

SDM عم Cisco IOS (WebVPN) SSL VPN نيوكت

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [المهمة](#)
- [الرسم التخطيطي للشبكة](#)
- [تكوين شبكة VPN الخاصة بـ SSL Thin-Client التكوين](#)
- [التحقق من الصحة](#)
- [التحقق من التكوين](#)
- [الأوامر](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [الأوامر المستخدمة لاستكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يمكن استخدام تقنية Thin-Client SSL VPN للسماح بالوصول الآمن للتطبيقات التي تستخدم المنافذ الثابتة. الأمثلة هي (23 Telnet و (22 SSH و (110 POP3 و (143 IMAP4 و (25 SMTP). يمكن أن يكون الجهاز العميل قليل السمك مدفوعا من قبل المستخدم أو مدفوعا بالسياسات أو كلاهما. يمكن تكوين الوصول على أساس كل مستخدم على حدة، أو يمكن إنشاء نهج مجموعة تتضمن مستخدما واحدا أو أكثر. يمكن تكوين تقنية SSL VPN في ثلاثة أوضاع رئيسية: WebVPN دون عميل (WebVPN) SSL، و Thin-Client SSL VPN (إعادة توجيه المنفذ)، و SSL VPN Client (وضع النفق الكامل SVC).

1. SSL VPN بدون عملاء (WebVPN):

يحتاج العميل البعيد فقط إلى مستعرض ويب يدعم SSL للوصول إلى خوادم الويب التي تدعم HTTP أو HTTPS على شبكة LAN الخاصة بالشركة. كما يتوفر الوصول أيضا لاستعراض ملفات Windows باستخدام نظام ملفات الإنترنت العام (CIFS). يعد عميل (Outlook Web Access (OWA مثلا جيدا للوصول إلى HTTP.

ارجع إلى [SSL VPN \(WebVPN\) بدون عملاء على Cisco IOS باستخدام مثال تكوين SDM](#) لمعرفة المزيد حول ClientLess SSL VPN.

2. Thin-Client SSL VPN (إعادة توجيه المنفذ)

يجب أن يقوم العميل البعيد بتنزيل تطبيق صغير قائم على Java للوصول الآمن إلى تطبيقات TCP التي تستخدم أرقام المنافذ الثابتة. UDP غير مدعوم. وتتضمن الأمثلة الوصول إلى POP3 و SMTP و IMAP و SSH و telnet. يحتاج المستخدم إلى امتيازات إدارية محلية لأنه يتم إجراء التغييرات على الملفات الموجودة على الجهاز المحلي. لا

تعمل هذه الطريقة ل SSL VPN مع التطبيقات التي تستخدم تعيينات المنافذ الديناميكية، على سبيل المثال، تطبيقات FTP المتعددة.

3. SSL VPN Client (SVC-Full Tunnel Mode):

يقوم عميل SSL VPN بتنزيل عميل صغير إلى محطة العمل البعيدة ويسمح بالوصول الكامل والأمن إلى الموارد على شبكة الشركة الداخلية. يمكن تنزيل SVC بشكل دائم إلى المحطة البعيدة، أو يمكن إزالته بعد انتهاء جلسة العمل الآمنة.

ارجع إلى [SSL VPN Client \(SVC\)](#) على [IOS باستخدام مثال تكوين SDM](#) لمعرفة المزيد حول عميل SSL VPN.

يوضح هذا المستند تكويننا بسيطاً ل SSL VPN الخاص بالعميل قليل السمك على موجه Cisco IOS®. يتم تشغيل شبكة VPN الخاصة ب SSL قليلة السمك على موجهات Cisco IOS التالية:

- الموجهات من السلسلة 870 و 1811 و 1841 و 2801 و 2811 و 2821 و 2851 من Cisco
- الموجهات من السلسلة 3725 و 3745 و 3825 و 3845 و 7200 و 7301 من Cisco

المتطلبات الأساسية

المتطلبات

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

متطلبات موجه Cisco IOS

- أي من الموجهات المدرجة المحملة ب SDM وصورة متقدمة من IOS الإصدار T(6)12.4 أو إصدار أحدث
- محطة الإدارة محملة ببرنامج إدارة قاعدة بيانات المحول (SDM) تقوم Cisco بشحن موجهات جديدة باستخدام نسخة مثبتة مسبقاً من إدارة قاعدة بيانات المحول (SDM). إذا لم يتم تثبيت إدارة قاعدة بيانات المحول (SDM) الخاصة بالموجه لديك، فيمكنك الحصول على البرنامج من [تنزيل البرامج-مدير أجهزة الأمان من Cisco](#). يجب أن تمتلك حساب CCO بعقد خدمة. ارجع إلى [تكوين الموجه لديك باستخدام مدير أجهزة الأمان](#) للحصول على تعليمات تفصيلية.

متطلبات أجهزة الكمبيوتر العملية

- يجب أن يتمتع العملاء البعيدين بامتيازات إدارية محلية؛ وهذا غير مطلوب، ولكنه مقترح بشدة.
- يجب أن يكون لدى العملاء البعيدين الإصدار 1.4 أو أعلى من بيئة وقت تشغيل (Java) (JRE).
- مستعرضات الأجهزة العميلة البعيدة: Internet Explorer 6.0 أو Netscape 7.1 أو Mozilla 1.7 أو Safari أو Firefox 1.0 أو 1.2.2
- تم تمكين ملفات تعريف الارتباط والإطارات المنبثقة المسموح بها على العملاء البعيدين

المكونات المستخدمة

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

- برنامج Cisco Advanced Enterprise Software، الإصدار T(9)12.4

- موجه الخدمات المدمجة الطراز 3825 من Cisco

- (Cisco Router and Security Device Manager) (SDM)، الإصدار 2.3.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين مسموح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر. تأتي عناوين IP المستخدمة لهذا التكوين من مساحة عنوان RFC 1918. ليست قانونية على الإنترنت.

الاصطلاحات

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

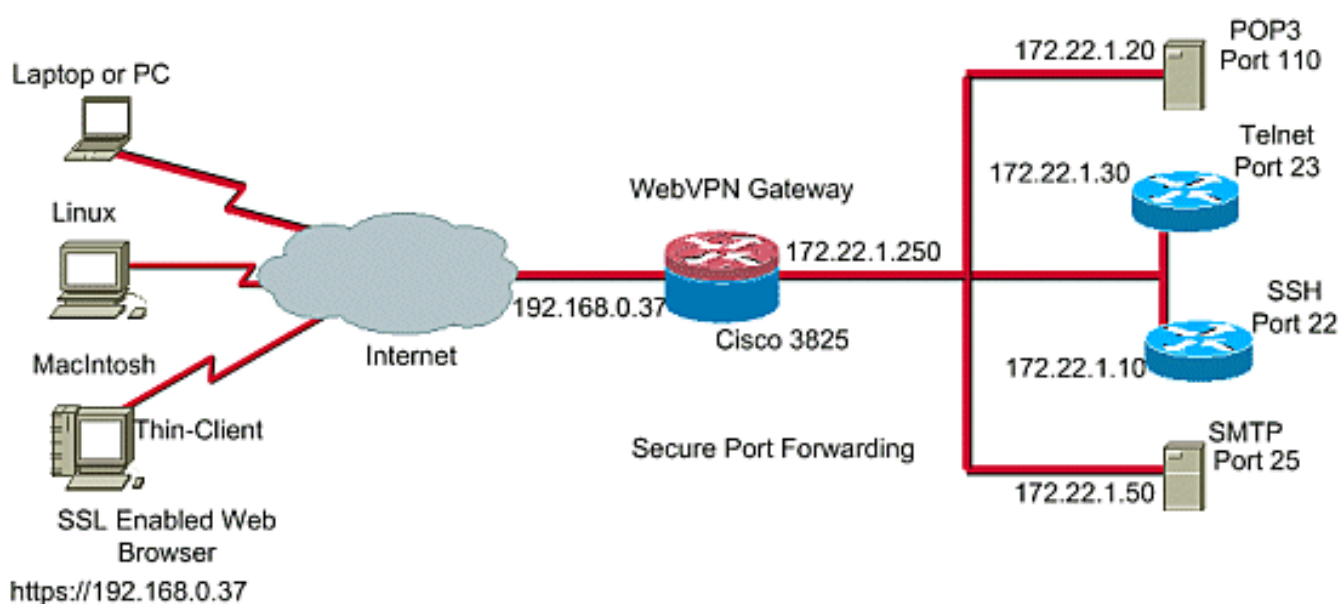
التكوين

المهمة

يحتوي هذا القسم على المعلومات اللازمة لتكوين الميزات الموضحة داخل هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين شبكة VPN الخاصة بـ SSL Thin-Client

