Application Note

Cisco Router and Security Device Manager Cisco WebVPN

Introduction

Cisco IOS® WebVPN provides Secure Sockets Layer (SSL) VPN remote-access connectivity using a Web browser. WebVPN supports both clientless and full-network-access SSL VPN capabilities.

Clientless WebVPN provides secure access to private Web resources and to a company's intranet sites. It uses a Web browser to connect to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix. This document gives an example of how to configure a WebVPN virtual server.

The TCP Application Helper (port-forwarding Java applet) provides support for additional TCP-based applications that are not Web-enabled. It extends the capability of the Web browser to enable remote access to TCP-based applications such as Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP), Telnet, and Secure Shell (SSH) Protocol.

The Cisco® SSL VPN Client enables dynamic, full network access remotely to any application. It offers extensive application support through its dynamically downloaded client for WebVPN. With the SSL VPN Client, Cisco Systems® delivers a lightweight, centrally configured, and easy-to-support SSL VPN tunneling client that allows network-layer connectivity access to virtually any applications.

Cisco Secure Desktop provides advanced endpoint security and offers data theft prevention on noncorporate devices. It is transparent to end users and automatically creates a secure session under Microsoft Windows 2000 or XP.

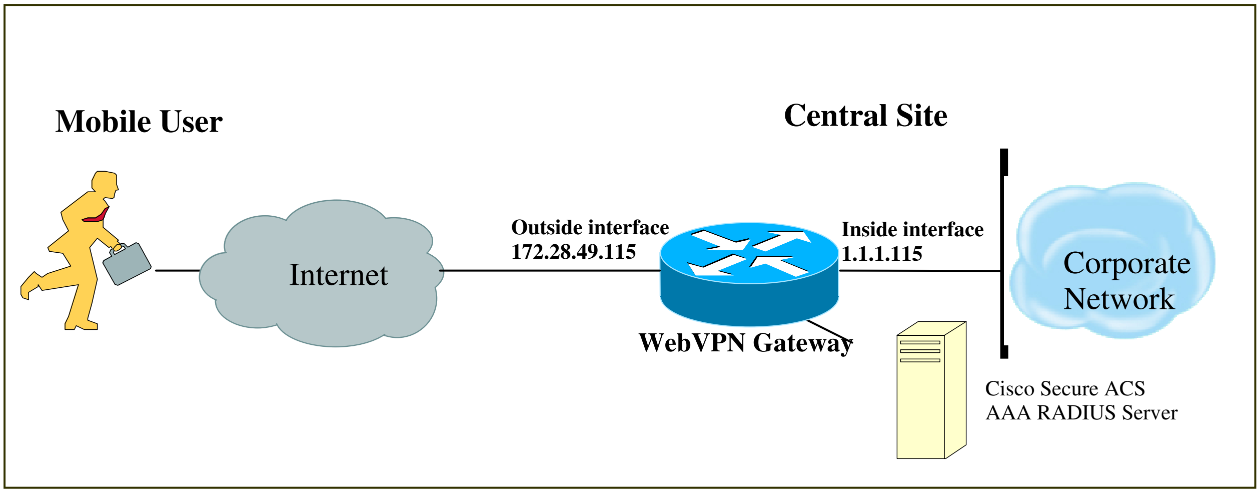
Cisco IOS WebVPN support

Cisco IOS WebVPN is supported by Cisco Router and Security Device Manager (SDM) v2.3 with Cisco IOS Software Release 12.4(6)T. Cisco SDM provides wizards for both basic and advanced configuration, and provides monitoring information and statistics for user sessions, clientless access, and full network access.

Deployment Scenario

This document demonstrates how to configure a Cisco IOS WebVPN gateway. The sample configuration is based on the following network topology (figure 1)

Figure 1. Network Diagram

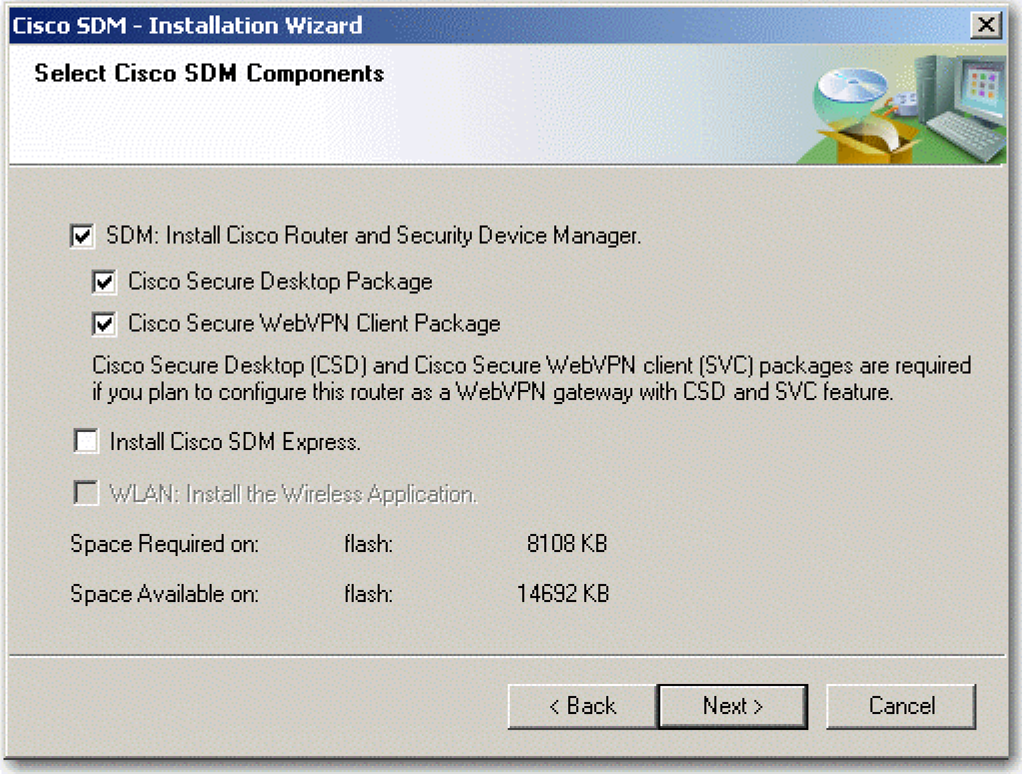


Sample Configuration

Prerequisites

The router is installed with Cisco Secure Desktop and Cisco Secure WebVPN Client in the flash memory during SDM installation/upgrade (Figure 2), or manually copied to router flash.

Figure 2. **Cisco SDM Components**



☑ SDM: Install Cisco Router and Security Device Manager.

☑ Cisco Secure Desktop Package

☑ Cisco Secure WebVPN Client Package

Cisco Secure Desktop (CSD) and Cisco Secure WebVPN client (SVC) packages are required if you plan to configure this router as a WebVPN gateway with CSD and SVC feature.

☐ Install Cisco SDM Express.

☐ WLAN: Install the Wireless Application.

Space Required on:	flash:	8108 KB
Space Available on:	flash:	14692 KB

Cisco SDM WebVPN Gateway

Although the Cisco WebVPN feature allows dynamic configuration of end-user policy and require less manual configuration by end users and field technicians, it still requires users to fully understand how to configure an authentication, authorization, and accounting (AAA) server, the group policy, and the dynamic crypto map on the WebVPN gateway side.

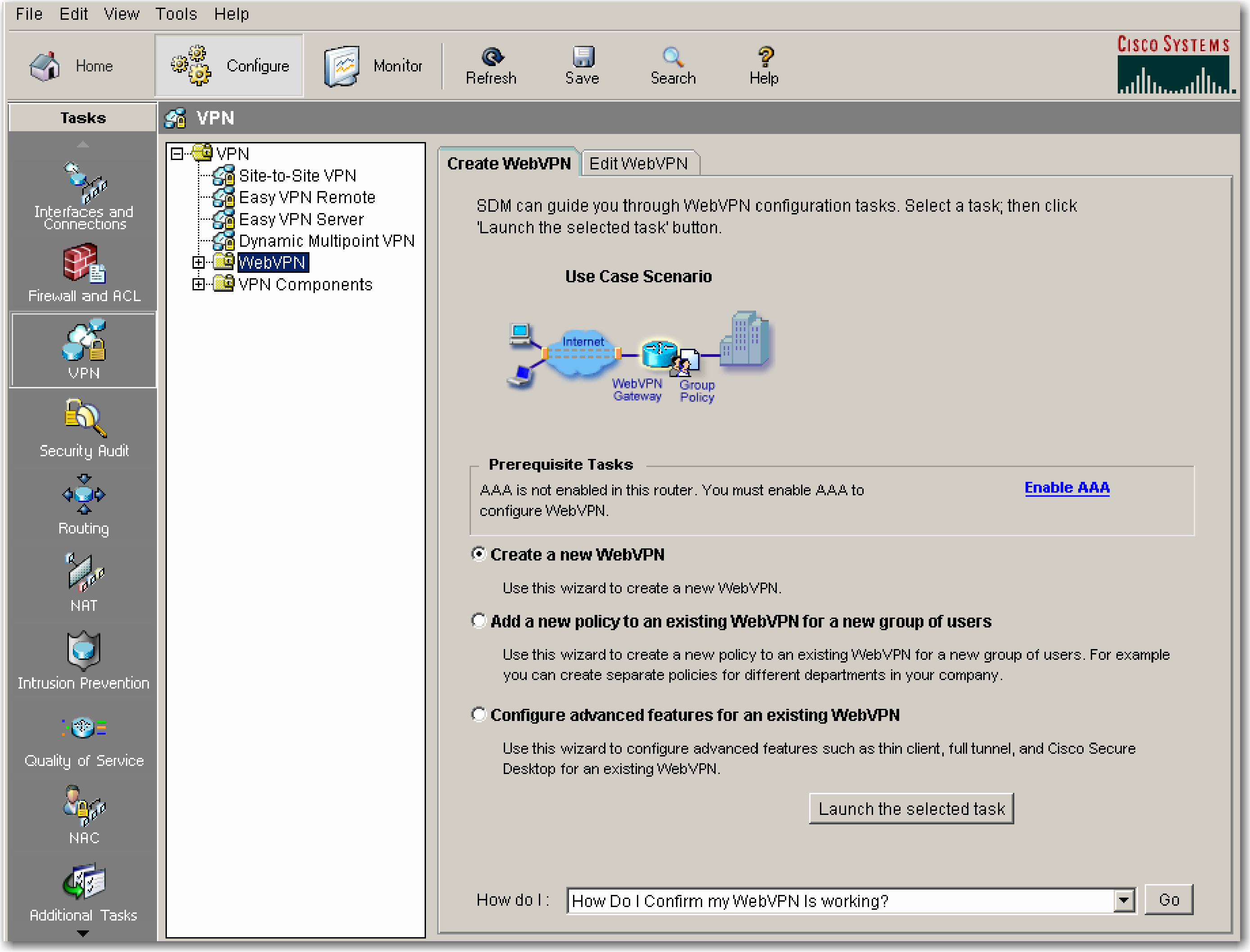
Cisco SDM allows users to easily configure the Cisco WebVPN gateway with limited information. The following steps are used to configure the deployment scenario using Cisco SDM.

