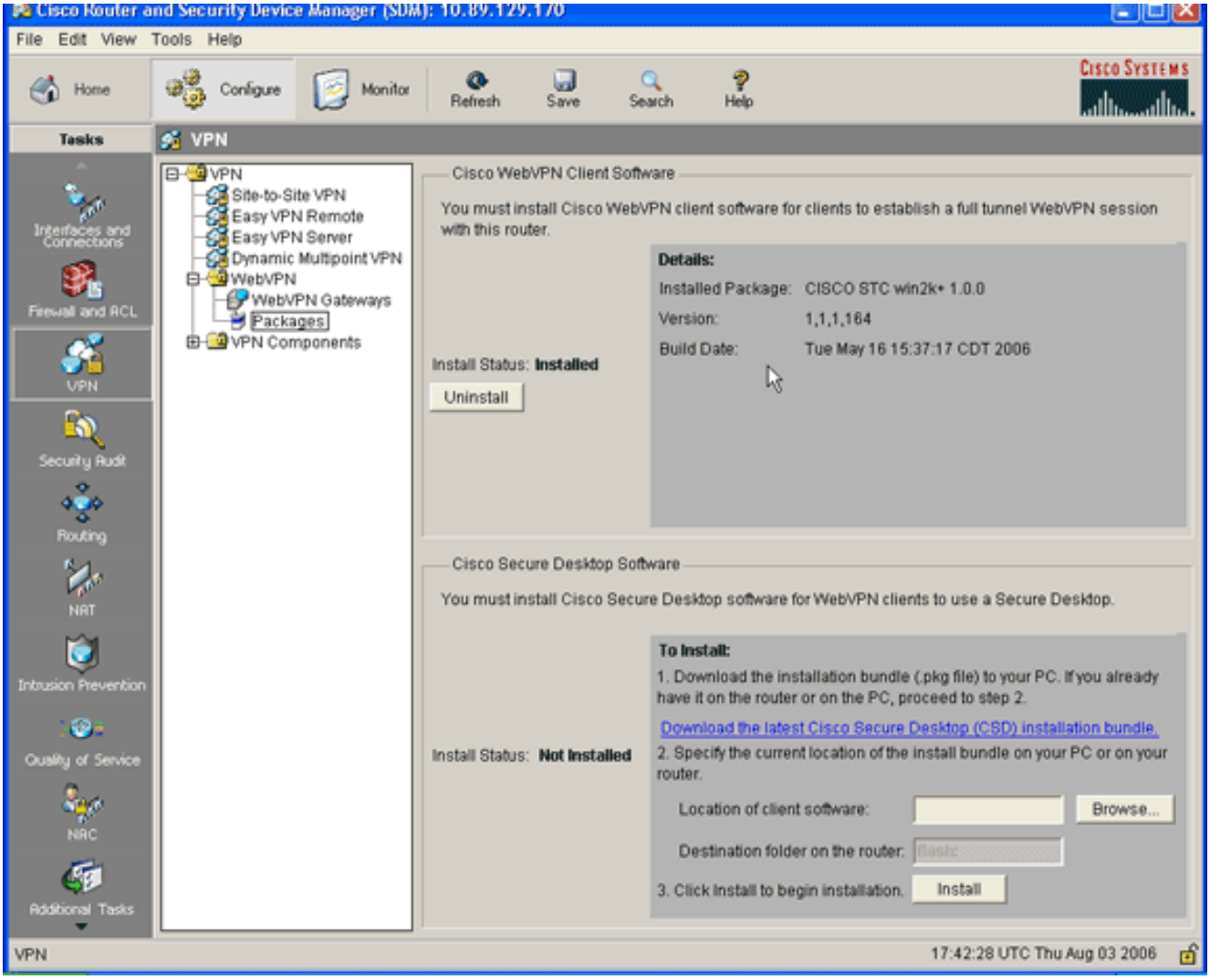
3. ضمن منطقة "برنامج عميل Cisco WebVPN"، انقر فوق الزر **إستعراض**.سوف يظهر مربع الحوار تحديد موقع SVC.



4. انقر فوق زر **راديو** My Computer"، ثم انقر فوق **إستعراض** لتحديد موقع حزمة SVC على كمبيوتر الإدارة الخاص بك.
5. انقر فوق **موافق**، ثم انقر فوق الزر **تثبيت**.



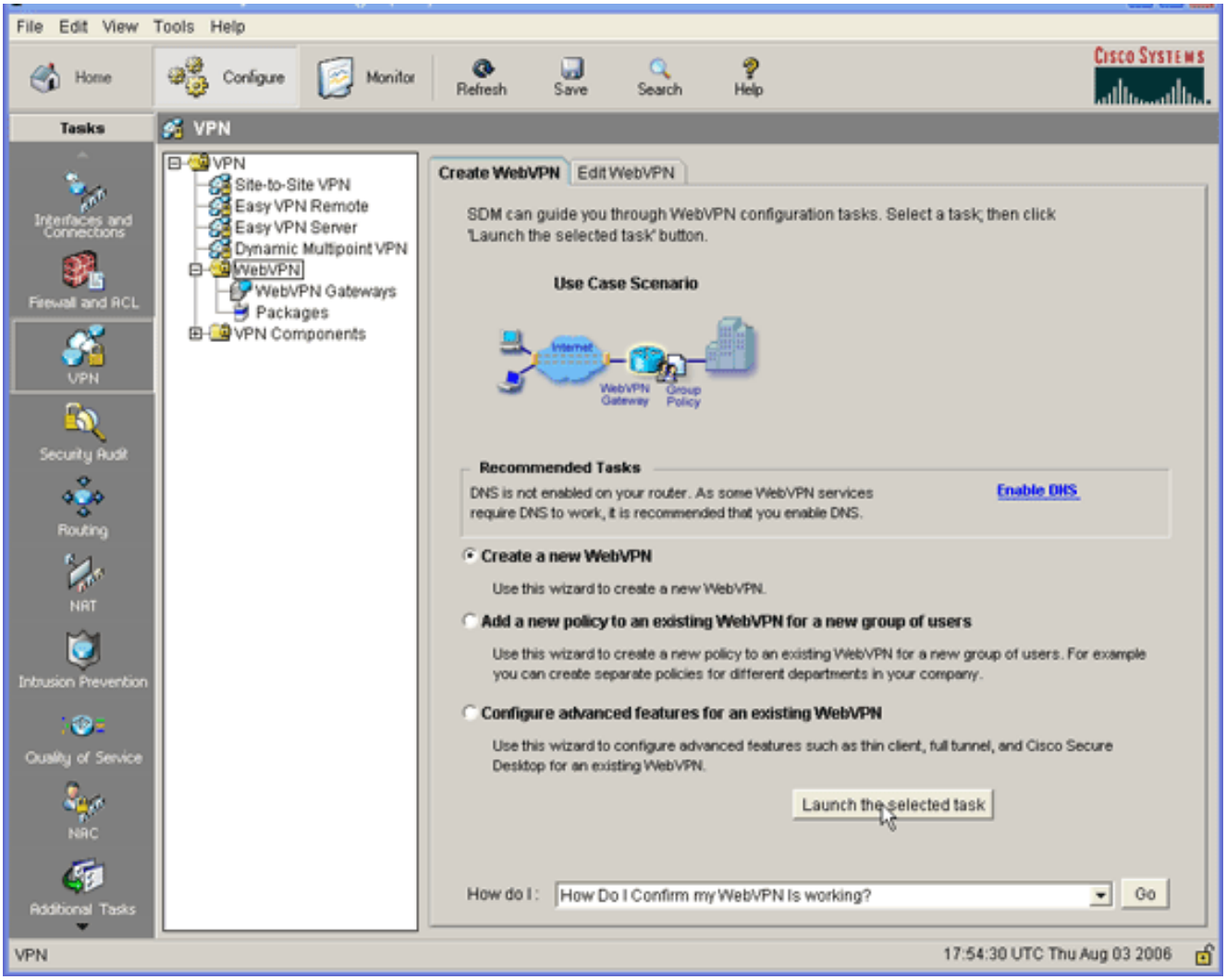
6. انقر فوق **نعم**، ثم انقر فوق **موافق**.يتم عرض تثبيت حزمة SVC بنجاح في هذه الصورة:



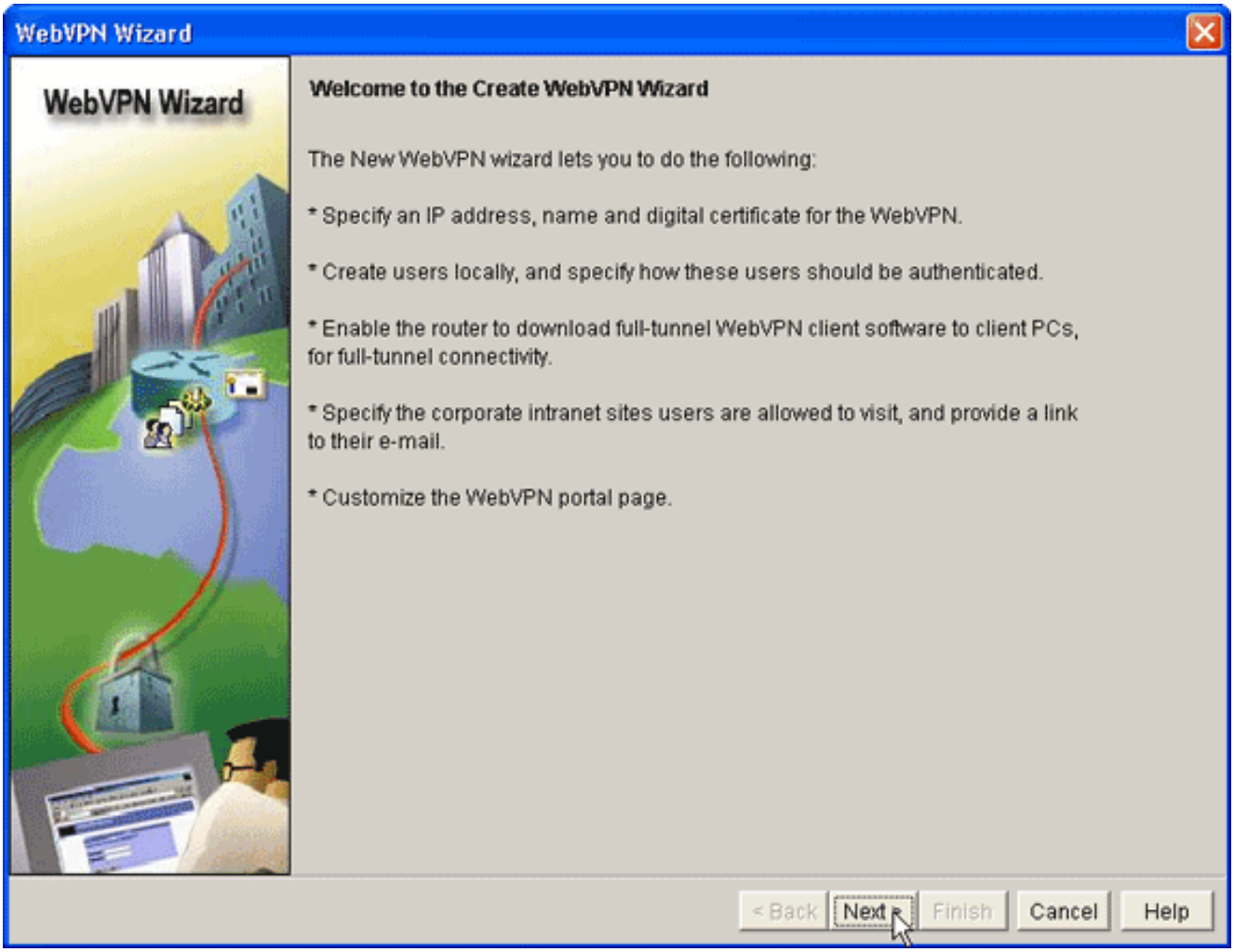
الخطوة 2. تكوين سياق WebVPN وبوابة WebVPN باستخدام معالج إدارة قاعدة بيانات المحول (SDM)