أستخدم المعالج المتوفر في واجهة مدير أجهزة الأمان (SDM) لتكوين شبكة VPN الخاصة بـ SSL للعميل الدقيق على Cisco IOS، أو تكوينه إما على واجهة سطر الأوامر (CLI) أو يدويا في تطبيق SDM. يستخدم هذا المثال المعالج.

1. أختار علامة التبويب تكوين. من لوحة التصفح، أختار WebVPN > VPN. انقر فوق علامة التبويب إنشاء WebVPN. انقر فوق زر الاختيار التالي لإنشاء WebVPN جديد. انقر فوق الزر تشغيل المهمة المحددة.

Cisco Router and Security Device Manager (SDM): 10.89.129.170

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks


VPN

- Site-to-Site VPN
- Easy VPN Remote
- Easy VPN Server
- Dynamic Multipoint VPN
- WebVPN**
 - WebVPN Gateways
 - Packages
 - VPN Components

Create WebVPN Edit WebVPN

SDM can guide you through WebVPN configuration tasks. Select a task; then click 'Launch the selected task' button.

Use Case Scenario



Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS. [Enable DNS](#)

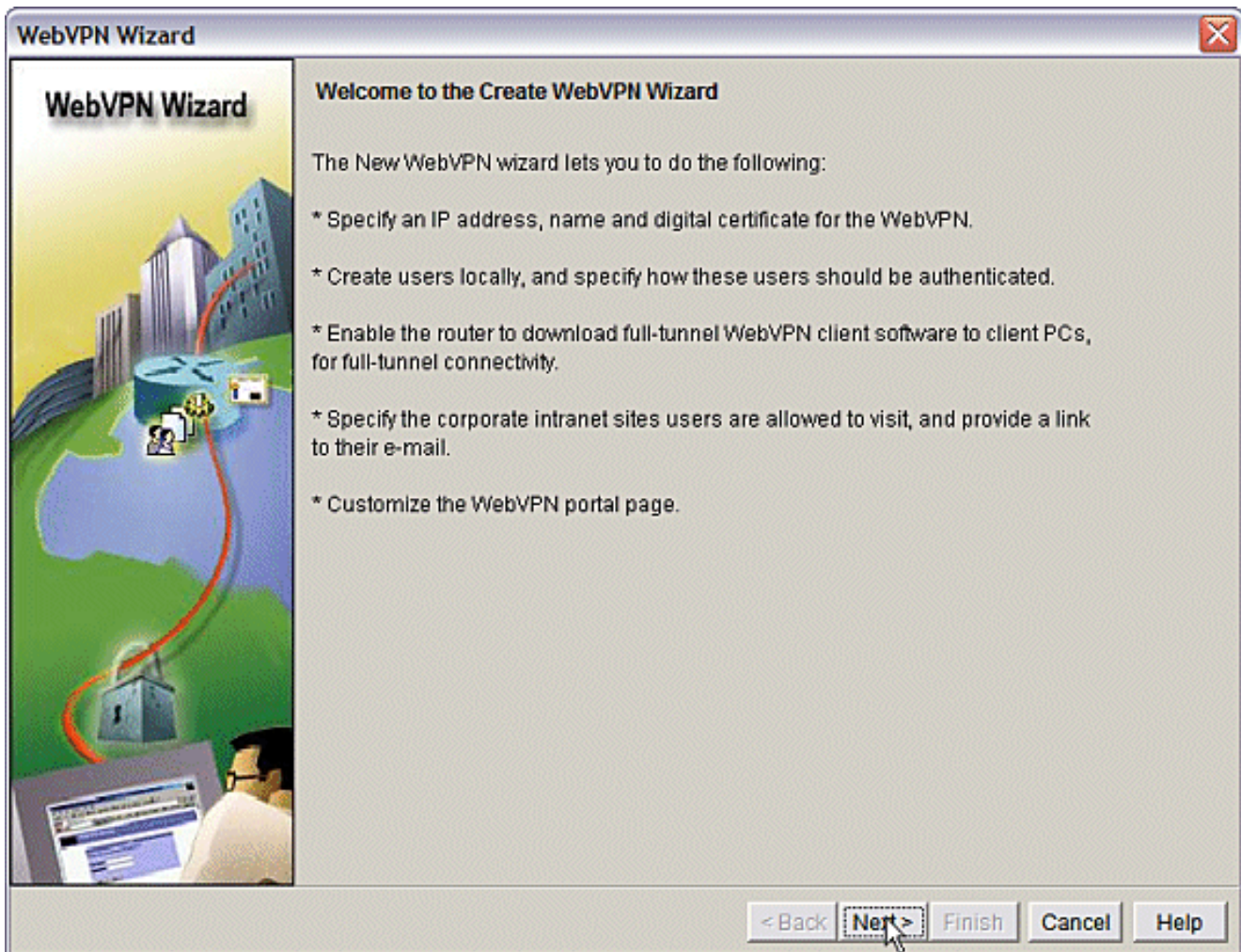
- Create a new WebVPN**
Use this wizard to create a new WebVPN.
- Add a new policy to an existing WebVPN for a new group of users**
Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.
- Configure advanced features for an existing WebVPN**
Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

Launch the selected task

How do I: **Go**

VPN 19:50:27 UTC Wed Jul 26 2006

2. يتم تشغيل معالج WebVPN. انقر فوق **Next** (التالي).



أدخل عنوان IP واسم فريد لبوابة WebVPN هذه. انقر فوق **Next** (التالي).

WebVPN Wizard

WebVPN Wizard

IP Address and Name
This is the IP address users will enter to access the WebVPN portal page. If multiple WebVPN services are configured in this router, the unique name is used to distinguish the service.

IP Address: Name:

Enable secure SDM access through 192.168.0.37

Digital Certificate
When users connect, this digital certificate will be sent to their web browser to authenticate the router.

Certificate:

Information

URL to login to this WebVPN service: <https://192.168.0.37/webvpn>

< Back Next > Finish Cancel Help

3. تتيح شاشة مصادقة المستخدم فرصة توفير مصادقة المستخدمين. يستخدم هذا التكوين حسابا تم إنشاؤه محليا على الموجه. يمكنك أيضا استخدام خادم المصادقة والتفويض والمحاسبة (AAA). لإضافة مستخدم، انقر فوق إضافة. أدخل معلومات المستخدم على الشاشة إضافة حساب، ثم انقر فوق موافق. طقطقت بعد ذلك على المستخدم صحة هوية شاشة.

WebVPN Wizard

WebVPN Wizard

User Authentication

You can configure user accounts locally on this router. You can configure user accounts on a AAA server so that the router can contact this server to authenticate users when they try to log on. Specify how WebVPN should authenticate the users when they login.