Create a Cisco WebVPN Gateway

To create a WebVPN gateway, at **Configure Mode**, select the **VPN**, select **WebVPN**, and then click the **Create WebVPN** tab to launch **Create a New WebVPN** wizard.

In our case, the AAA is not enabled (Figure 3). To enable AAA, click **Enable AAA**, read the message, and click **Yes** to continue.

Figure 3. Create WebVPN – Enable AAA



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

Use Case Scenario

Prerequisite Tasks

AAA is not enabled in this router. You must enable AAA to configure WebVPN. Enable AAA

● 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.

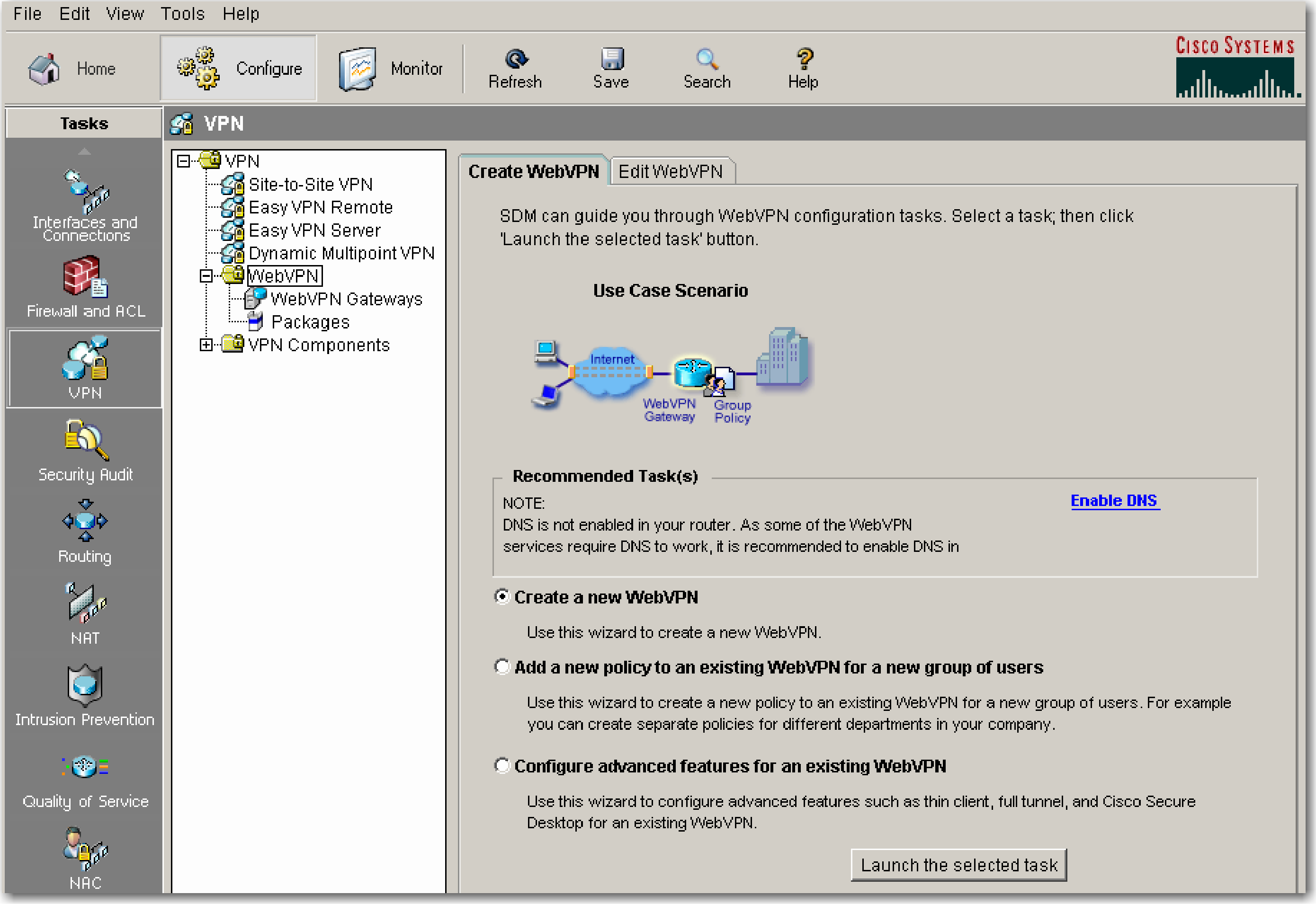
○ Configure advanced features for an existing WebVPN

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

How do I: How Do I Confirm my WebVPN Is working?

After the AAA server is enabled, the Prerequisite Tasks show that DNS is not enabled (Figure 4). To enable DNS, click **Enable DNS**. You will be directed to Additional Tasks/DNS properties to enable DNS.

Figure 4. Create WebVPN – Enable DNS



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

NOTE:
DNS is not enabled in your router. As some of the WebVPN services require DNS to work, it is recommended to enable DNS in

● 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.

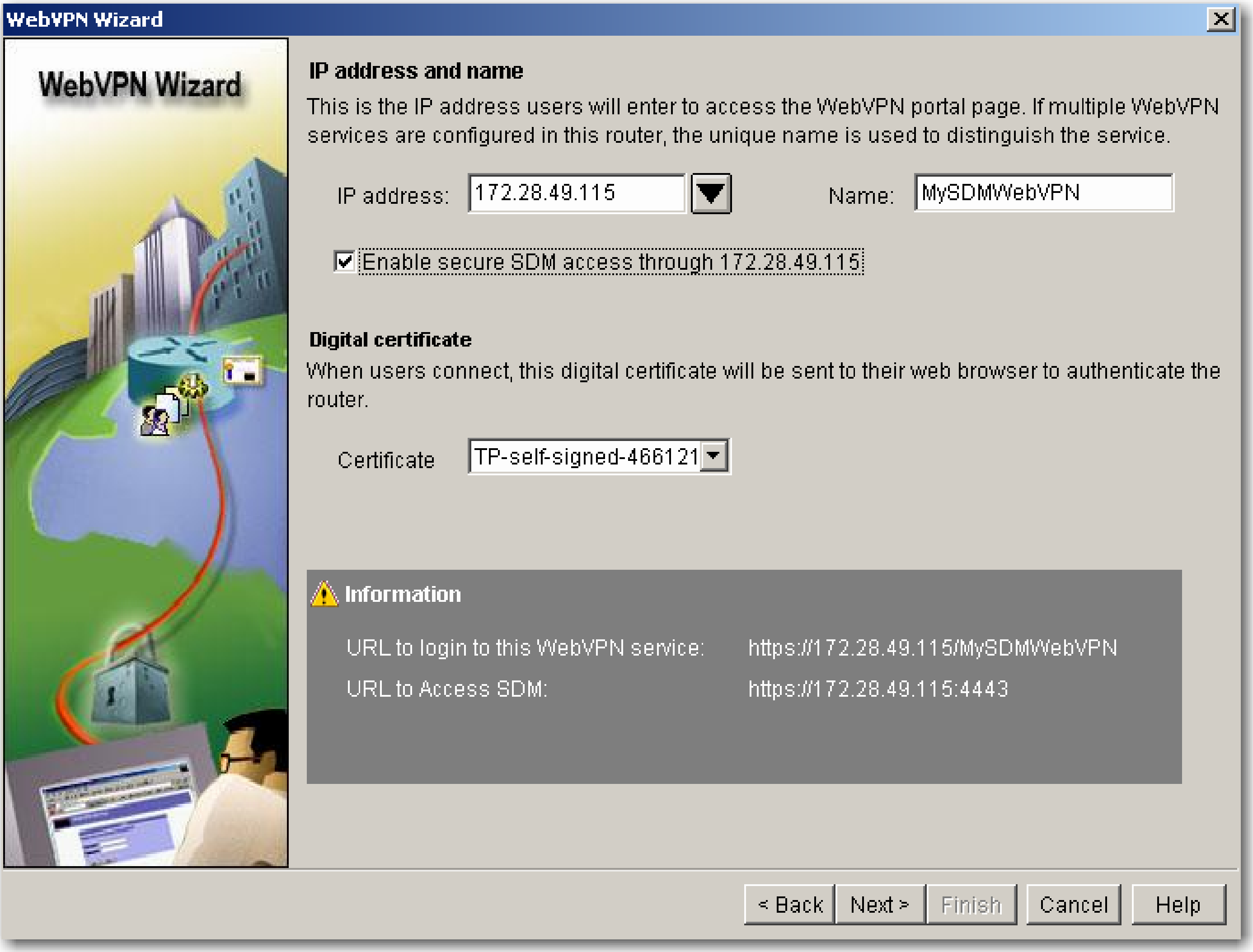
Click the **Launch the selected task** button to launch the WebVPN Wizard. Read the welcome note, and click **Next**.

