SDM を使用した IOS での SSL VPN Client (SVC) の設定例

目次

はじめに

SSL VPN クライアント (SVC) は、社内ネットワークと安全に通信するためのフル トンネルを提供します。 ユーザ単位でアクセス権を設定することもできれば、複数のユーザを配置するさまざまな WebVPN コンテキストを作成することもできます。

SSL VPN または WebVPN テクノロジーは、次の IOS ルータ プラットフォーム上でサポートされています。

- 870、1811、1841、2801、2811、2821、2851
- 3725、3745、3825、3845、7200、および 7301

次のモードで SSL VPN テクノロジーを設定できます。

- **クライアントレス SSL VPN (WebVPN)** : 企業のローカル エリア ネットワーク (LAN) 上の HTTP サーバまたは HTTPS Web サーバへアクセスする際に SSL 対応の Web ブラウザが

必要となるリモート クライアントです。 また、クライアントレス SSL VPN は、Common Internet File System（CIFS）プロトコルによる Windows ファイル ブラウジングへのアクセスも提供します。 Outlook Web Access（OWA）は、HTTP アクセスの一例です。クライアントレス SSL VPN の詳細については、「SDM を使用した Cisco IOS でのクライアントレス SSL VPN（WebVPN）の設定例」を参照してください。

- **シンクライアント SSL VPN（ポート転送）**：小規模な Java ベースのアプレットをダウンロードし、スタティックなポート番号を使用する Transmission Control Protocol（TCP; 伝送制御プロトコル）アプリケーションのセキュアなアクセスを可能にするリモート クライアントです。 Point Of Presence（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、セキュア シェル（SSH）および Telnet は、セキュアなアクセスの例です。 ローカル マシン上のファイルが変更されるため、この方法を使用するには、ユーザにローカル管理者特権が必要です。 SSL VPN のこの方法は、一部の File Transfer Protocol（FTP; ファイル転送プロトコル）アプリケーションなど、ダイナミックなポート割り当てを使用するアプリケーションでは使用できません。シンクライアント SSL VPN の詳細については、「SDM によるシンクライアント SSL VPN（WebVPN）の IOS 設定例」を参照してください。**注:** User Datagram Protocol（UDP; ユーザ データグラム プロトコル）はサポートされていません。
- **SSL VPN クライアント（SVC フル トンネル モード）**：リモート ワークステーションに小規模なクライアントをダウンロードし、社内ネットワーク上のリソースへの完全なセキュア アクセスを可能にします。 SVC をリモート ワークステーションへ永続的にダウンロードすることもできれば、セキュアなセッションが閉じられた後にクライアントを削除することもできます。

このドキュメントでは、SSL VPN クライアントによって使用される Cisco IOS ルータの設定を示しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Microsoft Windows 2000 または XP
- SUN JRE 1.4 以降を搭載した Web ブラウザまたは ActiveX コントロール対応ブラウザ
- クライアント上のローカルな管理者権限
- 高度なセキュリティ イメージ（12.4(6)T 以降）を搭載した「概要」に一覧されたルータのいずれか
- Cisco Security Device Manager（SDM）バージョン 2.3Cisco SDM がまだルータにロードされていない場合は、ソフトウェアのダウンロードのページ（登録ユーザ専用）からソフトウェアを無料で取得できます。 サービス契約を結んでいる CCO アカウントが必要です。 SDM のインストールと設定の詳細については、Cisco Router and Security Device Manager のページを参照してください。
- ルータのデジタル証明書この要件を満たすために、永続的な自己署名証明書または外部認証局（CA）を使用できます。 永続的な自己署名証明書の詳細については、永続的な自己署名証明書のページを参照してください。

使用するコンポーネント

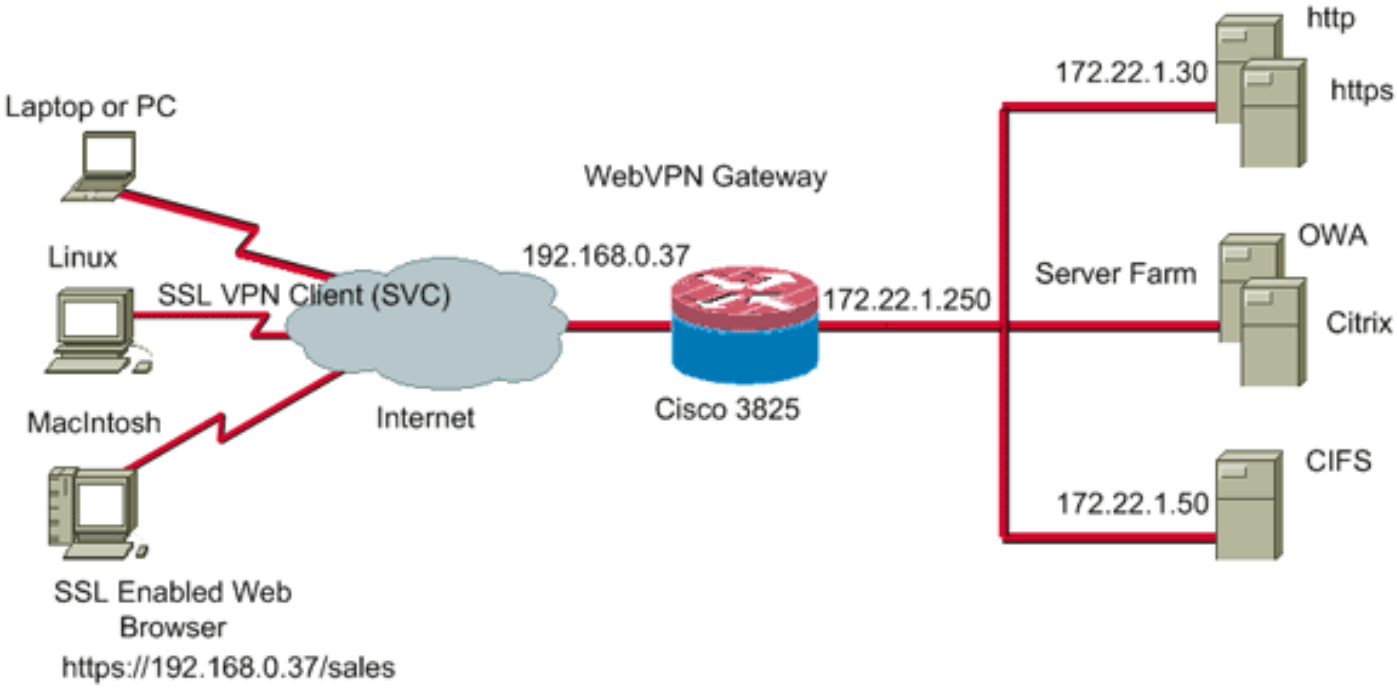
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ルータ 3825 シリーズ、12.4(9)T 搭載
- Security Device Manager（SDM）バージョン 2.3.1

注: このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定前の作業

1. ルータを SDM 対応に設定します。（オプション）適切なセキュリティ バンドル ライセンスがあるルータには、すでに SDM アプリケーションがフラッシュにロードされています。ソフトウェアの取得と設定の手順については、Cisco Router and Security Device Manager（SDM）のダウンロードおよびインストールのページを参照してください。
2. SVC のコピーを管理 PC にダウンロードします。SVC パッケージ ファイルのコピーは、ソフトウェアのダウンロード： Cisco SSL VPNクライアントのページ（登録ユーザ専用）から取得できます。 サービス契約を結んでいる有効な CCO アカウントが必要です。
3. 正しい日付、時間およびタイム ゾーンを設定し、その後、ルータにデジタル証明書を設定します。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

SVC は最初に WebVPN ゲートウェイ ルータにロードされます。 クライアントが接続するたびに、SVC のコピーがダイナミックに PC へダウンロードされます。 この動作を変更するには、クライアント コンピュータでソフトウェアを永続的に有効化するようにルータを設定します。

IOS での SVC の設定

この項では、このドキュメントに記載されている機能を設定するために必要な手順を示します。次の設定例では、SDM ウィザードを使用して IOS ルータで SVC の動作を有効にしています。

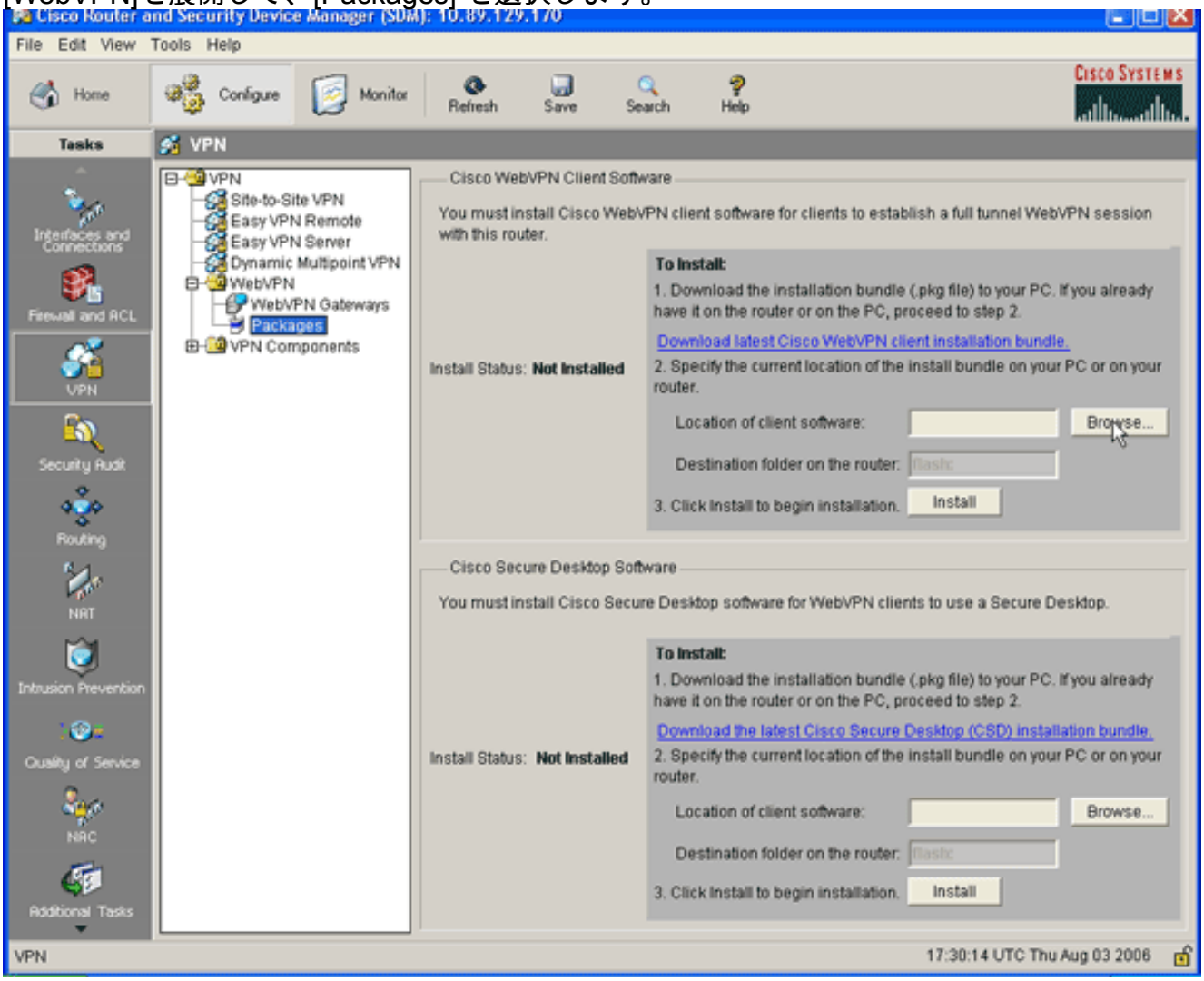
IOS ルータに SVC を設定するには、次の手順を実行します。

1. IOS ルータに SVC ソフトウェアをインストールし、有効にする
2. SDM ウィザードで WebVPN コンテキストと WebVPN ゲートウェイを設定する
3. SVC ユーザのユーザ データベースを設定する
4. ユーザに対して表示するリソースを設定する