Add an Account

Enter the username and password

Username:

Password:

New Password:

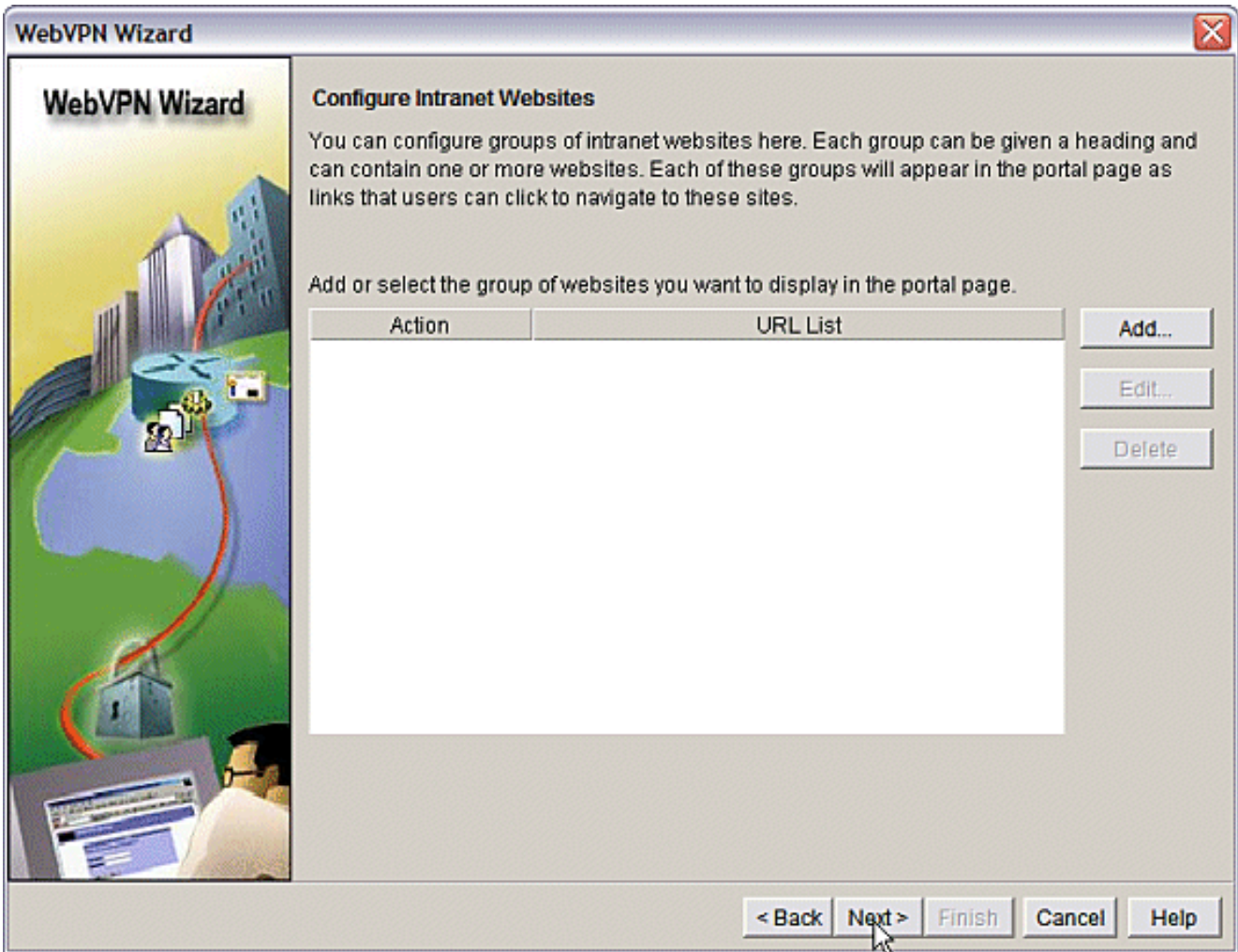
Confirm New Password:

Encrypt password using MD5 hash algorithm

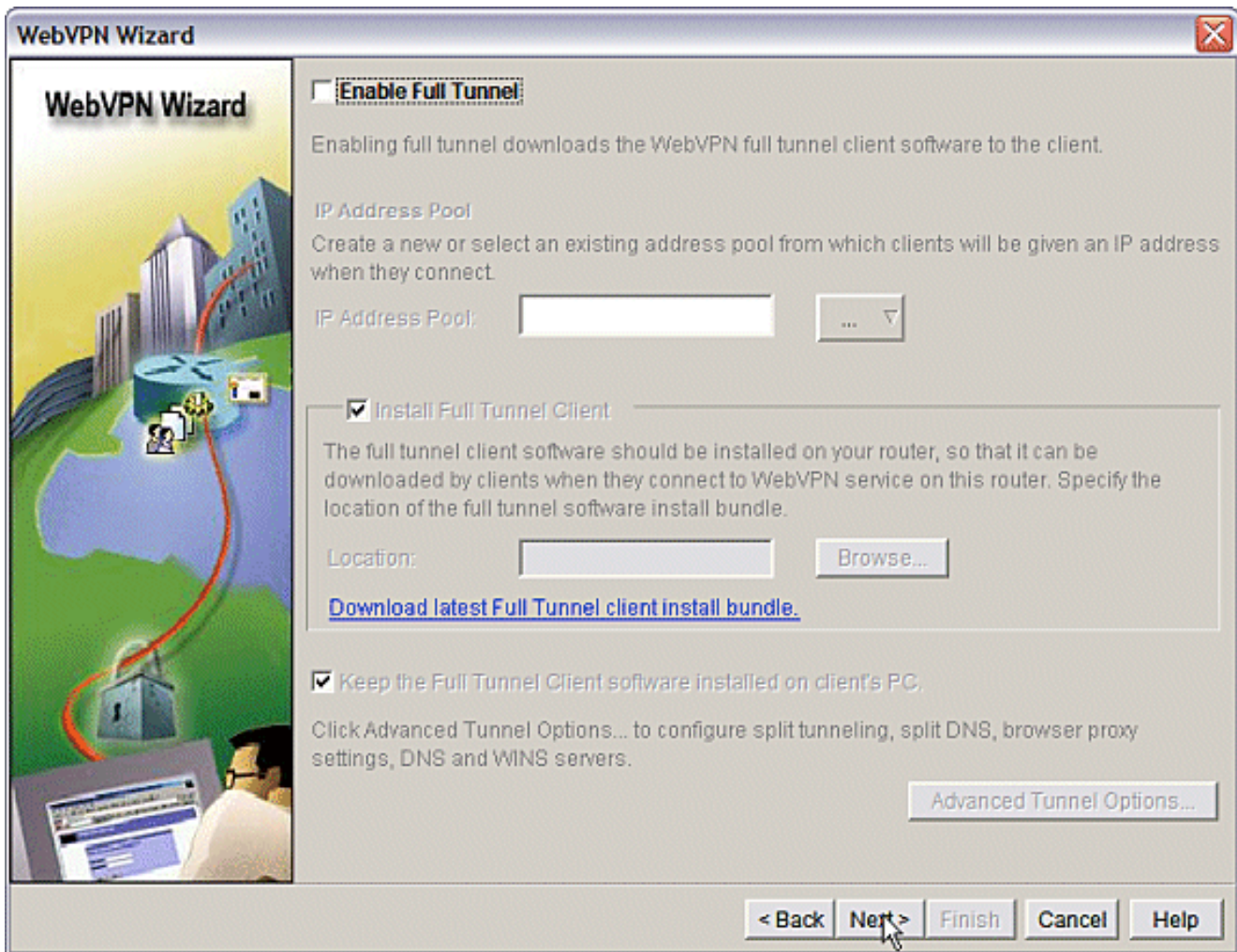
Privilege Level:

