

CHAPTER 8

Concentrator Remote Access Connections with PPTP, L2TP, and WebVPN

The last chapter introduced how to configure the VPN 3000 concentrators to accept IPsec remote access sessions. This chapter will focus on using a concentrator to terminate other types of remote access sessions, including:

- PPTP
- L2TP over IPsec
- WebVPN

The remainder of this chapter will focus on the configuration of the concentrator to support these types of remote access VPN implementations. I'll spend more time on implementing PPTP/L2TP connectivity in Chapter 13, "Windows Software Client." Most of this chapter is dedicated to the newest CiscoVPN implementation: SSL. Cisco refers to their SSL VPN implementation as WebVPN. I'll focus on setting up the concentrator to accept clientless connections (just a web browser), thin client connections (port forwarding), and network client connections (SSL VPN Client software).

PPTP and L2TP Remote Access

The configuration of PPTP and L2TP remote access is much simpler than that of IPsec, even if you'll be using L2TP over IPsec; this is because if you're using IPsec with Cisco remote access clients, you have many more IKE Mode Config features than what L2TP over IPsec clients support. The configuration of both of these protocols occurs in two locations on the VPN 3000 concentrator:

- User management
- Global configuration

Most of your configuration is done at the group level; very rarely will you have to change the global (system-wide) properties for PPTP or L2TP. The following three sections will discuss the configuration of these two protocols: group configurations for PPTP and L2TP, global configurations for PPTP, and global configurations for L2TP.

PPTP and L2TP Group Configuration

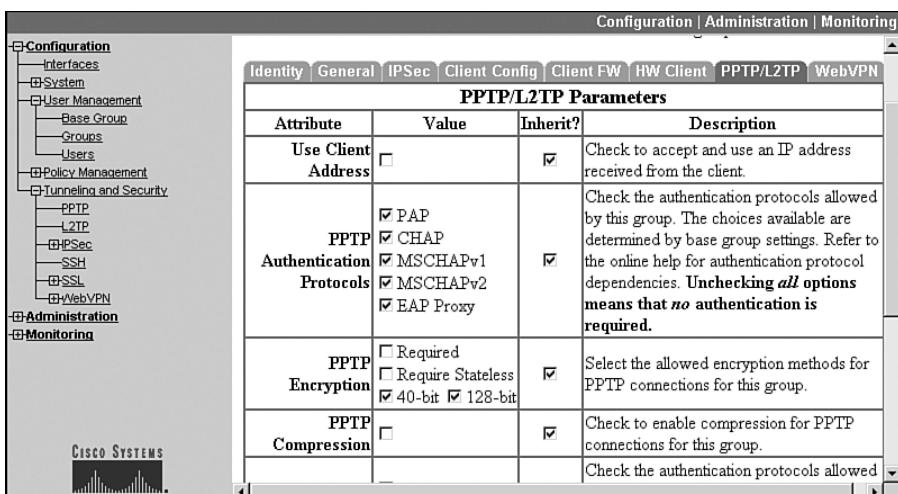
Most of your configuration for PPTP and L2TP will be done under a group's configuration: **Configuration > User Management > Groups**. In a group within the General tab, (discussed in the last chapter), the *Tunneling Protocols* parameter allows you to specify which tunneling protocols, if any, a group is allowed to use. If you want the group to be able to use PPTP or L2TP, you must select these.

NOTE

If you want to use L2TP over IPsec, the group no longer will be able to perform general IPsec connections to the concentrator.

The remainder of the group's configuration is done under the PPTP/L2TP tab; the top part of this screen is shown in Figure 8-1. The first parameter is the *Use Client Address* parameter, which is disabled. If you want the client to use its own address, make sure you've enabled this option in the **Configuration > System > Address Management > Address** section; this was discussed in the "Address Assignment" section earlier in the last chapter. However, because of various reasons, including security, it is recommended to have the concentrator assign an address to the client.

Figure 8-1 Group Configuration: PPTP/L2TP Tab



Below this there are two sets of parameters: one set applies to PPTP, which you can see in Figure 8-1, and one set applies to L2TP (you can't see this in Figure 8-1). Here are the parameters:

- **PPTP Authentication Protocols**—These check boxes specify the PPP authentication protocol to use to authenticate the device. These can include: "PAP," "CHAP," "MSCHAPv1," "MSCHAPv2," or "EAP Proxy." If you select "Required" under

PPTP Encryption, you must choose one or both MS-CHAP protocols. Also, EAP is not supported for connections that use encryption. Not selecting at least one authentication protocol means that *no* authentication is required to allow the PPTP connection. You might want to use this to test the connection; but immediately afterward, change it to one or more of the listed options. Because all of the authentication options are check boxes, you can select none, one, or all of them.

- **PPTP Encryption**—These check boxes specify the data encryption to use for the clients. Supported options include “Required,” “Require Stateless,” “40-bit,” or “128-bit.” If you choose “Required,” the PPTP client must use MPPE and only MS-CHAPv1 and MS-CHAPv2 are supported for authentication. Plus, you also must enable “40-bit” or “128-bit” encryption, which uses the RC-4 encryption algorithm. This option doesn’t support NT Domain user authentication. With “Require Stateless,” the encryption keys are changed on every packet transmitted. This option is not supported with NT Domain authentication; however, choosing this option might provide better performance in environments where packet loss is to be expected, such as dialup. Since all the encryption options are check boxes, you can select none, one, or all of them.
- **PPTP Compression**—If all your users in the group are using dialup for access, then enabling compression probably will enhance their transmission speeds. MPPC is used. This is disabled by default. Compression is supported only with stateless encryption.
- **L2TP Authentication Protocols**—See *PPTP Authentication Protocols*.
- **L2TP Encryption**—See *PPTP Encryption*.
- **L2TP Compression**—See *PPTP Compression*.

When you are done making your changes to your group, click the **Apply** button at the bottom of the screen to activate them.

NOTE

The *Use Client Address* parameter, *PPTP Authentication Protocols* parameters, and *L2TP Authentication Protocols* parameters can be overridden on a user-by-user basis in the user configuration: **Configuration > User Management > Users**. After selecting a user, you can go to the user’s PPTP/L2TP tab to override these parameters for a particular user.

CAUTION

Do not enable compression on the concentrator if you have a mixed group of users: dialup and broadband. The dialup users will notice a boost in speed; however, the broadband throughput will suffer if these users accidentally enable compression. If you have two groups of people—dialup and broadband—I recommend that you put them into two separate groups and enable compression for the dialup group.

PPTP Global Configuration

To configure system-wide PPTP options, go to **Configuration > Tunneling and Security > PPTP**. Here are the global options you can configure:

- **Enabled**—This check box allows you to globally enable or disable PPTP; un-checking it immediately terminates any current PPTP session.
- **Maximum Tunnel Idle Time**—This text box allows you to enter the amount of time to wait, in seconds, before disconnecting a PPTP tunnel that has no active sessions. The default is 5 seconds, but this can range from 5–86,400 seconds.
- **Packet Window Size**—This text box allows you to enter the PPTP packet window size for acknowledgments; the default is 16 packets, but this can range from 0–32 packets.
- **Limit Transmit Window**—This check box allows you to enable the use of windowing to the client’s window size; this is disabled by default.
- **Max. Tunnels**—This text box allows you to configure the maximum number of active PPTP tunnels that you want your concentrator to support; please note that you are restricted to a maximum based on the concentrator model the PPTP tunnels terminate on.
- **Max. Sessions/Tunnel**—This text box allows you to configure the maximum number of sessions allowed per tunnel. The default is 0 (no implied limit); and the maximum can be up to the maximum based on the concentrator model.
- **Packet Processing Delay**—This text box allows you to enter the packet processing delay for flow control of PPTP sessions. The number you enter is represented in tenths of a second. The default is 1 (1/10 of a second).
- **Acknowledgment Delay**—This text box allows you to enter the number of milliseconds the concentrator will wait before sending an acknowledgment to a client when there is no returning data to be sent to the client (a packet will have to be sent with only acknowledgment information); the default is 500 milliseconds, but this can range from 0–5,000 milliseconds, where 0 means an immediate acknowledgment response.
- **Acknowledgment Timeout**—This text box allows you to enter the number of seconds the concentrator will wait for a reply before determining that an acknowledgment has been lost. The default is 3 seconds, but this can range from 1–10 seconds.