أكمل هذه الخطوات لتكوين سياق WebVPN وبوابة WebVPN:

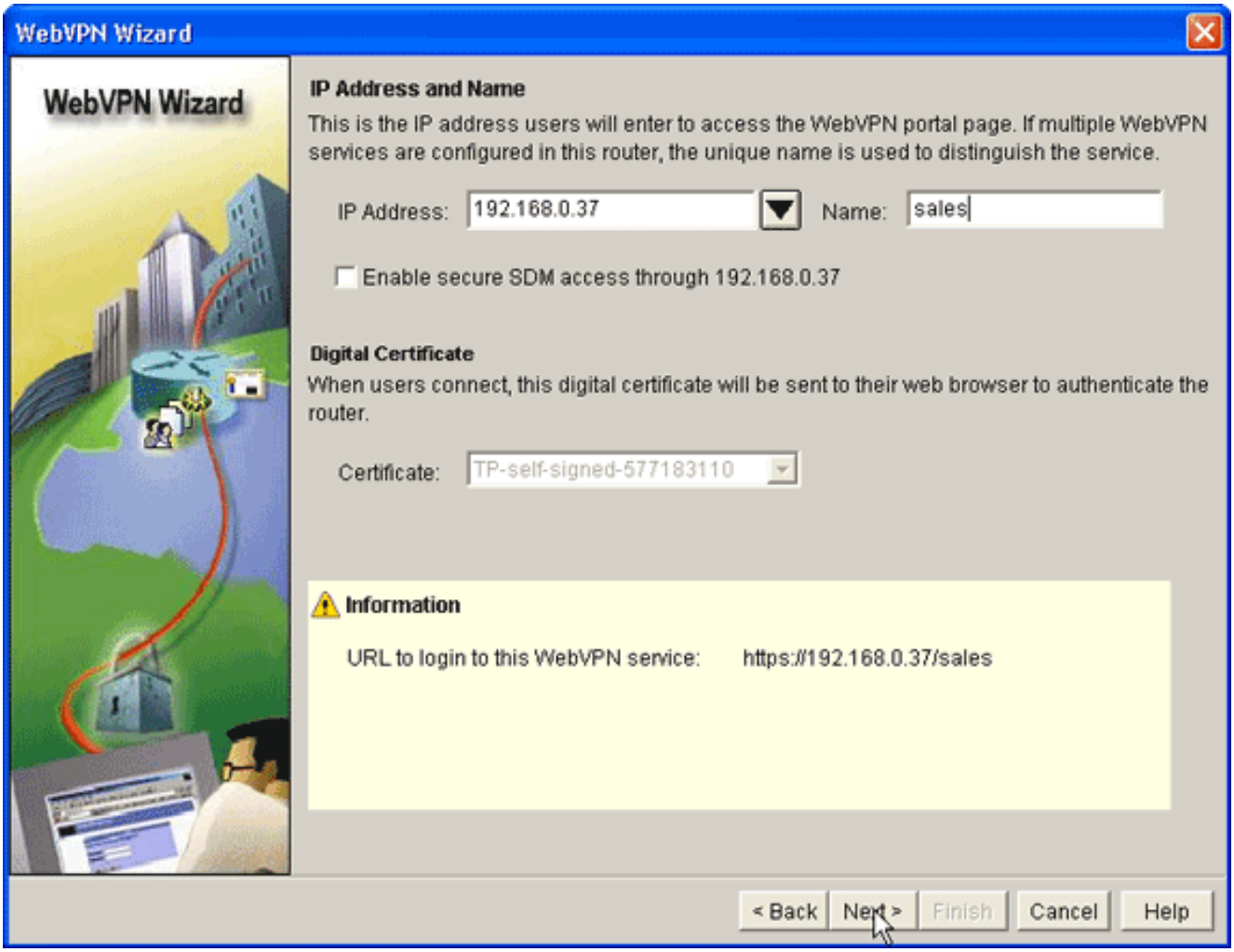
1. بعد تثبيت SVC على الموجه، انقر فوق **تكوين**، ثم انقر فوق **VPN**.
2. انقر فوق **WebVPN**، وانقر فوق علامة التبويب **إنشاء WebVPN**.



3. تحقق من زر **إنشاء** مرجع **WebVPN جديد**، ثم انقر فوق **تشغيل المهمة المحددة**.يظهر مربع الحوار معالج WebVPN.



4. انقر فوق **Next** (التالي).



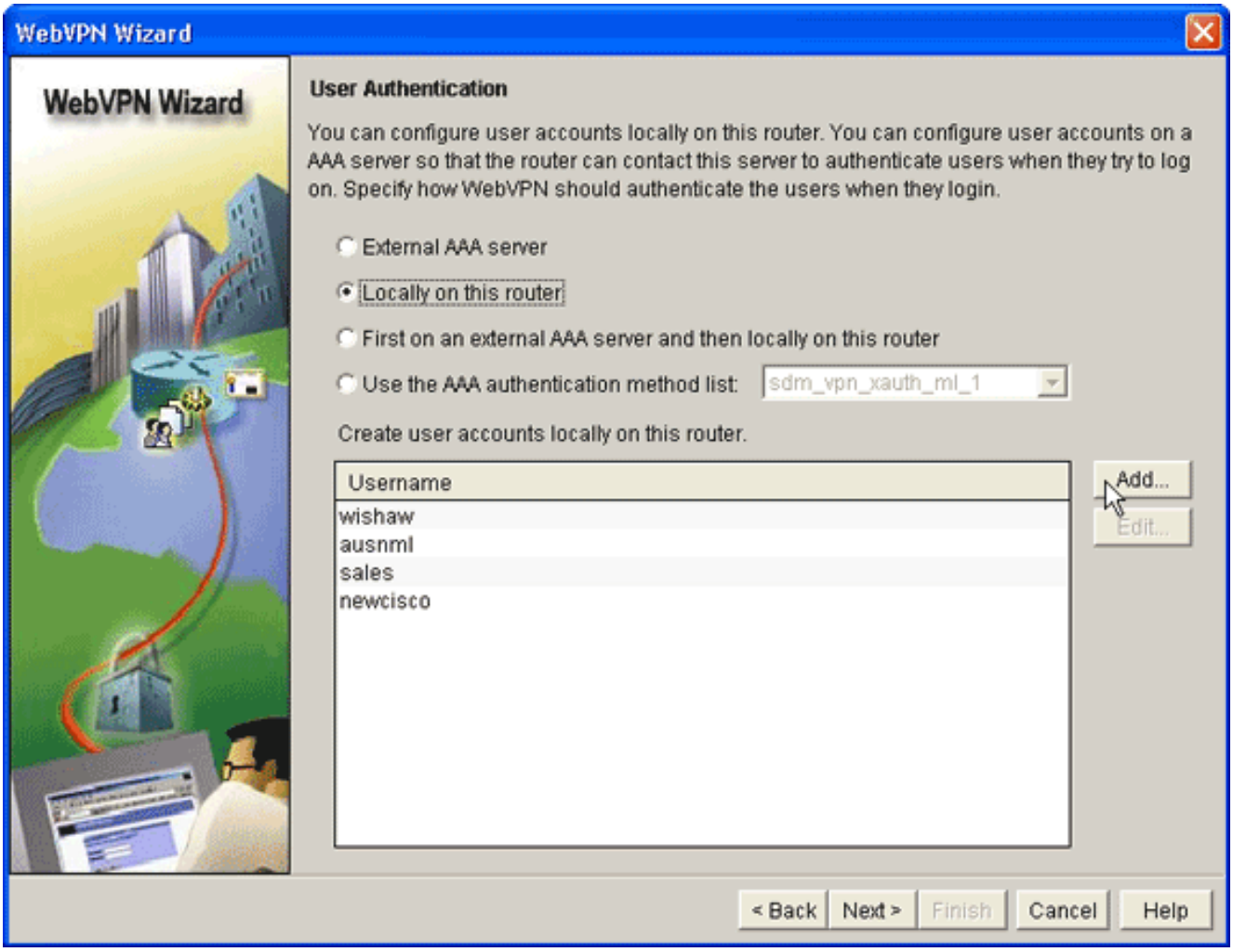
5. أدخل عنوان IP الخاص بوابة WebVPN الجديدة، وأدخل اسما فريدا لسياق WebVPN هذا.يمكنك إنشاء سياقات WebVPN مختلفة لنفس عنوان IP (عبارة WebVPN)، ولكن يجب أن يكون كل اسم فريدا. يستعمل هذا مثال هذا عنوان: *https://192.168.0.37/sales*
6. طقطقت **بعد ذلك**، واستمر إلى خطوة 3.

الخطوة 3. تكوين قاعدة بيانات المستخدم لمستخدمي SVC

للمصادقة، يمكنك إستخدام خادم AAA أو المستخدمين المحليين أو كليهما. يستخدم مثال التكوين هذا المستخدمين الذين تم إنشاؤها محليا للمصادقة.