< Back Finish Cancel Help

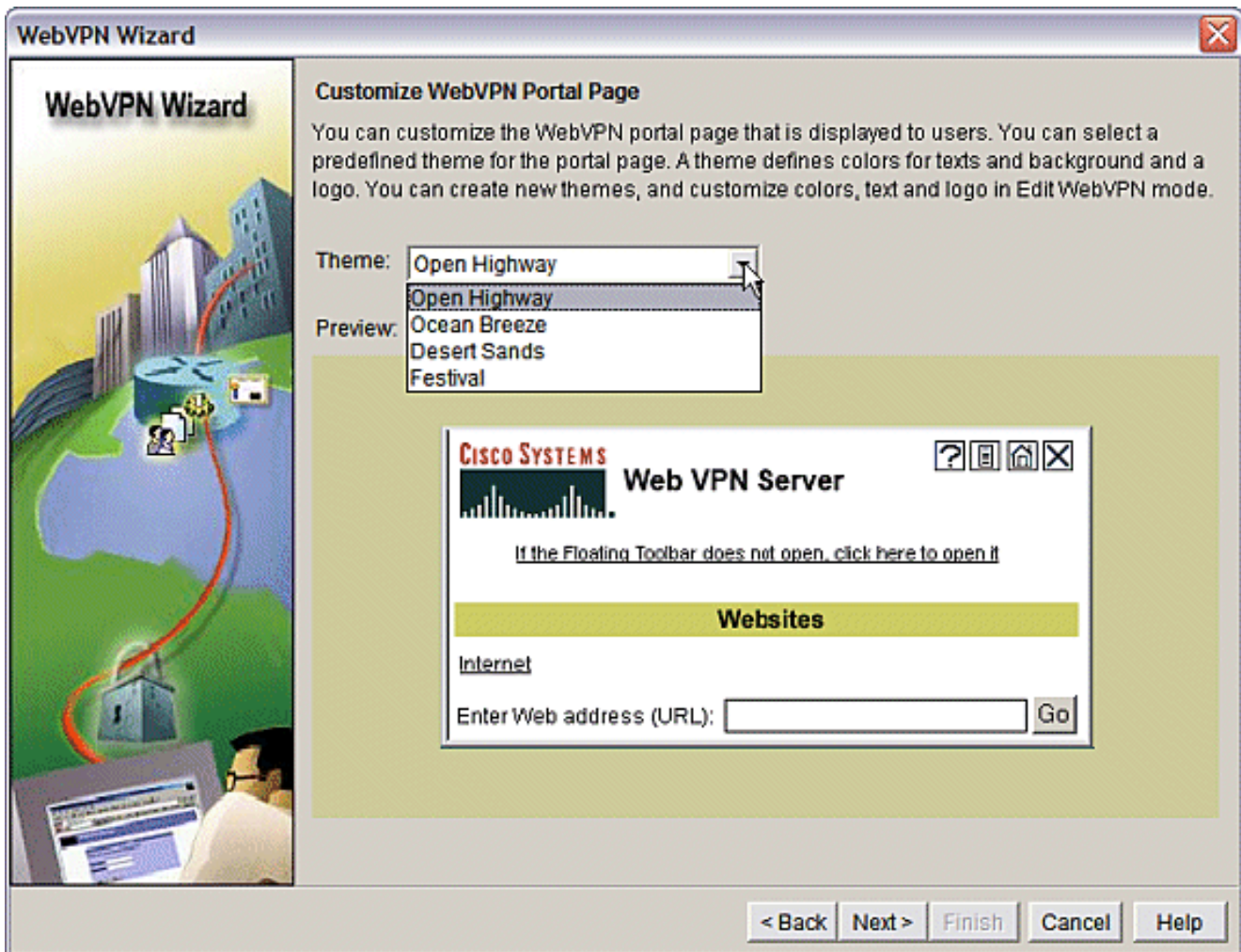
تسمح شاشة معالج WebVPN بتكوين مواقع ويب على إنترنت، ولكن يتم حذف هذه الخطوة لأن إعادة توجيه المنفذ يتم استخدامها للوصول إلى التطبيق هذا. إذا كنت ترغب في السماح بالوصول إلى مواقع الويب، فاستخدم تكوينات VPN الخاصة بـ SSL الخاص بالعميل الكامل أو دون عميل، والتي لا تقع ضمن نطاق هذا المستند.



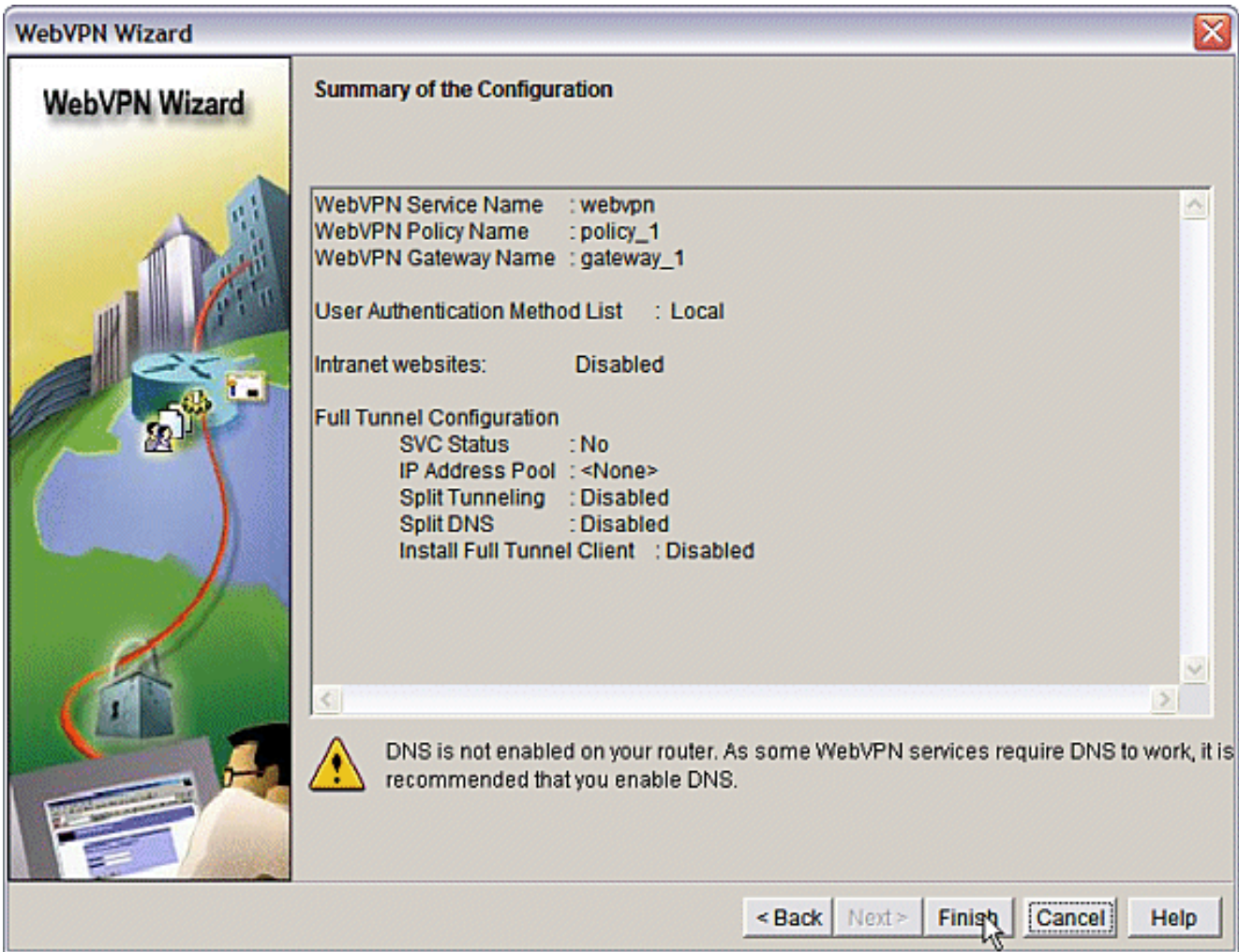
انقر فوق **Next** (التالي). يعرض المعالج شاشة تسمح بتكوين عميل النفق الكامل. لا ينطبق هذا على VPN ل SSL الخاص بالعميل قليل السمك (إعادة توجيه المنفذ). إلغاء تحديد تمكين النفق الكامل. انقر فوق **Next** (التالي).



