

SDMによるシンククライアントSSL VPN(WebVPN)Cisco IOSの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[タスク](#)

[ネットワーク図](#)

[シンククライアント SSL VPN の設定](#)

[コンフィギュレーション](#)

[確認](#)

[設定の確認](#)

[コマンド](#)

[トラブルシューティング](#)

[トラブルシューティングに使用するコマンド](#)

[関連情報](#)

概要

シンククライアント SSL VPN テクノロジーを使用して、スタティック ポートを使用するアプリケーションにセキュアなアクセスが可能です。セキュアなアクセスの例としては、Telnet (23)、SSH (22)、POP3 (110)、IMAP4 (143)、および SMTP (25) があります。シンククライアントは、ユーザ主導、ポリシー主導、またはその両方の場合があります。アクセス権はユーザ単位で設定でき、また 1 人以上のユーザを含むグループ ポリシーを作成できます。SSL VPN テクノロジーは 3 種類の主要なモードで設定できます。、すなわち、クライアントレス SSL VPN (WebVPN)、シンククライアント SSL VPN (ポート フォワーディング)、および SSL VPN クライアント (SVC フル トンネル モード) です。

1. クライアントレス SSL VPN (WebVPN):

リモート クライアント側で必要になるのは、企業 LAN 上にある http 対応または https 対応 Web サーバにアクセスするための SSL 対応 Web ブラウザだけです。このアクセスは、Common Internet File System (CIFS) による Windows ファイルのブラウズに利用可能です。http アクセスの例としては、Outlook Web Access (OWA) クライアントが挙げられます。

クライアントレス SSL VPN についての詳細は、『』を参照してください。

2. シンククライアント SSL VPN (ポート フォワーディング)

リモートクライアントにサイズの小さい Java ベースの アプレット をダウンロードすることで、静的ポート番号を使用する TCP アプリケーションの安全なアクセスを実現します。UDP はサポートされていません。このアクセス方法の例としては、POP3、SMTP、IMAP、SSH、および Telnet が挙げられます。ローカル マシン上のファイルに変更が加えられるため、ユーザにローカル管理者権限が必要になります。この SSL VPN 方式は、一部の FTP アプリケーションなど、動的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。

3. SSL VPN Client (SVCフルトンネルモード) :

SSL VPN クライアントがリモートワークステーションにスモールクライアントをダウンロードすることで、社内ネットワーク上のリソースへの安全な完全アクセスを実現します。SVC はリモートステーションにダウンロードしたままにしておくことも、安全なセッションの終了後に削除することも可能です。

SSL VPN Client の詳細は、『[SDM を使用した IOS での SSL VPN Client \(SVC \) の設定例](#)』を参照してください。

このドキュメントでは、Cisco IOS® ルータでのシンクライアント SSL VPN の簡単な設定を示します。シンクライアント SSL VPN は次の Cisco IOS ルータで動作します。

- Cisco 870、1811、1841、2801、2811、2821、および 2851 シリーズ ルータ
- Cisco 3725、3745、3825、3845、7200、および 7301 シリーズ ルータ

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。

Cisco IOS ルータの要件

- リストされたルータのいずれかで、SDM および IOS バージョン 12.4(6)T 以降の拡張イメージがロードされていること
- SDM をロードした管理ステーションシスコでは SDM のコピーをプリインストールした新しいルータを出荷しています。ご使用のルータに SDM がインストールされていない場合は、[\[Software Download-Cisco Security Device Manager\]](#) でソフトウェアを入手できます。サービス契約を結んでいる Cisco.com アカウントが必要です。詳細手順は、『[Security Device Manager でのルータの設定](#)』を参照してください。

クライアント コンピュータの要件

- リモートクライアントには、ローカルの管理者権限があること。これは必須事項ではありませんが、重要な推奨事項です。
- リモートクライアントには、Java Runtime Environment (JRE) バージョン 1.4 以降が必要です。
- リモートクライアント ブラウザ : Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2、Firefox 1.0 のいずれか
- リモートクライアントでクッキーがイネーブルにされており、ポップアップが許可されていること。

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いています。

- Cisco Advanced Enterprise ソフトウェア イメージ 12.4(9)T
- Cisco 3825 サービス統合型ルータ
- Cisco Router and Security Device Manager (SDM) バージョン 2.3.1

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ました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。この設定に使用されている IP アドレスは RFC 1918 アドレススペースからのものです。これらはインターネット上で正式なものではありません。