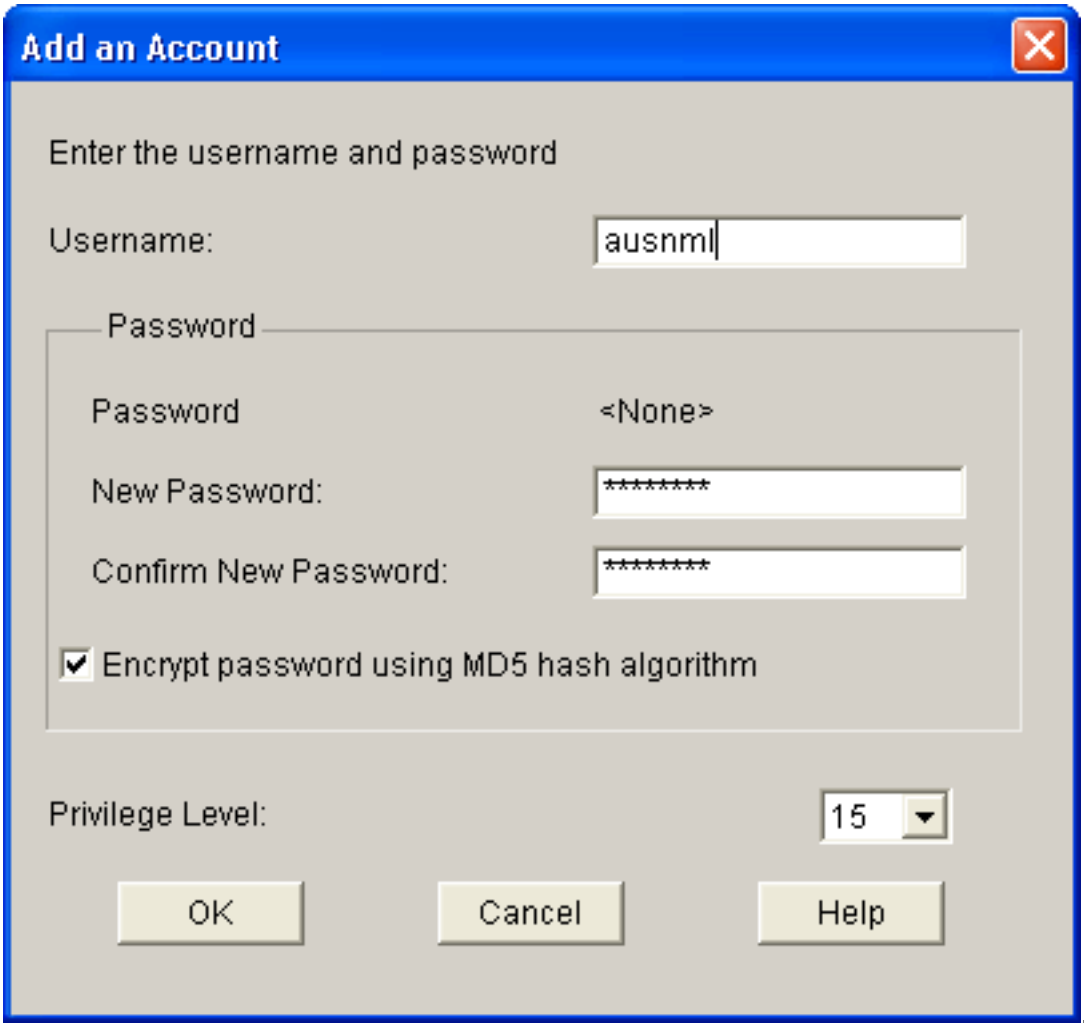
أتمت هذا steps in order to شكلت المستعمل قاعدة معطيات ل SVC مستعمل:

1. بعد اكتمال الخطوة 2، انقر فوق الزر **المحلي الموجود على** راديو **الموجه هذا** الموجود في مربع حوار مصادقة المستخدم لمعالج WebVPN.



يسمح لك مربع الحوار هذا بإضافة مستخدمين إلى قاعدة البيانات المحلية.

2. انقر فوق **إضافة**، وأدخل معلومات



المستخدم.

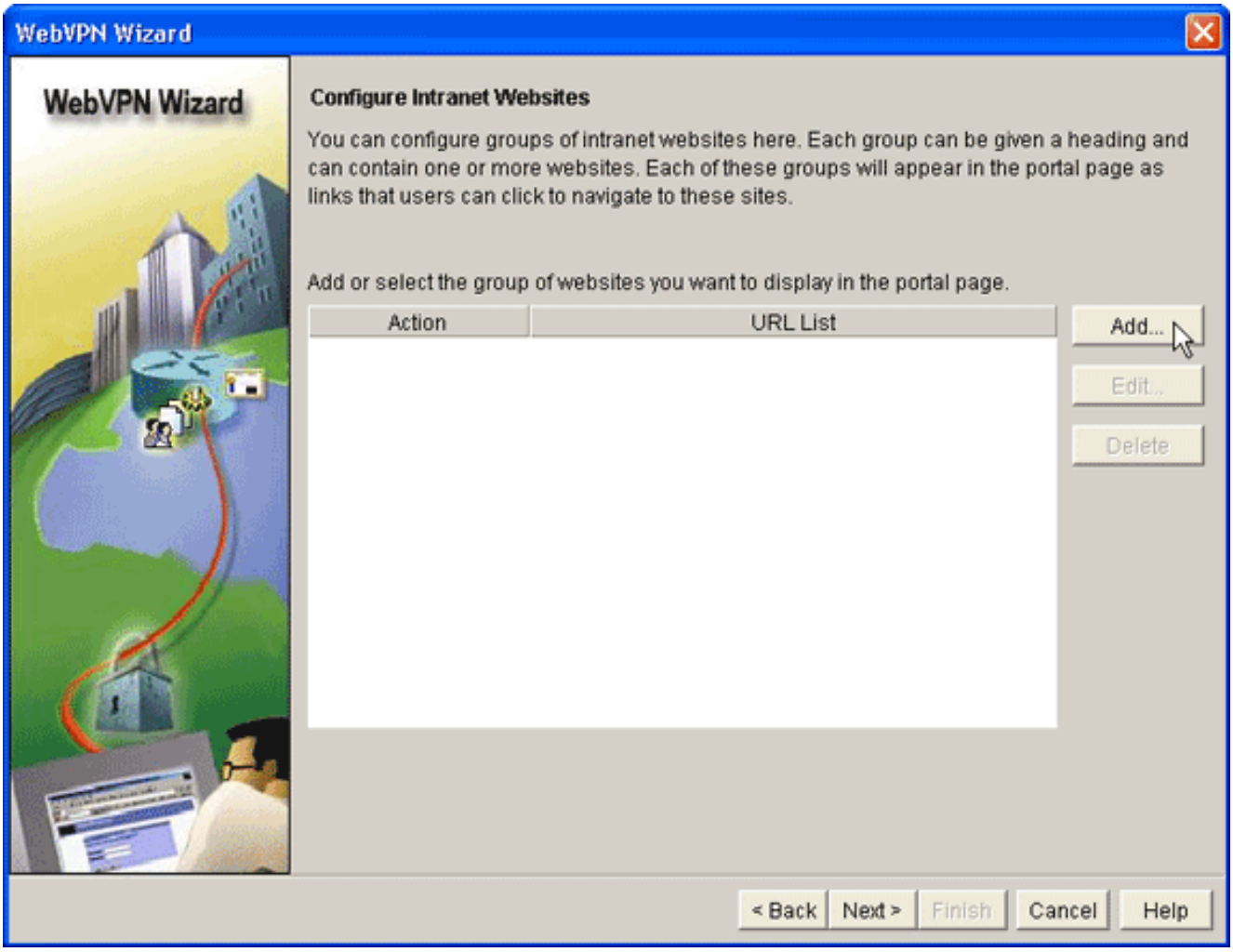
3. انقر فوق **موافق**، وقم بإضافة مستخدمين إضافيين حسب الضرورة.
4. بعد إضافة المستخدمين الضروريين، انقر فوق **التالي**، وتابع إلى الخطوة 4.

الخطوة 4. تكوين الموارد للتعريف للمستخدمين

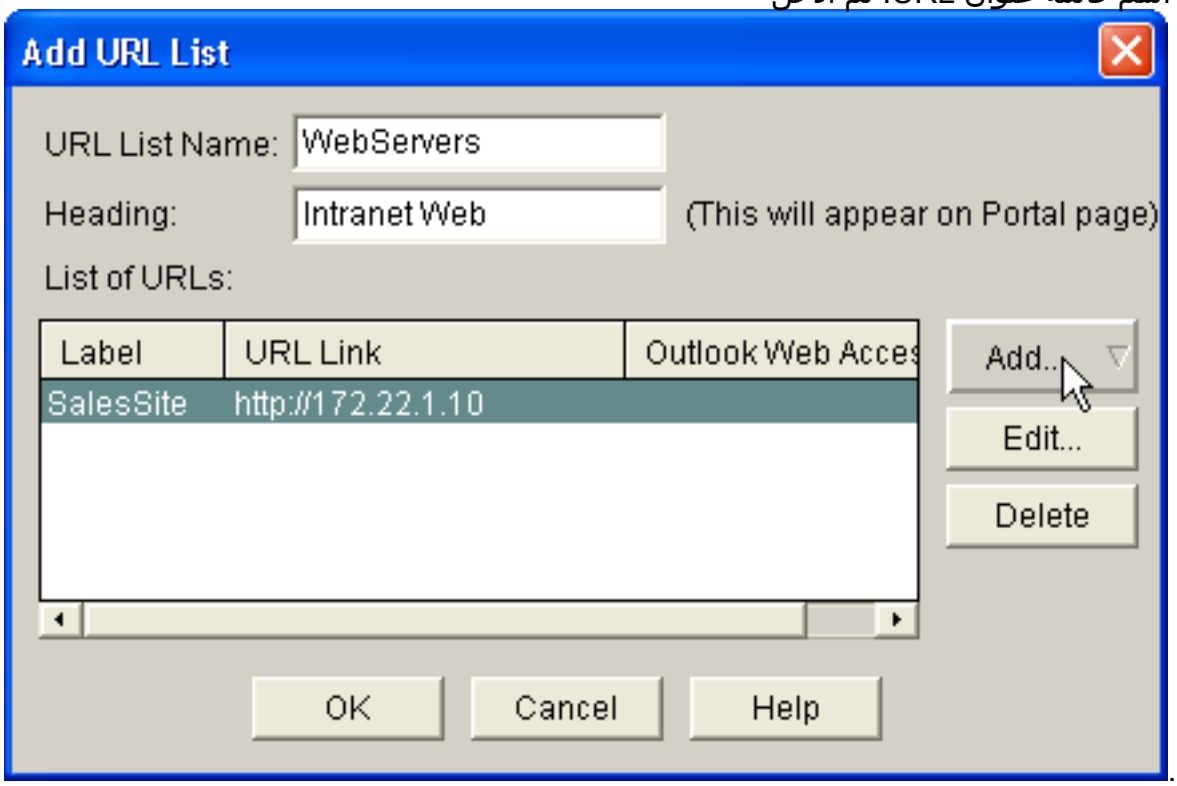
يتيح لك مربع الحوار "معالج تكوين مواقع ويب إنترانت على WebVPN" تحديد موارد إنترانت التي تريد عرضها على عملاء SVC.