4. تخصيص مظهر صفحة مدخل WebVPN أو قبول المظهر الافتراضي. انقر فوق **Next** (التالي).



قم بمعاينة ملخص التكوين ثم انقر فوق إنهاء <
حفظ.



5. لقد قمت بإنشاء عبارة WebVPN وسياق WebVPN باستخدام نهج مجموعة مرتبط. قم بتكوين منافذ الأجهزة العملية قليلة السمك، والتي يتم توفيرها عند اتصال العملاء بشبكة WebVPN. أخترت بشكل > VPN WebVPN. أخترت إنشاء WebVPN. أختار زر الخيار تكوين ميزات متقدمة لشبكة WebVPN موجودة وانقر فوق تشغيل المهمة المحددة.

Cisco Router and Security Device Manager (SDM): 10.89.129.170

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks VPN

VPN

- Site-to-Site VPN
- Easy VPN Remote
- Easy VPN Server
- Dynamic Multipoint VPN
- WebVPN
 - WebVPN Gateways
 - Packages
- VPN Components

Interfaced and Connections

Firewall and ACL

VPN

Security Audit

Routing

NAT

Intrusion Prevention

Quality of Service

NAC

Additional Tasks

Create WebVPN Edit WebVPN

SDM can guide you through WebVPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS. [Enable DNS](#)

- Create a new WebVPN

Use this wizard to create a new WebVPN.
- Add a new policy to an existing WebVPN for a new group of users

Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.
- Configure advanced features for an existing WebVPN

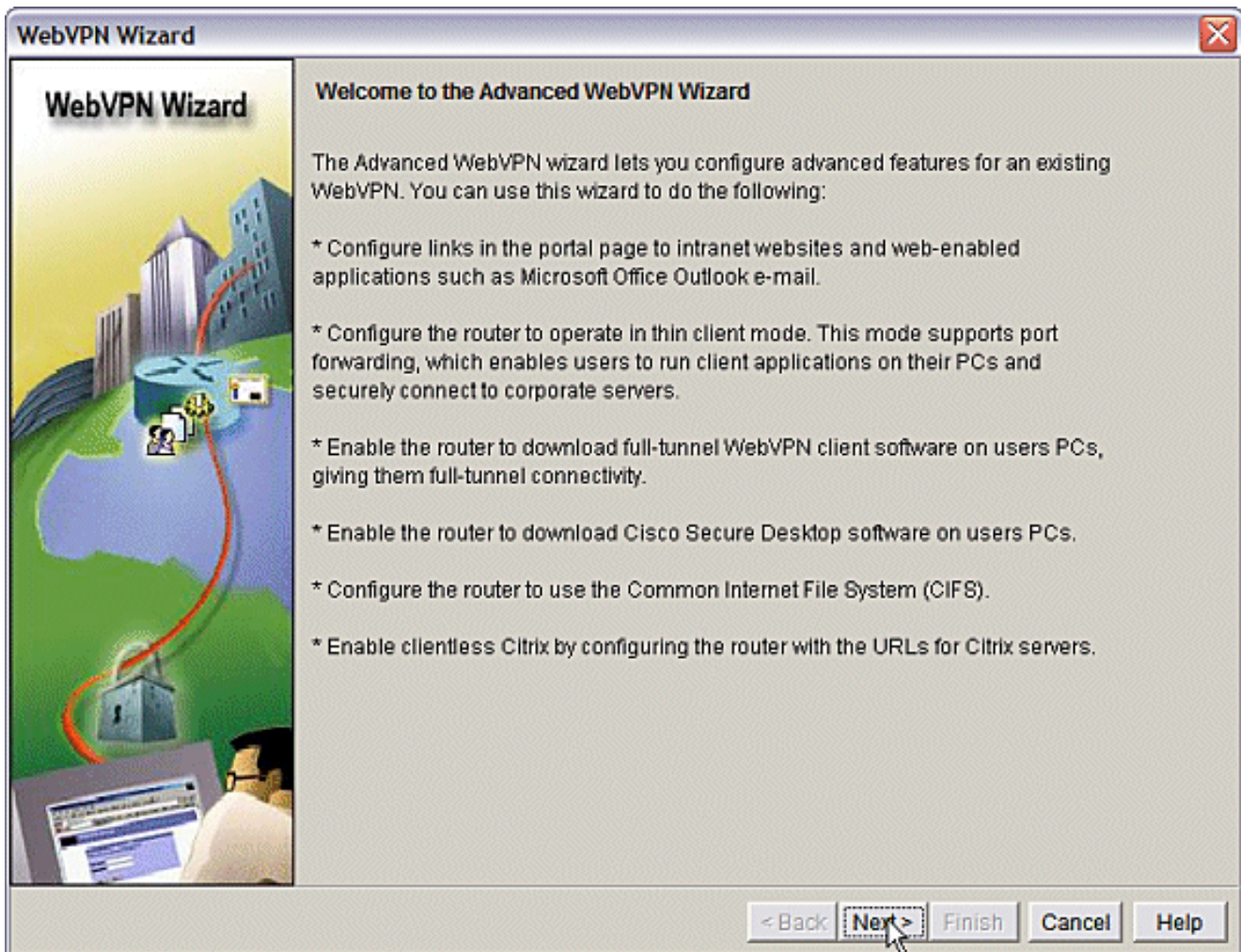
Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

Launch the selected task

How do I: Go

Delivering configuration to the router... 20:35:49 UTC Wed Jul 26 2006

توفر شاشة الترحيب الإبرازات لإمكانيات المعالج. انقر فوق **Next** (التالي).



أختر سياق WebVPN ومجموعة المستخدمين من القوائم المنسدلة. انقر فوق **Next** (التالي).

WebVPN Wizard

WebVPN Wizard

Select the WebVPN user group
Select the WebVPN and the user group within that WebVPN for whom you want to configure additional advanced features.

First select the WebVPN where the user group is defined and then select the user group.