手順 1：IOS ルータに SVC ソフトウェアをインストールし、有効にする

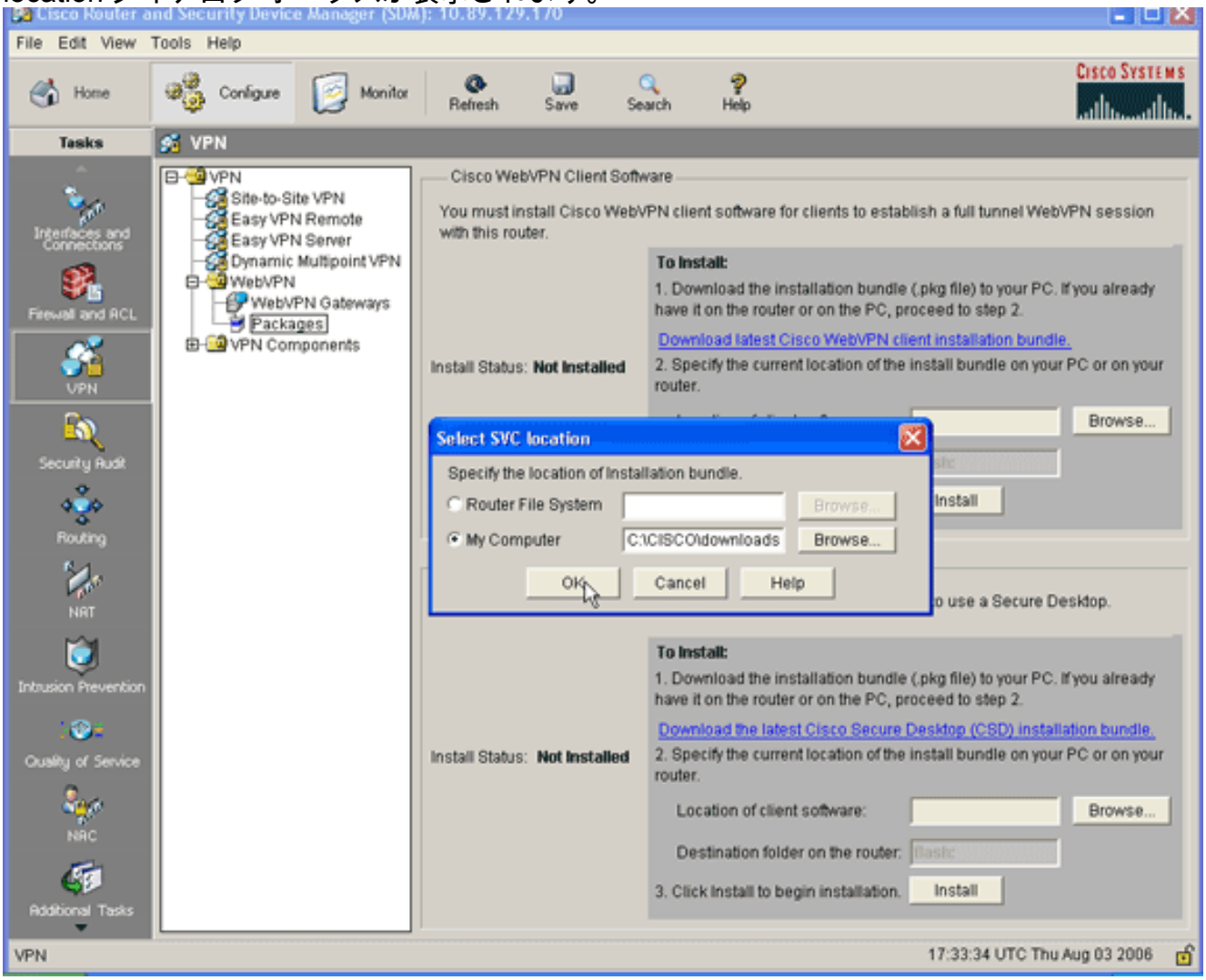
IOS ルータに SVC ソフトウェアをインストールして有効にするには、次の手順を実行します。

1. SDM アプリケーションを開き、[Configure]をクリックし、次に [VPN] をクリックします。
2. [WebVPN]を展開して、[Packages] を選択します。

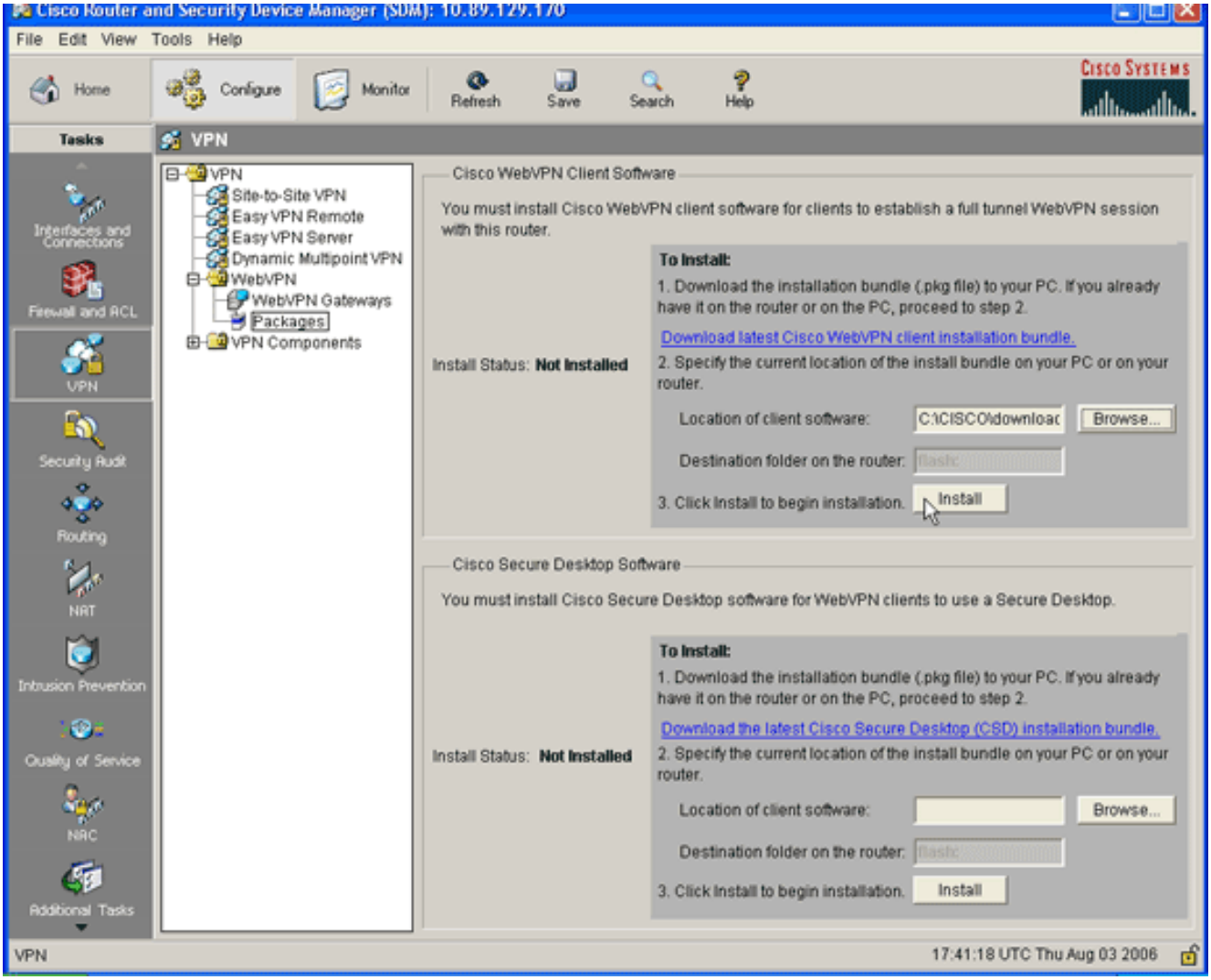


3. [Cisco WebVPN Client Software] エリアで、[Browse]ボタンをクリックします。Select SVC

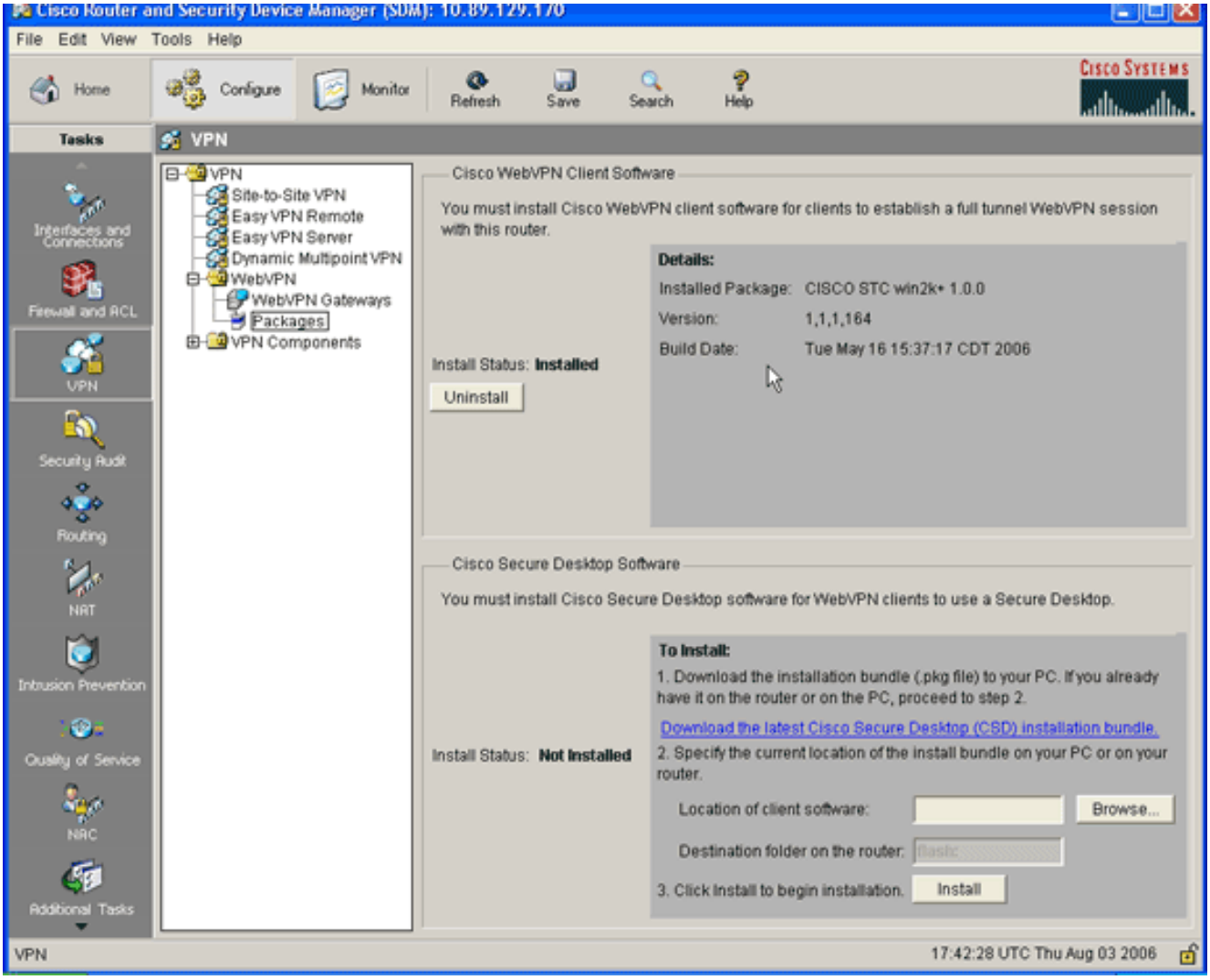
location ダイアログ ボックスが表示されます。



4. [My Computer]ラジオ ボタンをクリックし、次に、[Browse] をクリックして管理 PC 上の SVC パッケージを検索します。
5. [OK]をクリックし、次に、[Install] ボタンをクリックします。