For IP address and name, select the IP address that users will enter to access the WebVPN portal page; Cisco SDM lists the IP addresses of all configured router interfaces and all existing WebVPN gateways. In our example, use the IP address of the router's outside interface, select **172.28.49.115**, and give a unique name to access the gateway (in this case, the name = **MySDMWebVPN**). You will be asked to enable secure Cisco SDM access through 172.28.49.115; check the box (optional). If the box is checked, the URL that you must use to access Cisco SDM will change after you deliver the configuration to the router. Review the information area at the bottom of the screen to learn the URL to use.

For digital certificates, select the certificate that you want the router to present to clients when they log onto the gateway. In our example, we use the router's self-signed certificate.

In the Information area, Cisco SDM displays the URL to log into the WebVPN service: https://172.28.49.115/MySDMWebVPN and the URL to access Cisco SDM: https://172.28.49.115:4443 (Figure 5). Read and write down the information, and click **Next**.

Figure 5. **Select an Interface**



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: 172.28.49.115   Name: MySDMWebVPN

☑ Enable secure SDM access through 172.28.49.115

Digital certificate

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

Certificate TP-self-signed-466121

Information

URL to login to this WebVPN service: https://172.28.49.115/MySDMWebVPN

URL to Access SDM: https://172.28.49.115:4443

You will be prompted by a Cisco SDM Warning popup window. Read the information and click **Yes**.

Use the User Authentication window to specify how the router is to perform user authentication. The router can authenticate WebVPN users locally, or it can send authentication requests to a remote AAA server.

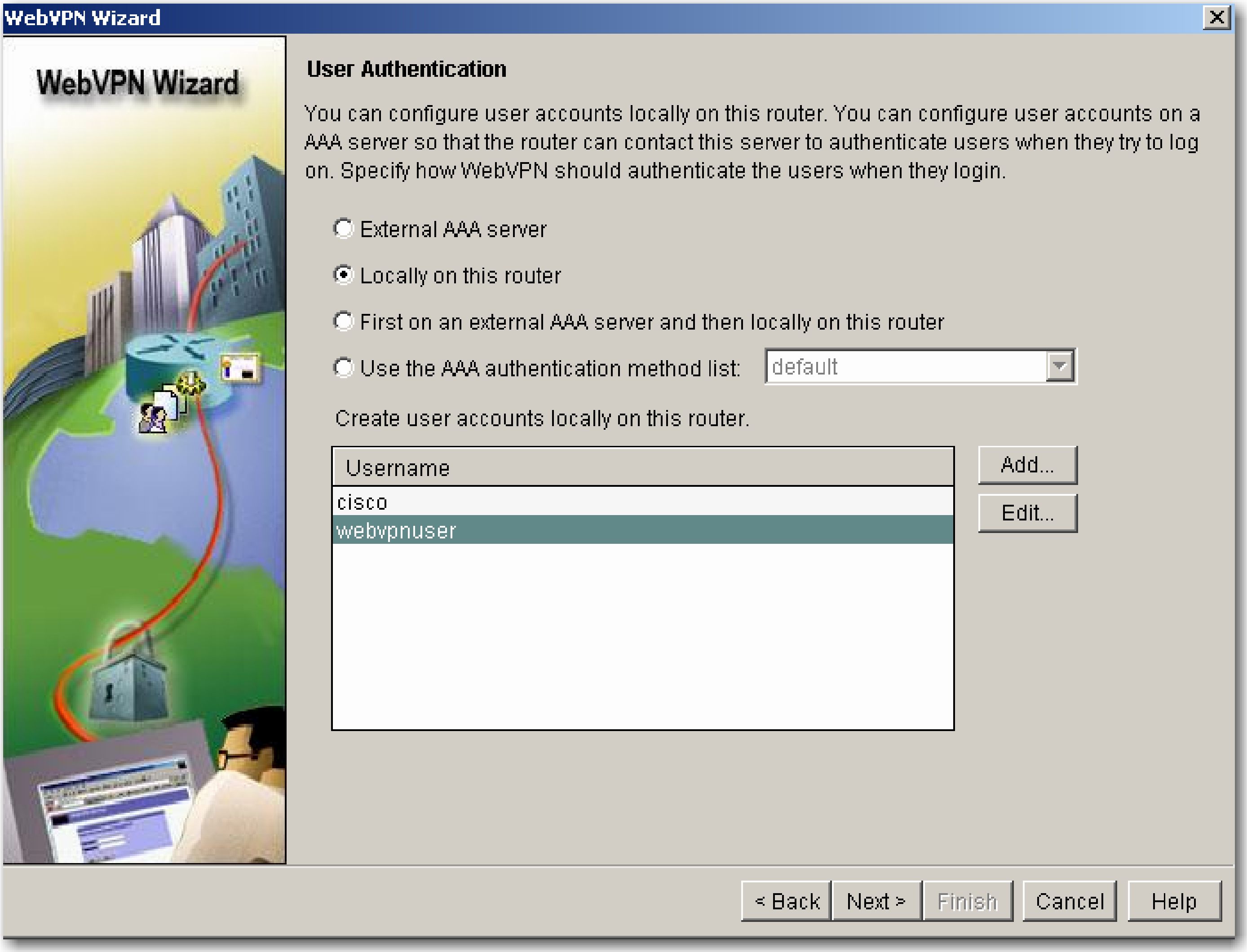
In our example, we do not have a remote AAA server; all users will be authenticated locally. Select **Locally on this router**. Click the **Add…** button to add a new user:

- Username: **webvpnuser**
- Password: **cisco123**
- Encrypt password using MD5 hash algorithm: **check**
- Privilege Level: **1**

Click **OK**.

The new user and the existing users will be listed (Figure 6). Click **Next**.

Figure 6. IKE Proposal



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.

○ External AAA server

● Locally on this router

○ First on an external AAA server and then locally on this router

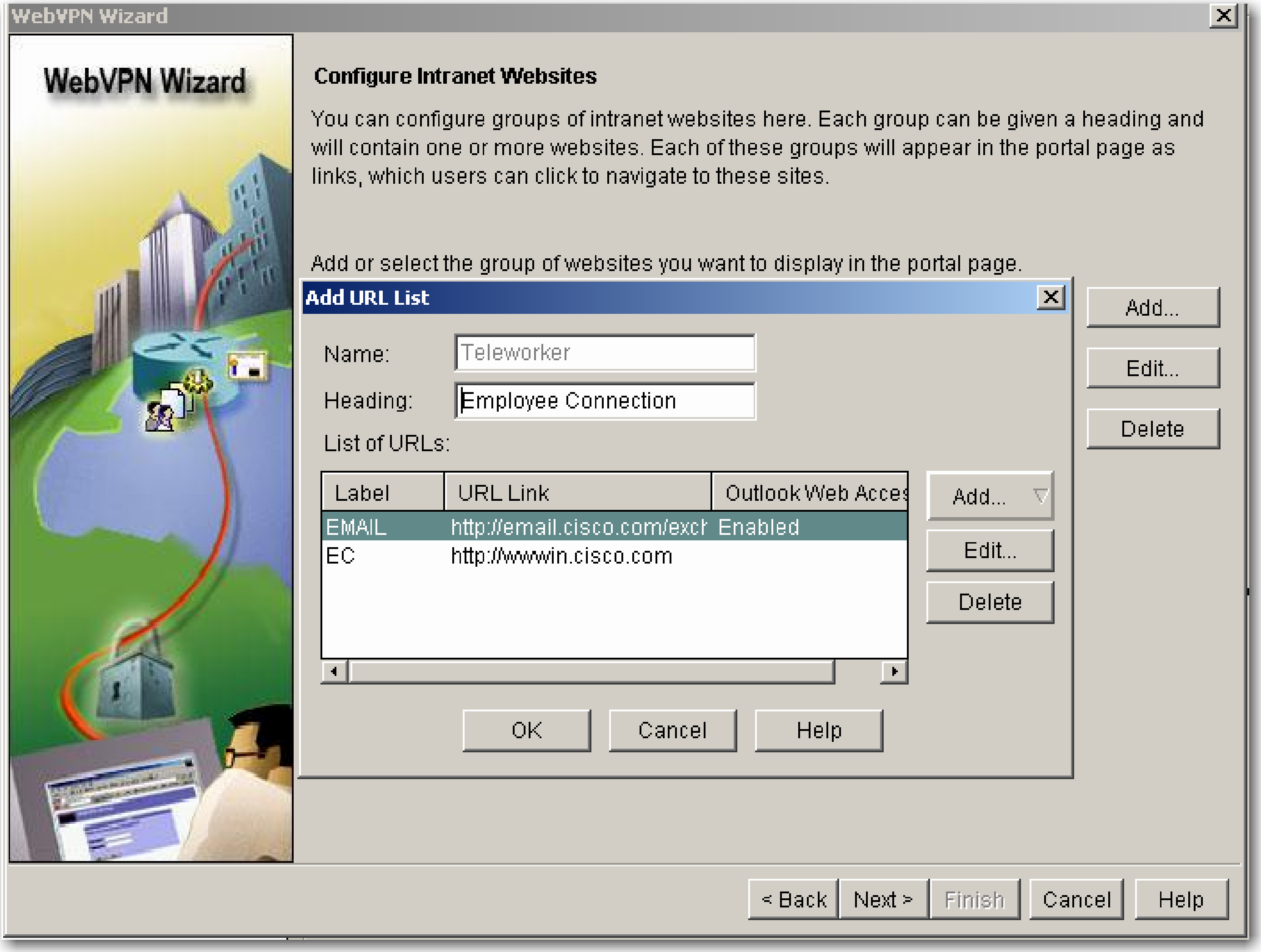
○ Use the AAA authentication method list: default

Create user accounts locally on this router.