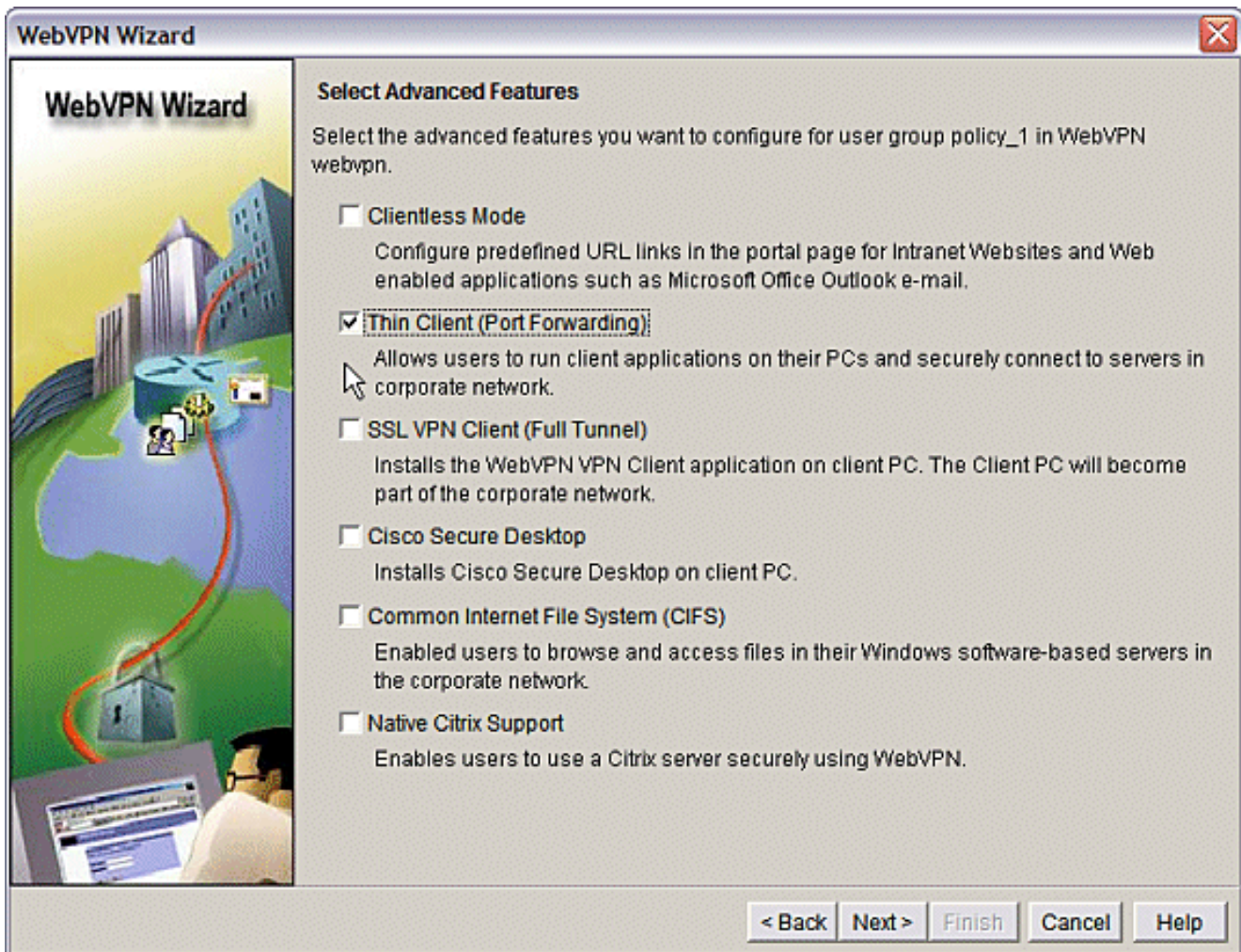
WebVPN:

User Group:

Default Group: policy_1

< Back Next > Finish Cancel Help

أختار جهاز عميل قليل السمك (إعادة توجيه المنافذ) وانقر فوق التالي.



أدخل الموارد التي تريد توفيرها من خلال إعادة توجيه المنفذ. يجب أن يكون منفذ الخدمة منفذًا ثابتًا، ولكن يمكنك قبول المنفذ الافتراضي على كمبيوتر العميل المعين بواسطة المعالج. انقر فوق **Next** (التالي).

WebVPN Wizard

WebVPN Wizard

Thin Client (Port Forwarding)

Thin client enabled WebVPN users to run client applications on their PCs and connect to servers in corporate network, For example clients could run an email client application on a public PC that connects to an e-mail (IMAP, SMTP) server on the corporate network.

Specify the servers and port numbers of applications you want WebVPN users to have access to.

Server	Port	Port on Client PC	Description
172.22.1.50	25	3000	Email
172.22.1.30	23	3001	Router1
172.22.1.10	22	3003	Router2 SSH

Buttons: Add..., Edit..., Delete

Add Port Forwarding Server

Server IP Address:

Server port on which service is listening:

Port on Client PC: [Learn more.](#)

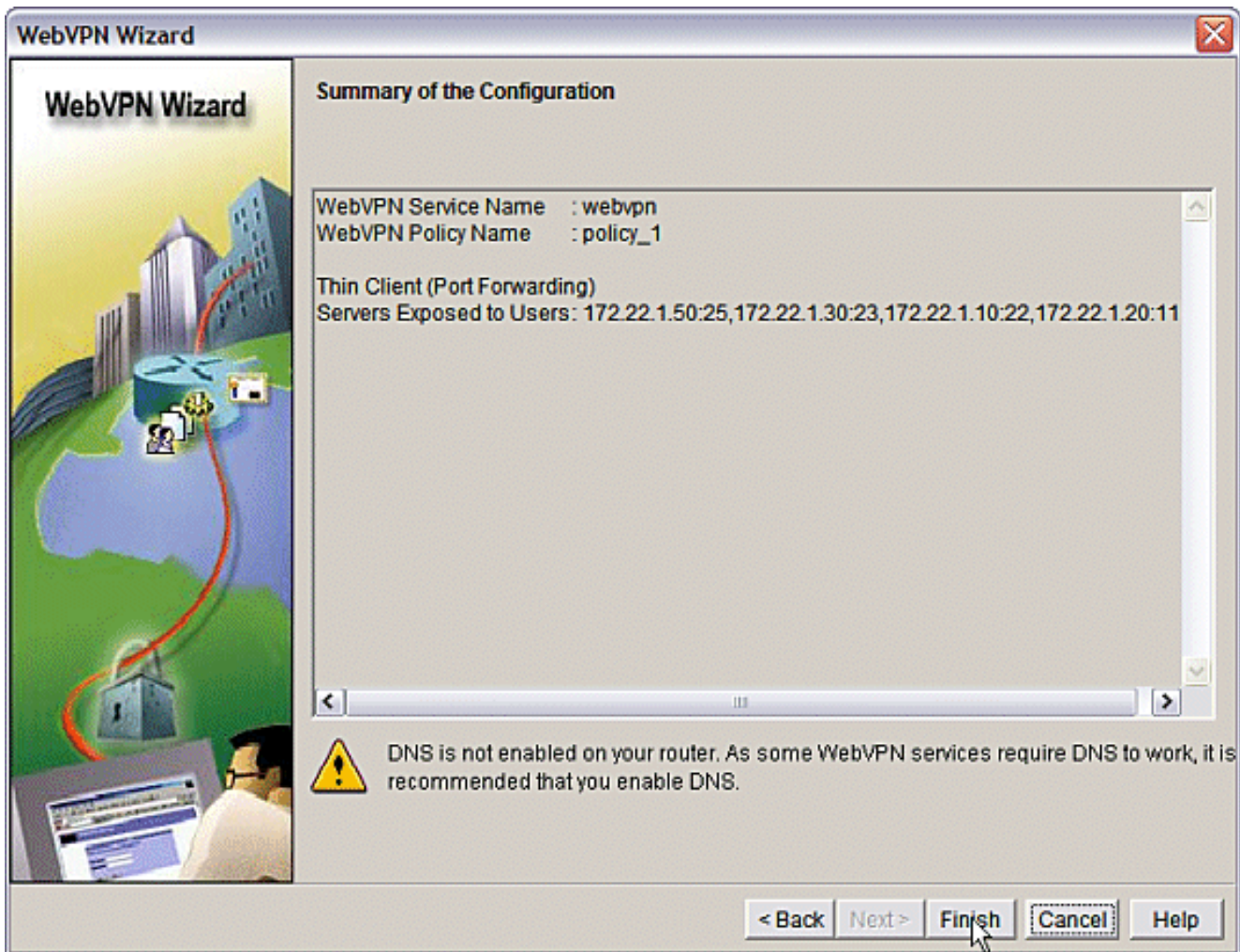
Description:

Buttons: OK, Cancel, Help

IP address of your SMTP

Buttons: < Back, Next >, Finish, Cancel, Help

قم بمعاينة ملخص التكوين ثم انقر فوق إنهاء < موافق > حفظ.