表記法

ドキュメント表記の詳細については、『[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。

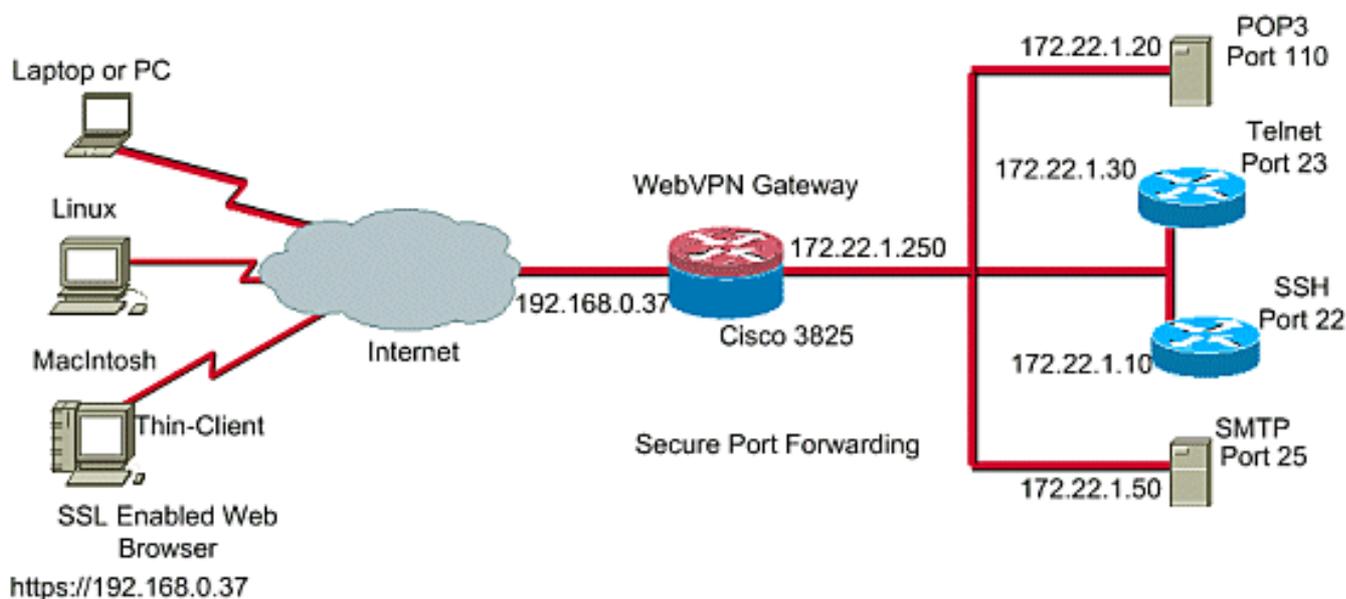
設定

タスク

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供します。

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 セットアップを使用します。

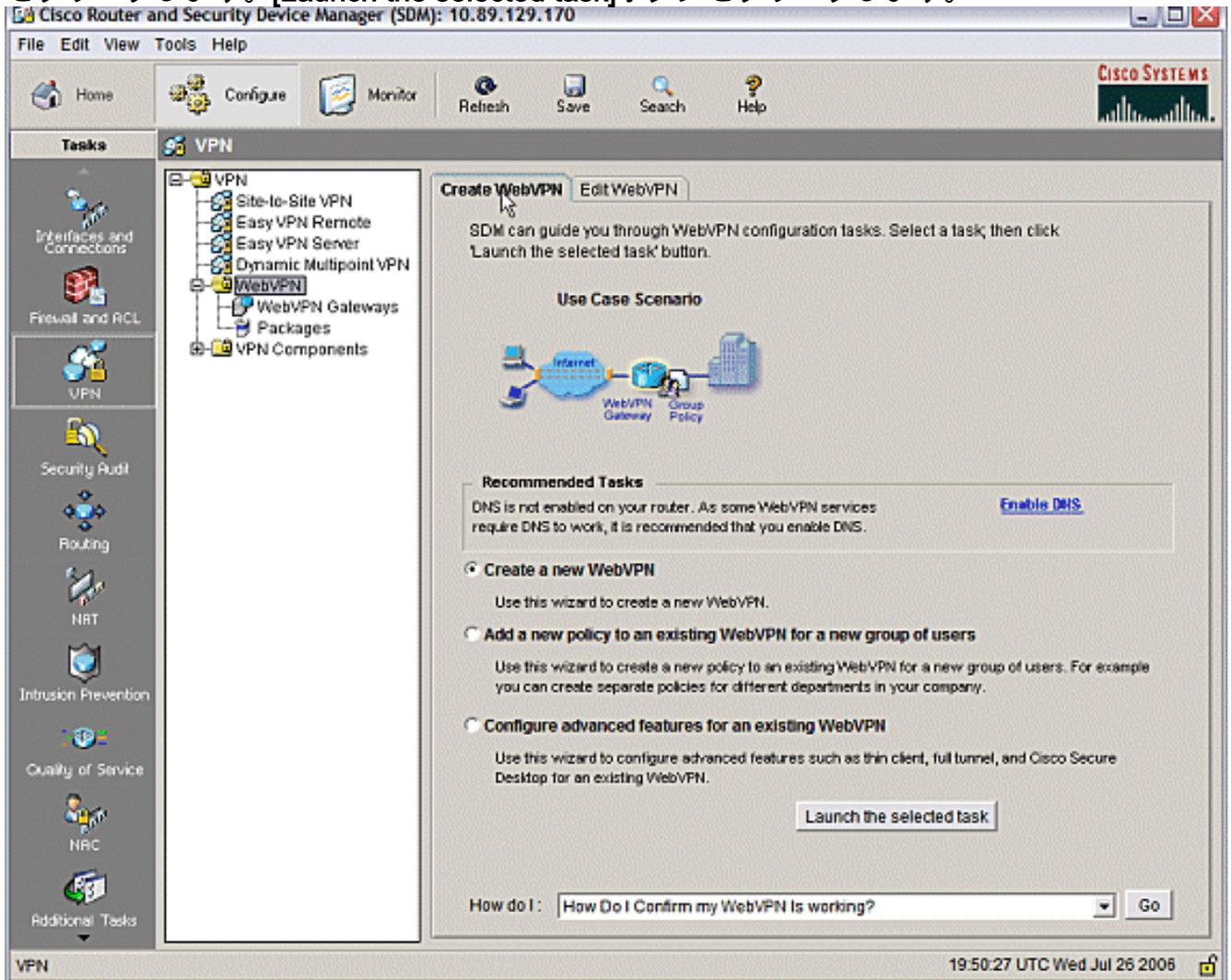


シンクライアント SSL VPN の設定

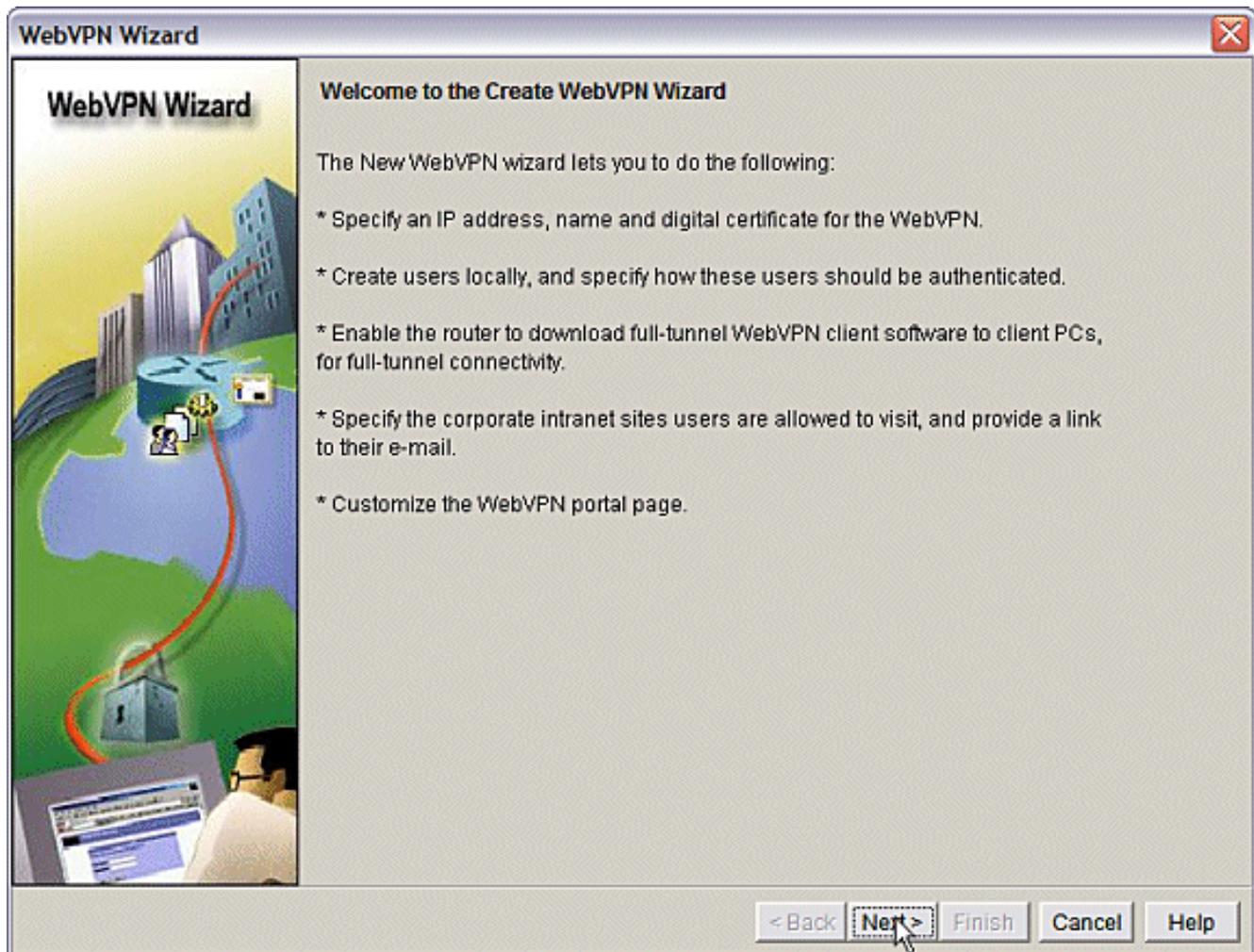
Security Device Manager (SDM) インターフェイスで提供されるウィザードを使用して、Cisco

IOS でシンクライアント SSL VPN を設定するか、コマンドライン インターフェイス (CLI) で設定するか、または SDM アプリケーションで手動で設定します。この例では、ウィザードを使用します。

1. [Configure] タブを選択します。ナビゲーション ペインで [VPN] > [WebVPN] を選択します。
。 [Create WebVPN] タブをクリックします。 [Create a new WebVPN] の横のラジオ ボタンをクリックします。 [Launch the selected task] ボタンをクリックします。



2. WebVPN ウィザードが起動します。 [next] をクリックします。



この WebVPN ゲートウェイの IP アドレスと一意な名前を入力します。[next] をクリックします。

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.