Username
cisco
webvpnuser

Configure the links and services that users will access in the **Configure Intranet Websites** window. Click **Add…** to add a URL list, and the **Add URL List** dialog will be displayed (Figure 7).

Figure 7. **Configure Intranet Websites**



WebVPN Wizard

Configure Intranet Websites

You can configure groups of intranet websites here. Each group can be given a heading and will contain one or more websites. Each of these groups will appear in the portal page as links, which users can click to navigate to these sites.

Add or select the group of websites you want to display in the portal page.

Add URL List

Name: Teleworker

Heading: Employee Connection

List of URLs:

Label	URL Link	Outlook Web Acces
EMAIL	http://email.cisco.com/exch	Enabled
EC	http://wwwin.cisco.com	

- Name: **Teleworker**
- Heading: **Employee Connection**
- Click **Add…** and select **Website**.
    - Label: **EC**
    - URL: **http://your company's intranet network** (in our example, WebVPN is configured with Cisco Employee Connection URL http://wwwin.cisco.com)
    - Click **OK**.
- Click **Add…** and select **E-mail…**

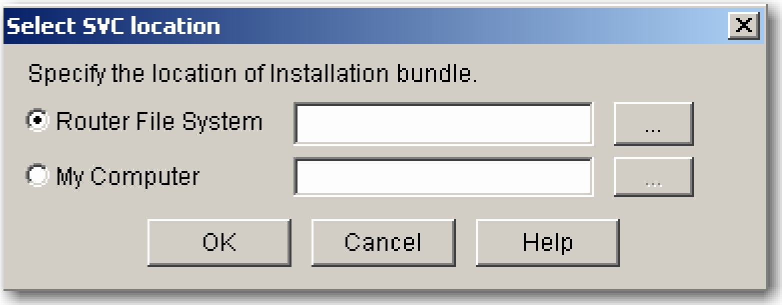
- Label: **Email**
- URL: **http:/your company's web mail server**; in our example, WebVPN is configured with Cisco's Outlook Web Access (OWA) http://email.cisco.com
- Click **OK**.

Action: check **Select**, click **Next**.

If a user requires access any application in the central site, the user's PC must download the full tunnel client software and obtain an IP address from the WebVPN gateway. In our example, we enable full tunnel feature and configure the full tunnel with following information:

- Check **Enable Full Tunnel**.
- IP Address Pool: Click **…** and select **Create a new IP Pool**
  - Pool name: **WebVPN-Full-Tunnel**
  - Start IP address: **1.1.1.1**
  - End IP address: **1.1.1.100**
- Check **Install Full Tunnel Client**
- Location: Click **…** to configure a SSL VPN Client location. Note: By default, Cisco SDM lists the SSL VPN Client loaded on the router file system. **Select SVC location** dialog appears (Figure 8).

Figure 8. **Select SVC Location**



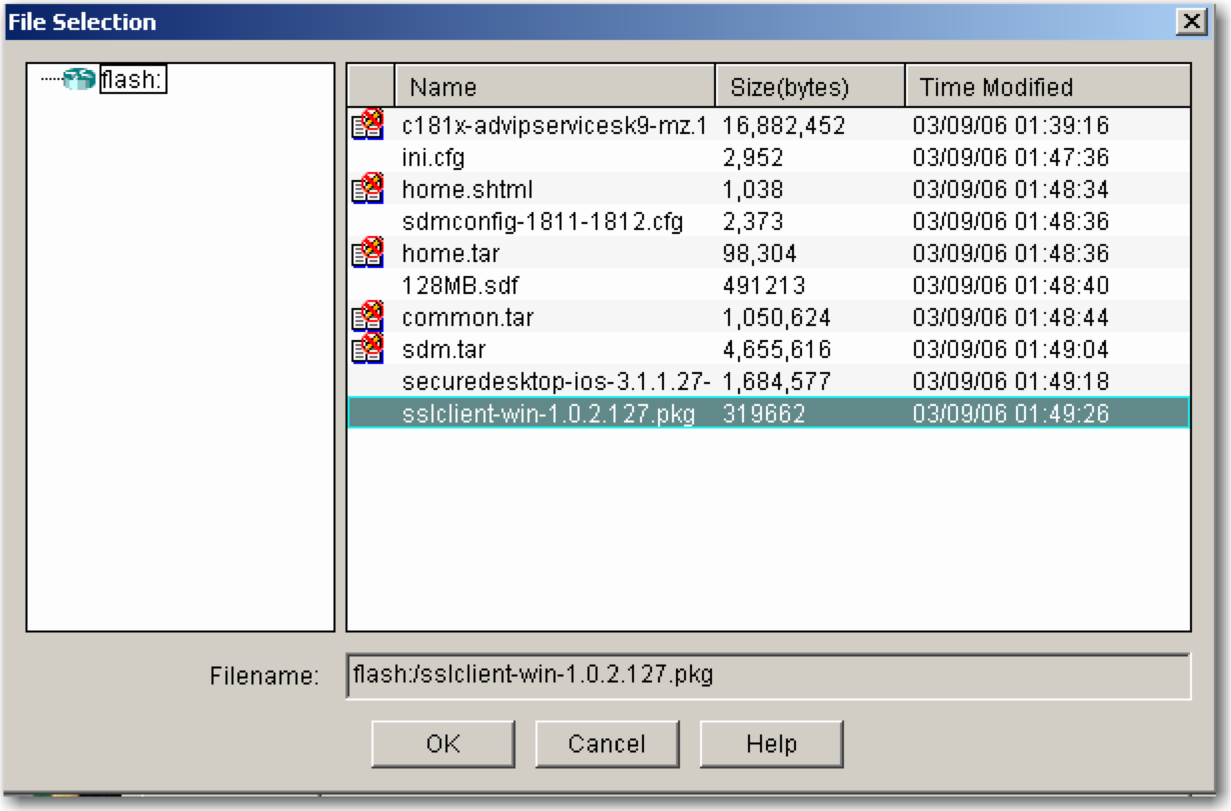
  - Select **Router File System**, click **…** button, **File Selection** dialog appears (Figure 9).

    Select **sslclient-win-1.0.2.127.pkg**[1]

    Click **OK**.

Figure 9. **File Selection**

[1] SSL VPN client files for full tunnel client are packaged with Cisco SDM. In our example, it is installed on the router flash.



Name	Size(bytes)	Time Modified
c181x-advipservicesk9-mz.1	16,882,452	03/09/06 01:39:16
ini.cfg	2,952	03/09/06 01:47:36
home.shtml	1,038	03/09/06 01:48:34
sdmconfig-1811-1812.cfg	2,373	03/09/06 01:48:36
home.tar	98,304	03/09/06 01:48:36
128MB.sdf	491213	03/09/06 01:48:40
common.tar	1,050,624	03/09/06 01:48:44
sdm.tar	4,655,616	03/09/06 01:49:04
securedesktop-ios-3.1.1.27-	1,684,577	03/09/06 01:49:18
sslclient-win-1.0.2.127.pkg	319662	03/09/06 01:49:26

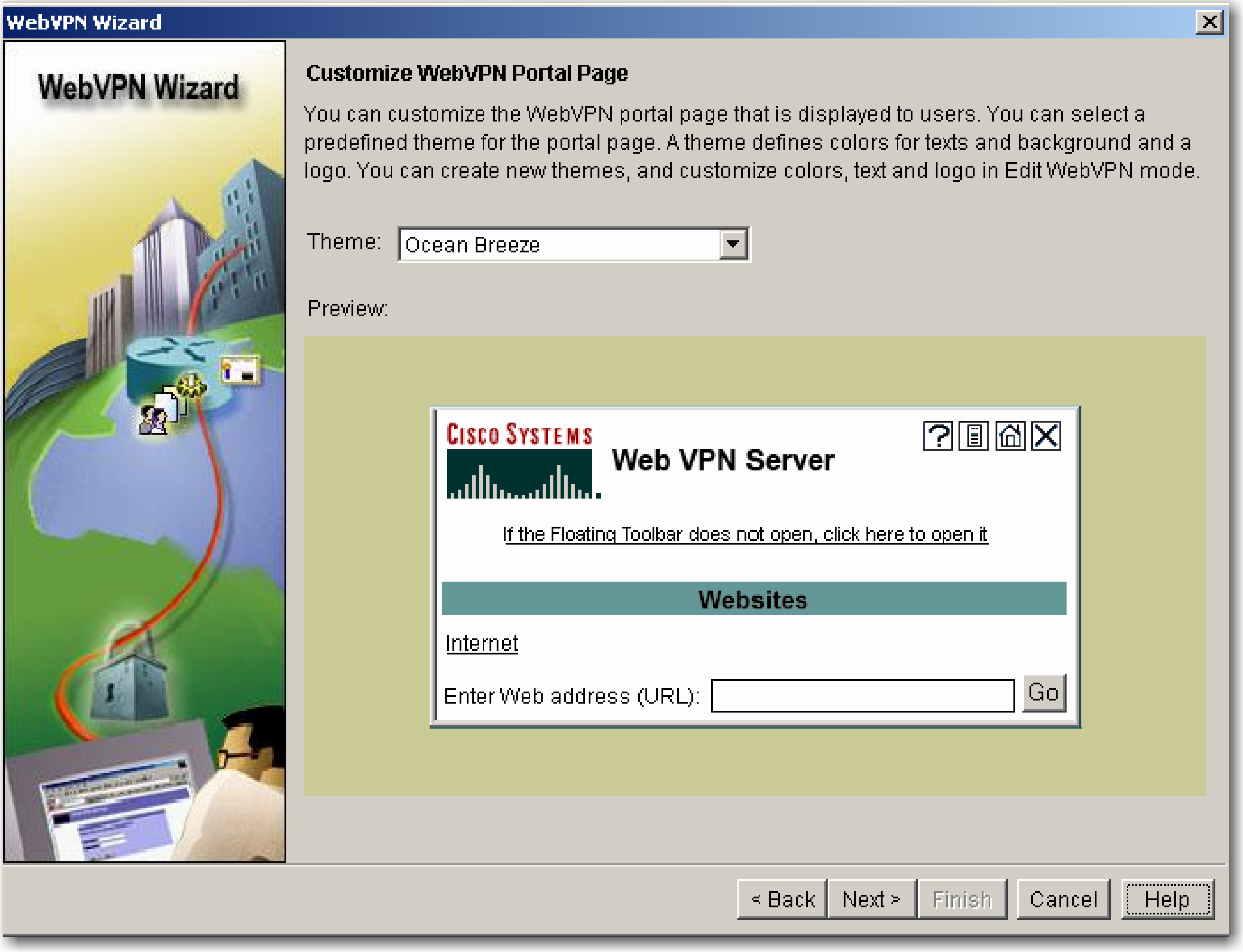
Filename: flash:/sslclient-win-1.0.2.127.pkg

- Click **OK**.