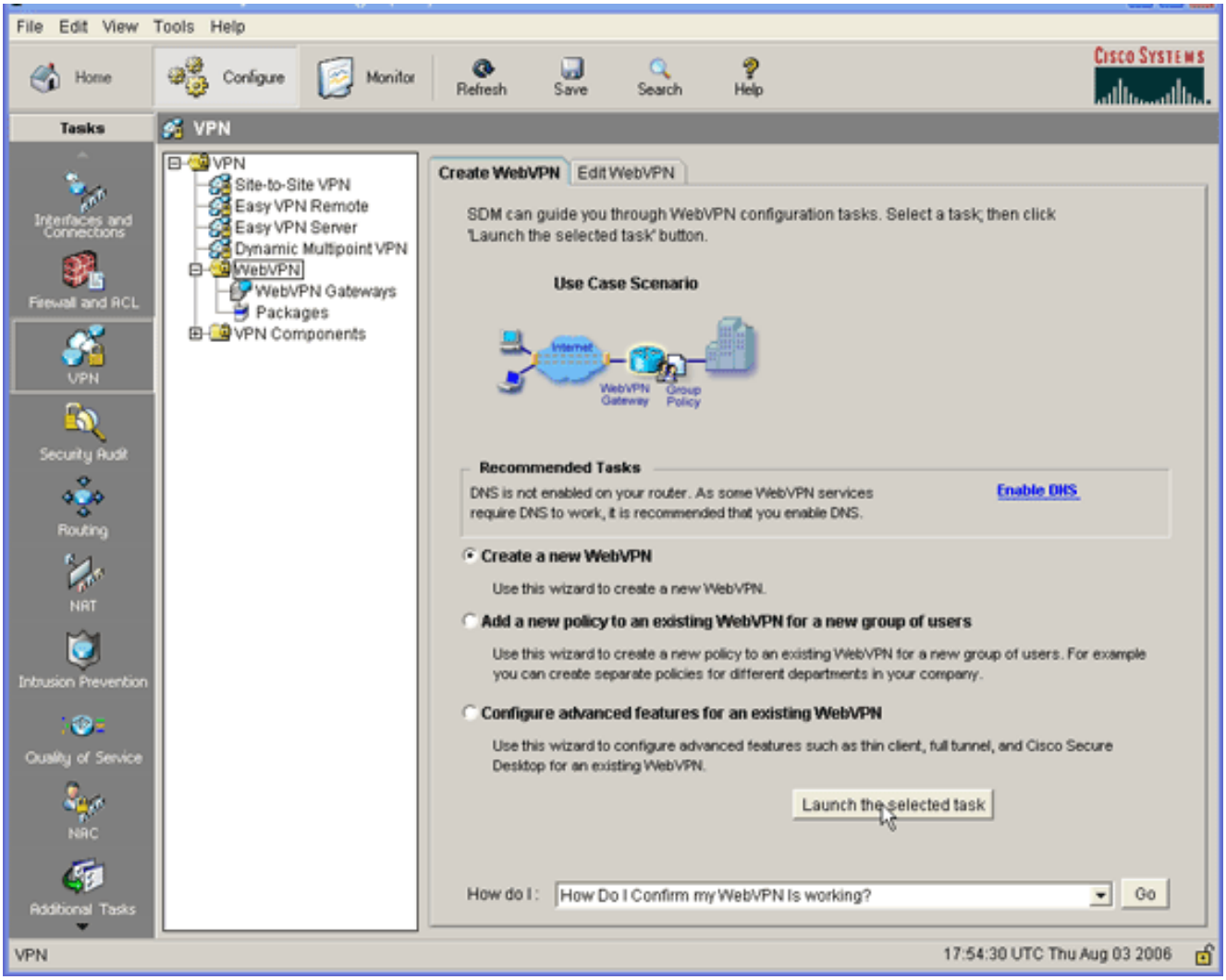
6. [Yes]をクリックし、次に、[OK] をクリックします。SVC パッケージが正常にインストールされると、次の図のように表示されます。



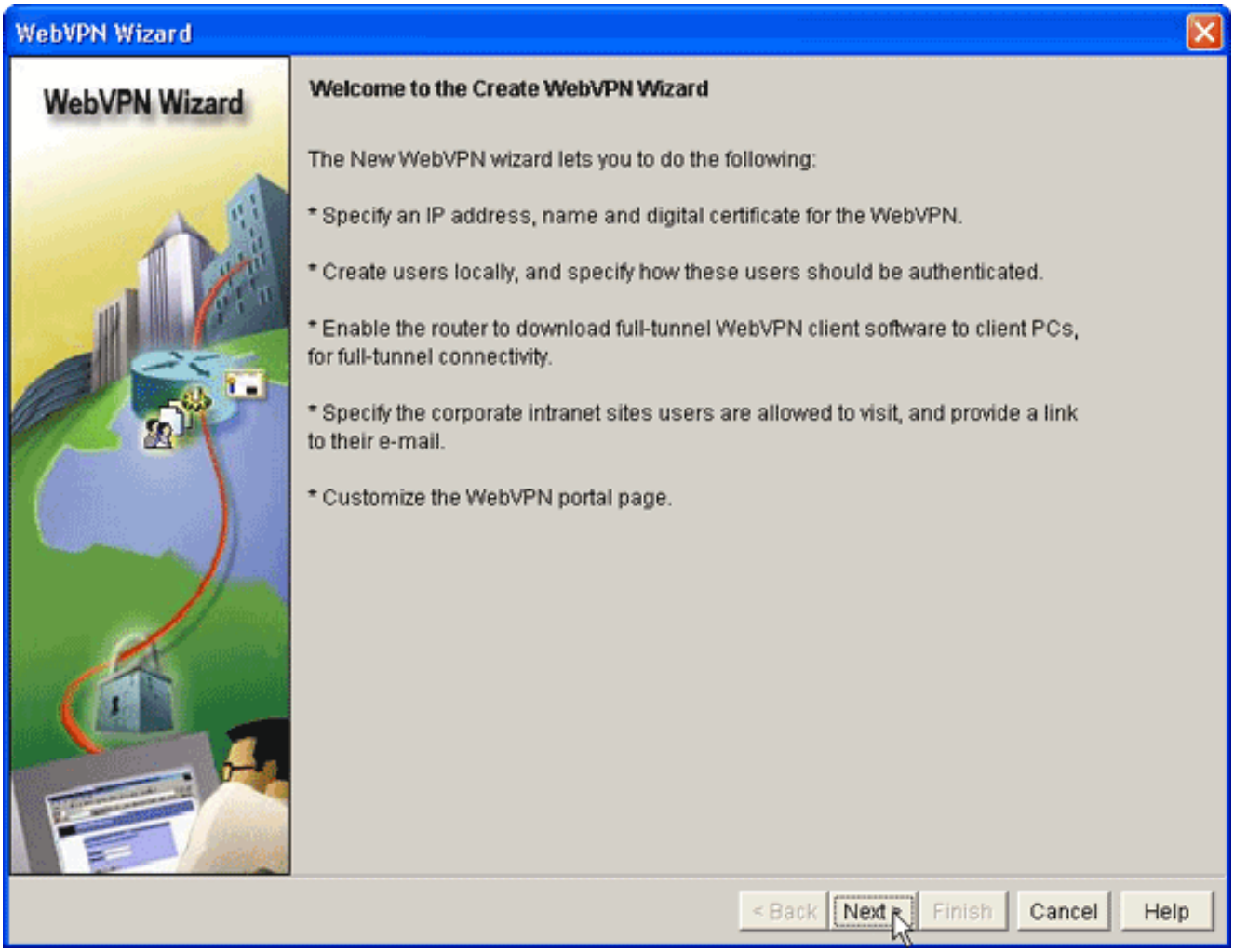
手順 2：SDM ウィザードで WebVPN コンテキストと WebVPN ゲートウェイを設定する

WebVPN コンテキストと WebVPN ゲートウェイを設定するには、次の手順を実行します。

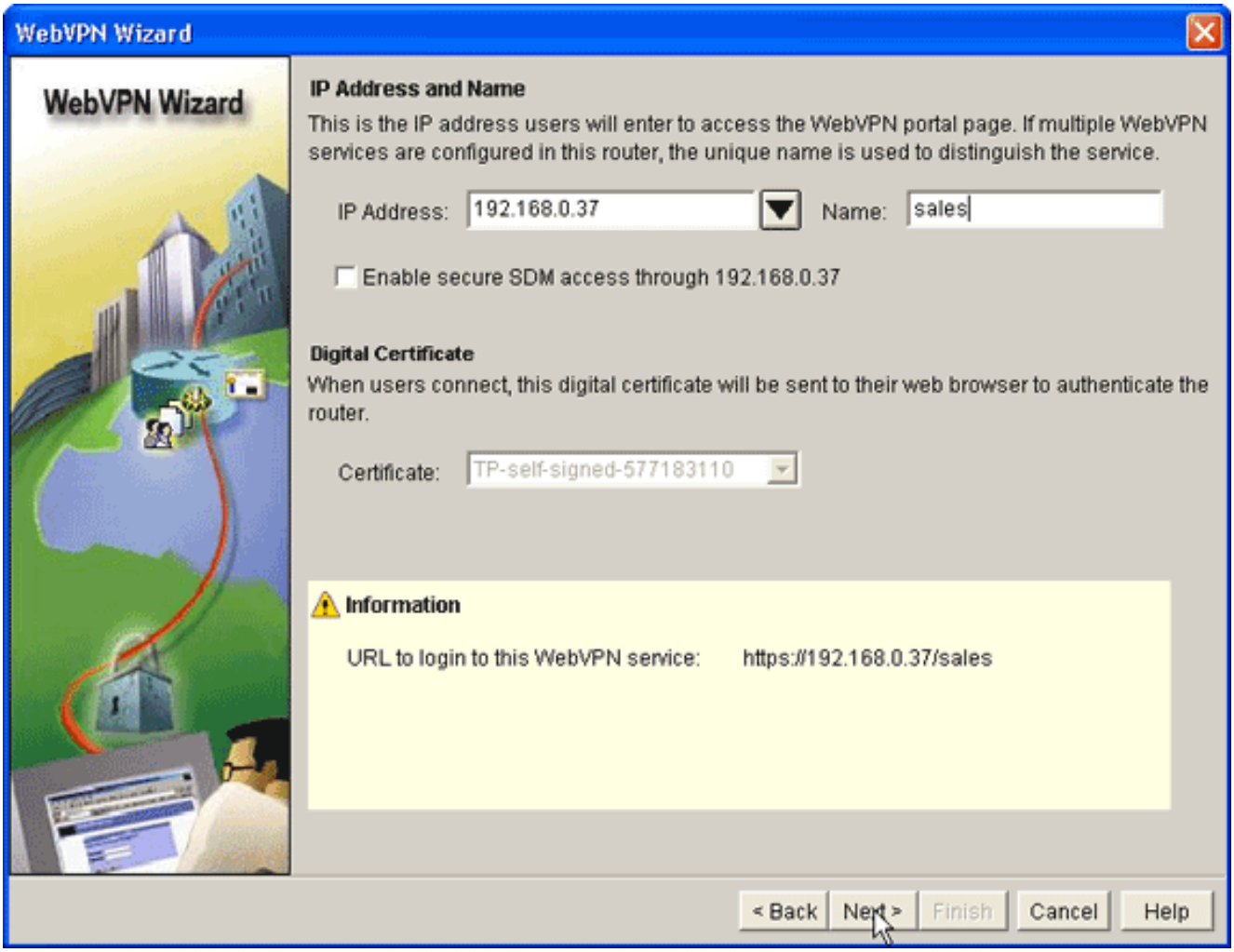
1. SVC がルータにインストールされた後、[Configure]をクリックし、次に、[VPN] をクリックします。
2. [WebVPN]をクリックし、[Create WebVPN] タブをクリックします。



3. [Create a New WebVPN]ラジオ ボタンをオンにして、選択したタスクの [Launch] をクリックします。[WebVPN Wizard] ダイアログボックスが表示されます。