أتمت هذا steps in order to شكلت الموارد أن يعرض إلى مستعمل:

1. بعد اكتمال الخطوة 3، انقر فوق الزر **إضافة** الموجود في مربع الحوار تكوين مواقع ويب على إنترانت.

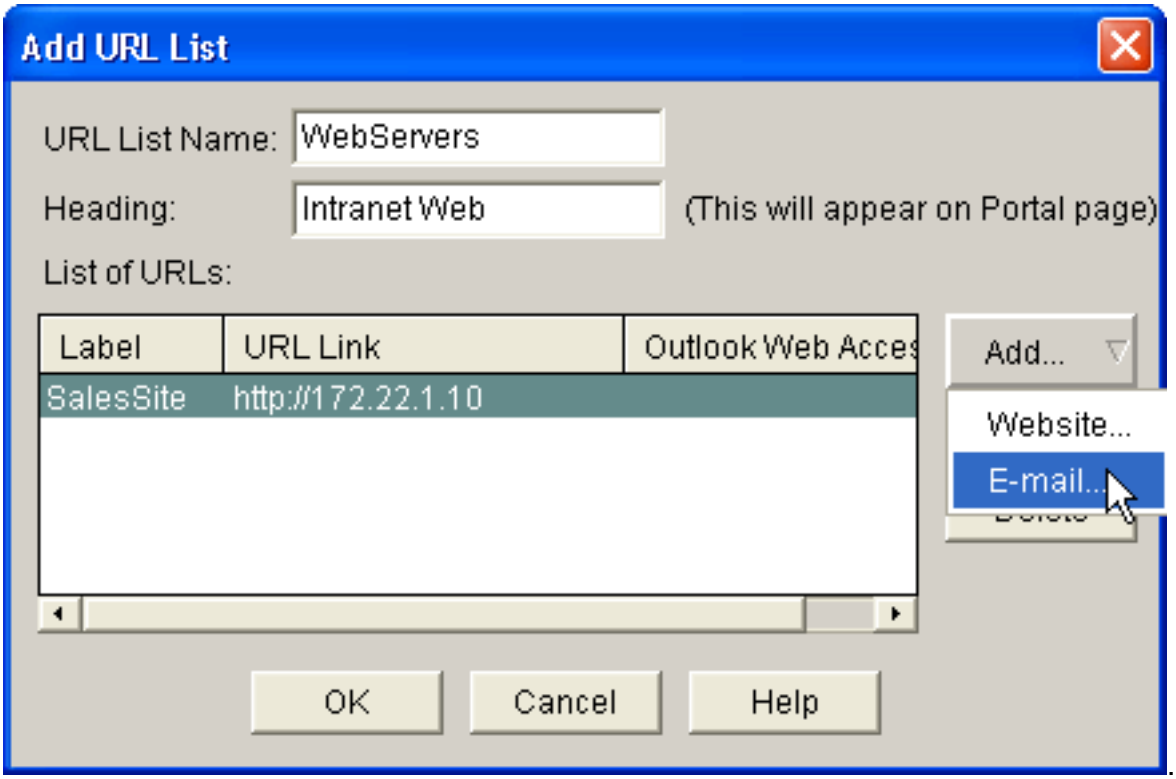


2. أدخل اسم قائمة عنوان URL، ثم أدخل



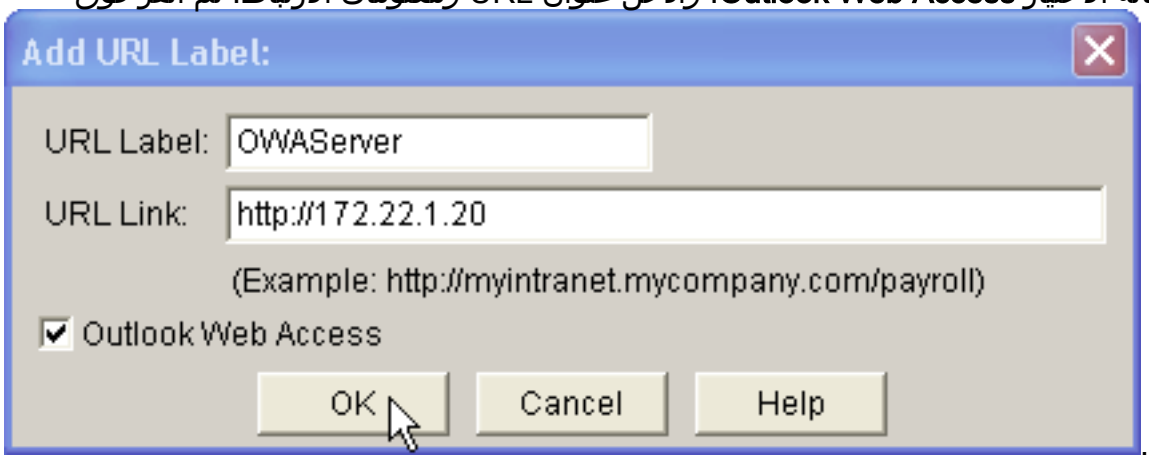
عنوانا.

3. انقر فوق **إضافة**، واختر **موقع ويب** لإضافة مواقع الويب التي تريد كشفها إلى هذا العميل.
4. أدخل معلومات عنوان URL والربط، ثم انقر فوق **موافق**.
5. لإضافة وصول إلى خوادم Exchange الخاصة ب OWA، انقر فوق **إضافة** واختر **البريد**



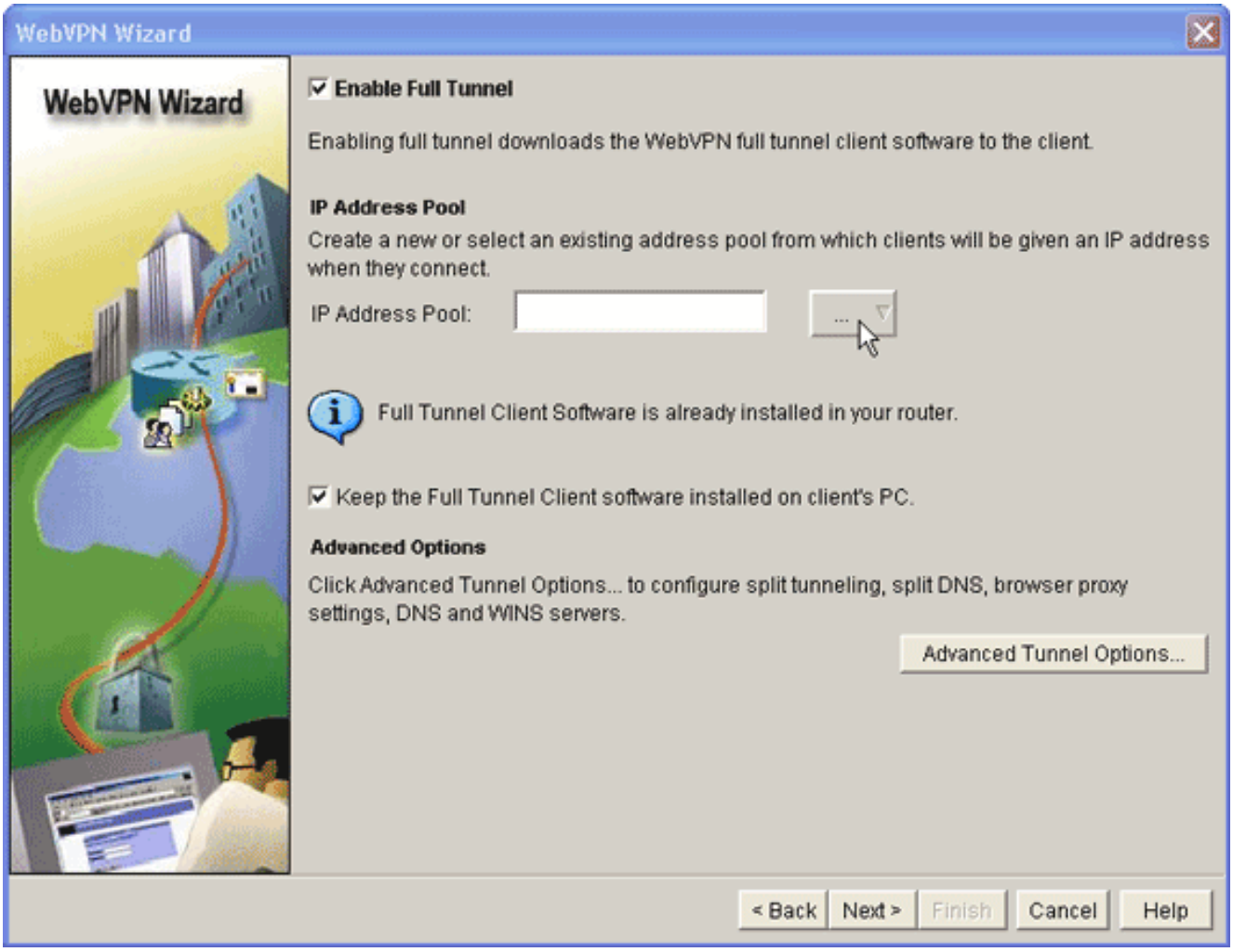
الإلكتروني.

6. حدد خانة الاختيار **Outlook Web Access**، وأدخل عنوان URL ومعلومات الارتباط، ثم انقر فوق

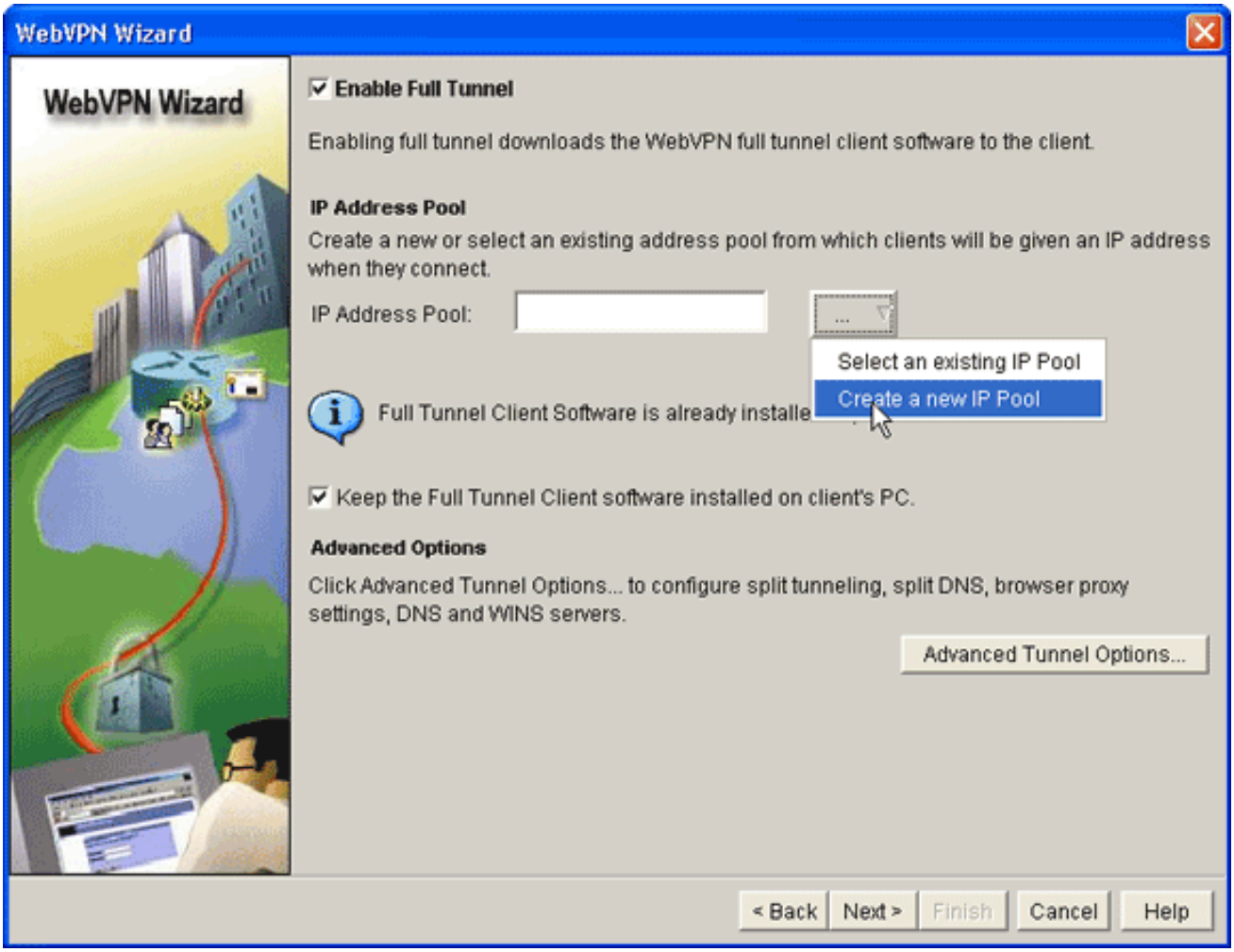


موافق.

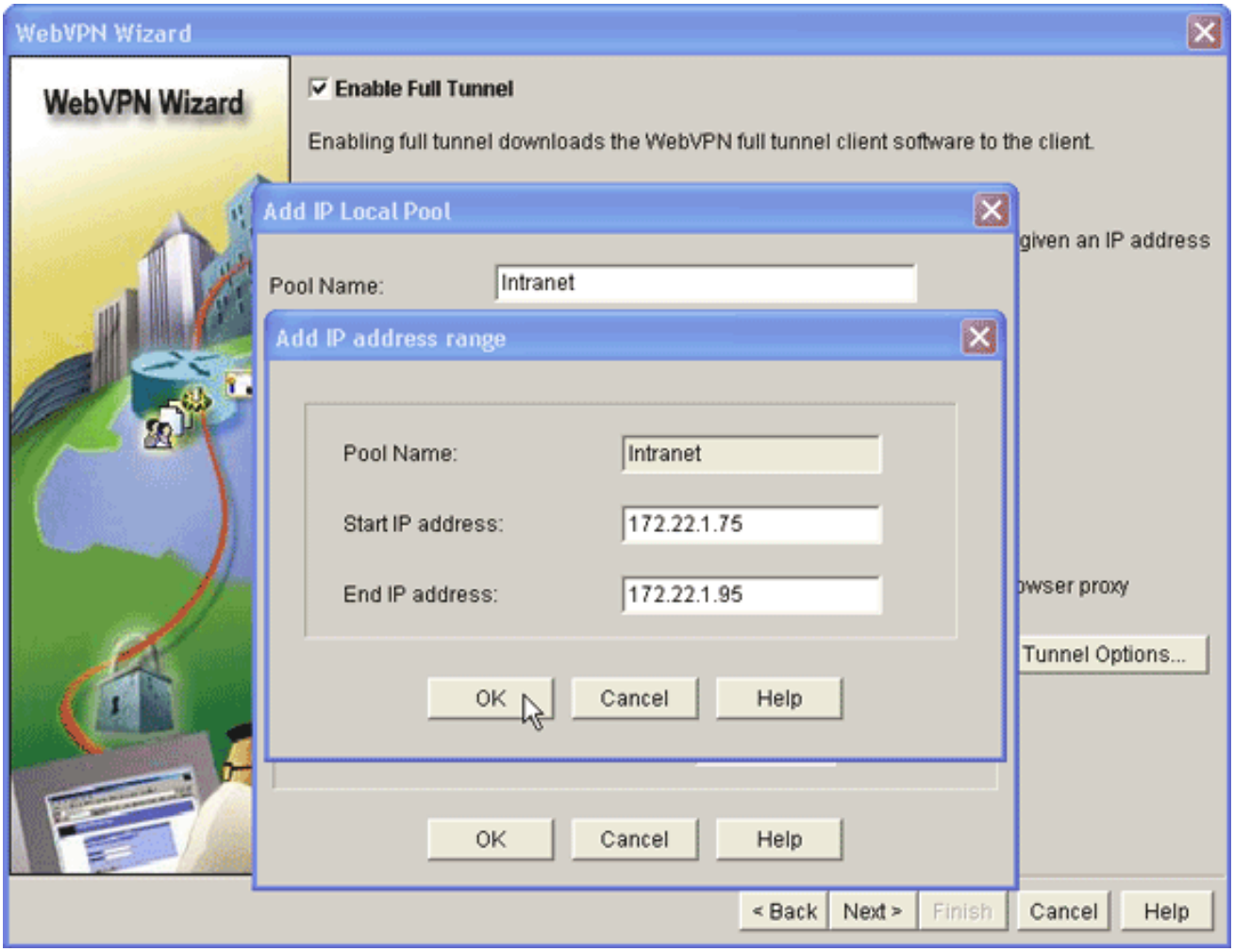
7. بعد إضافة الموارد المطلوبة، انقر فوق **موافق**، ثم انقر فوق **التالي**.يظهر مربع حوار النفق الكامل لمعالج WebVPN.



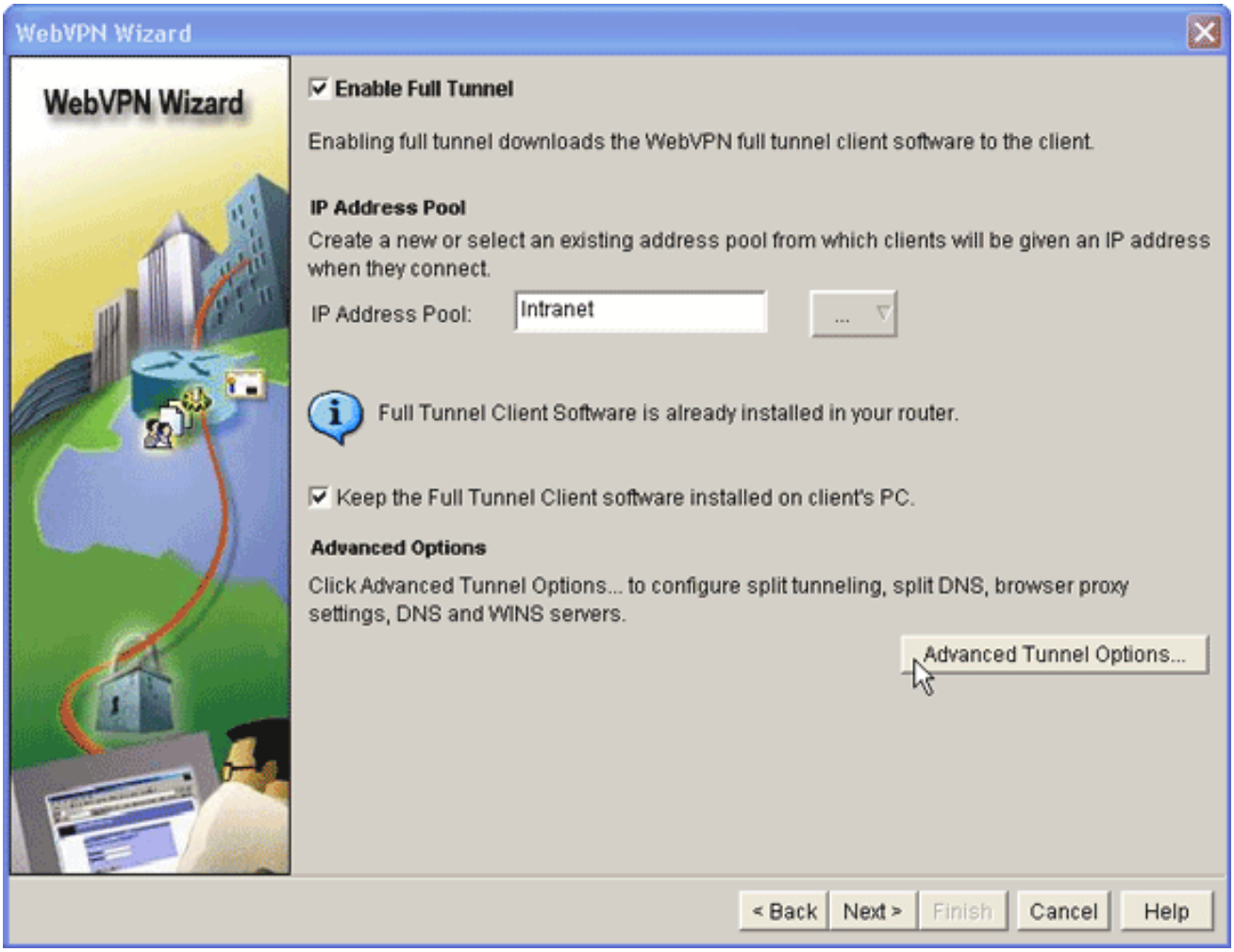
8. تحقق من تحديد خانة الاختيار **تمكين النفق الكامل**.
9. قم بإنشاء تجمع لعناوين IP يمكن لعملاء سياق WebVPN هذا إستخدامها. يجب أن يتوافق تجمع العناوين مع العناوين المتاحة والموجهة على إنترانت.
10. انقر فوق العناصر الناقصة (..) المجاورة لحقل تجمع عناوين IP، واختر **إنشاء تجمع IP جديد**.



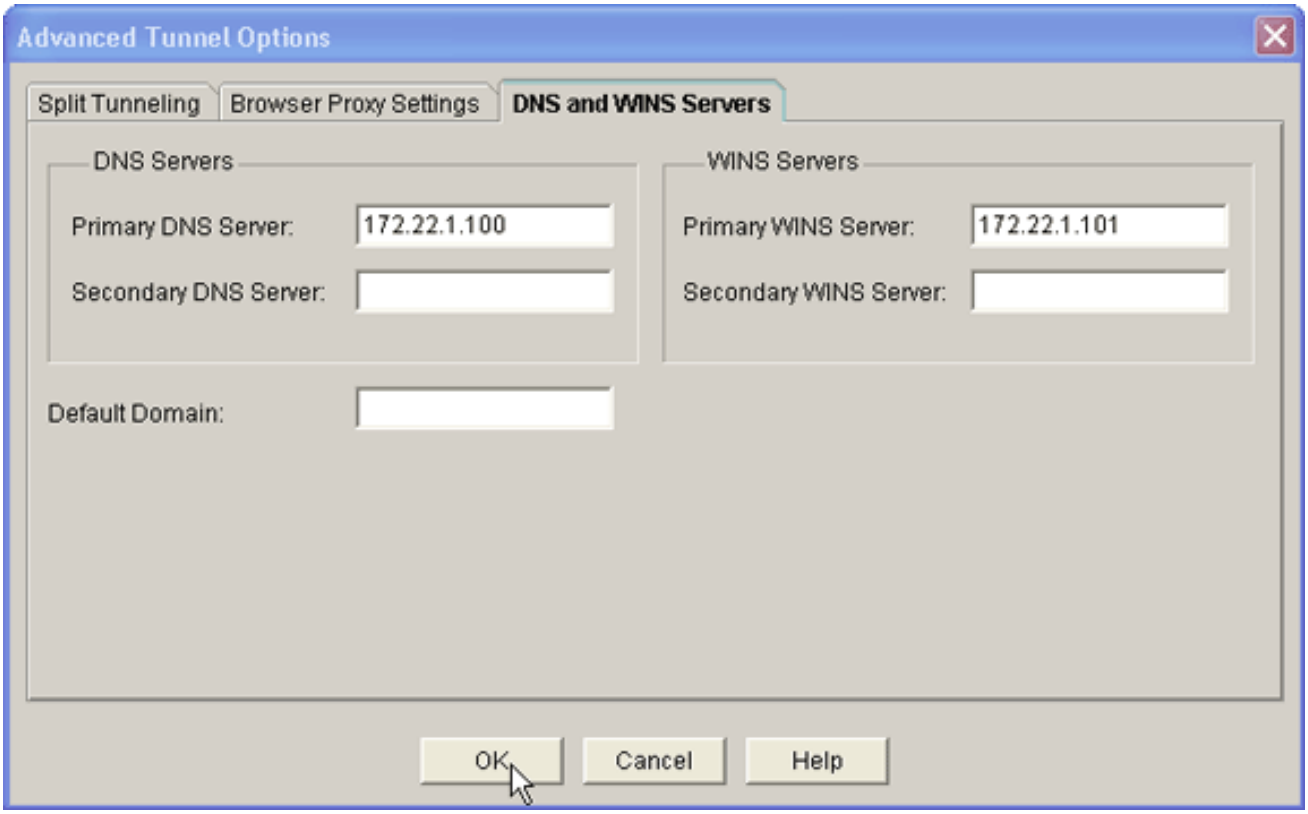
11. في شاشة إضافة تجمع IP المحلي، أدخل اسما للتجمع، وانقر **إضافة**.



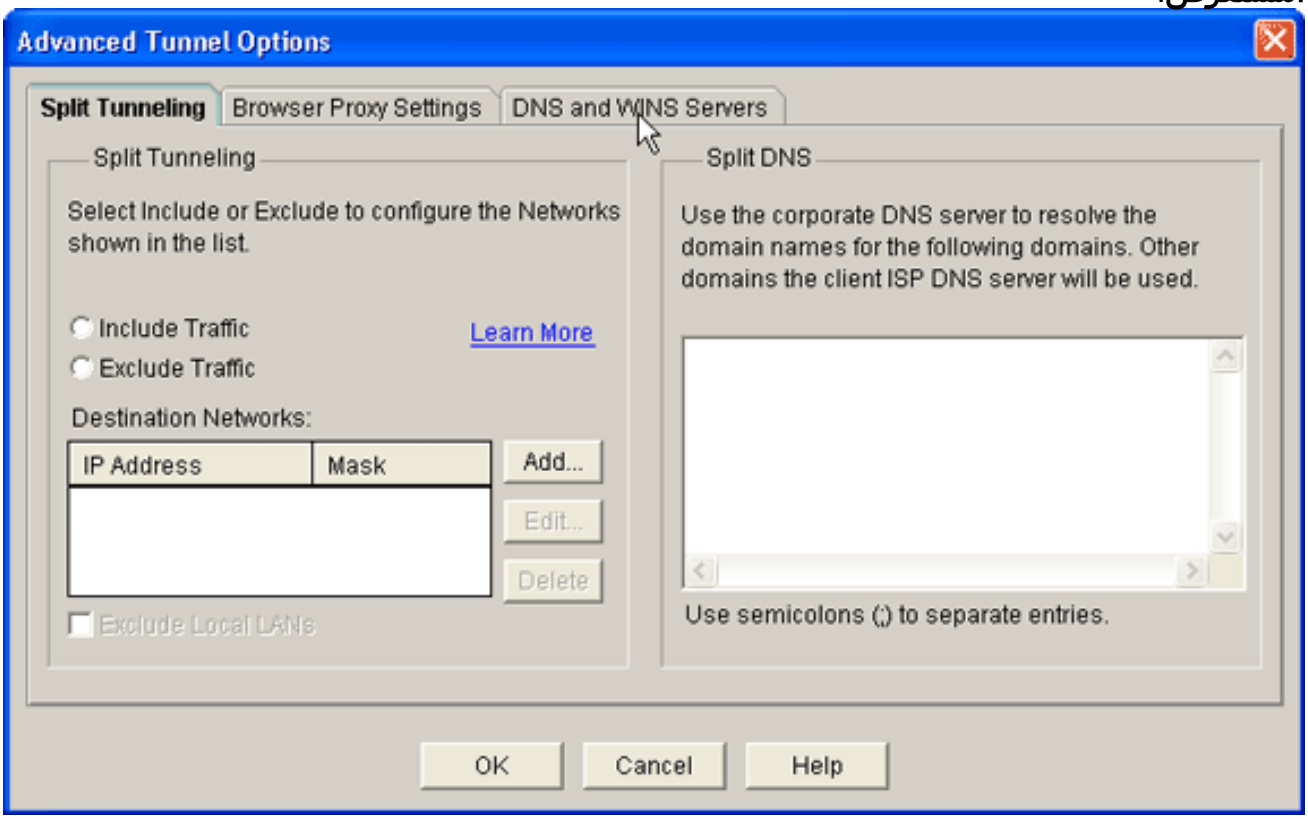
12. في شاشة إضافة نطاق عنوان IP، أدخل نطاق تجمع العناوين لعملاء SVC، وانقر **موافق**.**ملاحظة:** يجب أن يكون تجمع عناوين IP في نطاق واجهة متصلة مباشرة بالموجه. إذا كنت ترغب في إستخدام نطاق تجمع مختلف، فيمكنك إنشاء عنوان إسترجاع مقترن بالتجمع الجديد لتلبية هذا المتطلب.
13. وانقر فوق
.**OK**