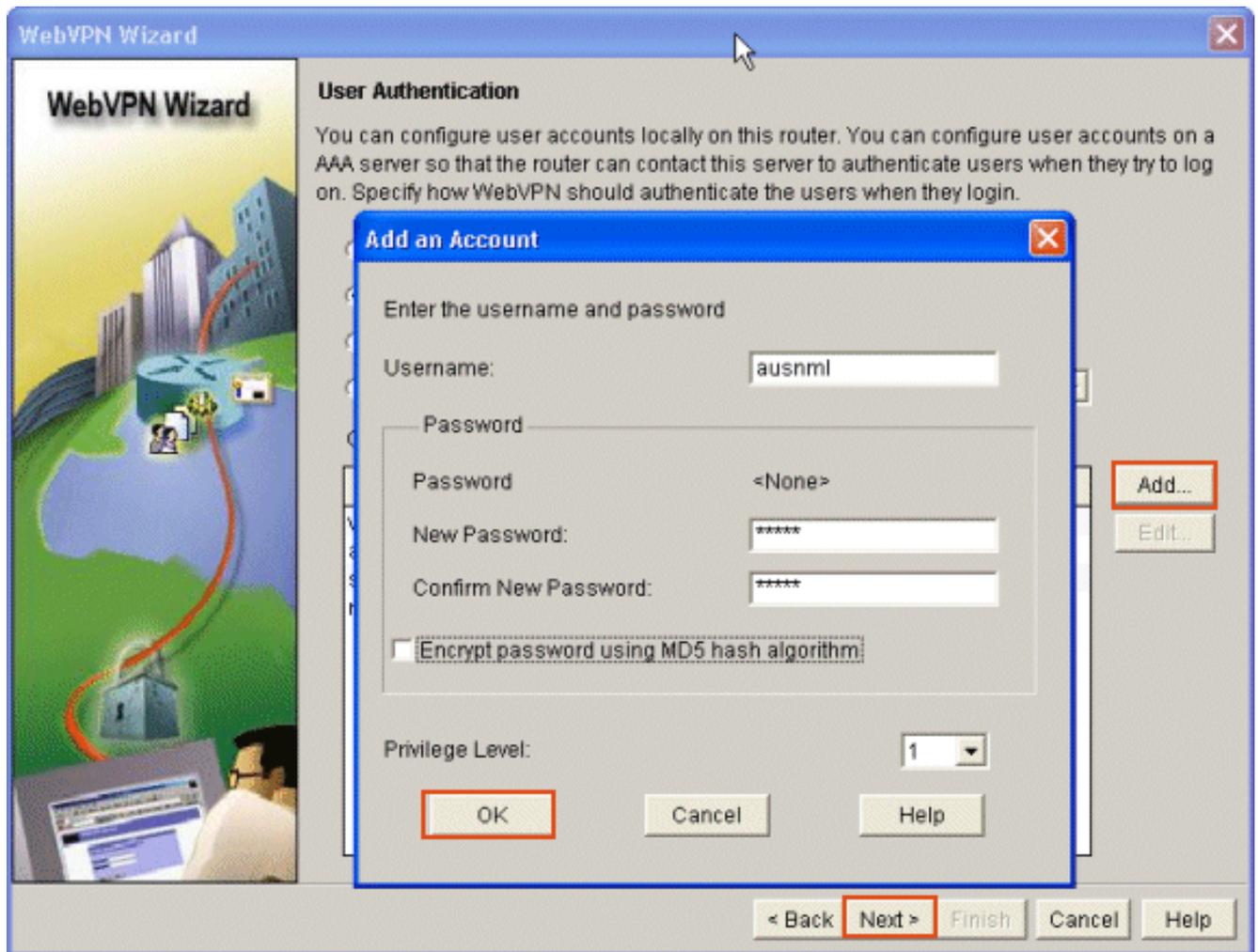
Certificate:

Information

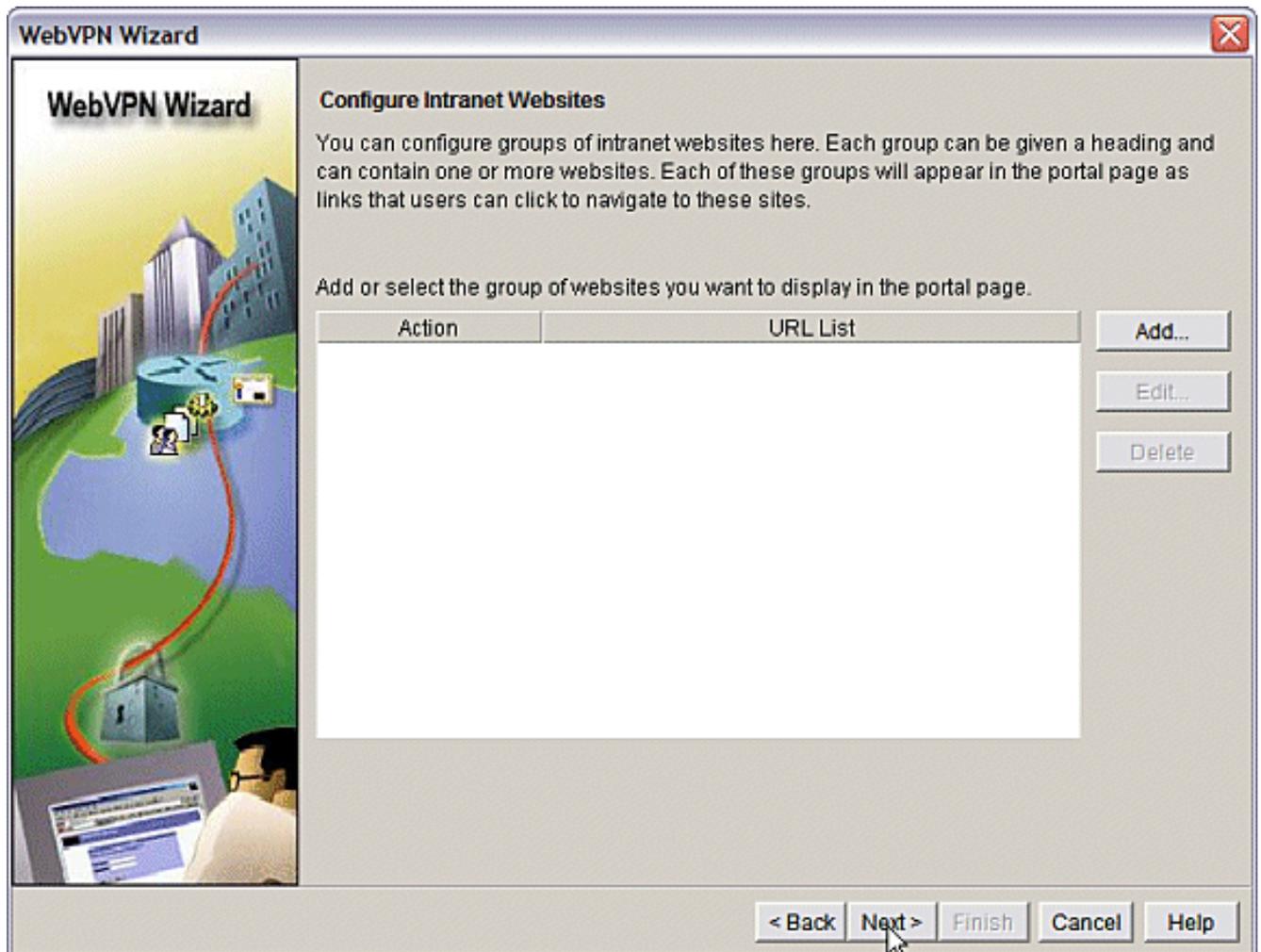
URL to login to this WebVPN service: <https://192.168.0.37/webvpn>