4. [Next] をクリックします。



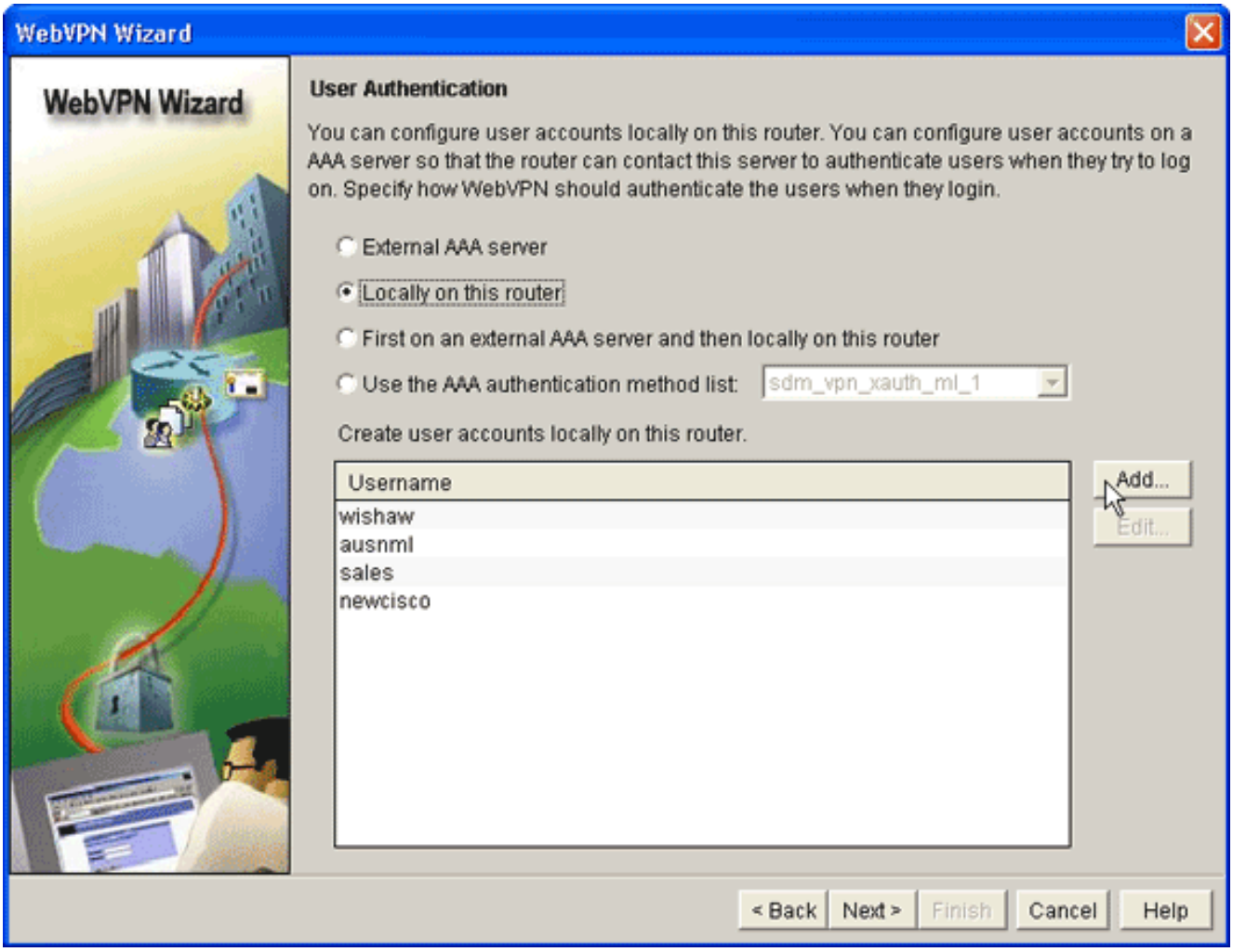
5. 新しい WebVPN ゲートウェイの IP アドレスを入力し、この WebVPN コンテキストの一意の名前を入力します。同じ IP アドレス (WebVPN ゲートウェイ) に異なった WebVPN コンテキストを作成することはできますが、それぞれの名前は一意にする必要があります。この例では、次の IP アドレスを使用します。 *https://192.168.0.37/sales*
6. [次へ]をクリックして、手順 3 に進みます。

手順 3 : SVC ユーザのユーザ データベースを設定する

認証には、AAA サーバ、ローカル ユーザ、またはその両方を使用できます。 この設定例では、ローカルに作成されたユーザを認証に使用しています。

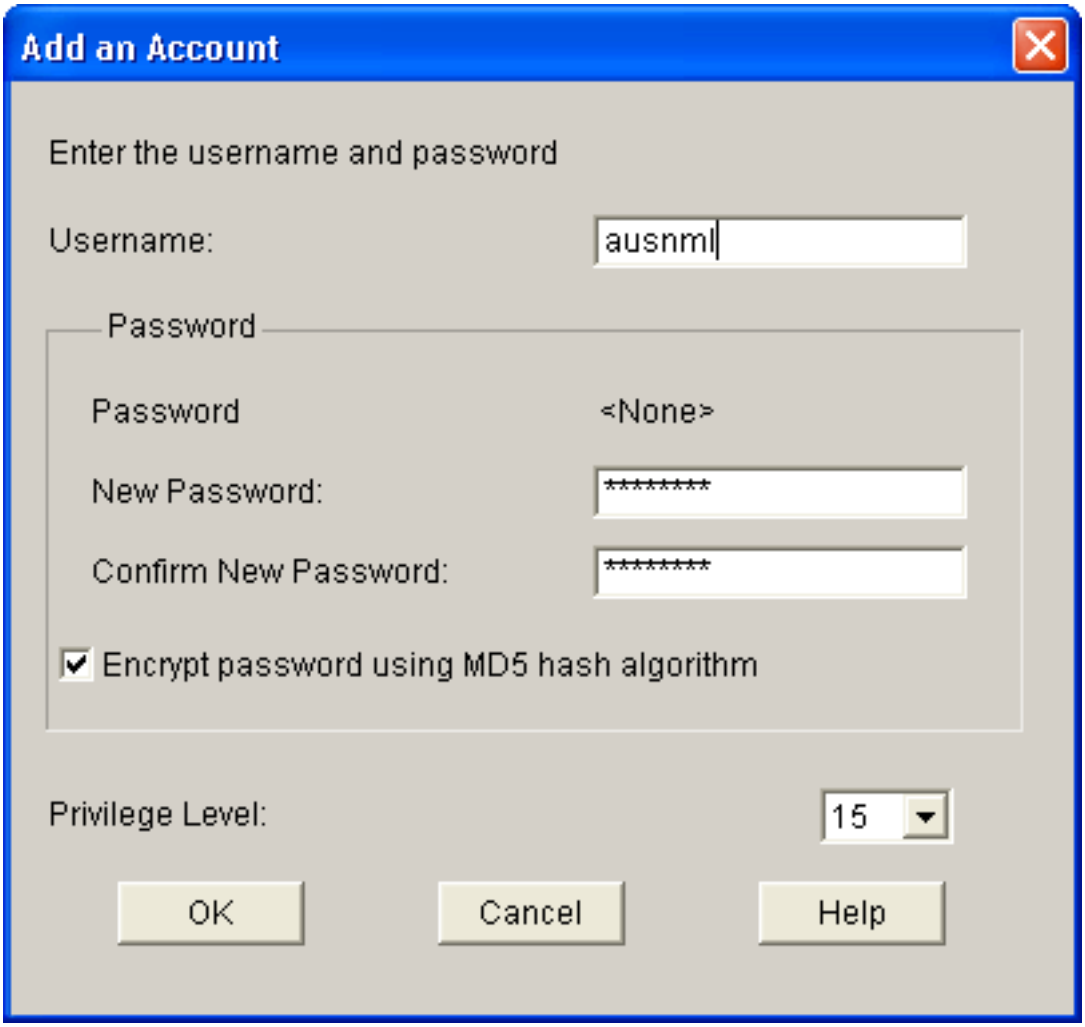
SVC ユーザ用のユーザ データベースを設定するには、次の手順を実行します。

1. 手順 2 を完了した後、[WebVPN Wizard] の [User Authentication] ダイアログ ボックスにある [Locally on this router] ラジオ ボタンをクリックします。



このダイアログ ボックスで、ユーザをローカル データベースに追加できます。

2. [Add]をクリックして、ユーザ情報を入力します。



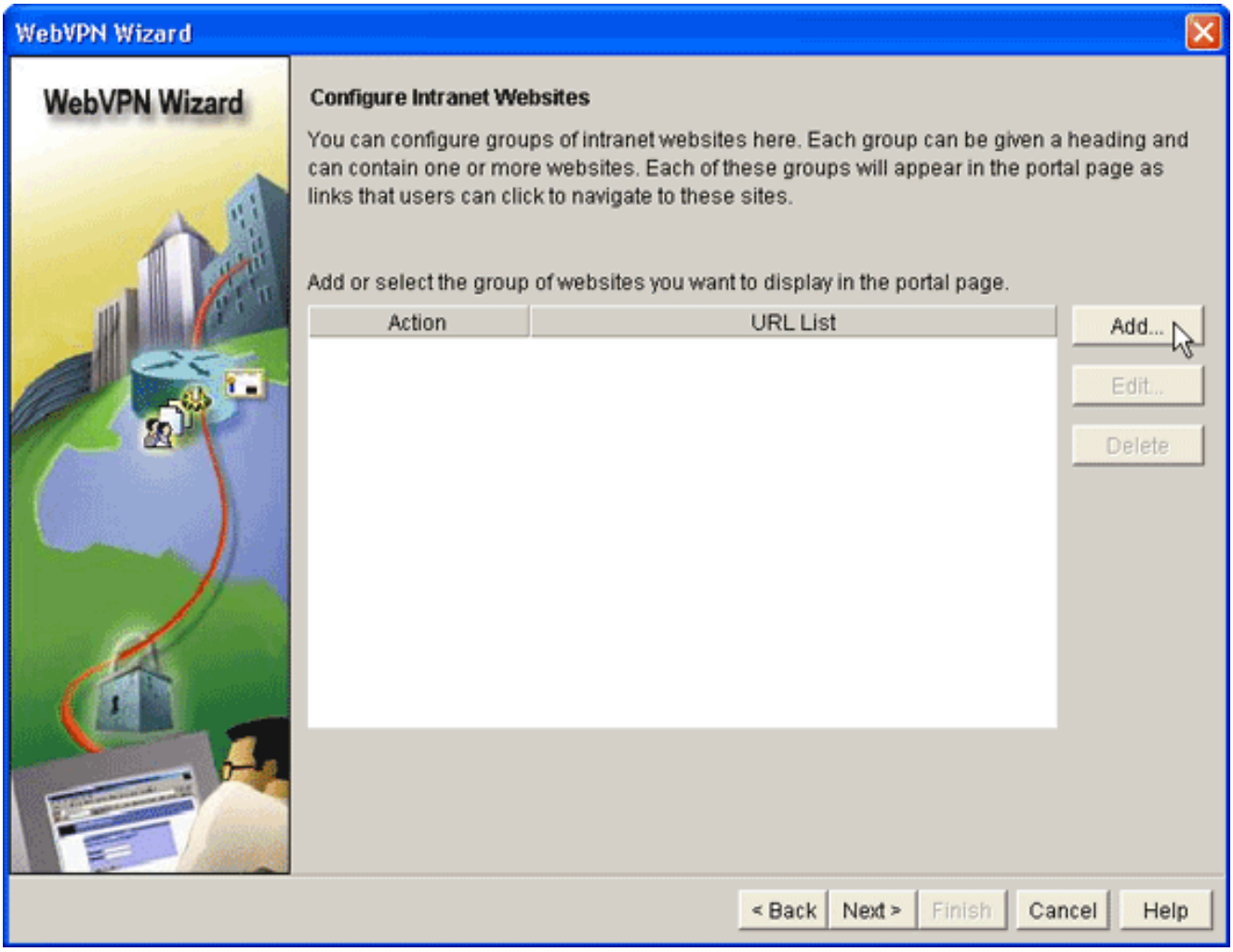
3. [OK]をクリックして、必要に応じてさらにユーザを追加します。
4. 必要なユーザを追加した後、[Next]をクリックして、手順 4 に進みます。

ステップ 4：ユーザに対して表示するリソースを設定する

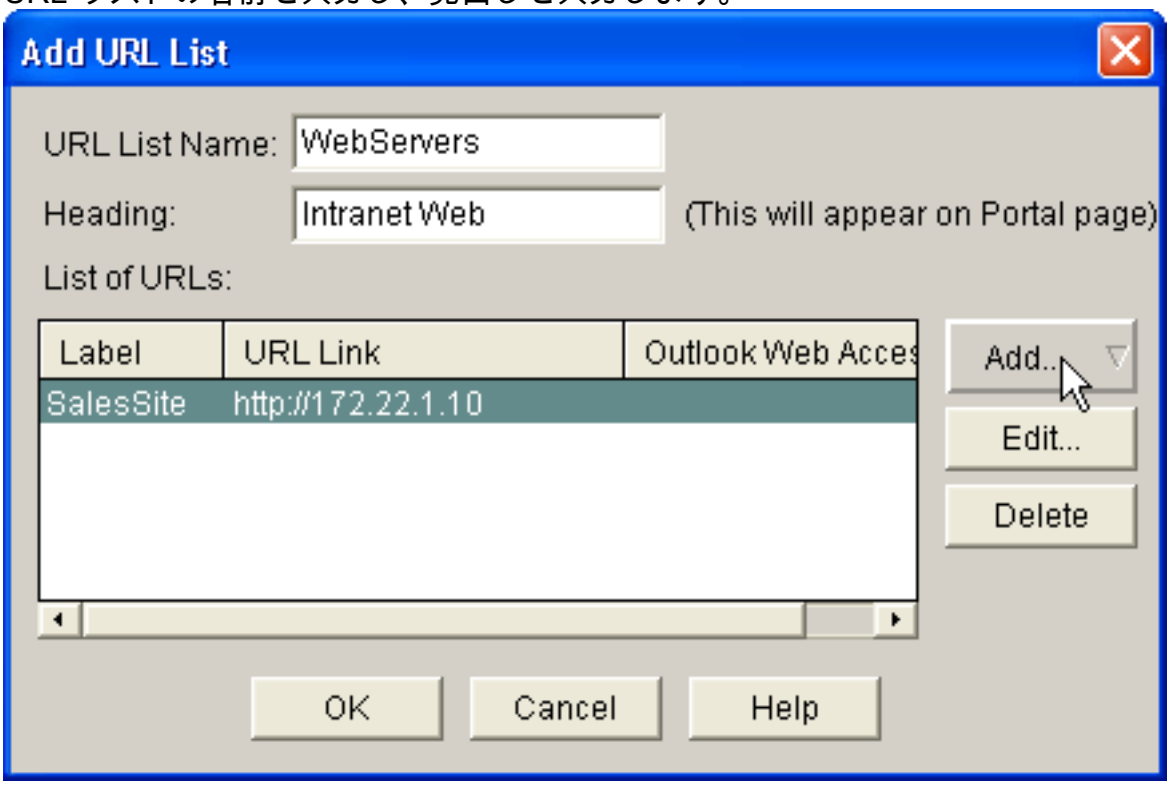
[WebVPN Wizard] の [Configure Intranet Websites] ダイアログ ボックスでは、SVC クライアントに対して表示するイントラネット リソースを選択できます。

ユーザに対して表示されるようにリソースを設定するには、次の手順を実行します。

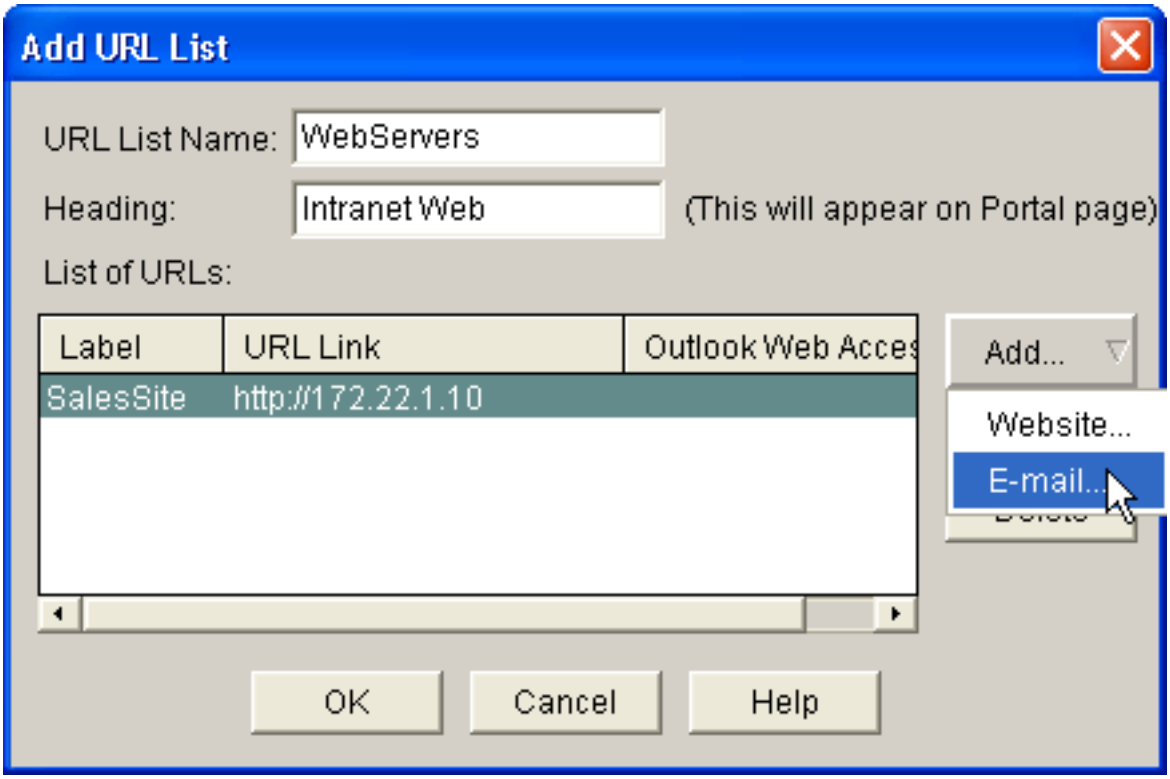
1. 手順 3 を完了した後、[Configure Intranet Websites] ダイアログ ボックスにある [Add] ボタンをクリックします。



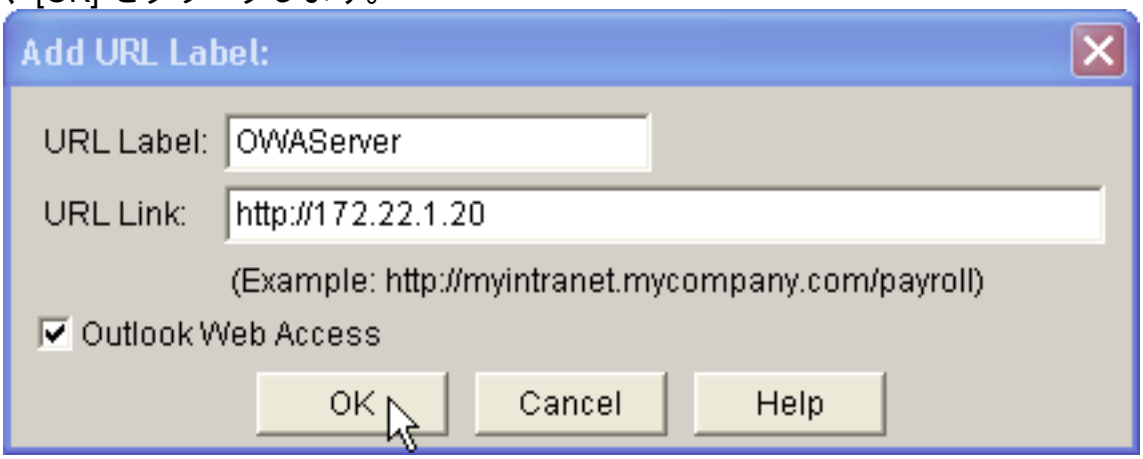
2. URL リストの名前を入力し、見出しを入力します。



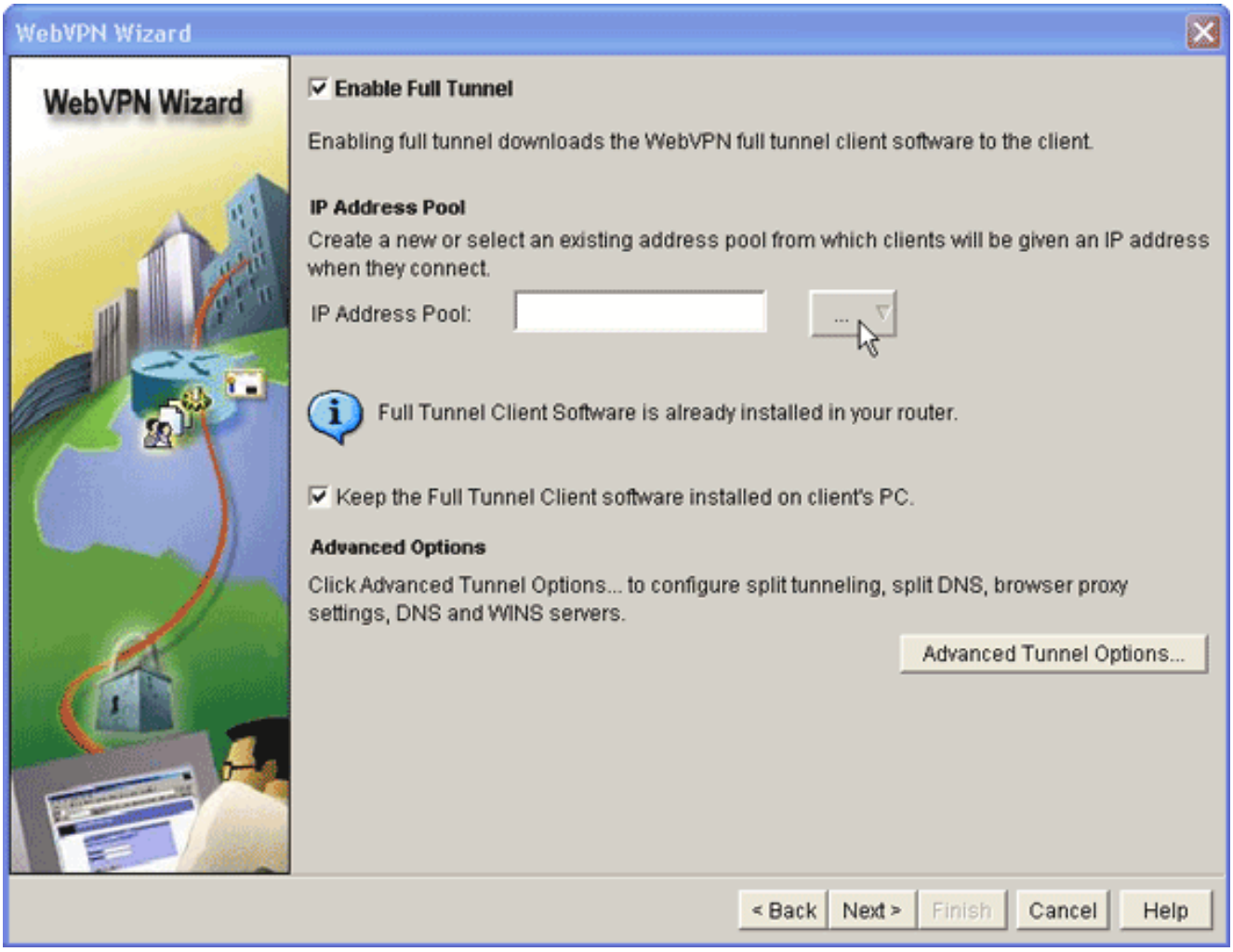
3. [Add]をクリックして、[Website] を選択し、このクライアントに対して表示する Web サイトを追加します。
4. URL とリンク情報を入力し、[OK]をクリックします。
5. OWA Exchange サーバへのアクセスを追加するには、[Add]をクリックして、[E-mail] を選択します。



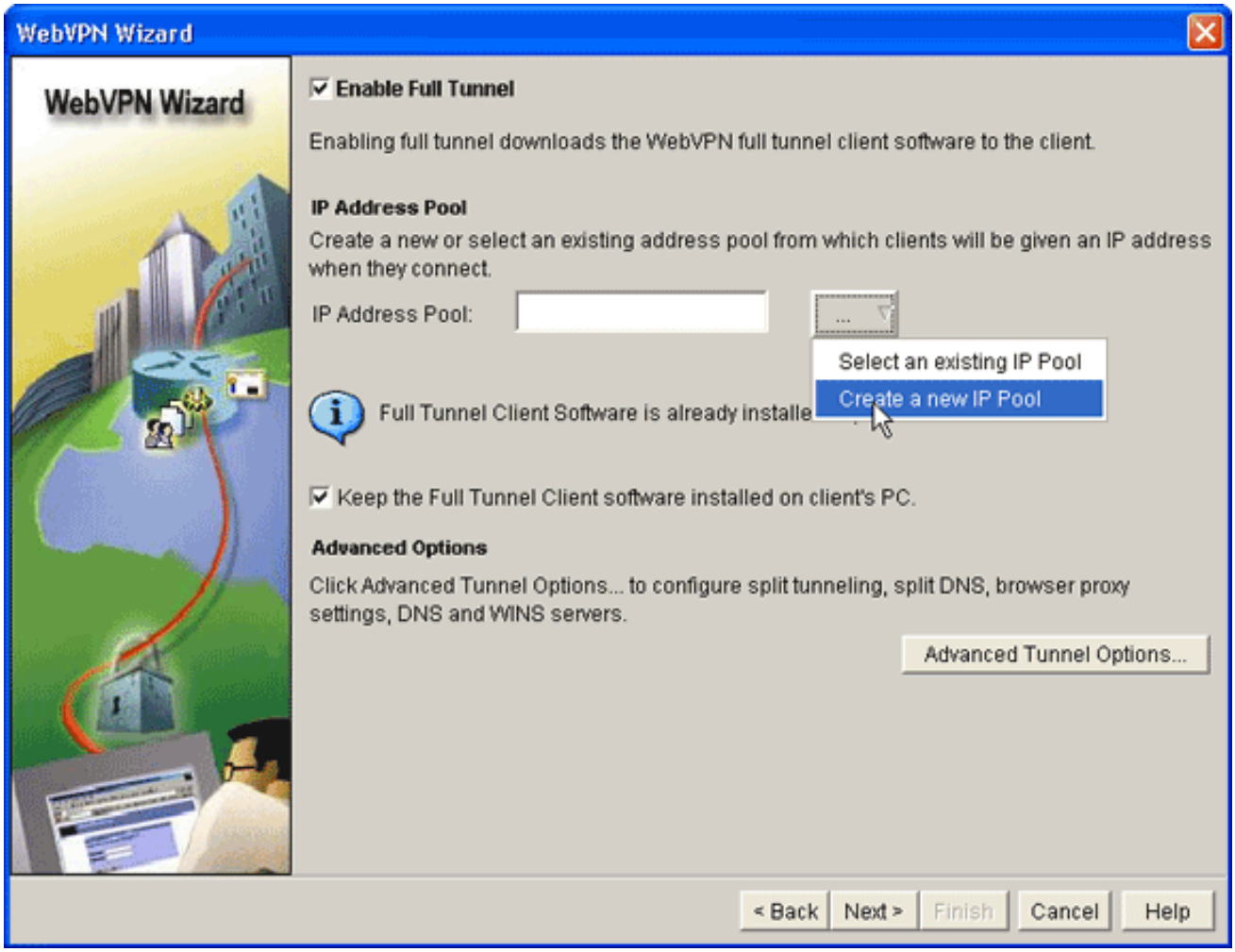
6. [Outlook Web Access]チェック ボックスをオンにして、URL ラベルとリンク情報を入力し、[OK] をクリックします。



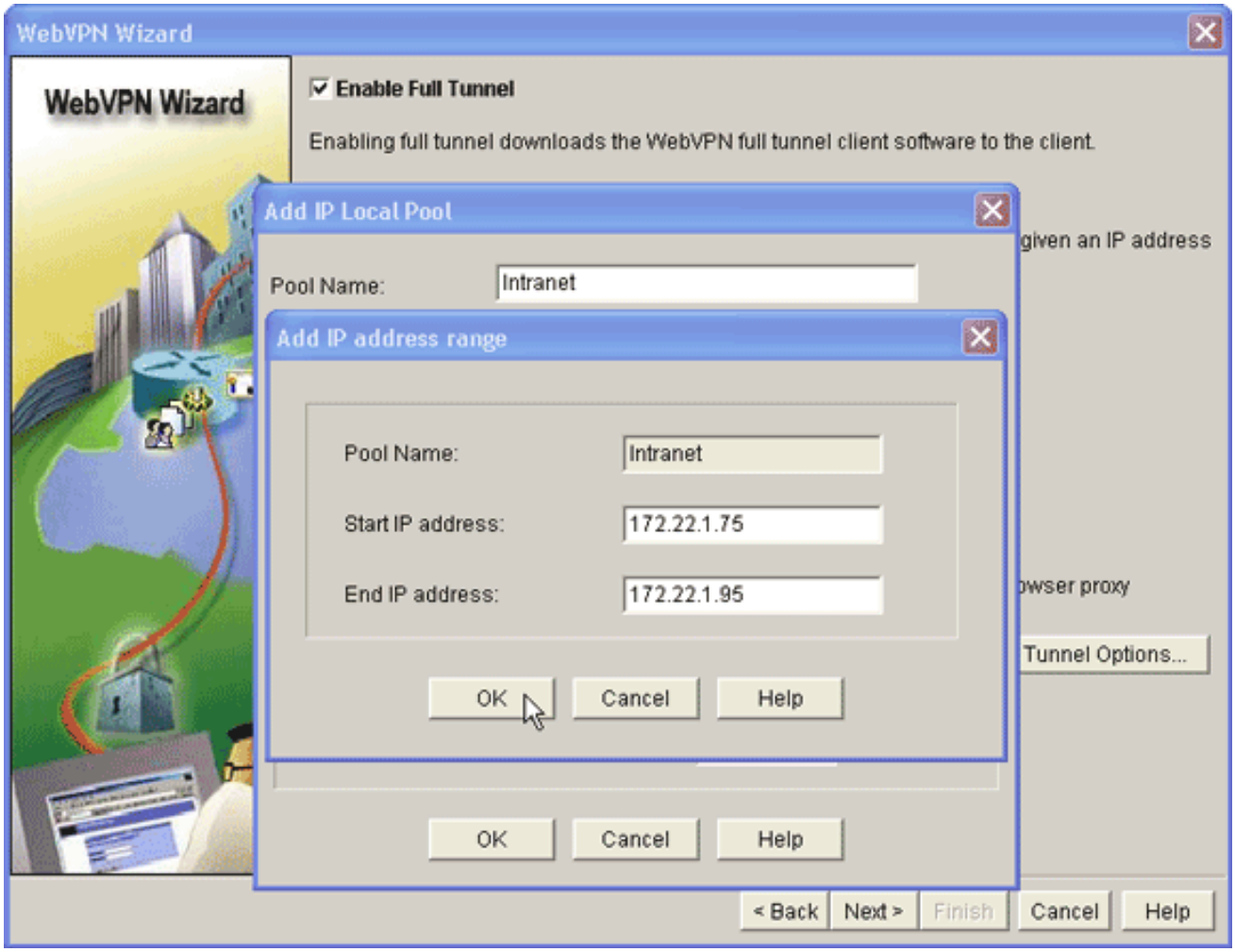
7. 必要なリソースを追加した後、[OK]をクリックし、次に、[Next] をクリックします。[WebVPN Wizard] のフル トンネルのダイアログボックスが表示されます。



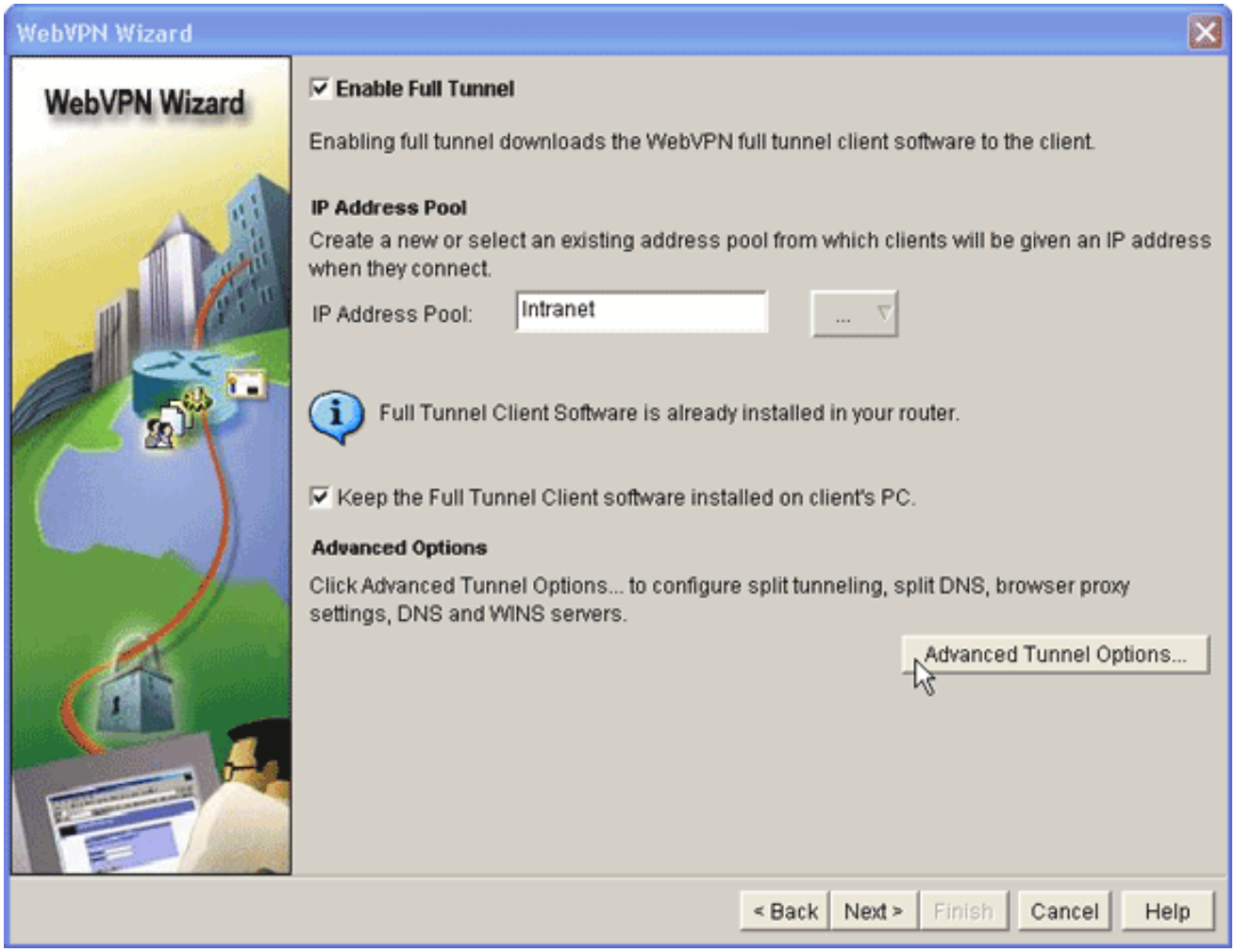
8. [Enable Full Tunnel] チェック ボックスにチェックマークが入っていることを確認します。
9. この WebVPN コンテキストのクライアントが使用できる IP アドレスのプールを作成します。 アドレスのプールは、イントラネット上で使用可能でルーティング可能なアドレスと対応している必要があります。
10. [IP Address Pool] フィールドの横の省略記号（[...]）をクリックし、 [Create a new IP Pool] を選択します。



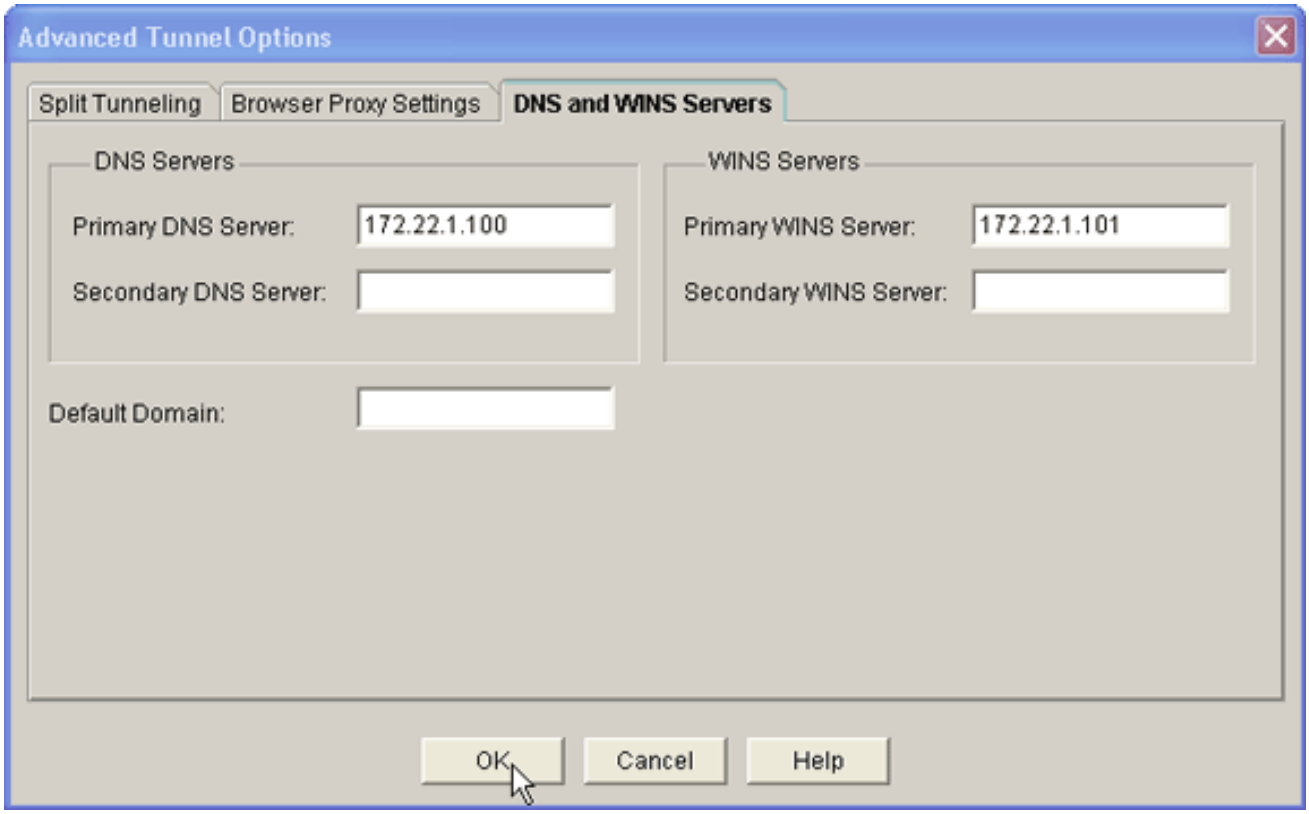
11. [Add IP Local Pool] ダイアログ ボックスで、プールの名前を入力し、[Add]をクリックします。



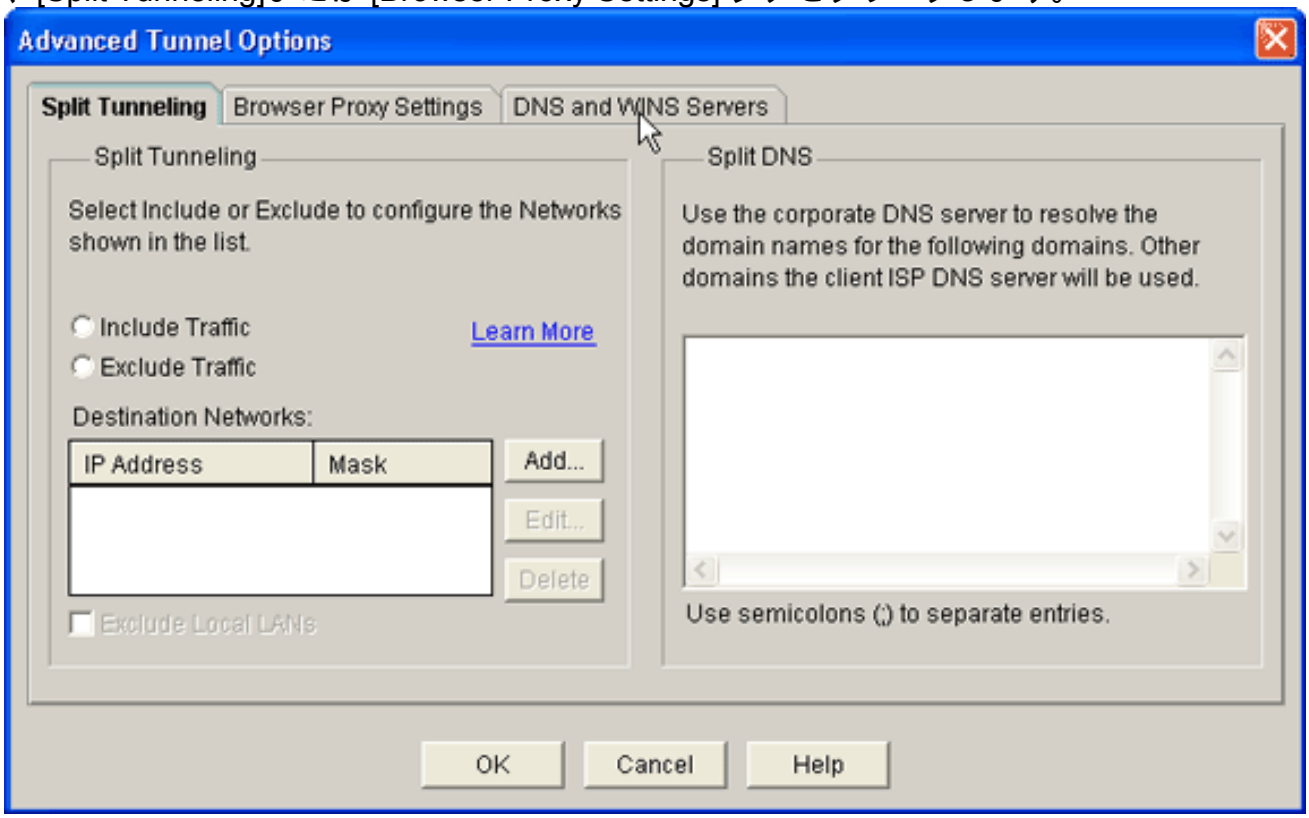
12. [Add IP address range] ダイアログボックスで、SVC クライアントのアドレス プールの範囲を入力し、[OK]をクリックします。**注:** IP アドレス プールは、ルータに直接接続されたインターフェイスの範囲内にする必要があります。 異なるプール範囲を使用する場合は、この要件を満たすために、新しいプールに関連付けるループバック アドレスを作成できます。
13. [OK] をクリックします。



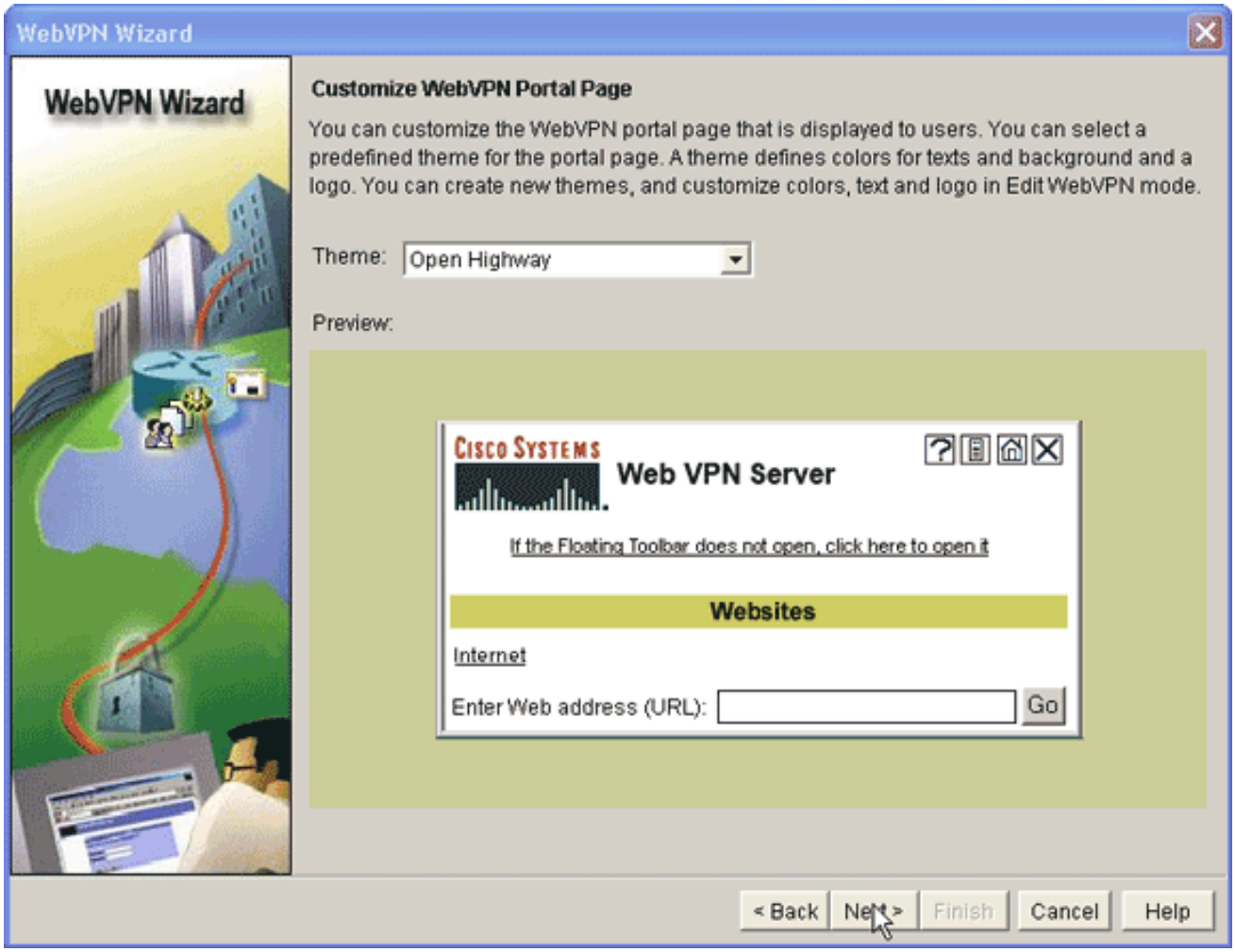
14. リモート クライアントに SVC のコピーを永続的に保存する場合は、[Keep the Full Tunnel Client Software installed on client's PC]をクリックします。 このオプションをクリアすると、クライアントは、接続するたびに SVC ソフトウェアをダウンロードするように要求されます。
15. スプリット トンネリング、スプリット DNS、ブラウザ プロキシ設定、DNS サーバと WNS サーバなどの拡張トンネル オプションを設定します。 シスコでは、最低限 DNS サーバと WINS サーバを設定することを推奨しています。拡張トンネル オプションを設定するには、次の手順を実行します。[Advanced Tunnel Options] ボタンをクリックします。



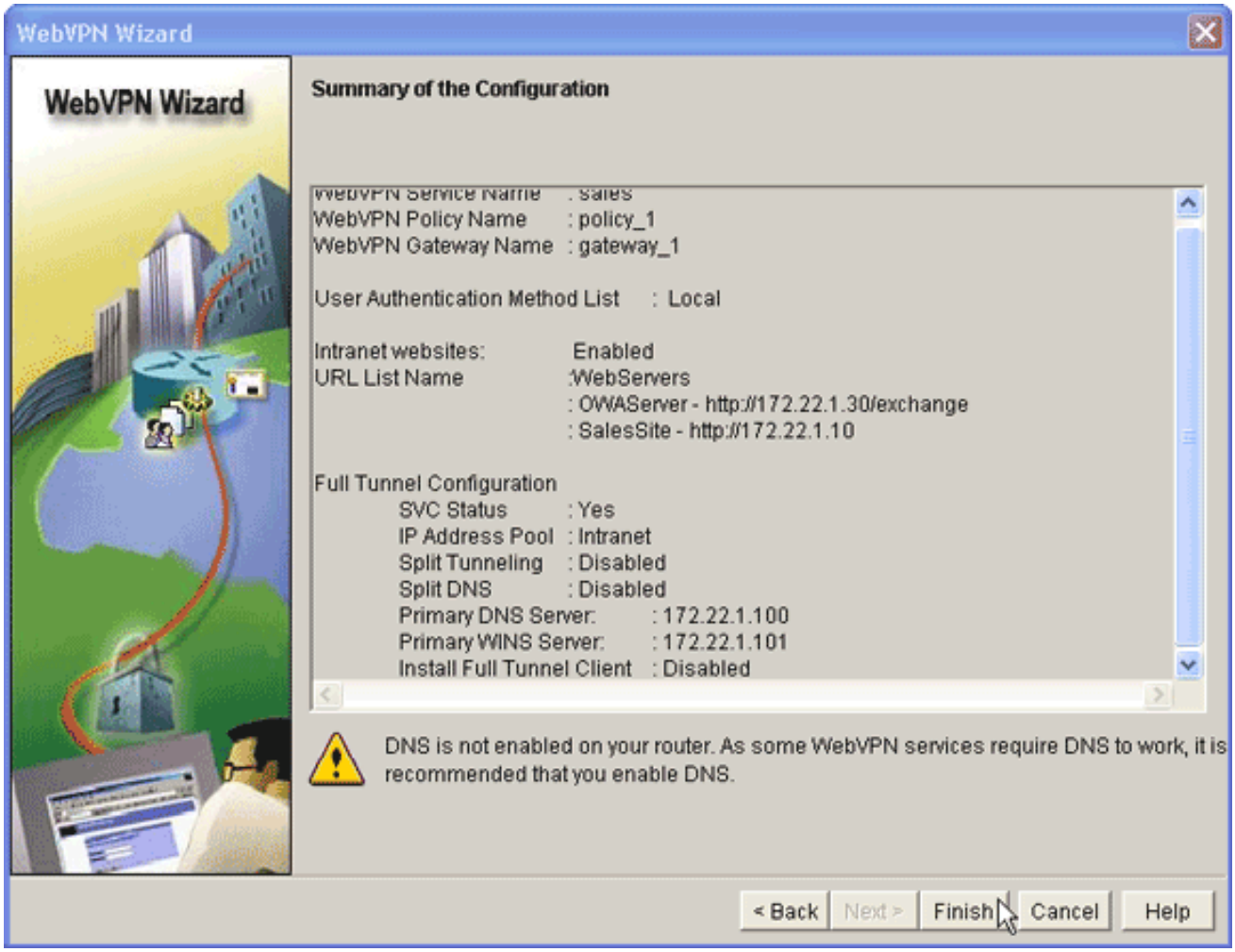
[DNS and WINS Servers]タブをクリックし、DNS サーバと WINS サーバのプライマリ IP アドレスを入力します。スプリット トンネリングとブラウザ プロキシ設定を設定するには、[Split Tunneling]または [Browser Proxy Settings] タブをクリックします。