For the Advanced Option, click **Advanced…** (optional). Cisco SDM allows you to control the traffic that is encrypted, specify the DNS servers on the corporate intranet, and specify the proxy server settings that are to be sent to client browsers. In our example, we do not configure the advance features. Click **Cancel** and then click **Next**.

Cisco SDM allows you to determine the appearance of the portal page. You can select among the predefined themes listed, and obtain a preview of the portal page. Select Theme: **Ocean Breeze** (Figure 10), click **Next**.

Figure 10. **Customize WebVPN Portal Page**



Customize WebVPN Portal Page

You can customize the WebVPN portal page that is displayed to users. You can select a predefined theme for the portal page. A theme defines colors for texts and background and a logo. You can create new themes, and customize colors, text and logo in Edit WebVPN mode.

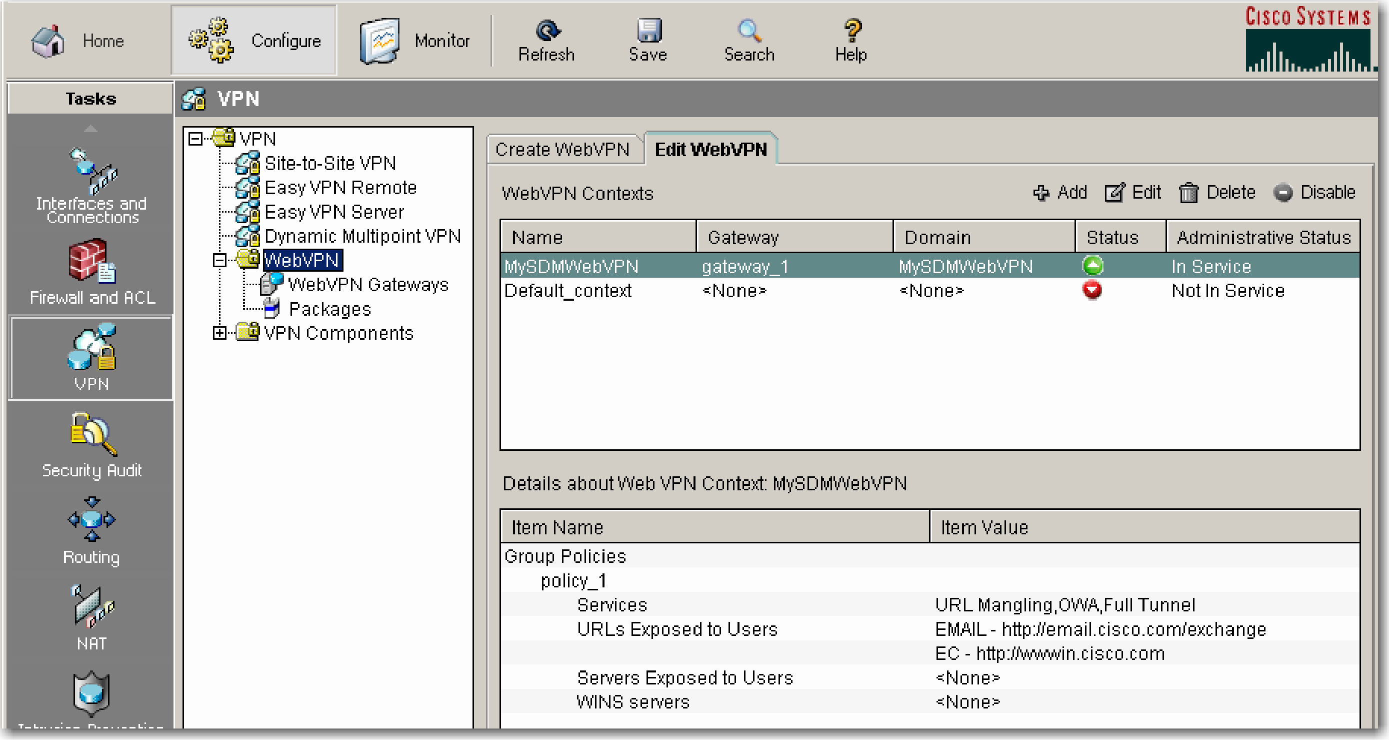
Theme: Ocean Breeze

Preview:

View the Summary of Configuration. Click **Finish** if you are satisfied with the configuration, or click **Back** to revise the configuration. You will be prompted by an alert. Read the information, click **I read and understood**, click **Save shortcut on Desktop** if necessary, and click **OK**. Once the commands are delivered to the router, you will be directed to the VPN / Web VPN / Edit WebVPN page. MySDMWebVPN should be created and in service (Figure 11). Close Cisco SDM.

Re-launch Cisco SDM as instructed. At **Configure Mode**, select the **VPN** from the left panel, click **WebVPN**, and select the **Edit WebVPN** tab. The Edit Web VPN window allows you modify or create WebVPN configurations. The top portion of the tab lists the configured WebVPN contexts. The bottom portion displays details for that context (Figure 11).

Figure 11. **Edit WebVPN**



WebVPN Contexts

Name	Gateway	Domain	Status	Administrative Status
MySDMWebVPN	gateway_1	MySDMWebVPN	▲	In Service
Default_context	<None>	<None>	▼	Not In Service

Details about Web VPN Context: MySDMWebVPN

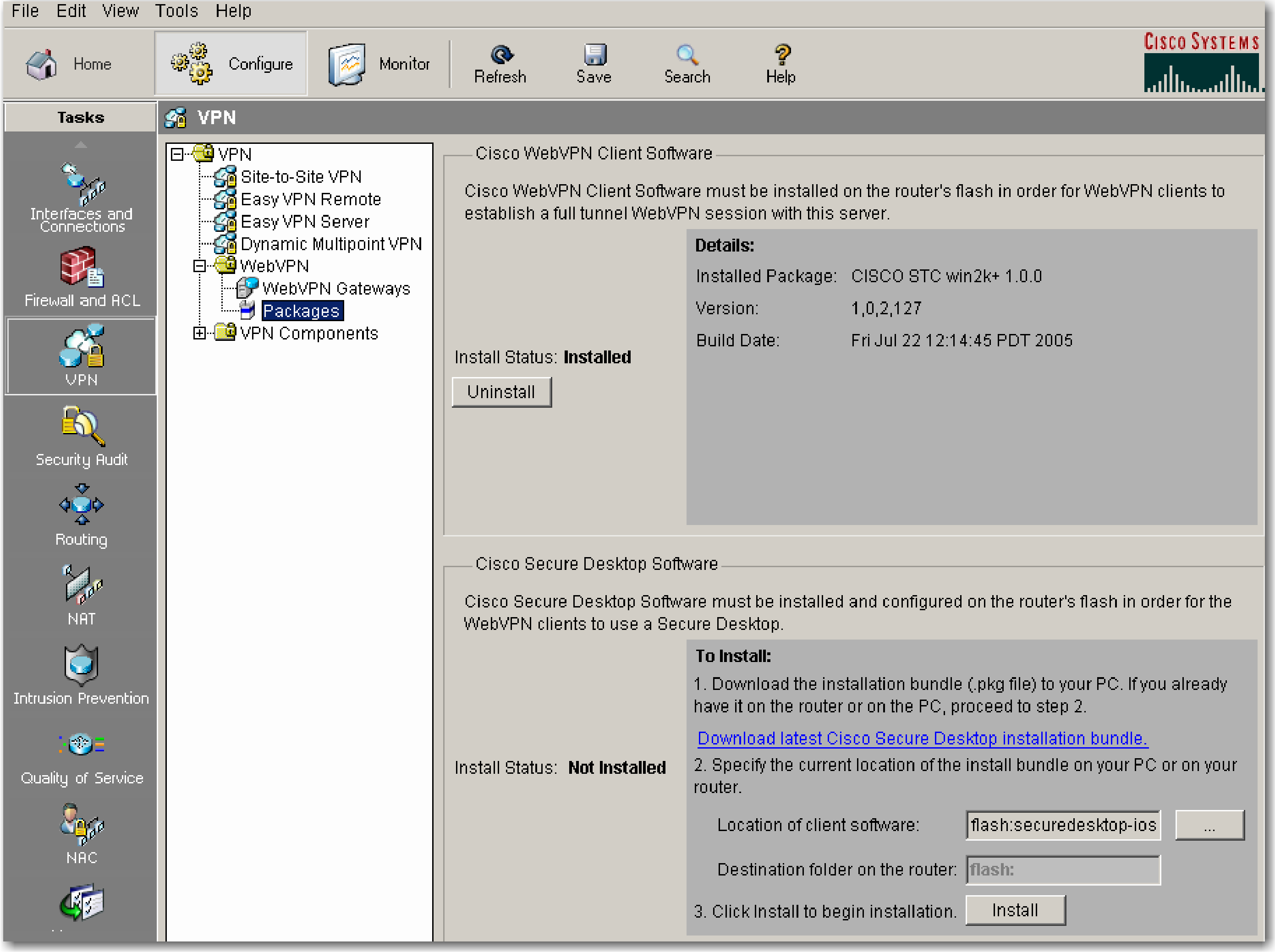
Item Name	Item Value
Group Policies	
policy_1	
Services	URL Mangling,OWA,Full Tunnel
URLs Exposed to Users	EMAIL - http://email.cisco.com/exchange
	EC - http://wwwin.cisco.com
Servers Exposed to Users	<None>
WINS servers	<None>

To view the newly created WebVPN gateway, at **Configure Mode**, select the **VPN**, expand **WebVPN**, and select **WebVPN Gateways**. The WebVPN Gateway window provides the IP address and the digital certificate for the WebVPN contexts that use it. You can provide the information for a gateway in this window, and the information that will allow users to access a portal page.