التكوين

نتائج تكوين إدارة قاعدة بيانات المحول (SDM).

```

أوسن ml-3825-01
...Building configuration

Current configuration : 4343 bytes
!
Last configuration change at 15:55:38 UTC Thu Jul 27 2006 by ausnml
NVRAM config last updated at 21:30:03 UTC Wed Jul 26 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
/enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi

```



```

!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
no dspfarm
Self-Signed Certificate Information crypto pki ---!
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !----- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDxladDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end

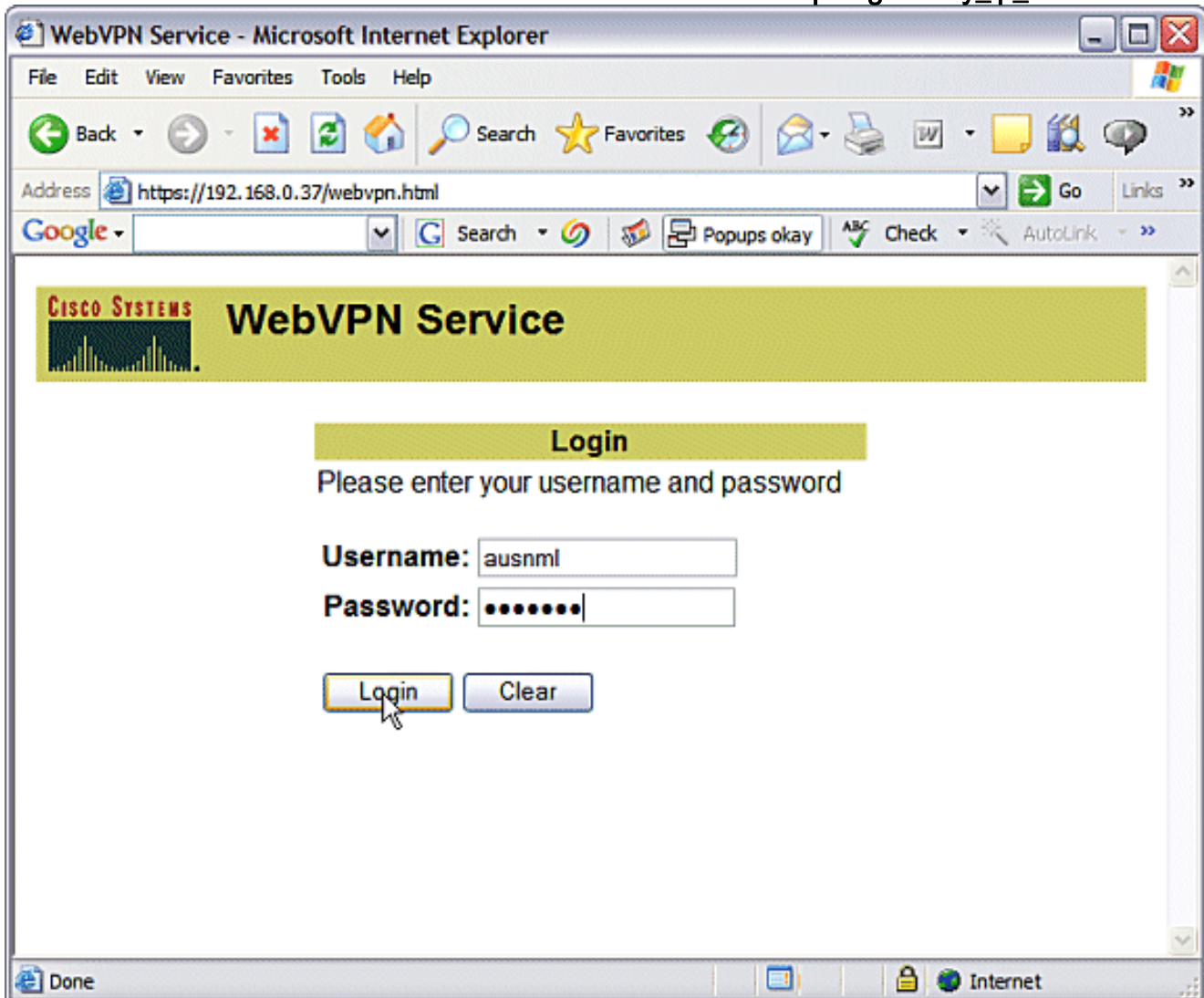
```