< Back Next > Finish Cancel Help

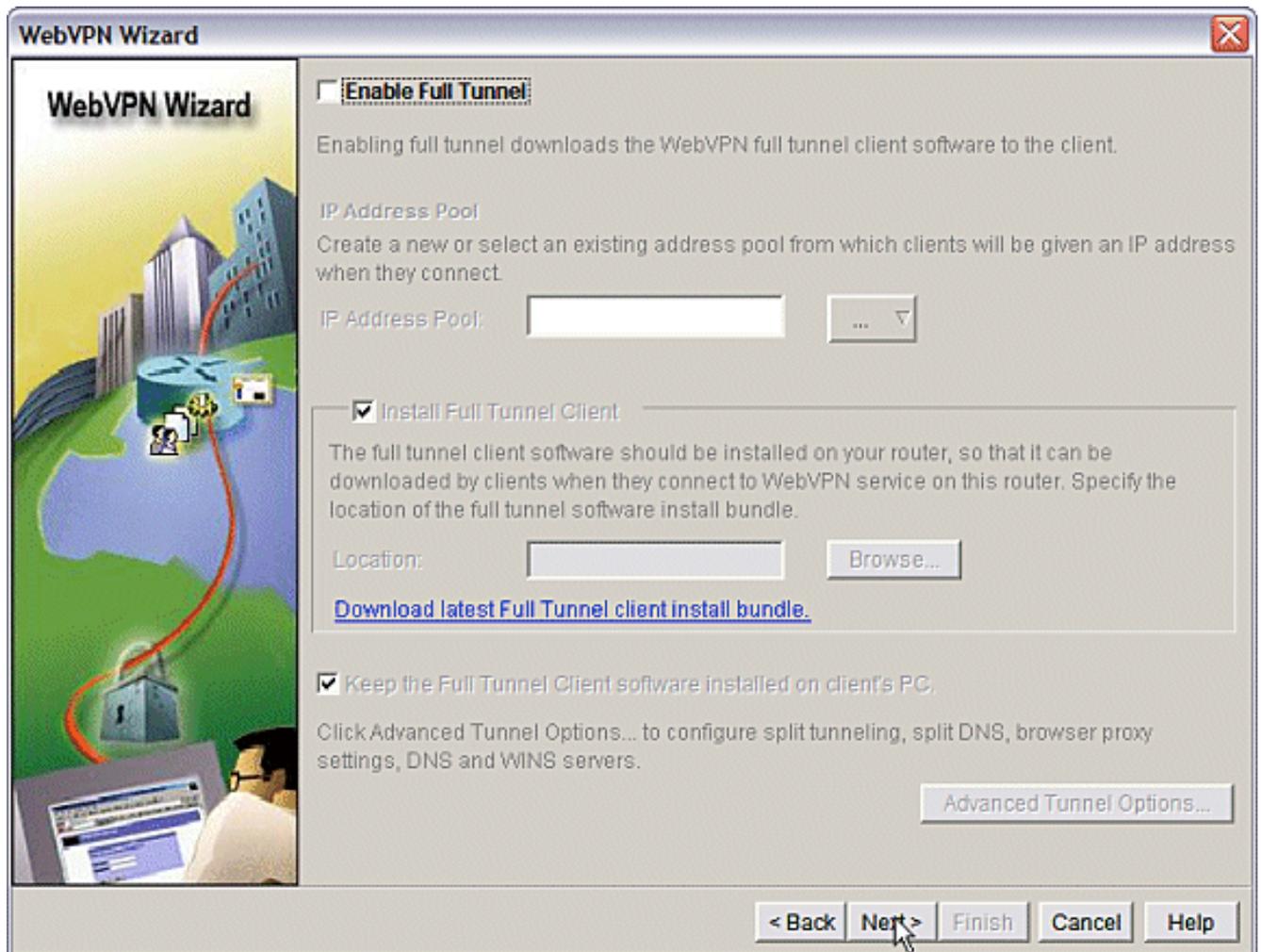
3. [User Authentication] 画面でユーザの認証を実行できます。この設定では、ルータでローカルに作成されたアカウントを使用します。Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントリング) サーバを使用することもできます。ユーザを追加するには、[Add] をクリックします。[Add an Account] 画面でユーザ情報を入力し、[OK] をクリックします。[User Authentication] 画面で [Next] をクリックします。



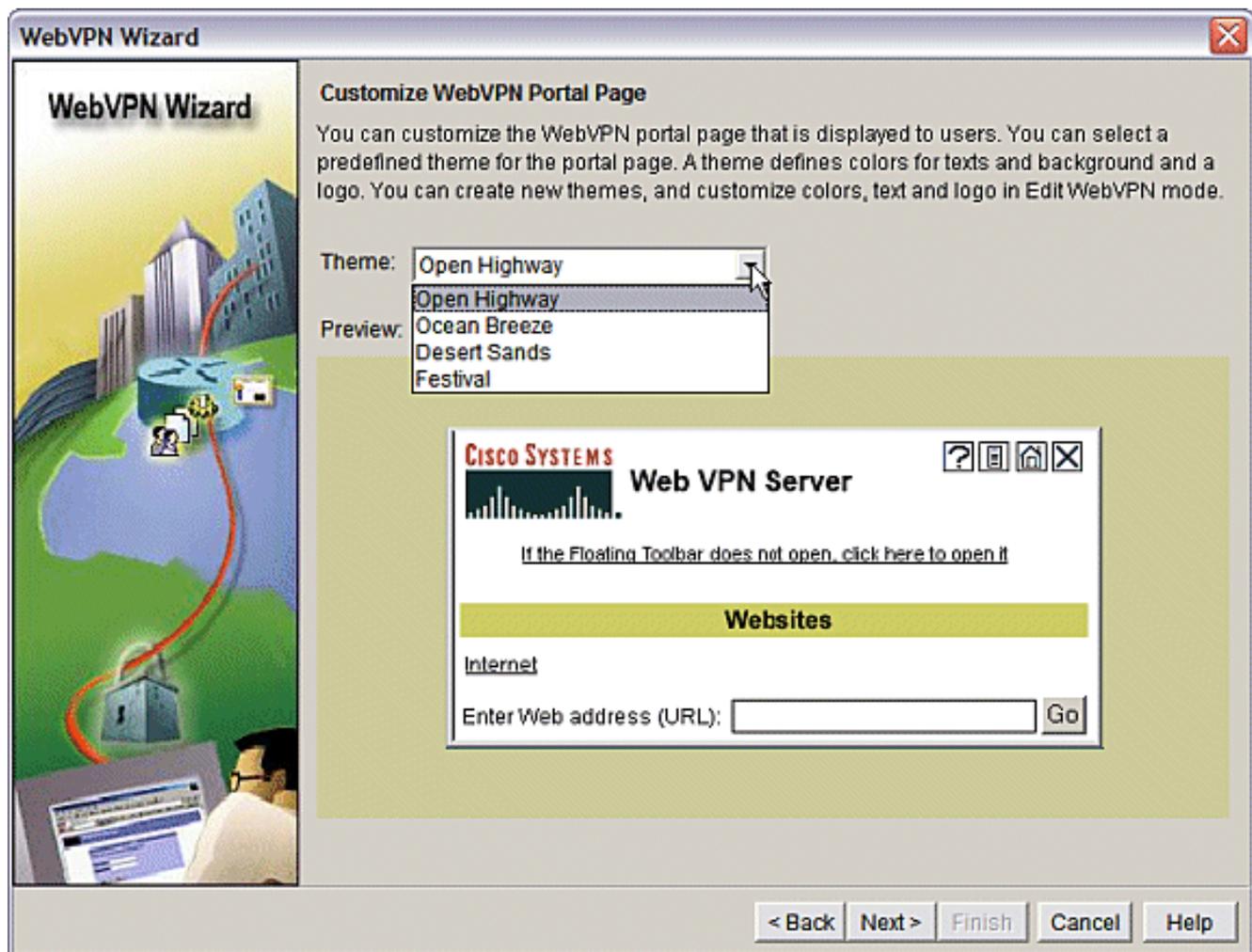
WebVPN ウィザード画面でイントラネット Web サイトを設定できますが、このアプリケーション アクセスにはポート フォワーディングが使用されているため、この手順は省略されます。Web サイトへのアクセスを許可する場合は、クライアントレス SSL VPN 設定またはフル クライアント SSL VPN 設定を使用します。これについての説明はこのドキュメントの範囲外です。