At **Configure Mode**, select the **VPN**, expand **WebVPN,** and select **Packages** (Figure 12). This window enables you to obtain software install bundles that must be downloaded to WebVPN clients to support WebVPN features, and to load them on the router. You can also use this window to remove install bundles that have been installed.

In our example, you should see the Cisco WebVPN Client software is installed, and Cisco Secure Desktop software has been loaded into the router flash but not installed. Click the **Install** button to install the software.

Figure 12. **Packages**



Cisco WebVPN Client Software

Cisco WebVPN Client Software must be installed on the router's flash in order for WebVPN clients to establish a full tunnel WebVPN session with this server.

Install Status: **Installed**

Uninstall

Details:

Installed Package: CISCO STC win2k+ 1.0.0

Version: 1,0,2,127

Build Date: Fri Jul 22 12:14:45 PDT 2005

Cisco Secure Desktop Software

Cisco Secure Desktop Software must be installed and configured on the router's flash in order for the WebVPN clients to use a Secure Desktop.

Install Status: **Not Installed**

To Install:

1. Download the installation bundle (.pkg file) to your PC. If you already have it on the router or on the PC, proceed to step 2.

Download latest Cisco Secure Desktop installation bundle.

2. Specify the current location of the install bundle on your PC or on your router.

Location of client software: flash:securedesktop-ios ...

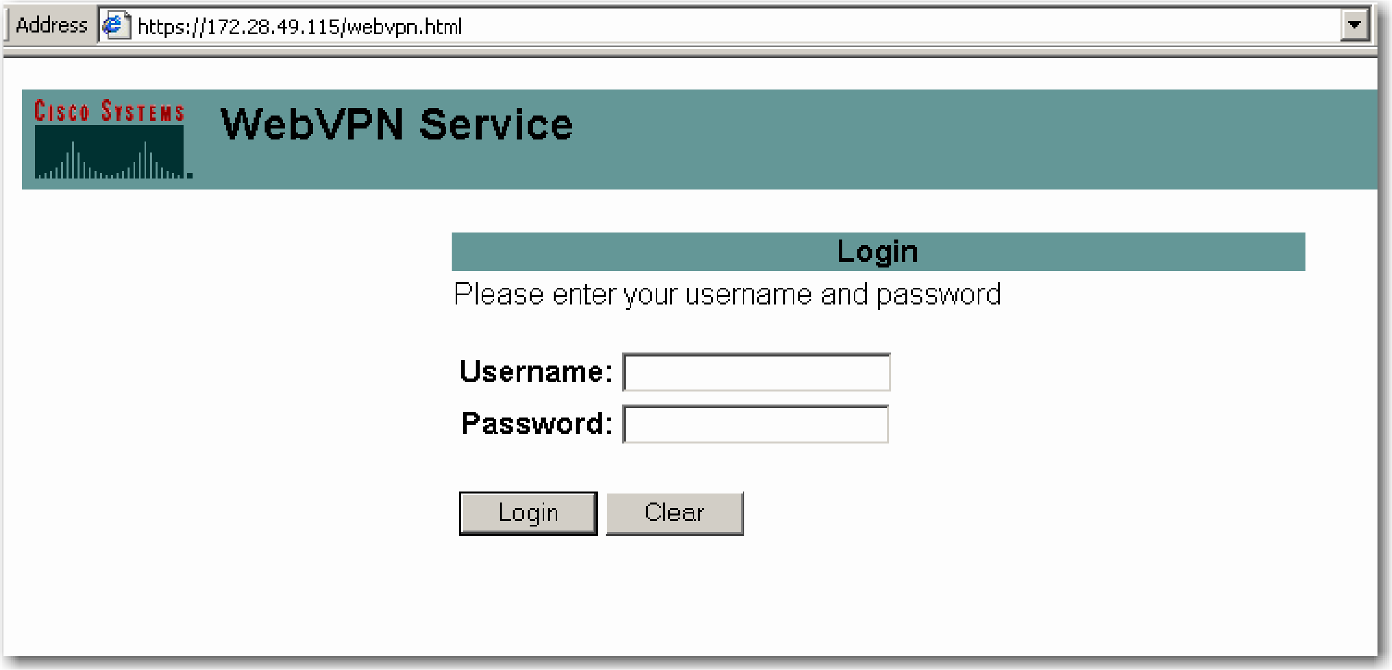
Destination folder on the router: flash:

3. Click Install to begin installation. Install

Access WebVPN Portal

Launch the WebVPN portal as instructed. In our example, https://172.28.49.115/MyWebVPN is given by the WebVPN wizard. Click **Yes** when prompted by the Security Alert. The WebVPN Service Login displays (Figure 13).

Figure 13. **WebVPN Service**



Address https://172.28.49.115/webvpn.html

WebVPN Service

Login

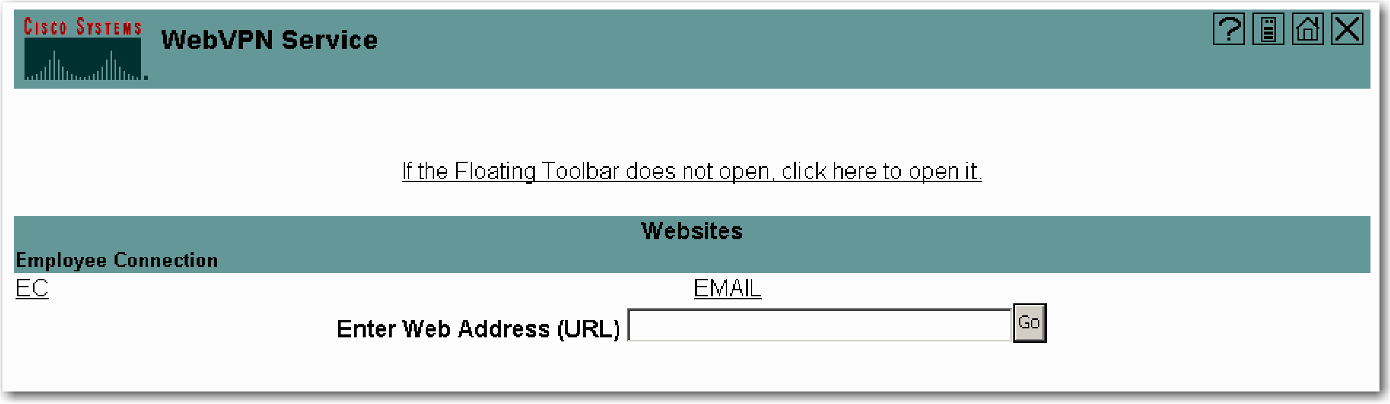
Please enter your username and password

Username:

Password:

Enter username/password = **webvpnuser/cisco123** to log in. Click **OK** to continue when prompted. The WebVPN Service Portal displays (Figure 14).

Figure 14. **WebVPN Service Portal**



WebVPN Service

If the Floating Toolbar does not open, click here to open it.

Websites

Employee Connection

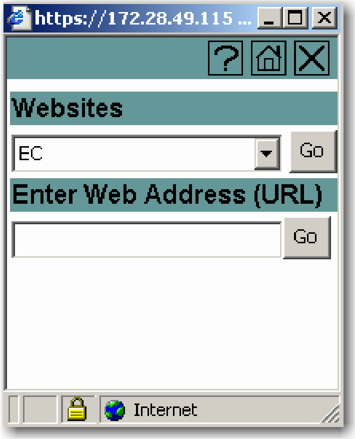
EC

EMAIL

Enter Web Address (URL)

A floating toolbar will be opened in a separate window (Figure 15).

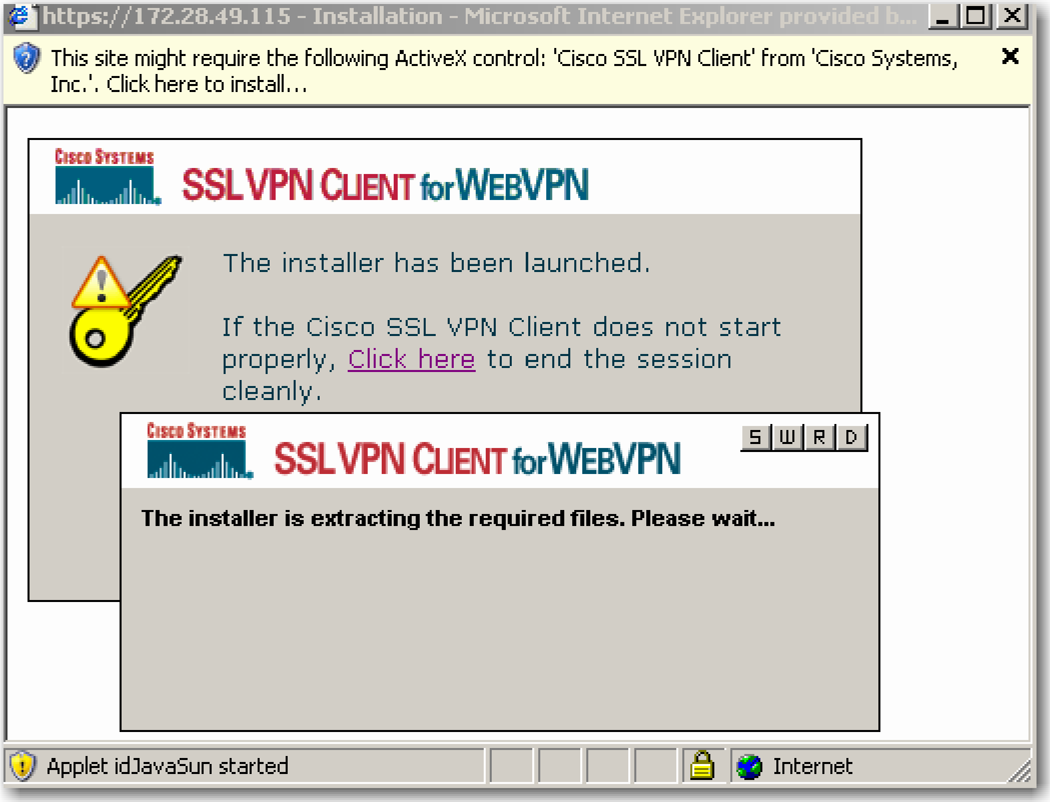
Figure 15. **Floating Toolbar**



If full tunnel is not enabled, you can access HTML-based URLs by entering the full URL path. You can also click the preconfigured URL EC and EMAIL on the portal, or select the URL from the floating toolbar.