Click the **Apply** button at the bottom of the screen to save your changes.

L2TP Global Configuration

To configure system-wide L2TP options, go to **Configuration > Tunneling and Security > L2TP**. Here are the global options you can configure:

- **Enabled**—This check box allows you to globally enable or disable L2TP; un-checking it immediately terminates any current L2TP session.

- **Maximum Tunnel Idle Time**—This text box allows you to enter the amount of time to wait, in seconds, before disconnecting an L2TP tunnel that has no active sessions. The default is 5 seconds, but this can range from 5–86,400 seconds.
- **Control Window Size**—This text box allows you to enter the L2TP window size for unacknowledged control channel packets; the default is 4 packets, but this can range from 0–16 packets.
- **Control Retransmit Interval**—This text box allows you to enter the number of seconds to wait before the concentrator retransmits an unacknowledged L2TP tunnel control message; the default is 1 second, but this can range from 1–10.
- **Control Retransmit Limit**—This text box allows you to enter the maximum number of times the concentrator will send L2TP tunnel control packets to a client before assuming the client is dead; the default is 4 times, but this can range from 1–32.
- **Max. Tunnels**—This text box allows you to configure the maximum number of active L2TP tunnels you want your concentrator to support; please note that you are restricted to a maximum based on the concentrator model the PPTP tunnels terminate on.
- **Max. Sessions/Tunnel**—This text box allows you to configure the maximum number of sessions allowed per tunnel. The default is 0 (no implied limit); and the maximum can be up to the maximum based on the concentrator model.
- **Hello Interval**—This text box allows you to enter the hello interval value, which determines when the concentrator sends a hello message after a period of idle time on an L2TP tunnel; the default is 60 seconds, but this can range from 1–3,600 seconds.

Click the **Apply** button at the bottom of the screen to save your changes. In Chapter 13, “Windows Software Client,” I’ll discuss how to configure Microsoft’s client for accessing the concentrator.

NOTE

Cisco highly recommends that you do not change the global properties for PPTP or L2TP sessions without contacting TAC first—the odds are that you’ll create more problems than you will solve.

WebVPN Remote Access

The third type of remote access connectivity I will discuss is how to set up the concentrator to accept WebVPN sessions. I discussed SSL VPNs in Chapter 5, along with the Cisco implementation of SSL VPNs: WebVPN.

SSL uses digital certificates for authentication (in most cases this is server-side authentication). By default, the concentrator will create a self-signed SSL server certificate when it boots up. Or, you can install a third-party SSL identity certificate on the concentrator; however, if you choose this option, you also must install certificates on your web browser clients.

If you choose the latter option, you'll need to obtain a certificate for your concentrator, which I explained previously in Chapter 7 in the "Digital Certificates" section.

The remainder of this section will focus on the five areas concerning the setup of WebVPN on the VPN 3000 concentrators:

- HTTPS access
- System-wide WebVPN parameters
- Group WebVPN configuration
- SSL VPN Client (SVC)
- Cisco Secure Desktop (CSD) for WebVPN access

HTTPS Access

One of the first steps you'll need to perform is to make sure that HTTPS access and WebVPN access are allowed to the concentrator. The following two sections will discuss how you allow HTTPS and WebVPN access.

First, you need to make sure that HTTPS access is allowed by your concentrator. There are two areas that you'll need to examine and possibly change:

- HTTPS properties
- WebVPN interface configuration

HTTPS Properties

To access the concentrator's HTTPS properties, go to **Configuration > Tunneling and Security > SSL**. There are two options on this page:

- *HTTPS*
- *Protocols*

If you click the **HTTPS** hyperlink, you'll find three options:

- **Enable HTTPS**—This check box enables or disables HTTPS access; by default it is enabled.
- **HTTPS Port**—This text box allows you to change the TCP port number that HTTPS access will use; this defaults to 443, but you can change it to another number to enhance your security. Please note that IPsec over TCP cannot use a port that WebVPN will be using.
- **Client Authentication**—This check box, when checked, allows the concentrator to verify the client's digital certificate. If you choose this option, you must install certificates manually on all of your client's web browsers as well as on your concentrator. You also must configure an authorization server using RADIUS or LDAP. I discussed

this in the last chapter in the “Authorization Servers” section. Next, in the group configuration’s IPsec tab, set *Authentication* to “None” and the *Authorization Type* to either “RADIUS” or “LDAP.” Remember that the concentrator will send the contents specified by the *DN Field* parameter in this tab to the authorization server, which typically is the information found in the Common Name (CN) field of the certificate. Instead of using a client-side certificate, you can use usernames and passwords for user authentication. In most implementations I’ve set up I have not put certificates on the client; however, I have set up WebVPN only in small environments. For a large environment, I would seriously consider the use of certificates.

Click the **Apply** button to accept your changes.

NOTE

There are two important things to point out about the information on this screen. First, if you want to install certificates on both the concentrators and clients, the WebVPN Port Forwarding feature will no longer work. The Port Forwarding feature uses Java for its implementation, and Java doesn’t have the ability to access the web browser’s certificate for user authentication. Second, when you click the **Apply** button on this screen, even if you haven’t made any changes on the screen, the concentrator automatically breaks any web browser management session, forcing you to log back in to the concentrator.

If you click the **Protocols** hyperlink from the **Configuration > Tunneling and Security > SSL** screen, you’ll find these options:

- **Encryption Protocols**—These check boxes enable the encryption algorithms that clients can use for SSL connections. If you uncheck all of them, SSL is disabled. You can choose any or all of the following (in order of strength): “3DES-168/SHA,” “RC-128/MD5,” and “DES-56/SHA.” I highly recommend that you don’t use RC4-128, because it seriously affects the performance of the WebVPN connection.
- **SSL Version**—This drop-down selector allows you to choose the SSL version that clients must use for WebVPN access. Your options include the following:
 - “**Negotiate SSL V3/TLS V1**”—The concentrator first tries SSLv3 and then TLSv1; this is the default choice because most web browser clients support these.
 - “**Negotiate SSL V3**”—The concentrator tries SSLv3, but will use a less secure access method.
 - “**Negotiate TLS V1**”—The concentrator tries TLSv1, but will use a less secure access method.
 - “**SSL V3 Only**”—Only SSLv3 clients are allowed access.
 - “**TLS V1 Only**”—Only TLSv1 clients are allowed access.

NOTE

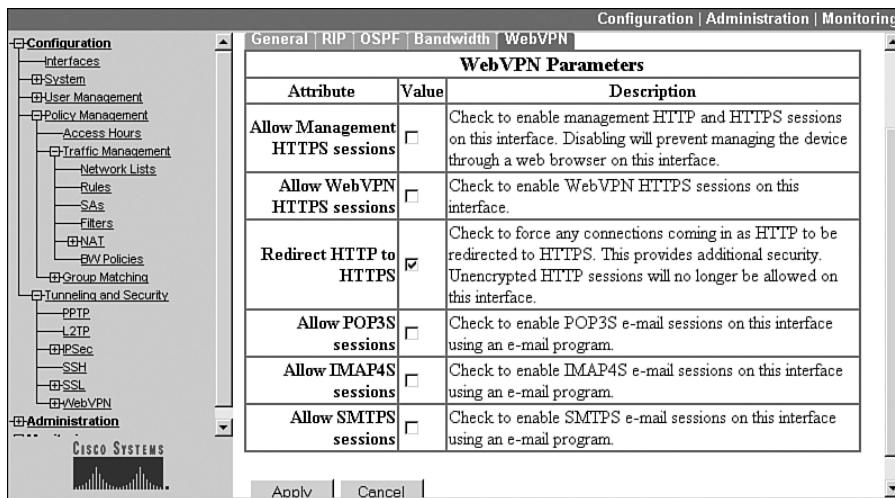
If you'll be using the Port Forwarding feature in WebVPN access, you'll need to choose either "Negotiate SSL V3/TLS V1" or "Negotiate SSL V3"; other SSL version options, if chosen, will cause Port Forwarding to break.