التحقق من الصحة

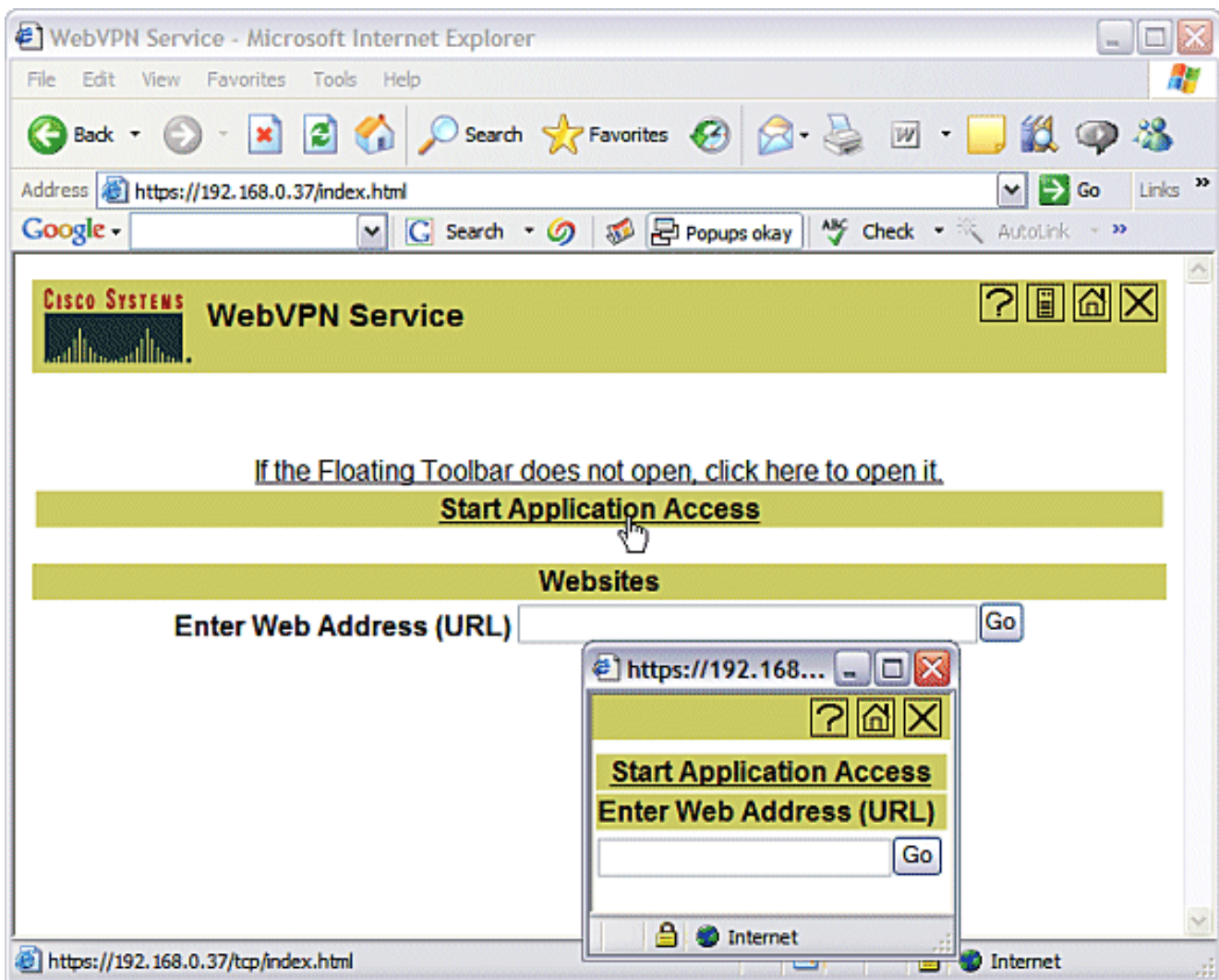
التحقق من التكوين

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

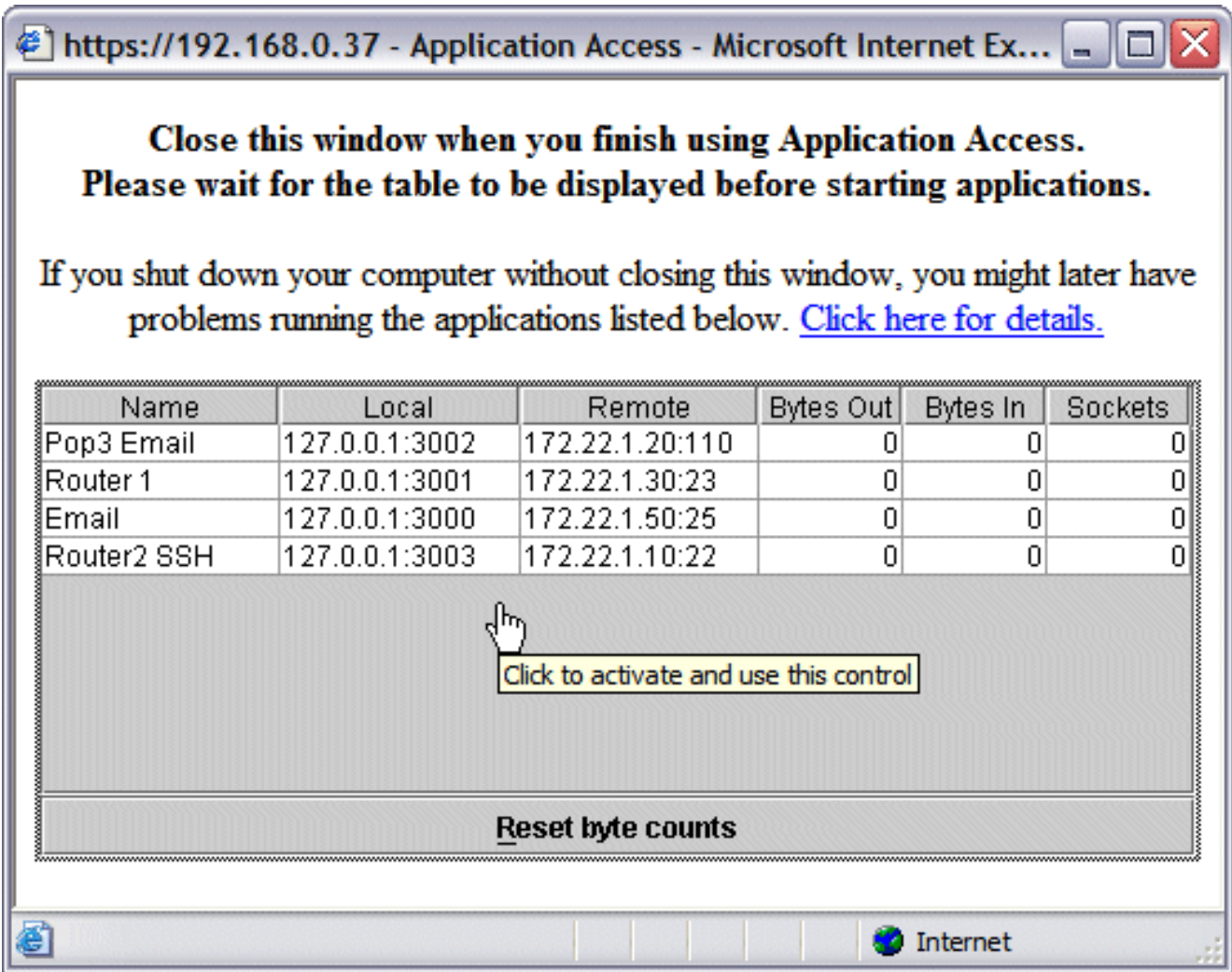
1. أستخدم كمبيوتر عميل للوصول إلى بوابة WebVPN على https://gateway_ip_address. تذكر تضمين اسم مجال WebVPN إذا قمت بإنشاء سياقات WebVPN فريدة. على سبيل المثال، إذا قمت بإنشاء مجال يسمى "المبيعات"، فأدخل https://gateway_ip_address/sales.



2. قم بتسجيل الدخول وقبول الشهادة التي توفرها بوابة WebVPN. انقر على بدء الوصول إلى التطبيق.



3. تظهر شاشة الوصول إلى التطبيق. يمكنك الوصول إلى تطبيق باستخدام رقم المنفذ المحلي وعنوان IP للاسترجاع المحلي الخاص بك. على سبيل المثال، إلى Telnet إلى الموجه 1، أدخل 3001 127.0.0.1 Telnet. يرسل تطبيق جافا الصغير هذه المعلومات إلى بوابة WebVPN، والتي بعد ذلك تربط طرفي الجلسة معا بطريقة آمنة. يمكن أن تؤدي الاتصالات الناجحة إلى زيادة وحدات البايت ووحدات البايت في الأعمدة.



الأوامر

يتم إقران العديد من أوامر العرض مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات ومعلومات أخرى. للاطلاع على استخدام أوامر show بالتفصيل، ارجع إلى [التحقق من تكوين WebVPN](#).

تدعم [أداة مترجم الإخراج \(للعلماء المسجلين فقط\)](#) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر show.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

يجب تحميل أجهزة الكمبيوتر العميلة بالإصدار 1.4 من Sun Java أو إصدار أحدث. الحصول على نسخة من هذا البرنامج من [تنزيل برامج جافا](#)

الأوامر المستخدمة لاستكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر debug.

- **show webVPN**؟ — هناك العديد من أوامر العرض المرتبطة ب WebVPN. يمكن تنفيذ ذلك في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات والمعلومات الأخرى. للاطلاع على استخدام أوامر show بالتفصيل، ارجع إلى [التحقق من تكوين WebVPN](#).
- **debug webVPN**؟ — يمكن أن يؤثر استخدام أوامر debug سلبا على الموجه. راجع استخدام أوامر تصحيح

[الأخطاء في مزيد من التفاصيل، باستخدام أوامر تصحيح الأخطاء لـ WebVPN.](#)

معلومات ذات صلة

- [Cisco من IOS SSLVPN](#)
- [SSL VPN - WebVPN](#)
- [Cisco IOS WebVPN Q&A](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco م ل خ ت . ف ر ت م م مچرت م ا م د ق م م ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ل م ل ا ح ل ا ن ا ل ا دن ت س م ل ا