In our example, you will be prompted to install the SSL VPN Client for WebVPN. Read the security warning, and allow the installer to launch ActiveX. Figure 16 shows the installer has been launched.

Figure 16. **SSL VPN Client**


https://172.28.49.115 - Installation - Microsoft Internet Explorer provided b...
Cisco Systems
SSL VPN Client for WebVPN
S
W
R
D
Applet idJavaSun started
Internet

This site might require the following ActiveX control: 'Cisco SSL VPN Client' from 'Cisco Systems, Inc.'. Click here to install...

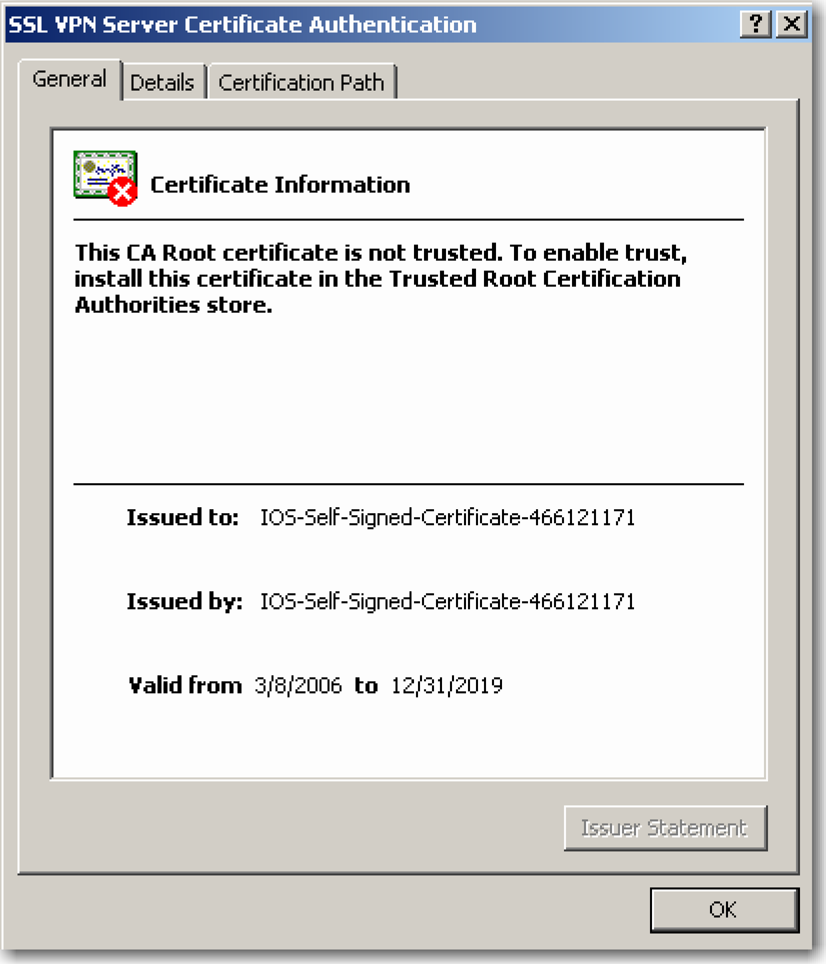
The installer has been launched.

If the Cisco SSL VPN Client does not start properly, Click here to end the session cleanly.

The installer is extracting the required files. Please wait...

You will be asked to authenticate the SSL VPN Server Certificate signed by an untrusted certificate authority. Click **Yes** to view the certificate. The SSL VPN Server Certificate Authentication window appears. Read the certificate and click **OK** to accept it. In our example, the router does not receive a certificate from a Certificate Authority server; a self-signed certificate is used (Figure 17).

Figure 17. **Certificate Information**



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

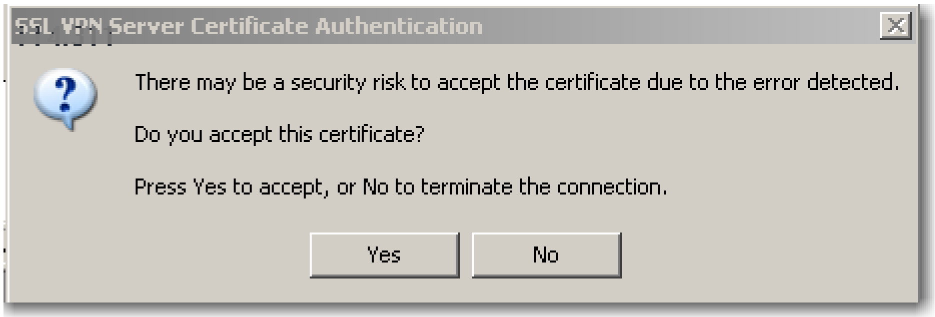
Issued to: IOS-Self-Signed-Certificate-466121171

Issued by: IOS-Self-Signed-Certificate-466121171

Valid from 3/8/2006 to 12/31/2019

You will be prompted to accept the certificate again. Read the statement and click **Yes** to accept the self-signed certificate (Figure 18).

Figure 18. **SSL VPN Server Certificate Authentication**

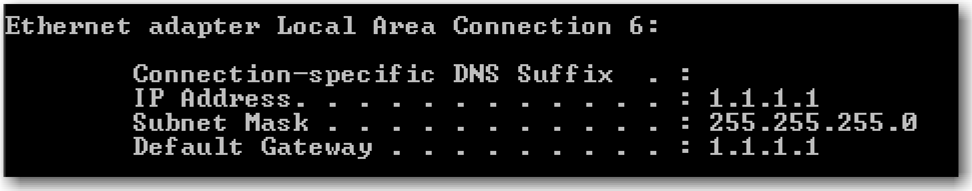


There may be a security risk to accept the certificate due to the error detected.

Do you accept this certificate?

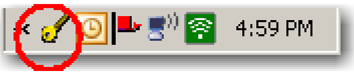
Press Yes to accept, or No to terminate the connection.

Your local host (a PC or a laptop) will be assigned a new address from the **WebVPN-Full-Tunnel**.



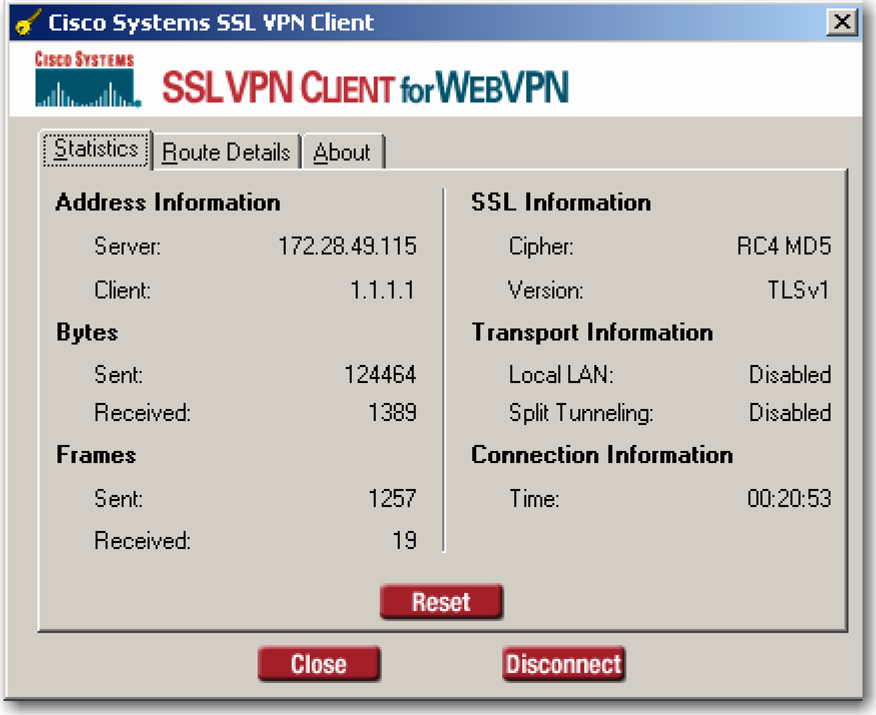
```
Ethernet adapter Local Area Connection 6:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 1.1.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 1.1.1.1
```



Locate and double click the SSL VPN Client icon from your toolbar to check the statistics and router details of the full tunnel (Figure 19).