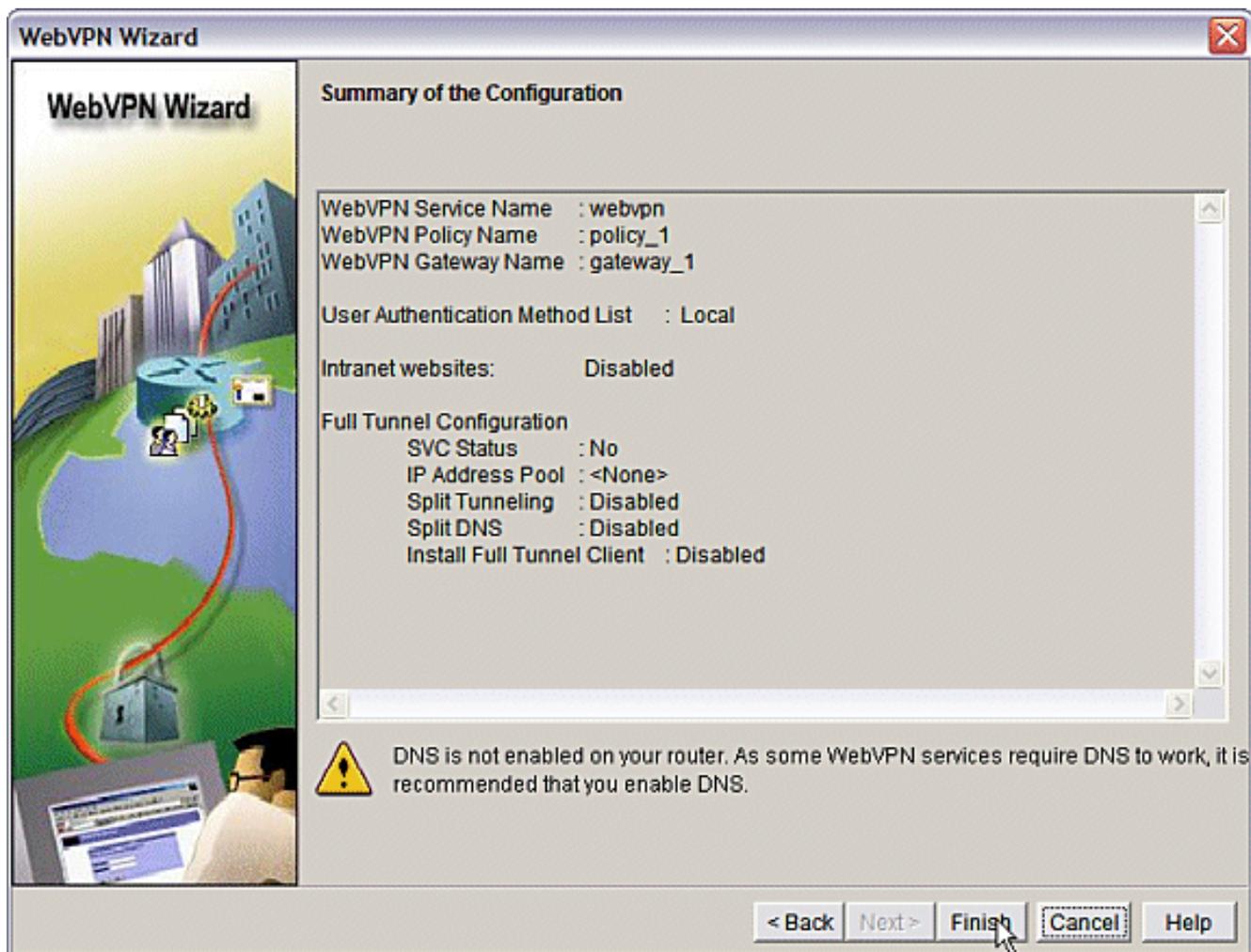
[next] をクリックします。ウィザードでフルトンネルクライアントを設定できる画面が表示されます。これは、シンクライアント SSL VPN (ポートフォワーディング) には適用されません。[Enable Full Tunnel] のチェックマークを外します。[next] をクリックします。



4. WebVPN ポータル ページの外観をカスタマイズするか、デフォルトの外観を承認します。
[next] をクリックします。



設定の概要をプレビューし、[Finish] > [Save] をクリックします。



5. WebVPN ゲートウェイとグループ ポリシーにリンクした WebVPN コンテキストが作成されました。クライアントが WebVPN に接続すると使用可能になるシンクライアント ポートを設定します。[Configure] を選択します。[VPN] > [WebVPN] を選択します。[Create WebVPN] を選択します。[Configure advanced features for an existing WebVPN] ラジオ ボタンを選択し、[Launch the selected task] をクリックします。

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

Interfaces 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](#)

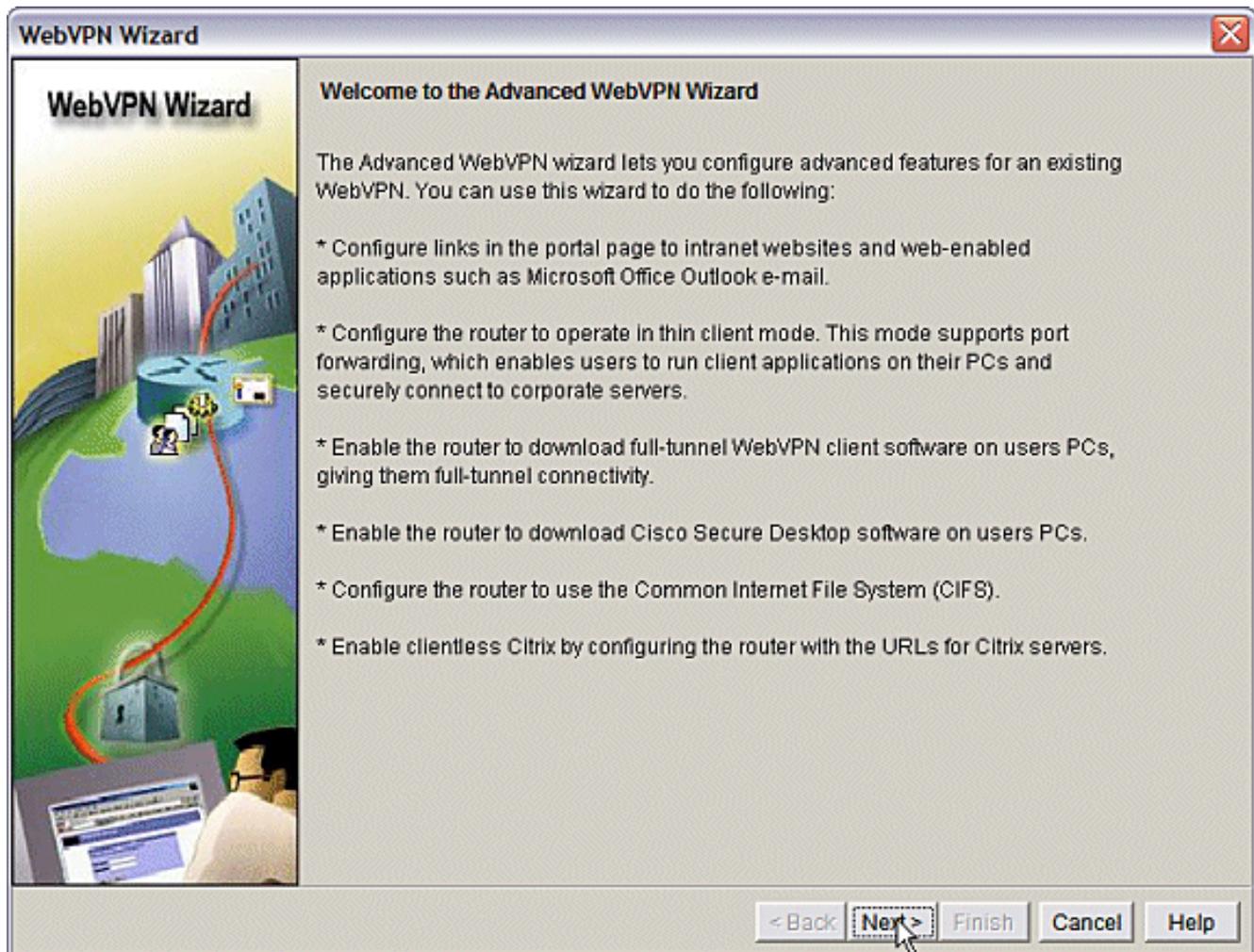
- Create a new WebVPN
Use this wizard to create a new WebVPN.
- Add a new policy to an existing WebVPN for a new group of users
Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.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