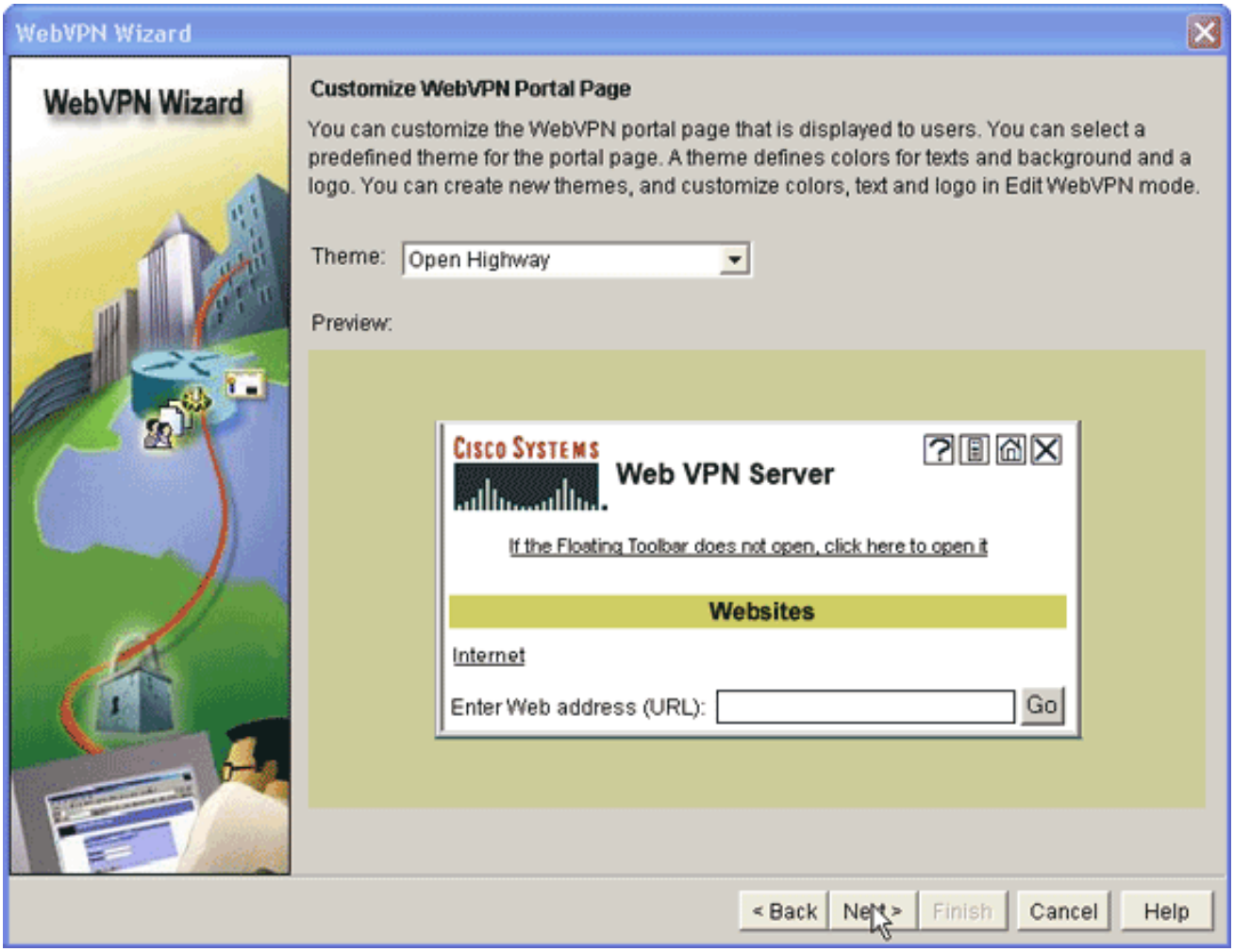
14. إذا كنت تريد أن يقوم عملاؤك البعيدين بتخزين نسخة من SVC بشكل دائم، فانقر فوق خانة الاختيار **الاحتفاظ ببرنامج عميل النفق الكامل مثبتا على كمبيوتر العميل**. امسح هذا الخيار لتطلب من العميل تنزيل برنامج SVC في كل مرة يتصل فيها العميل.
15. تكوين خيارات النفق المتقدمة، مثل تقسيم الاتصال النفقي، و DNS المقسم، وإعدادات وكيل المستعرض، وخوادم DNS و WNS. cisco يوصي أنت يشكل على الأقل DNS و WINS نادل.لتكوين خيارات النفق المتقدمة، أكمل الخطوات التالية:انقر فوق زر **خيارات النفق المتقدمة**.



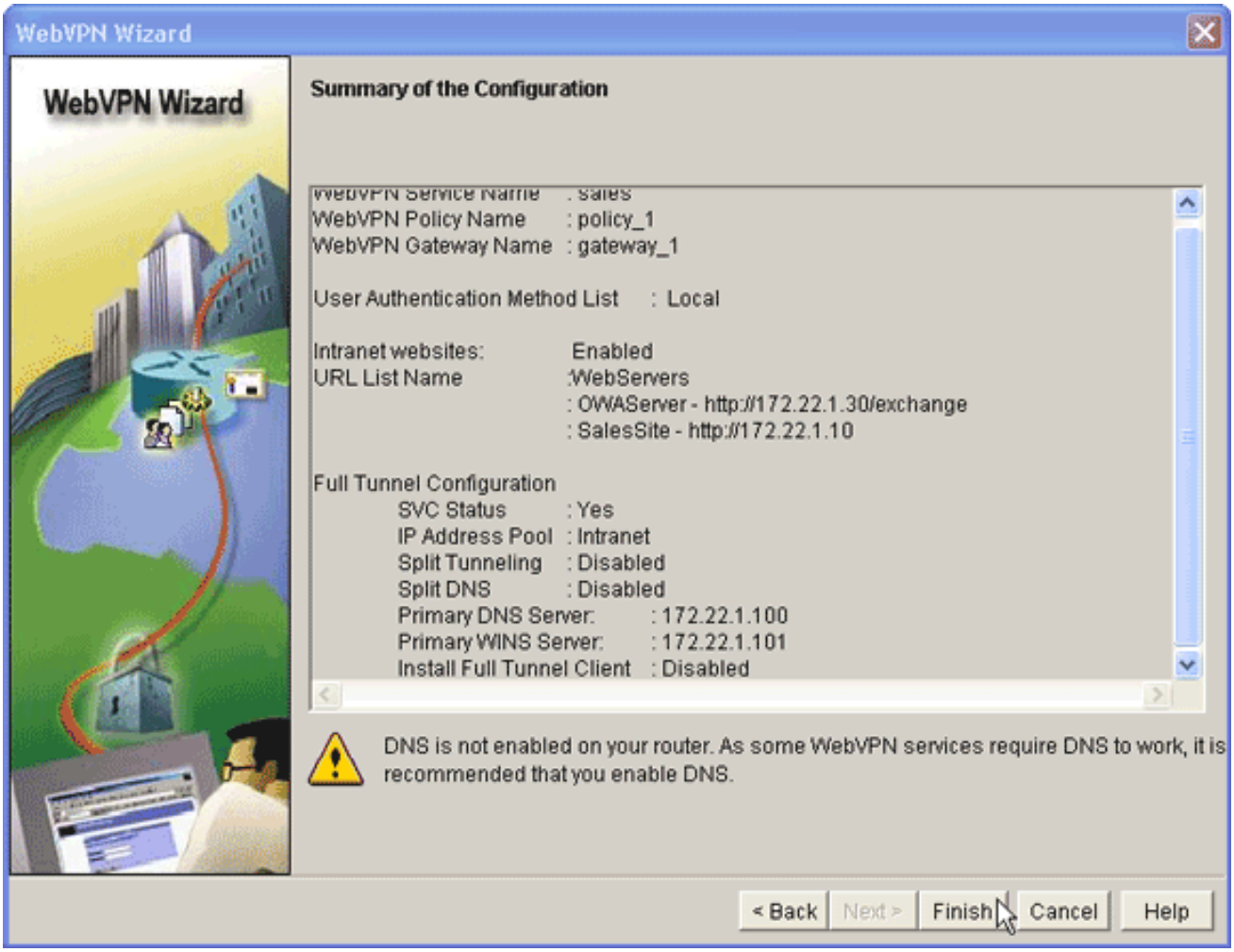
انقر فوق علامة التبويب **خوادم DNS و WINS**، وأدخل عناوين IP الأساسية لخوادم DNS و WINS.لتكوين إعدادات تقسيم الاتصال النفقي ووكيل المستعرض، انقر فوق علامة التبويب **تقسيم الاتصال النفقي** أو **إعدادات وكيل المستعرض**.



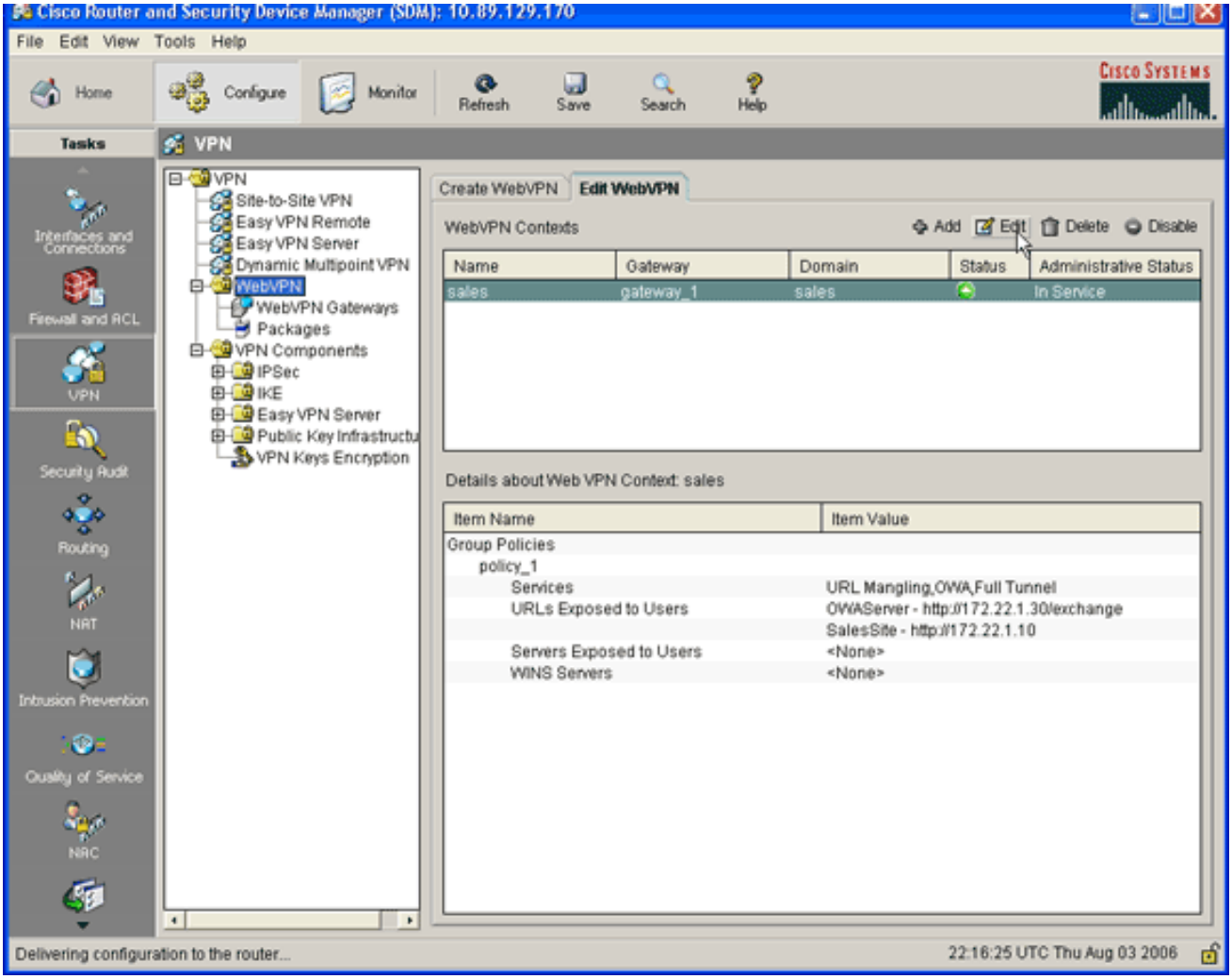
16. بعد أن تقوم بتكوين الخيارات الضرورية، انقر فوق **التالي**.
17. تخصيص صفحة مدخل WebVPN أو تحديد القيم الافتراضية.تتيح لك صفحة "تخصيص مدخل WebVPN" تخصيص كيفية ظهور صفحة مدخل WebVPN لعملائك.