Figure 19. **SSL VPN Client Statistics**



Cisco Systems SSL VPN Client

SSL VPN CLIENT for WEBVPN

Statistics | Route Details | About

Address Information

Server: 172.28.49.115

Client: 1.1.1.1

Bytes

Sent: 124464

Received: 1389

Frames

Sent: 1257

Received: 19

SSL Information

Cipher: RC4 MD5

Version: TLSv1

Transport Information

Local LAN: Disabled

Split Tunneling: Disabled

Connection Information

Time: 00:20:53

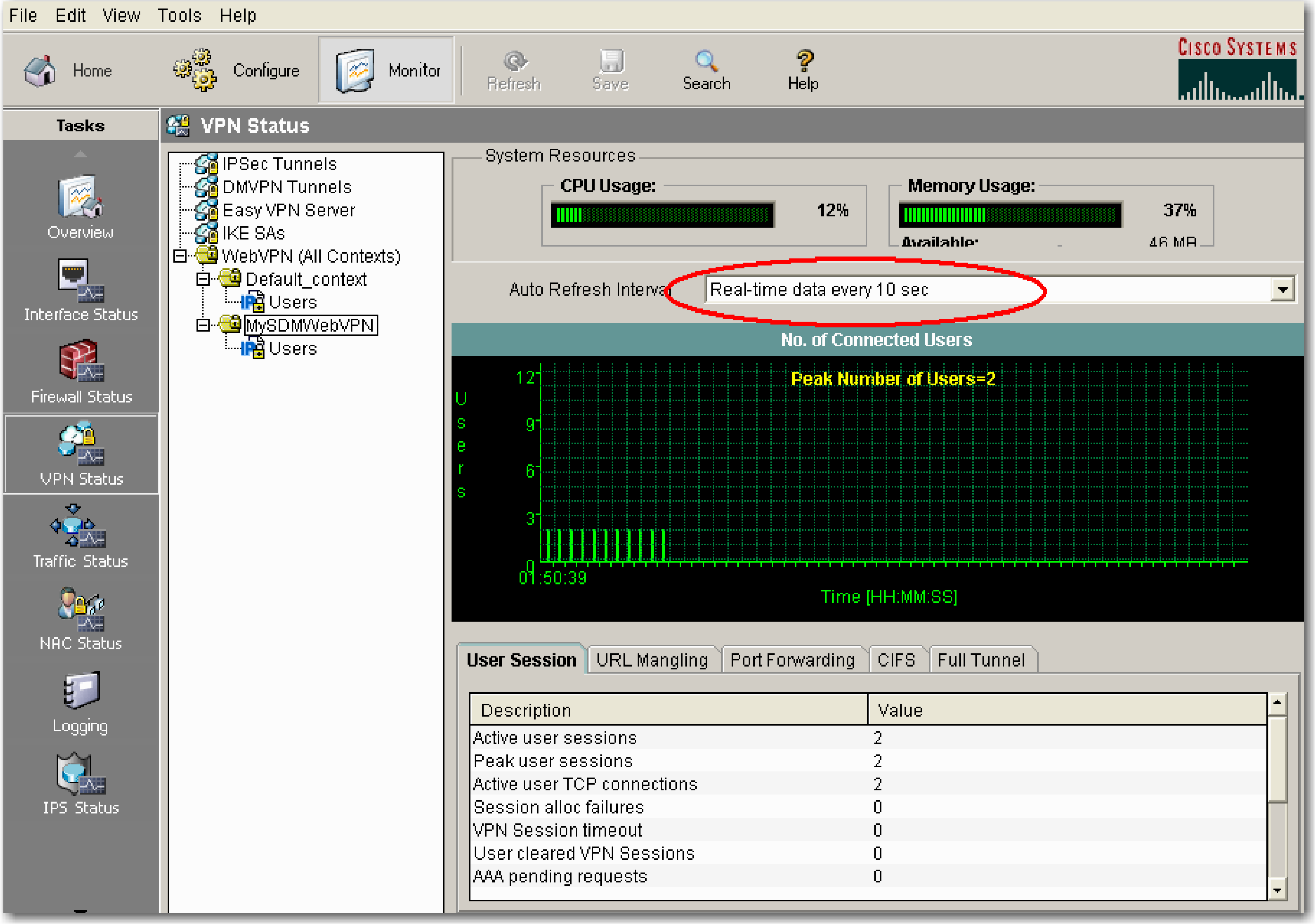
Click **Disconnect** to terminate the full tunnel. The SSL VPN Client will be removed from your local host.

Monitoring

Users can go to **Monitor Mode**, select **VPN Status**, and expand **Web VPN (All Contexts)**. Click **MySDMWebVPN** (Figure 20) to display the data gathered for this WebVPN contexts configured on the router. By default, this data is refreshed every 10 seconds. If 10 seconds is too short an interval for you to view data before the next refresh, you can select an auto-refresh interval of **Real-time data every minute**.

The tabbed area gathered statistics in a series of tabs for easier viewing.

Figure 20. **MySDMWebVPN Context**



CPU Usage: 12%

Memory Usage: 37%

Available: 46 MB

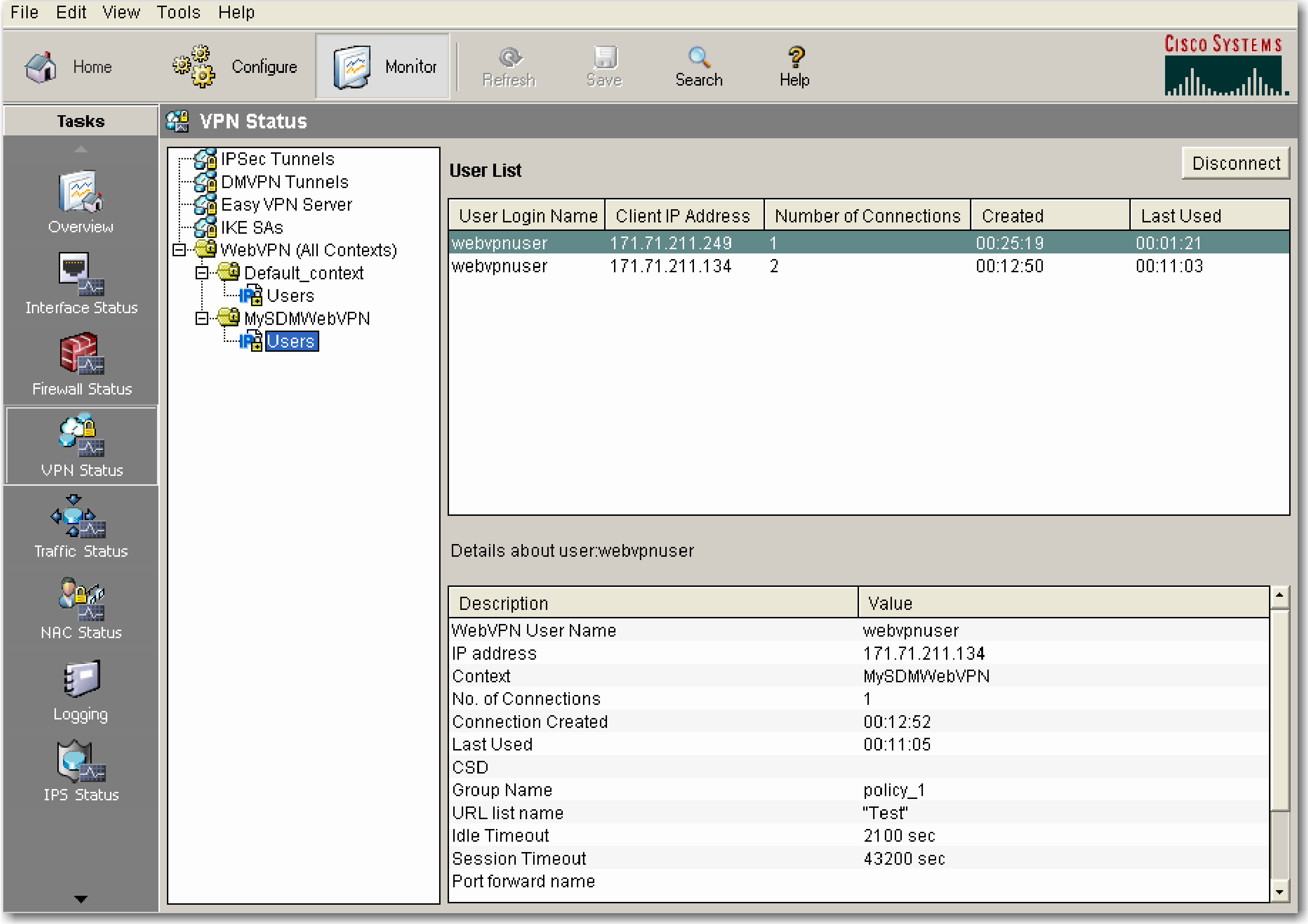
Auto Refresh Interval: Real-time data every 10 sec

Description	Value
Active user sessions	2
Peak user sessions	2
Active user TCP connections	2
Session alloc failures	0
VPN Session timeout	0
User cleared VPN Sessions	0
AAA pending requests	0

Go to **Monitor Mode**, select **VPN Status**, and expand **Web VPN (All Contexts)**. Expand **MySDMWebVPN**, and click **Users** (Figure 21). This window displays user information for the context. Because there might be multiple group polices configured for the context, each using their own URL list and server lists, this screen provides valuable information about how individual users are using their WebVPN connections.

You can control individual WebVPN users in this window by choosing a user and clicking the **Disconnect** button.

Figure 21. **User List**



User List

User Login Name	Client IP Address	Number of Connections	Created	Last Used
webvpnuser	171.71.211.249	1	00:25:19	00:01:21
webvpnuser	171.71.211.134	2	00:12:50	00:11:03

Details about user:webvpnuser

Description	Value
WebVPN User Name	webvpnuser
IP address	171.71.211.134
Context	MySDMWebVPN
No. of Connections	1
Connection Created	00:12:52
Last Used	00:11:05
CSD	
Group Name	policy_1
URL list name	"Test"
Idle Timeout	2100 sec
Session Timeout	43200 sec
Port forward name	

In summary, by using the Cisco SDM WebVPN wizards, users can create a WebVPN gateway with minimum knowledge of Cisco IOS SSL VPN technology.

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico• The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA