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

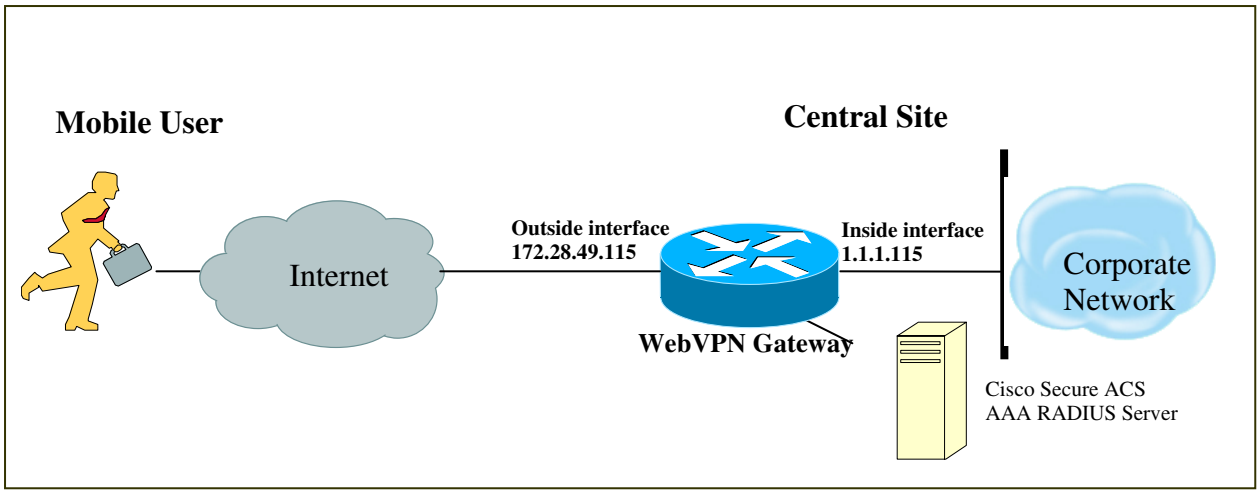
Cisco IOS WebVPN is supported by Cisco Router and Security Device Manager (SDM) v2.3 with Cisco IOS Software Release 12.4(6)T. Cisco SDM provides wizards for both basic and advanced configuration, and provides monitoring information and statistics for user sessions, clientless access, and full network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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

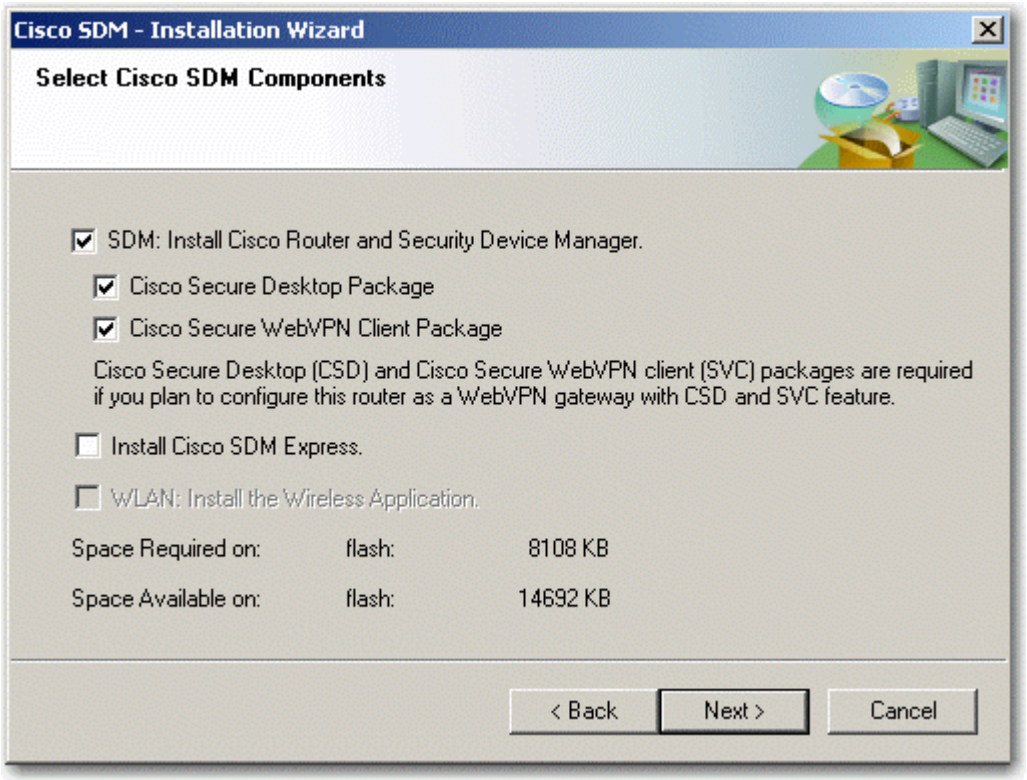


Sample Configuration

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



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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.

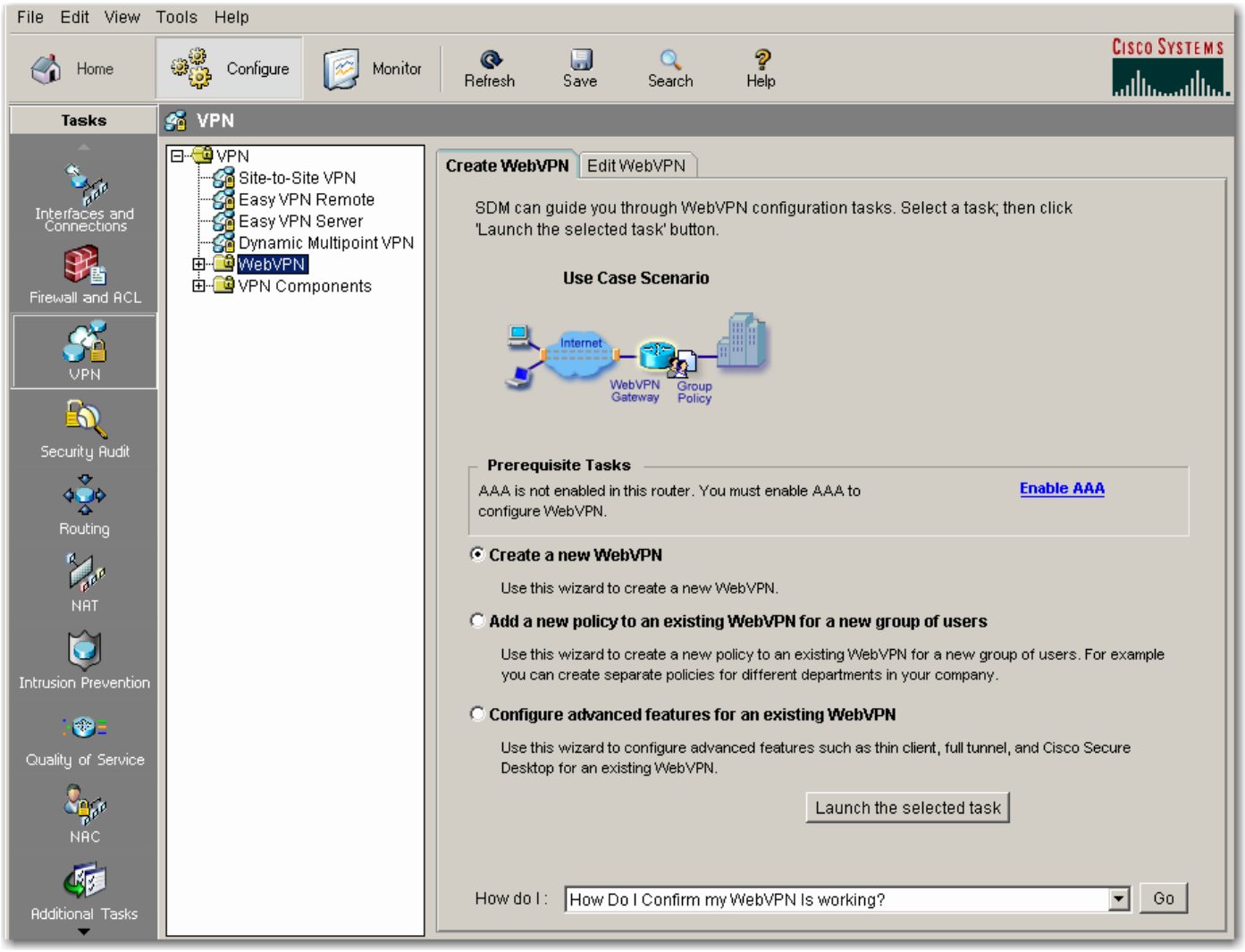
Cisco SDM allows users to easily configure the Cisco WebVPN gateway with limited information. The following steps are used to configure the deployment scenario using Cisco SDM.

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.

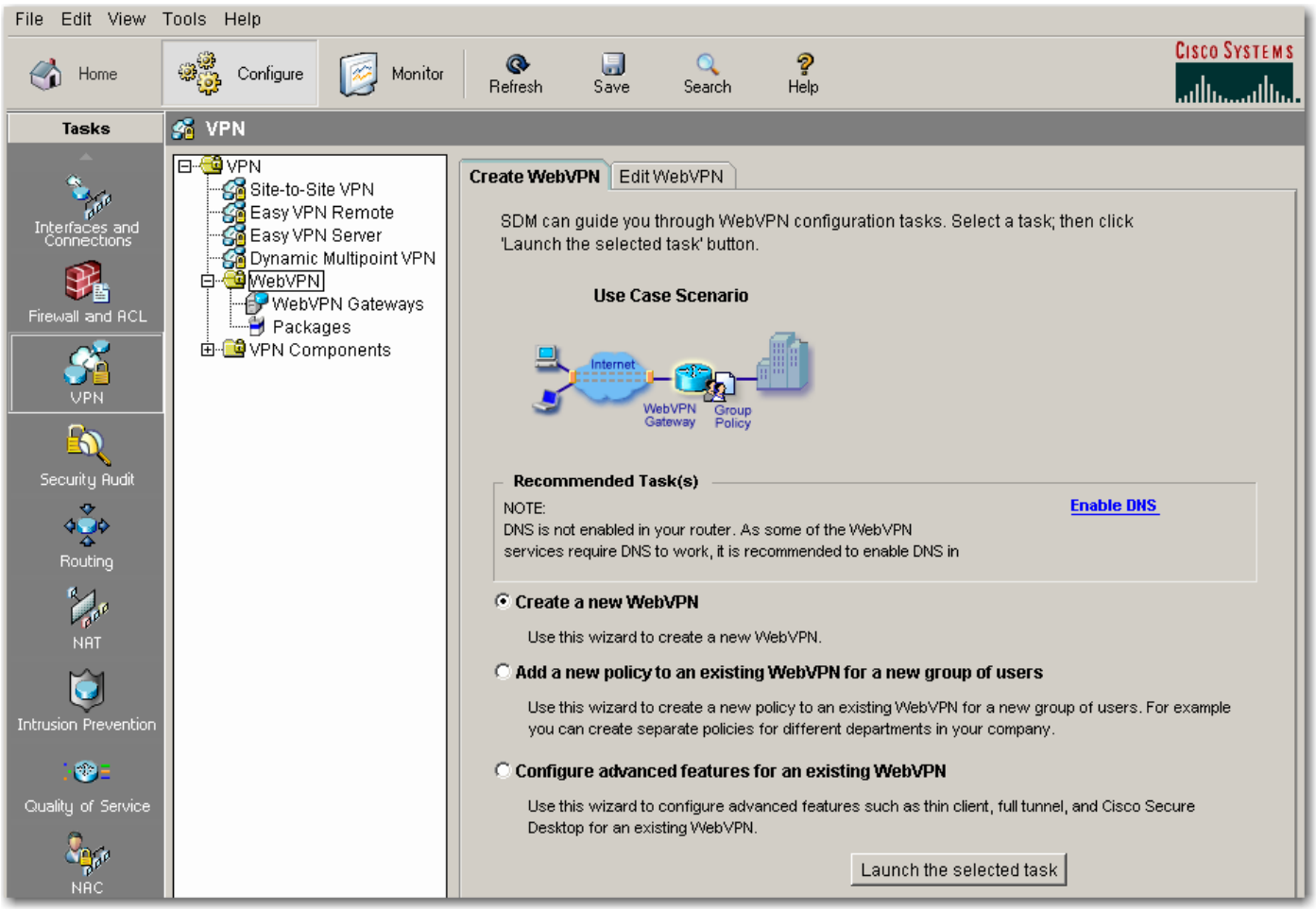
Figure 3. Create WebVPN – Enable AAA



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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



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

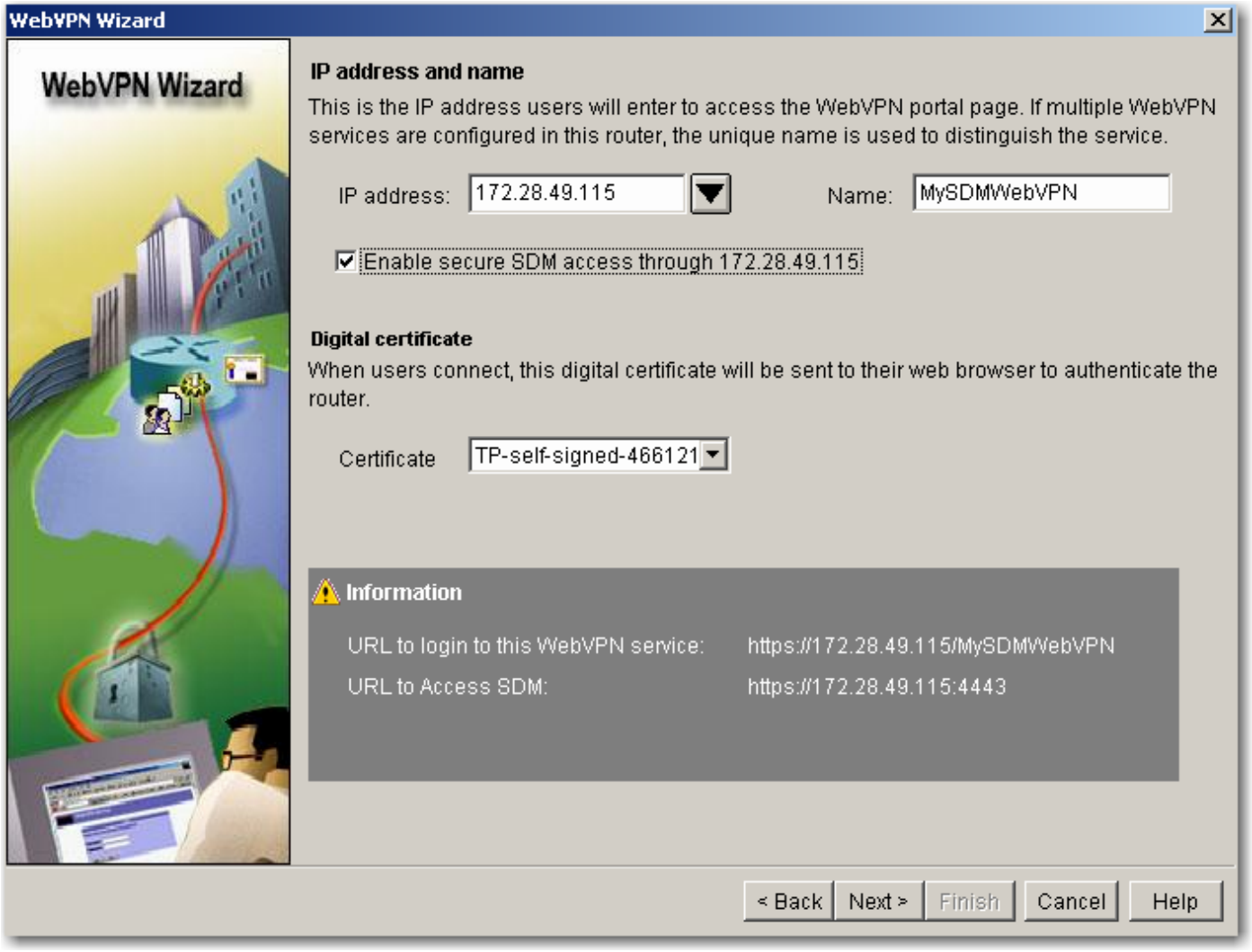
© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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



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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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.

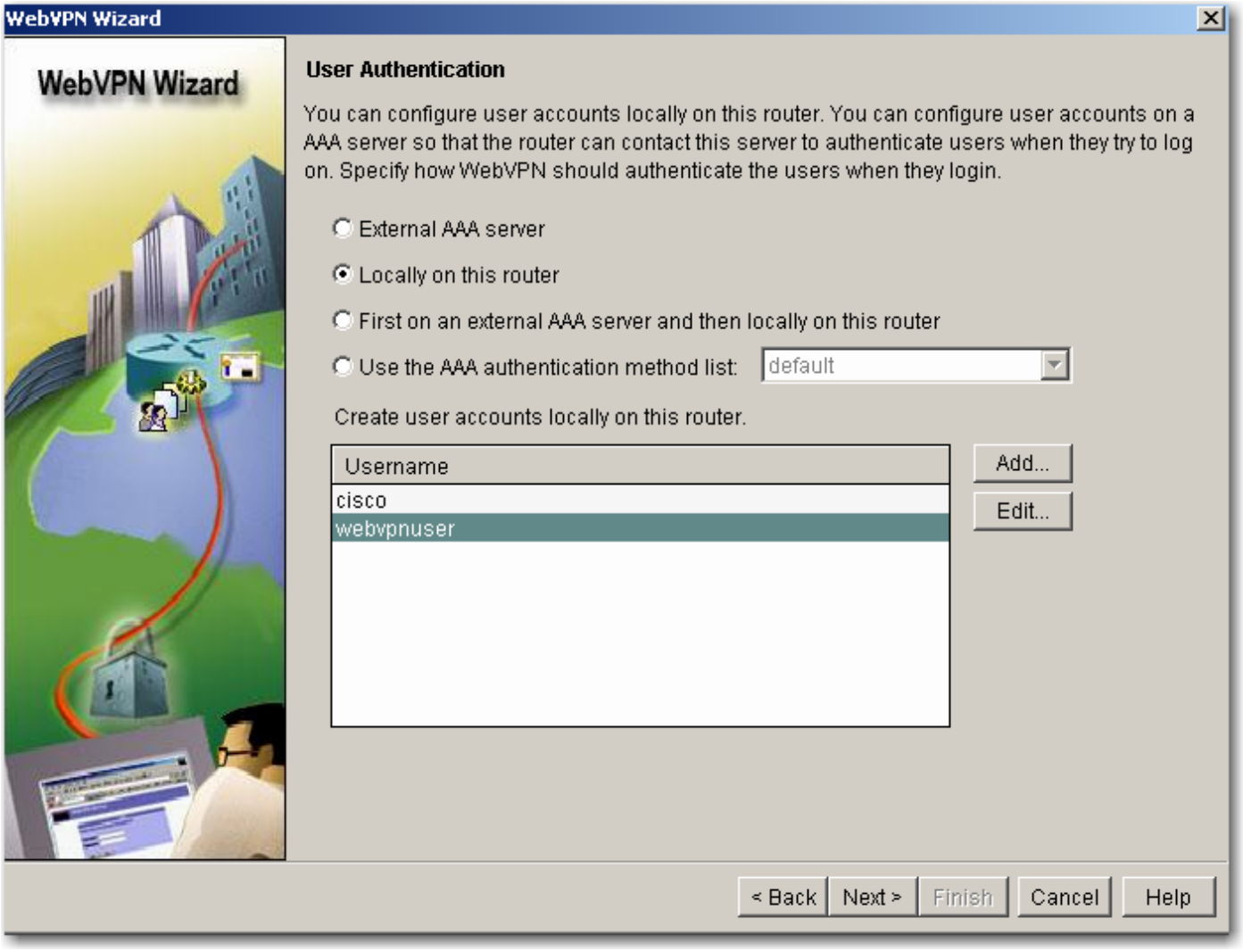
In our example, we do not have a remote AAA server; all users will be authenticated locally. Select **Locally on this router**. Click the **Add…** button to add a new user:

- 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**.

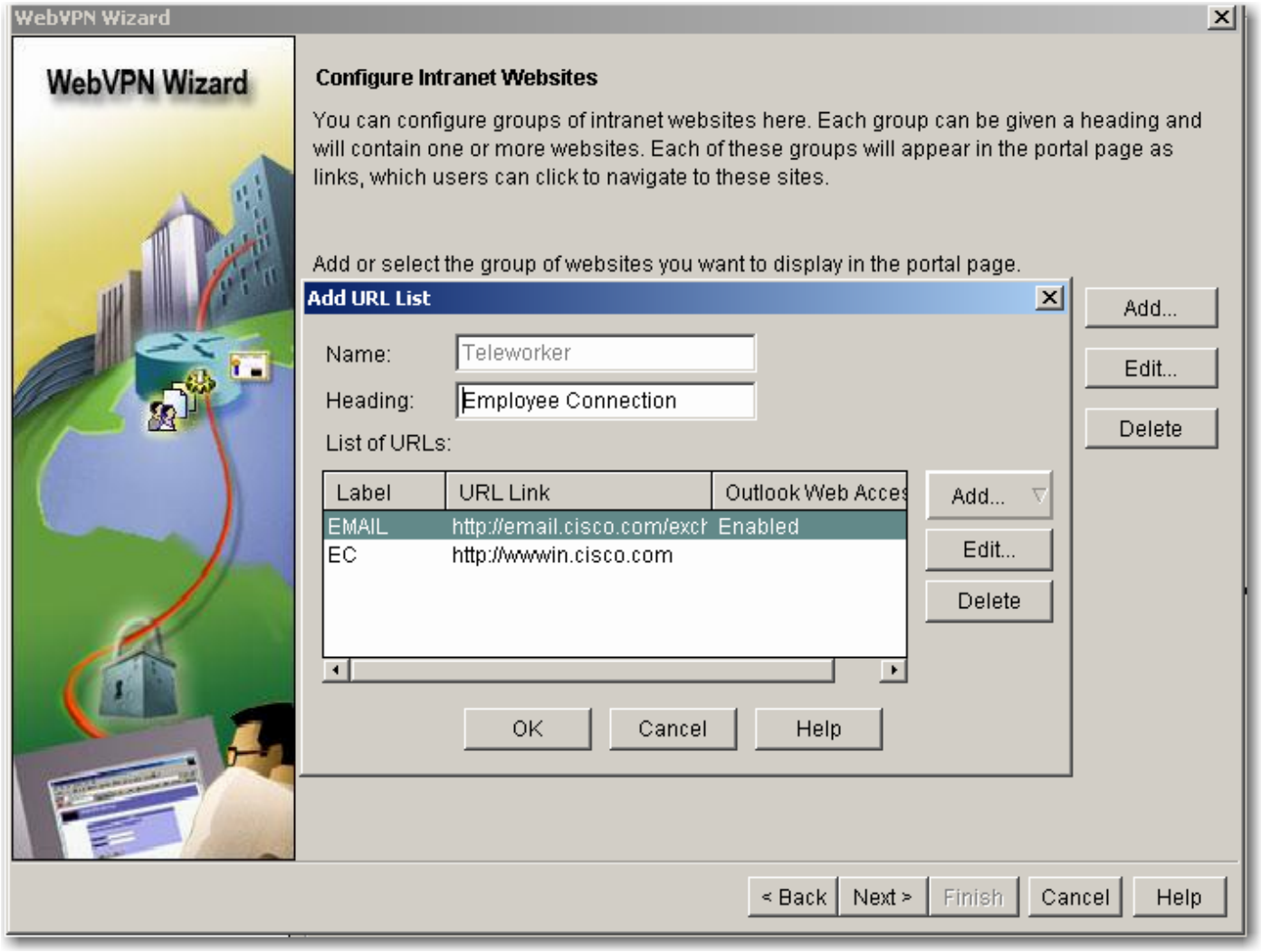
Figure 6. IKE Proposal



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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



- 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…**

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

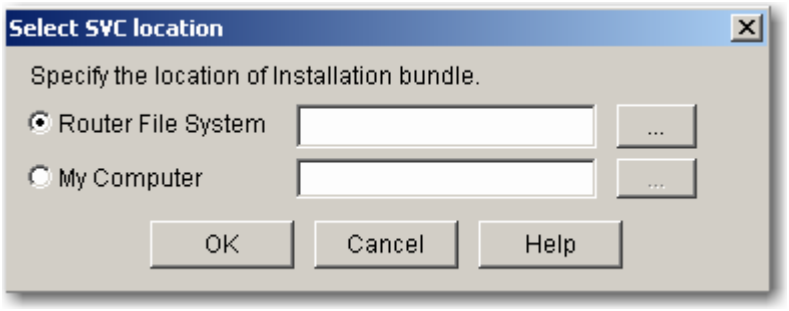
- Label: **Email**
- URL: **http:/your company's web mail server**; in our example, WebVPN is configured with Cisco's Outlook Web Access (OWA) http://email.cisco.com
- Click **OK**.

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).

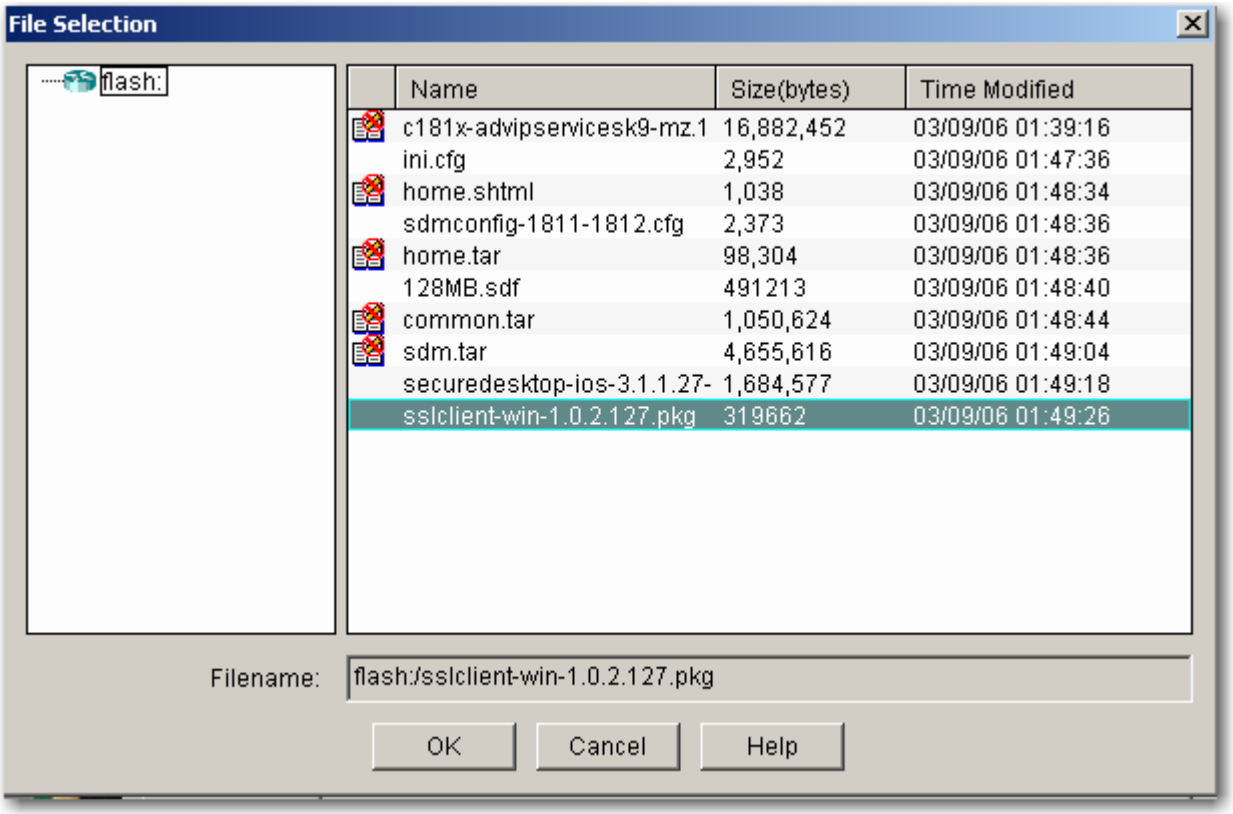
  Select **sslclient-win-1.0.2.127.pkg**[1]

  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.

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com



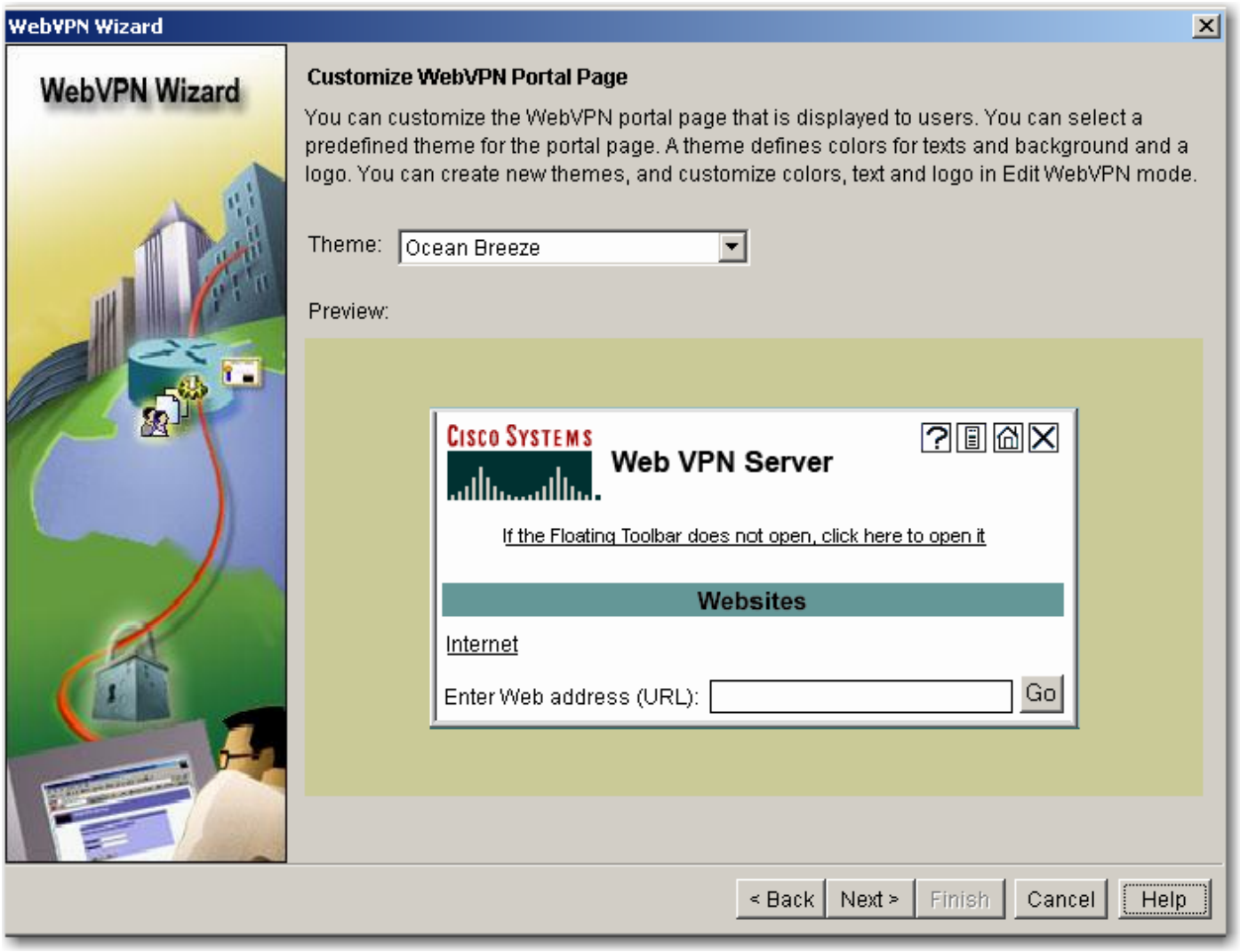
- Click **OK**.

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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

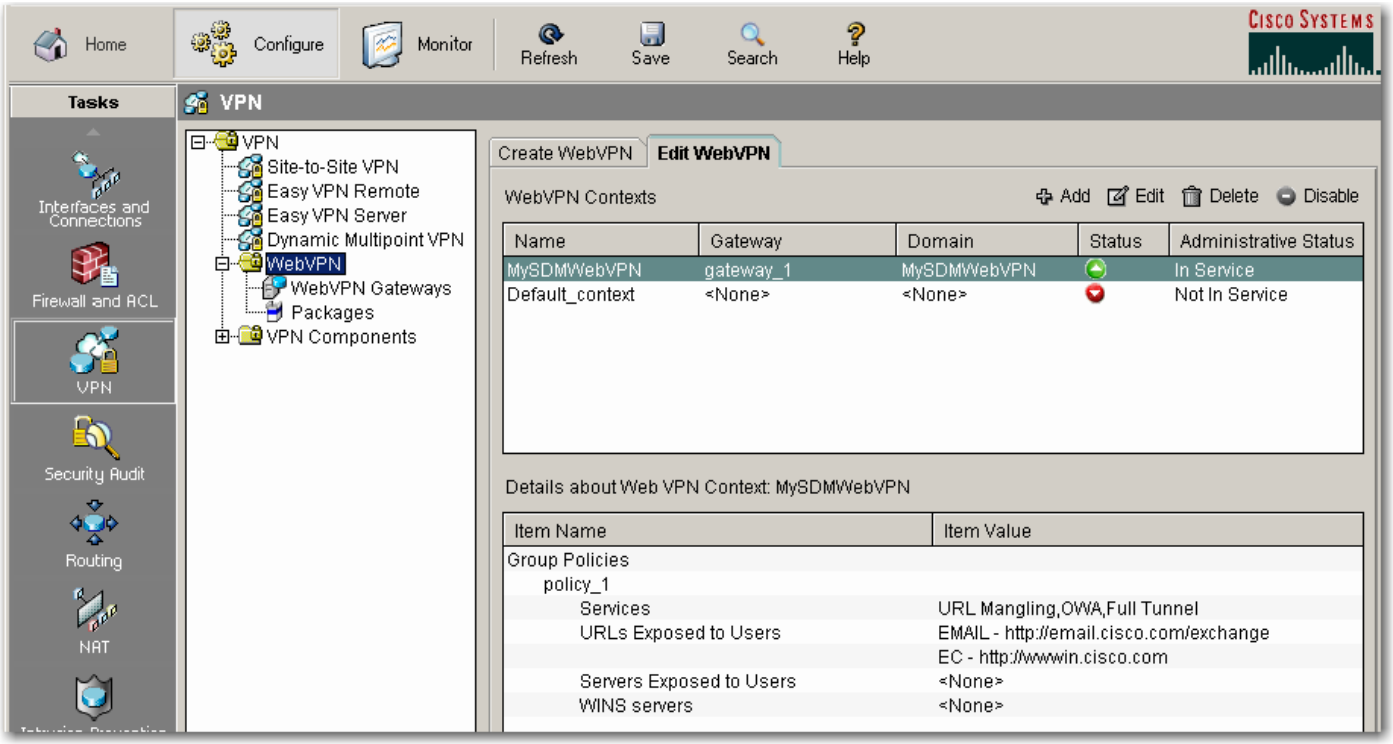


View the Summary of Configuration. Click **Finish** if you are satisfied with the configuration, or click **Back** to revise the configuration. You will be prompted by an alert. Read the information, click **I read and understood**, click **Save shortcut on Desktop** if necessary, and click **OK**. Once 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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com



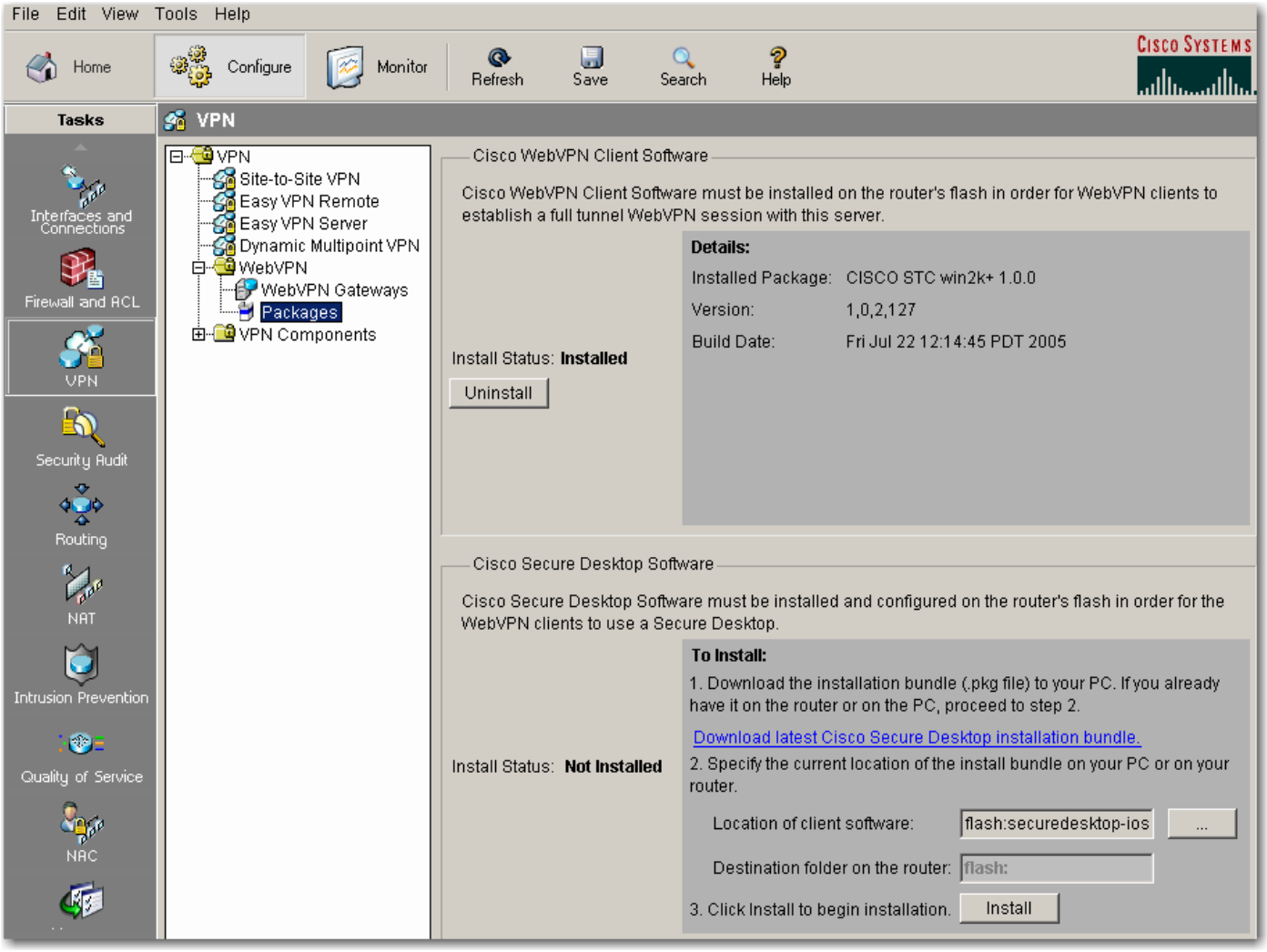
To view the newly created WebVPN gateway, at **Configure Mode**, select the **VPN**, expand **WebVPN**, and select **WebVPN Gateways**. The WebVPN Gateway window provides the IP address and the digital certificate for the WebVPN contexts that use it. You can provide the information for a gateway in this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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

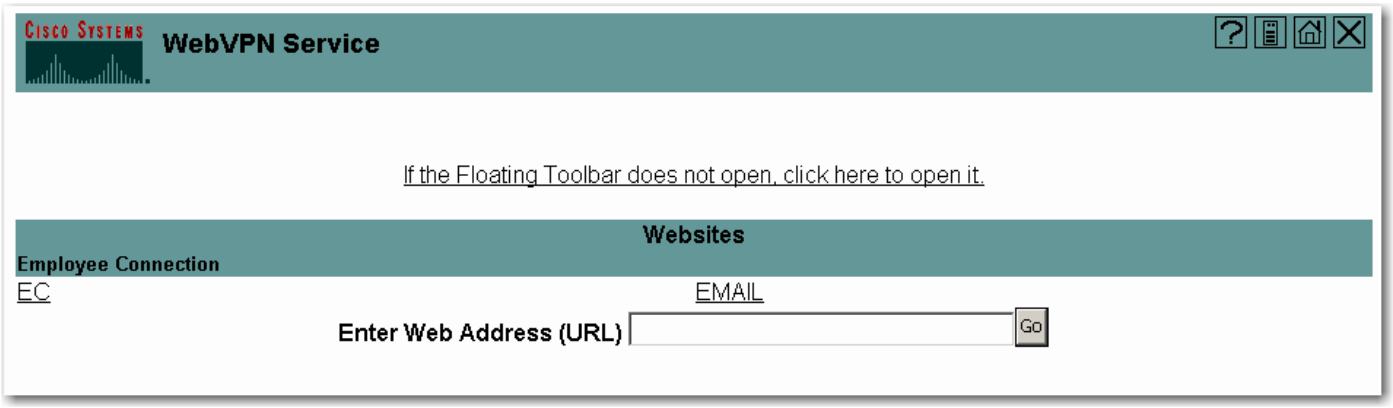
Access WebVPN Portal

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

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

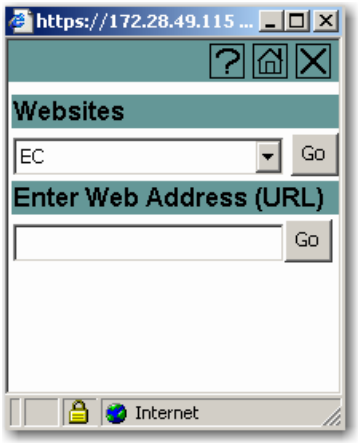
Figure 14. WebVPN Service Portal



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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.

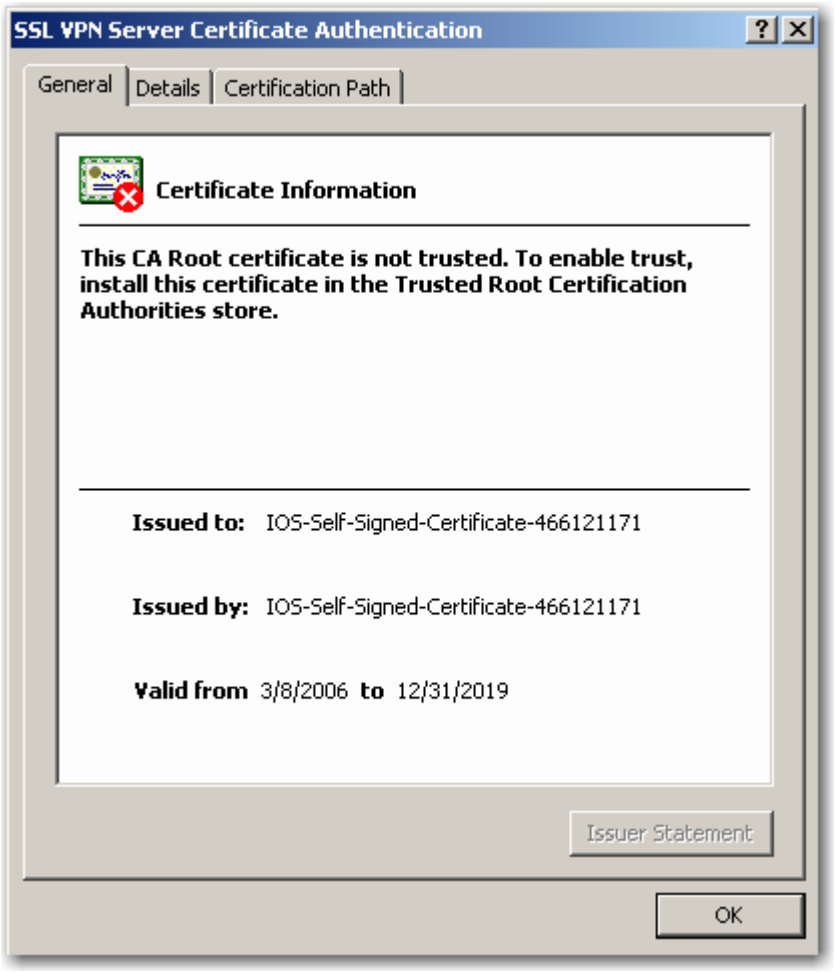
In our example, you will be prompted to install the SSL VPN Client for WebVPN. Read the security warning, and allow the installer to launch ActiveX. Figure 16 shows the installer has been launched.

Figure 16. SSL VPN Client

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

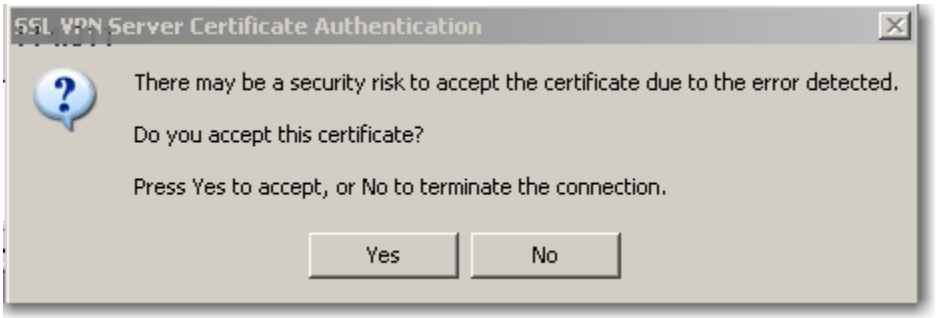
You will be asked to authenticate the SSL VPN Server Certificate signed by an untrusted certificate authority. Click **Yes** to view the certificate. The SSL VPN Server Certificate Authentication window appears. Read the certificate and click **OK** to accept it. In our example, the router does not receive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

Figure 17. Certificate Information



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



© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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

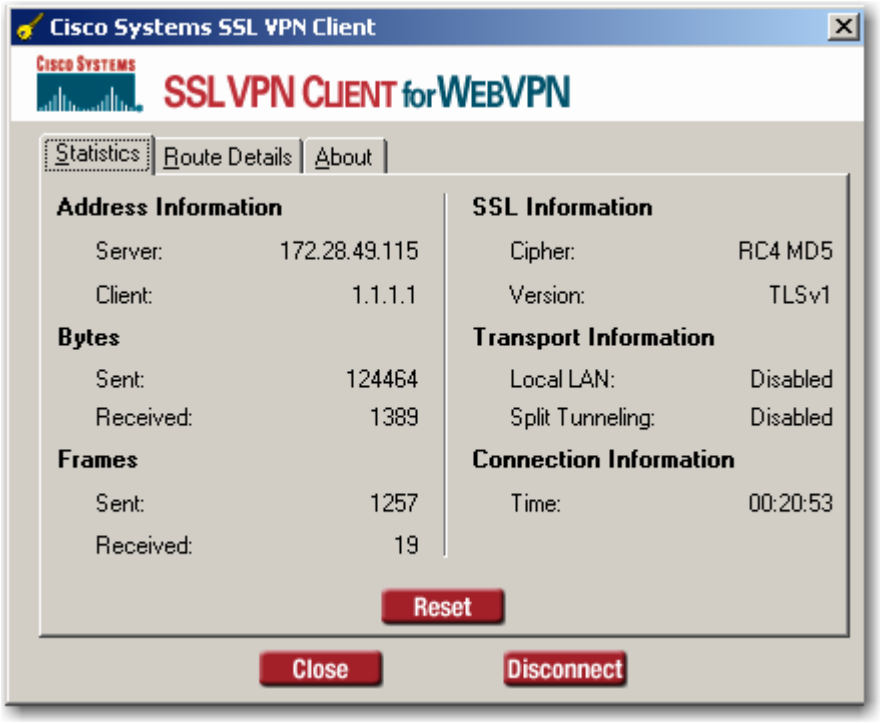
```
Ethernet adapter Local Area Connection 6:

        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**



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

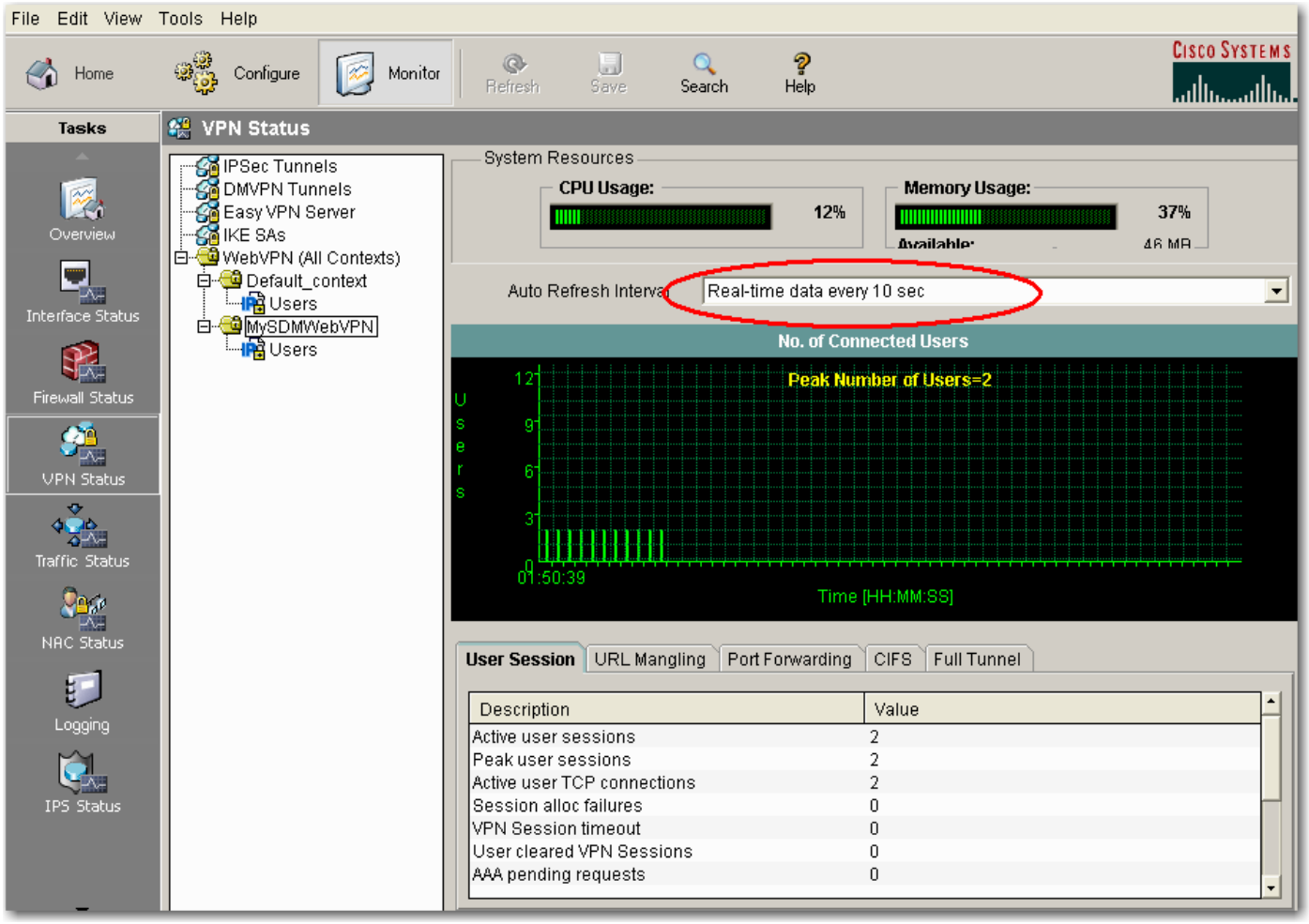
Monitoring

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**

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

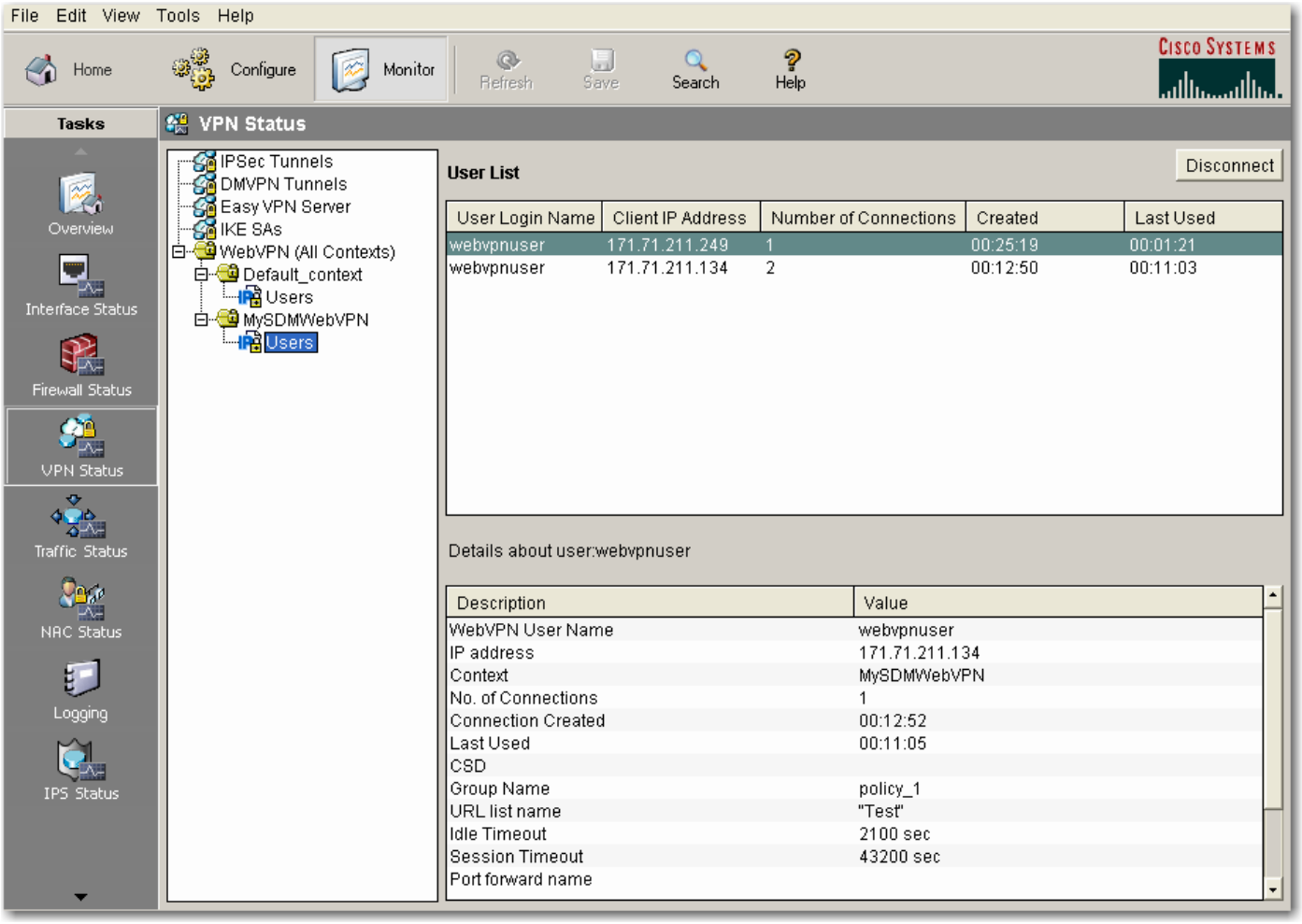


Go to **Monitor Mode**, select **VPN Status**, and expand **Web VPN (All Contexts)**. Expand **MySDMWebVPN**, and click **Users** (Figure 21). This window displays user information for the context. Because there might be multiple group polices configured for the context, each using their own URL list 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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com



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

© 2006 Cisco Systems, Inc. All right reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on Cisco.com

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

Copyright 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrat, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in the USA