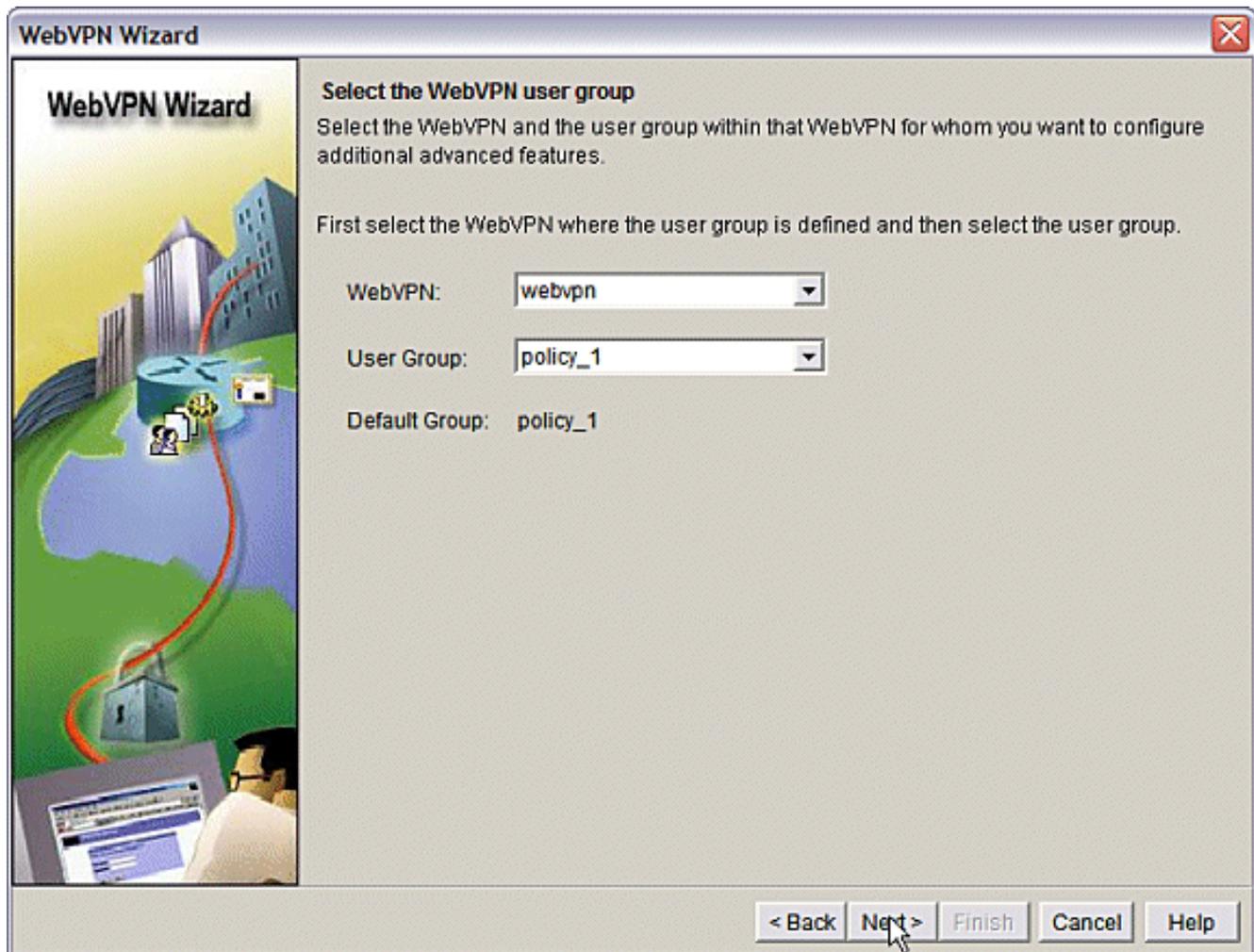
How do I: Go

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

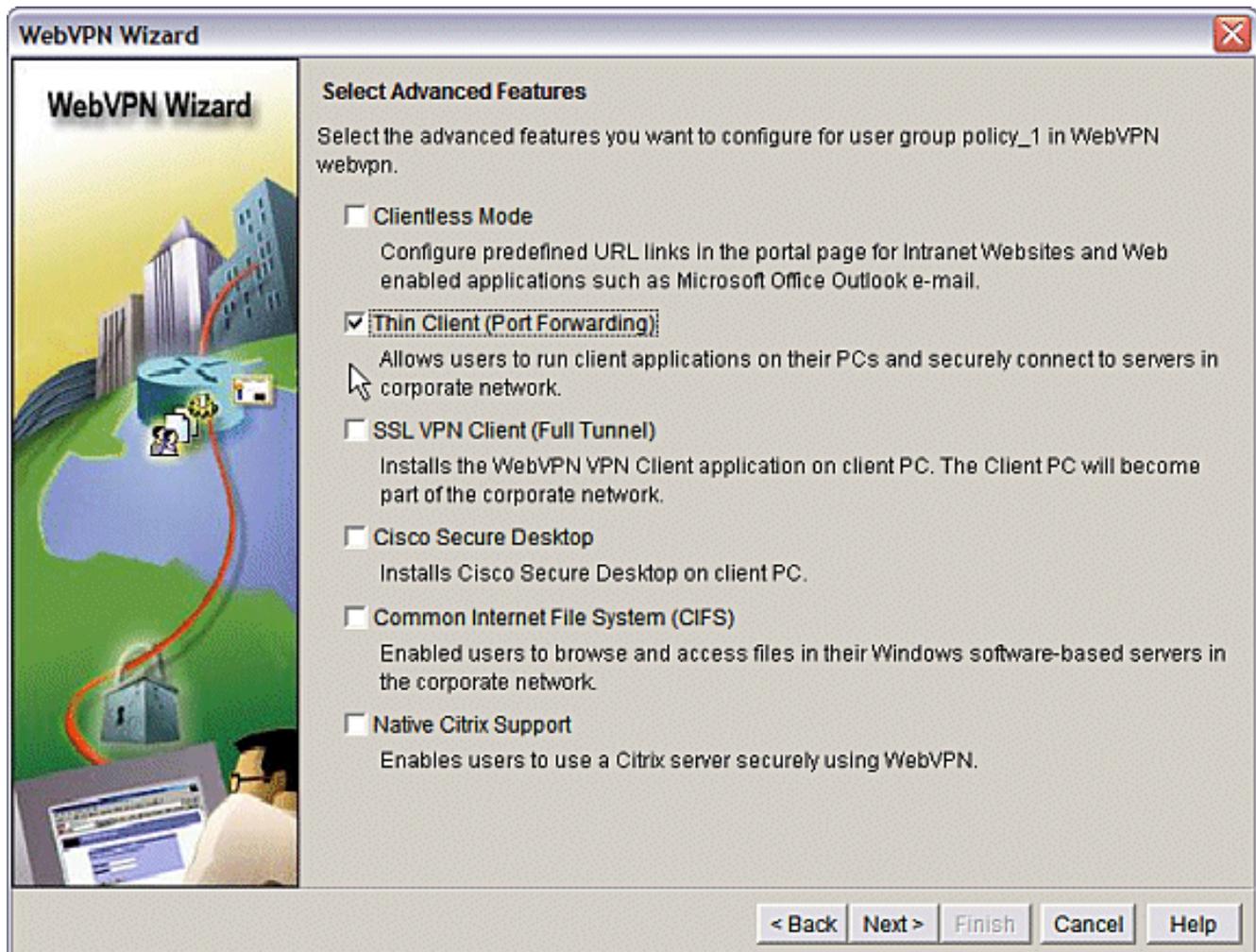
初期画面には、ウィザードの機能の概要が説明されています。[next] をクリックします。



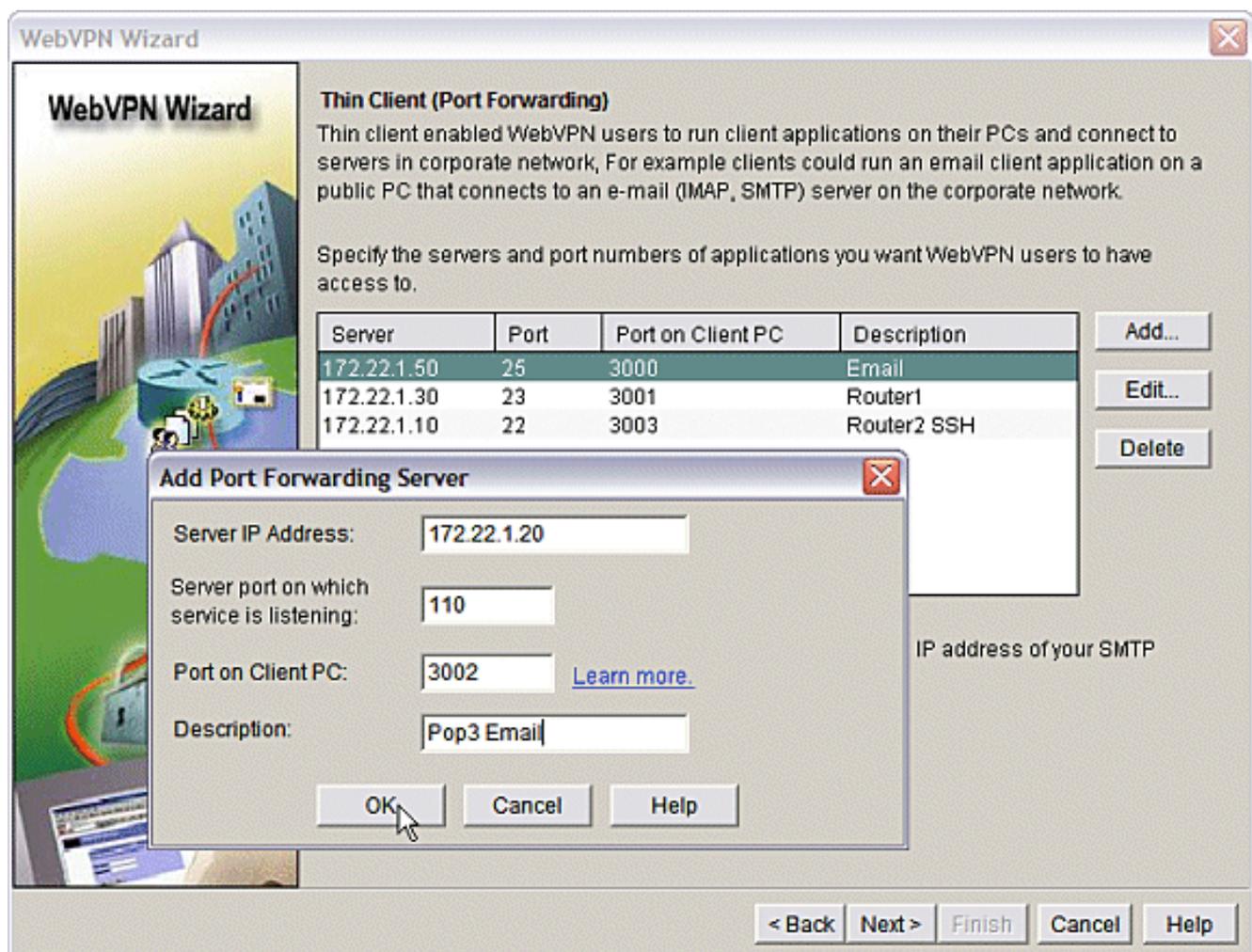
ドロップダウン メニューから WebVPN コンテキストとユーザ グループを選択します。
[next] をクリックします。



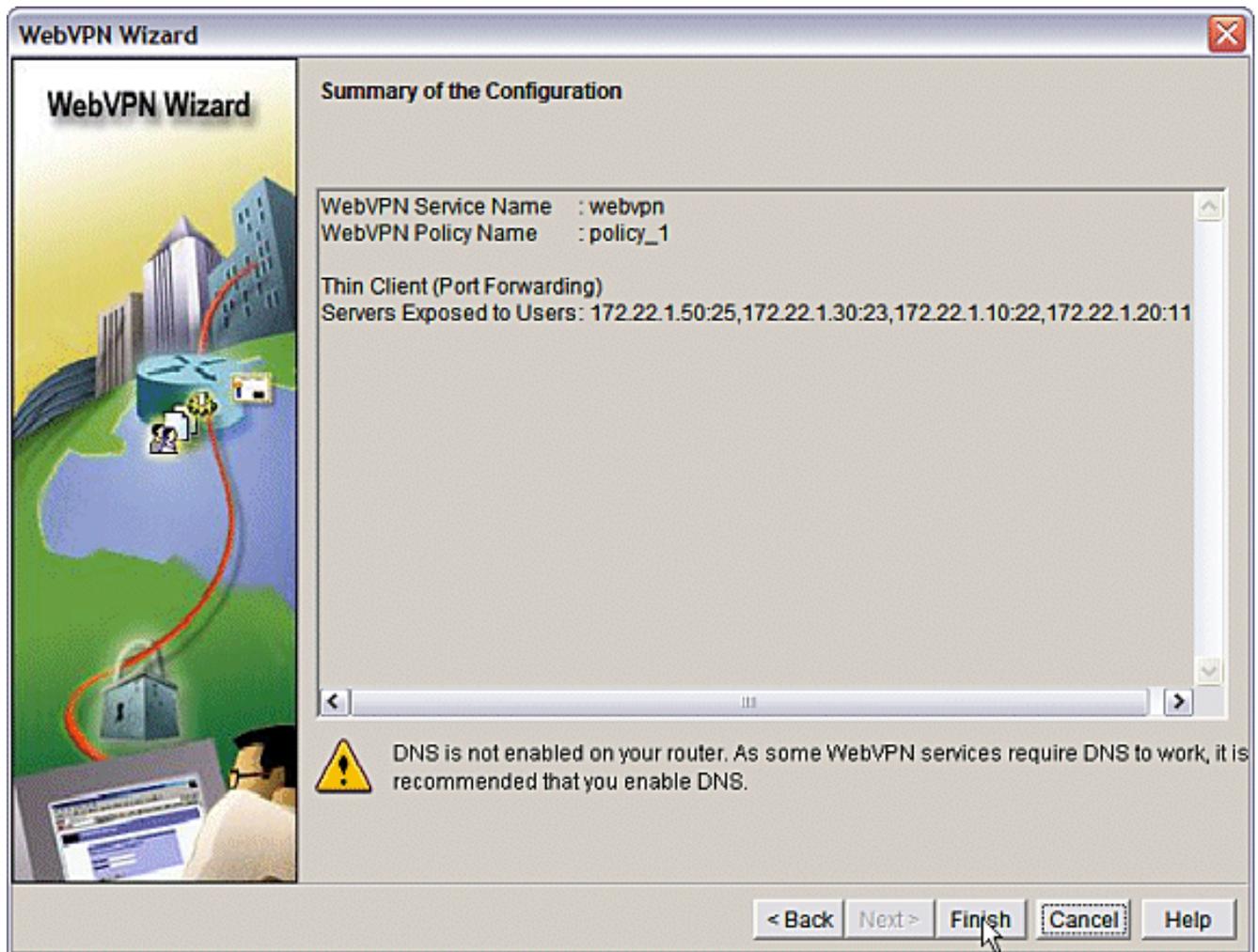
[Thin Client (Port Forwarding)] を選択して、[Next] をクリックします。



ポート フォワーディングで使えるようにするリソースを入力します。サービス ポートはスタティックポートにする必要がありますが、クライアント PC でウィザードによって割り当てられたデフォルトのポートを受け入れることができます。[next] をクリックします。



設定の概要をプレビューして、[Finish] > [OK] > [Save] をクリックします。



コンフィギュレーション

SDM の設定の結果

ausnml-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
brevis 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