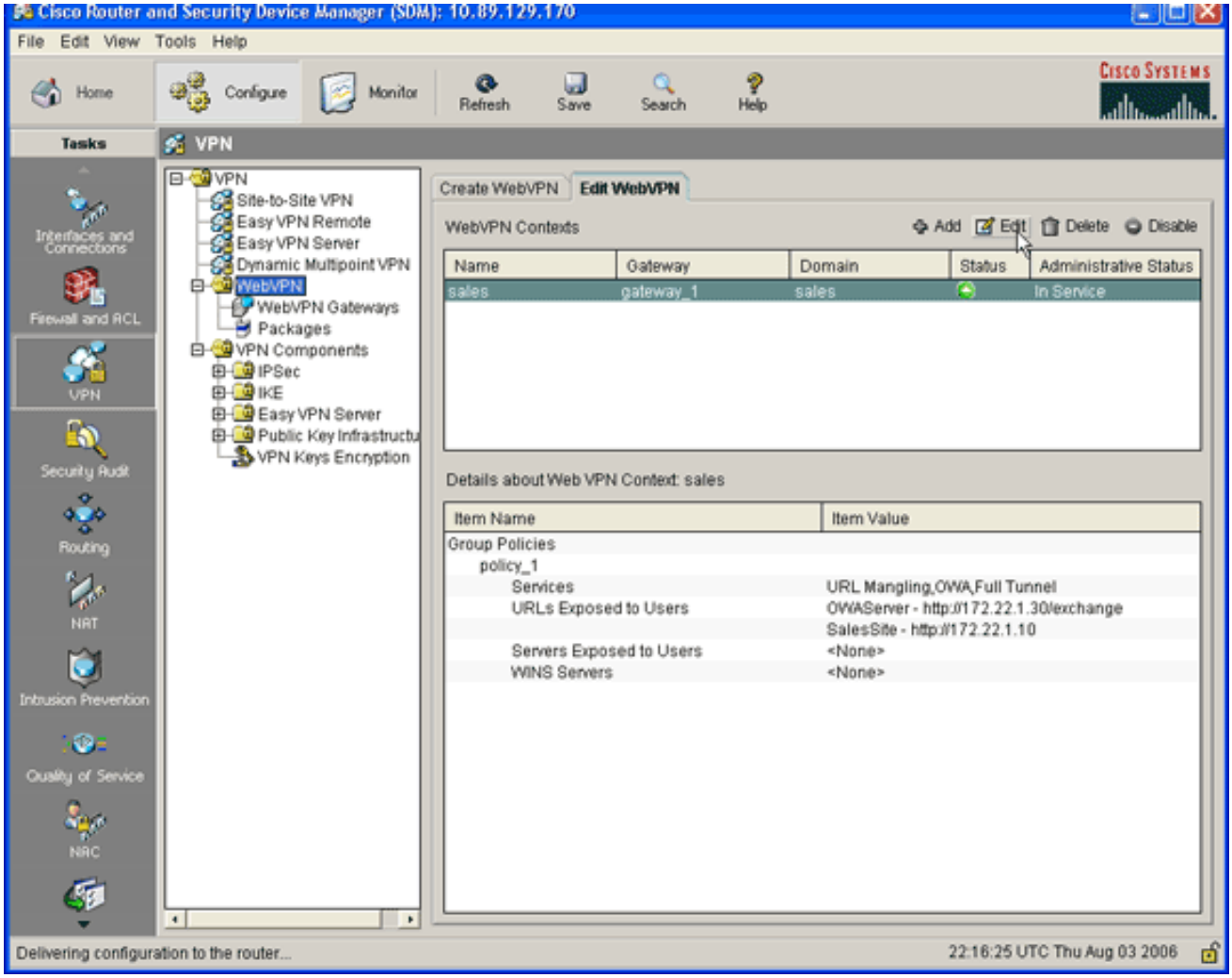
16. 必要なオプションを設定したら、[Next] をクリックします。
17. WebVPN ポータル ページをカスタマイズするか、またはデフォルト値を選択します。[Customize WebVPN Portal Page] では、WebVPN ポータル ページのお客様への表示方法をカスタマイズできます。



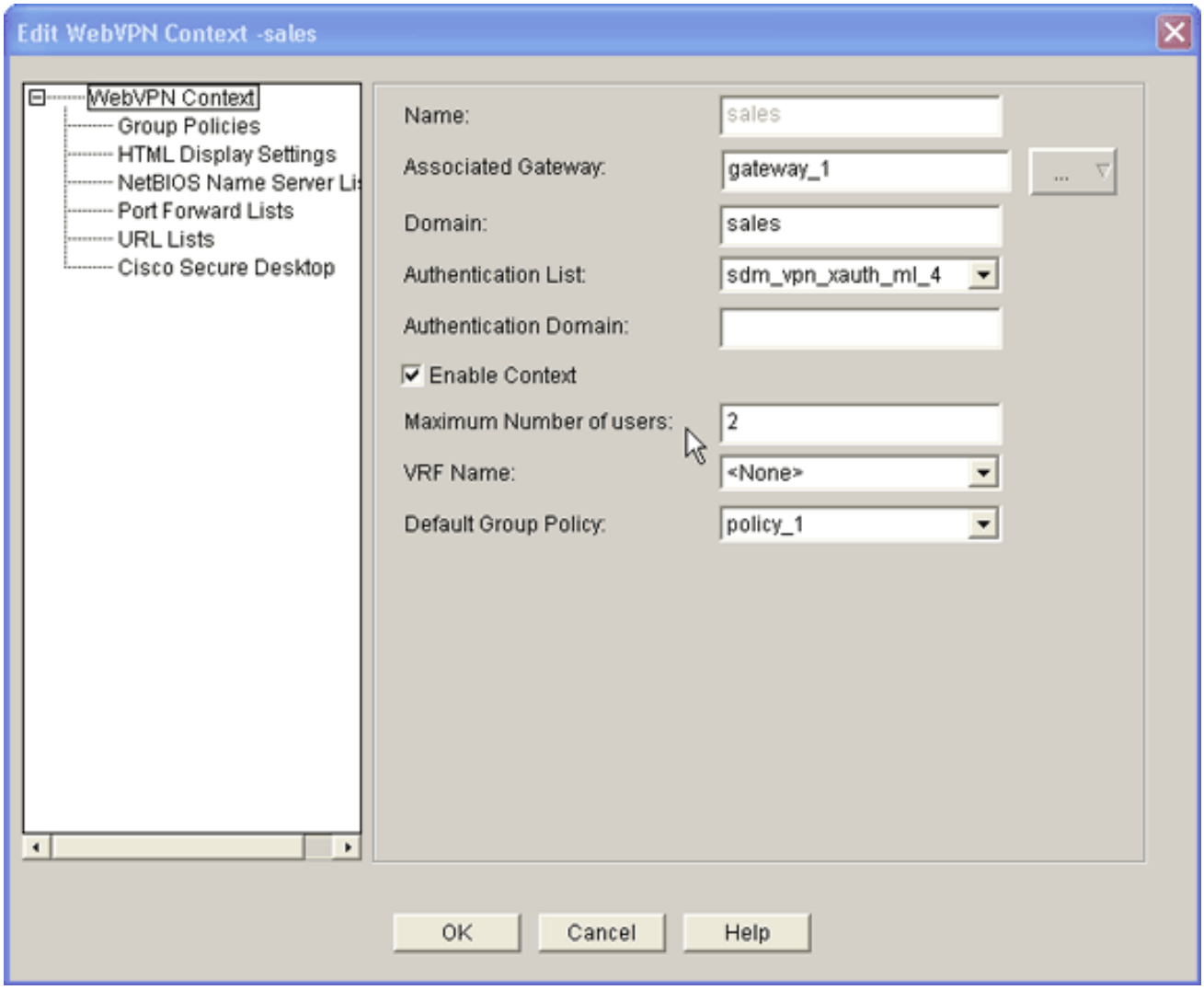
18. WebVPN ポータル ページを設定した後、[Next]をクリックし、[Finish] をクリックしてから、[OK] をクリックします。WebVPN ウィザードは、ルータへ一連のコマンドを送信します。
19. [OK]をクリックして、設定を保存します。**注:** エラー メッセージが表示された場合は、WebVPN ライセンスが不正な可能性があります。 エラー メッセージは、次の図の例のように表示されます。



ライセンス問題を修正するには、次の手順を実行します。[Configure]をクリックし、次に[VPN] をクリックします。[WebVPN]を展開し、[Edit WebVPN] タブをクリックします。



新規作成したコンテキストを選択して、[Edit]ボタンをクリックします。



[Maximum Number of users] フィールドで、ライセンスの正確なユーザ数を入力します。[OK]をクリックし、次に、[OK] をクリックします。コマンドが設定ファイルに書き込まれます。[Save] をクリックし、次に [Yes] をクリックして変更を確定します。

結果

ASDM は次のコマンドライン設定を作成します。

ausnml-3825-01

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

手順

設定をテストするには、SSL 対応のクライアントの Web ブラウザに *http://192.168.0.37/sales* を入力します。

コマンド

いくつかの **show** コマンドは WebVPN に関連しています。 これらのコマンドをコマンドライン インターフェイス (CLI) で実行して、統計情報や他の情報を表示できます。 **show** コマンドの詳細については、「WebVPN 設定の検証」を参照してください。

注: Output Interpreter Tool (OIT) (登録ユーザ専用) では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

SSL 接続の問題

問題： SSL VPN クライアントがルータに接続できない。

解決策： IP アドレスのプールの IP アドレスが不十分なため、この問題が発生している可能性があります。 この問題を解決するには、ルータの IP アドレス プールの IP アドレス数を増やします。

トラブルシューティングのためのコマンド

いくつかの **clear コマンド**は、WebVPN に関連しています。 これらのコマンドの詳細については、「WebVPN の Clear コマンドの使用」を参照してください。

いくつかの **debug コマンド**は、WebVPN に関連しています。 これらのコマンドの詳細については、「WebVPN の Debug コマンドの使用」を参照してください。

注: **debug** コマンドを使用すると、シスコ デバイスに悪影響が及ぶ可能性があります。 **debug コマンド**を使用する前に、「debug コマンドの重要な情報」を参照してください。

関連情報

- Cisco IOS SSLVPN

- SSL VPN - WebVPN
- SDM を使用した Cisco IOS でのクライアントレス SSL VPN (WebVPN) の設定例
- SDM によるシンクライアント SSL VPN (WebVPN) の IOS 設定例
- WebVPN および DMVPN コンバージェンス導入ガイド
- テクニカル サポートとドキュメント – Cisco Systems