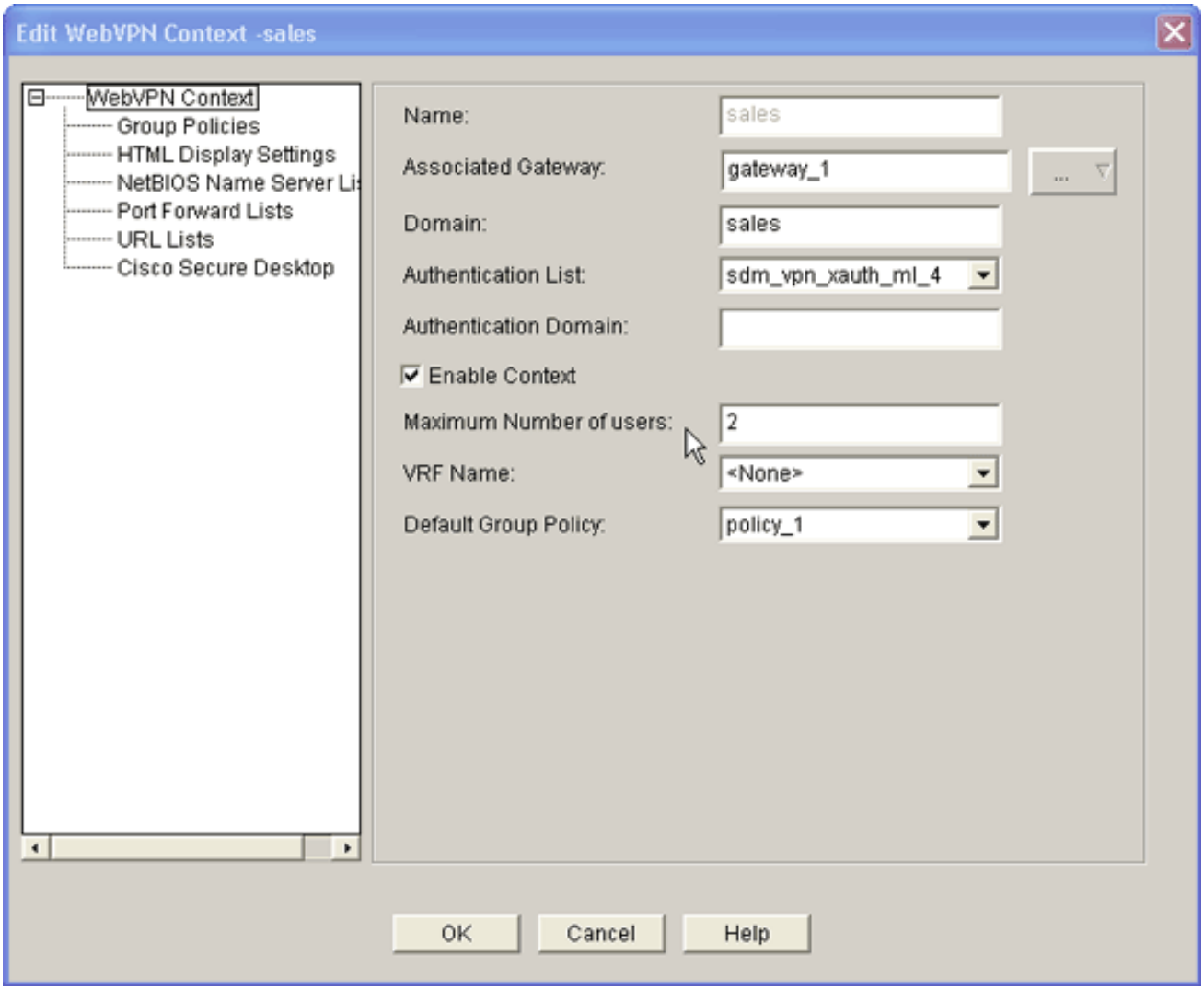
18. بعد تكوين صفحة مدخل WebVPN، انقر فوق **التالي**، ثم انقر فوق **إنهاء**، ثم انقر فوق **موافق**.يرسل معالج WebVPN أوامر جولة إلى الموجه.
19. انقر فوق **موافق** لحفظ التكوين الخاص بك.**ملاحظة:** إذا تلقيت رسالة خطأ، فقد يكون ترخيص WebVPN غير صحيح. تظهر رسالة خطأ نموذجية في هذه الصورة:



لتصحيح مشكلة ترخيص، أكمل الخطوات التالية:طقطقت **يشكل**، وبعد ذلك طقطقت **VPN**.قم بتوسيع **WebVPN**، وانقر فوق علامة التبويب **Edit** **WebVPN**.



قم بتمييز السياق الذي تم إنشاؤه حديثا، وانقر فوق الزر **تحرير**.



في حقل الحد الأقصى لعدد المستخدمين، أدخل العدد الصحيح للمستخدمين للترخيص الخاص بك.طقطقت **ok**، وبعد ذلك طقطقت **ok**.تتم كتابة الأوامر الخاصة بك إلى ملف التكوين.انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

النتائج

يقوم ASDM بإنشاء تكوينات سطر الأوامر هذه:

أوسن01-ml-3825

```
ausnml-3825-01#show run
...Building configuration

Current configuration : 4393 bytes
!
Last configuration change at 22:24:06 UTC Thu Aug 3 !
2006 by ausnml
NVRAM config last updated at 22:28:54 UTC Thu Aug 3 !
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
```

```
                                                boot-start-marker
 boot system flash c3825-adventerprisek9-mz.124-9.T.bin
                                                  boot-end-marker
                                                                !
                                             no logging buffered
                                                                !
                                                   aaa new-model
                                                                !
    Added by SDM for local aaa authentication. aaa ---!
      authentication login sdm_vpn_xauth_ml_1 local aaa
      authentication login sdm_vpn_xauth_ml_2 local aaa
      authentication login sdm_vpn_xauth_ml_3 local aaa
    authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
   name cisco.com ! voice-card 0 no dspfarm !--- Digital
 certificate information. crypto pki trustpoint TP-self-
    signed-577183110 enrollment selfsigned subject-name
   cn=IOS-Self-Signed-Certificate-577183110 revocation-
 check none rsakeypair TP-self-signed-577183110 ! crypto
         pki certificate chain TP-self-signed-577183110
   certificate self-signed 01 3082024E 308201B7 A0030201
   02020101 300D0609 2A864886 F70D0101 04050030 30312E30
   2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
   43657274 69666963 6174652D 35373731 38333131 30301E17
   0D303630 37323731 37343434 365A170D 32303031 30313030
   30303030 5A303031 2E302C06 03550403 1325494F 532D5365
   6C662D53 69676E65 642D4365 72746966 69636174 652D3537
   37313833 31313030 819F300D 06092A86 4886F70D 01010105
   0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
  suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
 15 password 7 044E1F505622434B username sales privilege
    15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
                          newcisco privilege 15 secret 5
            $1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
 ip virtual-reassembly duplex auto speed auto media-type
    rj45 no keepalive ! interface GigabitEthernet0/1 ip
   address 172.22.1.151 255.255.255.0 duplex auto speed
   auto media-type rj45 !--- Clients receive an address
     from this pool. ip local pool Intranet 172.22.1.75
   172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
      server ip http timeout-policy idle 600 life 86400
   requests 100 ! control-plane ! line con 0 stopbits 1
 line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
   20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
    inservice !--- SVC package file. webvpn install svc
    flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
 context sales title-color #CCCC66 secondary-color white
    text-color black ssl authenticate verify all ! !---
         Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
   value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
        for the context. policy group policy_1 url-list
    "WebServers" functions svc-enabled svc address-pool
    "Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
   wins-server primary 172.22.1.101 default-group-policy
```

```
     policy_1 aaa authentication list sdm_vpn_xauth_ml_4
gateway gateway_1 domain sales max-users 2 inservice ! !
                                                      end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الإجراء

لاختبار التكوين الخاص بك، أدخل *http://192.168.0.37/sales* في مستعرض ويب لعميل تم تمكين SSL له.

الأوامر

يتم إقران العديد من أوامر **العرض** مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات ومعلومات أخرى. للحصول على معلومات تفصيلية حول **أوامر العرض**، ارجع إلى التحقق من تكوين WebVPN.

ملاحظة: الإنتاج مترجم يساند أداة (يسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

مشكلة في اتصال SSL

مشكلة: يتعذر على عملاء SSL VPN توصيل الموجه.

الحل: قد تتسبب عناوين IP غير الكافية في تجمع عناوين IP في هذه المشكلة. قم بزيادة عدد عناوين IP في تجمع عناوين IP على الموجه لحل هذه المشكلة.

أوامر استكشاف الأخطاء وإصلاحها

يتم إقران العديد من أوامر **المسح** مع WebVPN. للحصول على معلومات تفصيلية حول هذه الأوامر، ارجع إلى إستخدام أوامر مسح WebVPN.

تقترن العديد من أوامر **تصحيح الأخطاء** ب WebVPN. للحصول على معلومات تفصيلية حول هذه الأوامر، ارجع إلى إستخدام أوامر تصحيح الأخطاء ل WebVPN.

ملاحظة: يمكن أن يؤثر إستخدام أوامر **تصحيح الأخطاء سلبا** على جهاز Cisco الخاص بك. قبل إستخدام أوامر **debug**، ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء.

معلومات ذات صلة

- Cisco من IOS SSLVPN
- SSL VPN - WebVPN
- SDM مع مثال تكوين Cisco IOS على (ClientWithout SSL VPN (WebVPN

- مثال تكوين IOS للعميل قليل السمك (WebVPN SSL VPN) مع SDM
- دليل نشر تقارب WebVPN و DMVPN
- 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).