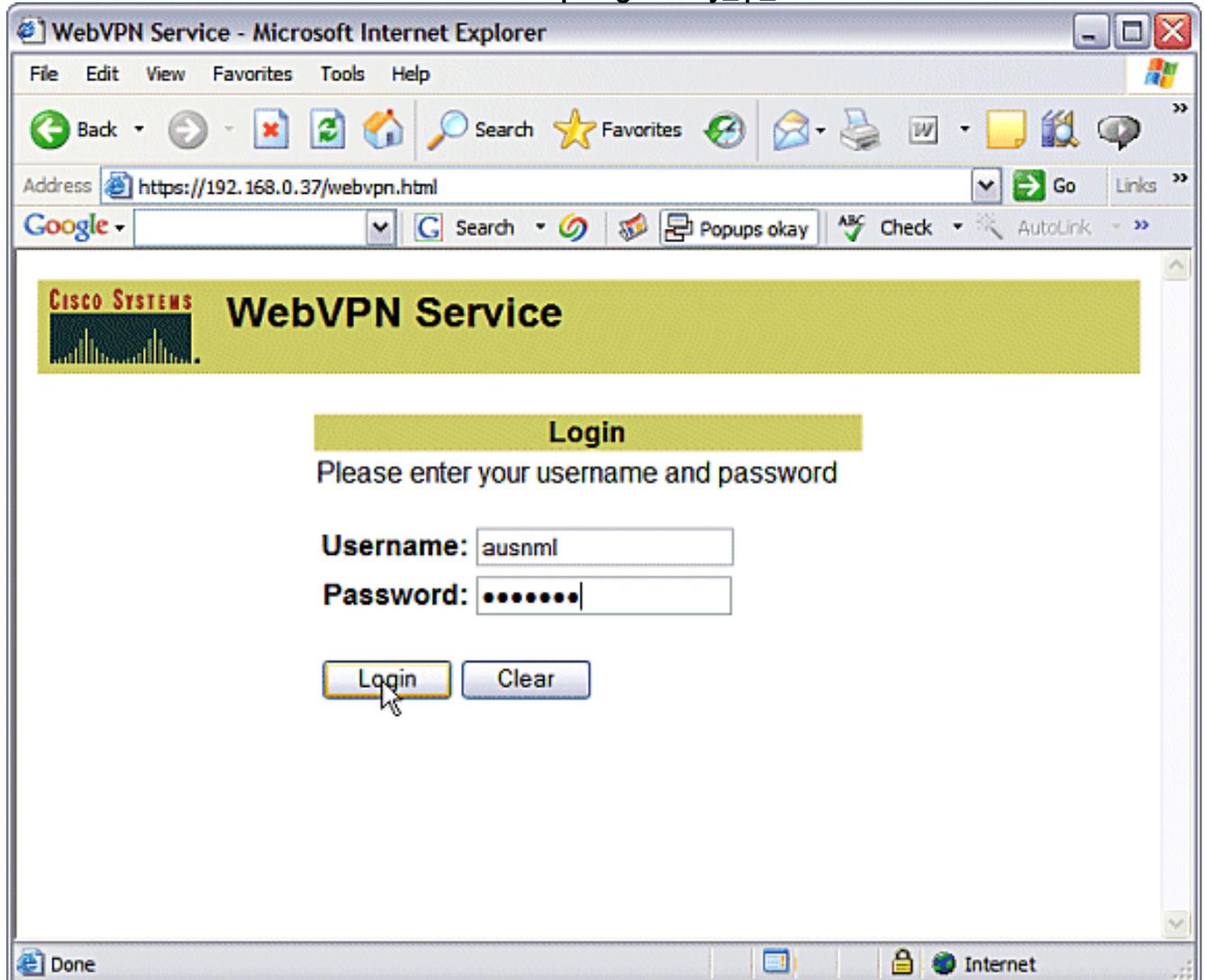
```

確認

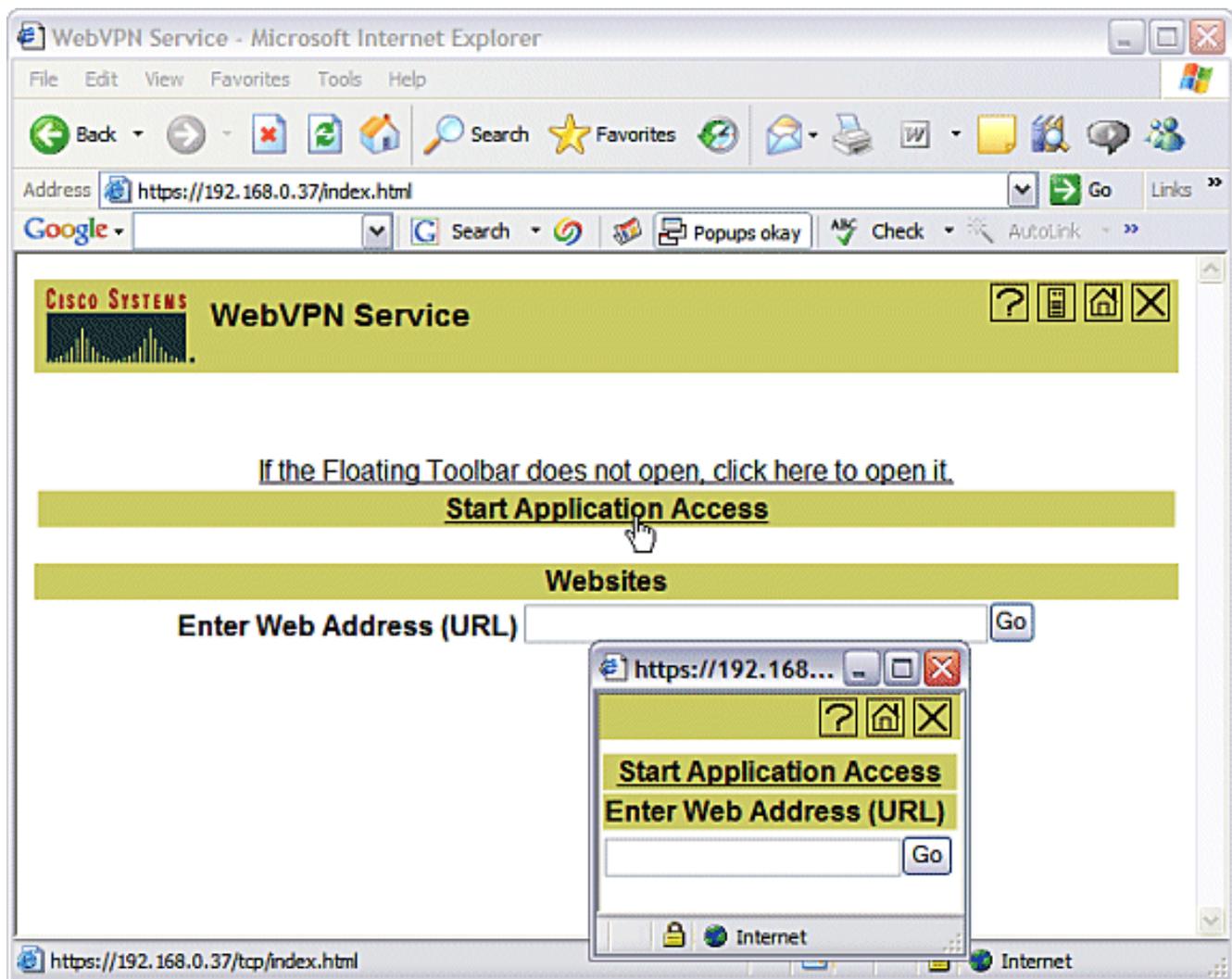
設定の確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. クライアント コンピュータを使用して、WebVPN ゲートウェイ (https://gateway_ip_address) にアクセスします。一意の WebVPN コンテキストを作成する場合、WebVPN ドメイン名を含めることを忘れないでください。たとえば、「sales」という名前のドメインを作成した場合は、https://gateway_ip_address/sales と入力します。



2. ログインして、WebVPN ゲートウェイで提供される証明書を受け入れます。[Start Application Access] をクリックします。



3. [Application Access] 画面が表示されます。ローカル ポート番号とローカル ループバック IP アドレスでアプリケーションにアクセスできます。たとえば、ルータ 1 に Telnet 接続するには、`telnet 127.0.0.1 3001` と入力します。小さな Java アプレットがこの情報を WebVPN ゲートウェイに送信し、続いてこのゲートウェイでセッションの両端が安全に接続されます。接続に成功すると、[Bytes Out] および [Bytes In] 列の数字が増える場合があります。

Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. [Click here for details.](#)

Name	Local	Remote	Bytes Out	Bytes In	Sockets
Pop3 Email	127.0.0.1:3002	172.22.1.20:110	0	0	0
Router 1	127.0.0.1:3001	172.22.1.30:23	0	0	0
Email	127.0.0.1:3000	172.22.1.50:25	0	0	0
Router2 SSH	127.0.0.1:3003	172.22.1.10:22	0	0	0

Click to activate and use this control

Reset byte counts

Internet

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` コマンドの使用方法についての詳細は、『[WebVPN 設定の確認](#)』を参照してください。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の `show` コマンドをサポートします。OIT を使用して、`show` コマンドの出力の分析を表示します。

トラブルシューティング

このセクションは、設定のトラブルシューティングを行う際に参照してください。

クライアント コンピュータには SUN Java バージョン 1.4 以降がロードされている必要があります。[Java ソフトウェアのダウンロード ページ](#)からこのソフトウェアのコピーを入手してください。

トラブルシューティングに使用するコマンド

注 : `debug` コマンドを使用する前に、『[デバッグコマンドの重要な情報](#)』を参照してください。

- `show webvpn ?` : WebVPN に関連するさまざまな `show` コマンドが用意されています。CLI で実行すると、統計情報やその他の情報が表示されます。`show` コマンドの使用方法について

の詳細は、[『WebVPN 設定の確認』](#)を参照してください。

- `debug webvpn ?` : `debug` コマンドの使用は ASA に悪影響を及ぼす場合があります。 `debug` コマンドの使用方法についての詳細は、[『WebVPN Debug コマンドの使用』](#)を参照してください。

[関連情報](#)

- [Cisco IOS SSLVPN](#)
- [SSL VPN - WebVPN](#)
- [Cisco IOS WebVPN Q&A](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)