WebVPN Interface Configuration

Once you've set up your HTTPS properties, you'll need to allow WebVPN access to the concentrator. The simplest way to accomplish this is to configure the WebVPN properties under the interface for which these remote access sessions will terminate (typically the public interface). To allow WebVPN access, go to **Configuration > Interfaces** and click the hyperlink of the interface name, like **Ethernet 2 (Public)**. Then click the **WebVPN** tab at the top, showing you the screen in Figure 8-2. Here are the parameter options on this screen:

- **Allow Management HTTPS sessions**—When this check box is selected, you can use HTTPS to manage the concentrator from this interface. Enable this option only when the concentrator is at a remote site and you need to manage it from its public interface.
- **Allow WebVPN HTTPS sessions**—You must select this check box to allow WebVPN HTTPS traffic into the concentrator.
- **Redirect HTTP to HTTPS**—This check box allows you to force any incoming HTTP connections to the concentrator's interface to be redirected to using HTTPS. I highly recommend that you enable this for convenience purposes, because many users might forget to include the "s" in "https" in the URL address bar.
- **Allow POP3S sessions**—This check box, when selected, allows the POP3S (secure POP3) to access a configured POP3S proxy behind the concentrator. The default port number for POP3S is 995.
- **Allow IMAP4S sessions**—This check box, when selected, allows the IMAP4S (secure IMAP4) to access a configured IMAP4S proxy behind the concentrator. The default port number for IMAP4 is 993.
- **Allow SMTPS sessions**—This check box, when selected, allows the SMTPS (secure SMTP) to access a configured SMTPS proxy behind the concentrator. The default port number for SMTP is 998.

Using this screen will update the rules in the concentrator's interface filter automatically based on the options you chose here. When you are done, click the **Apply** button at the bottom of the screen to accept your changes.

Figure 8-2 Interface Configuration: WebVPN Tab

WebVPN Global Configuration

To configure system-wide WebVPN parameters, go to the **Configuration > Tunneling and Security > WebVPN** screen. The following sections will cover the hyperlinks that appear on this page and the configuration options within the hyperlinks.

HTTP/HTTPS Proxy

Clicking the **HTTP/HTTPS Proxy** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to set up HTTP and HTTPS proxy services for users. The concentrator can terminate inbound HTTPS connections and forward any HTTP/HTTPS requests to a real proxy server. This process provides better scalability. The **HTTP/HTTPS Proxy** screen is shown in Figure 8-3. Here are the options on this screen:

- **HTTP Proxy**—This is the IP address of the internal HTTP proxy device (inside server) that the concentrator will forward web requests to; entering an IP address of 0.0.0.0 specifies that no internal proxy is to be used.
- **HTTP Proxy Port**—This is the TCP port number that the internal HTTP proxy is listening on; it defaults to 80.
- **HTTPS Proxy**—This is the IP address of the internal HTTPS proxy device to which the concentrator will forward web requests; entering an IP address of 0.0.0.0 specifies that no internal proxy is to be used.
- **HTTPS Proxy Port**—This is the TCP port number the internal HTTPS proxy is listening on; it defaults to 443.

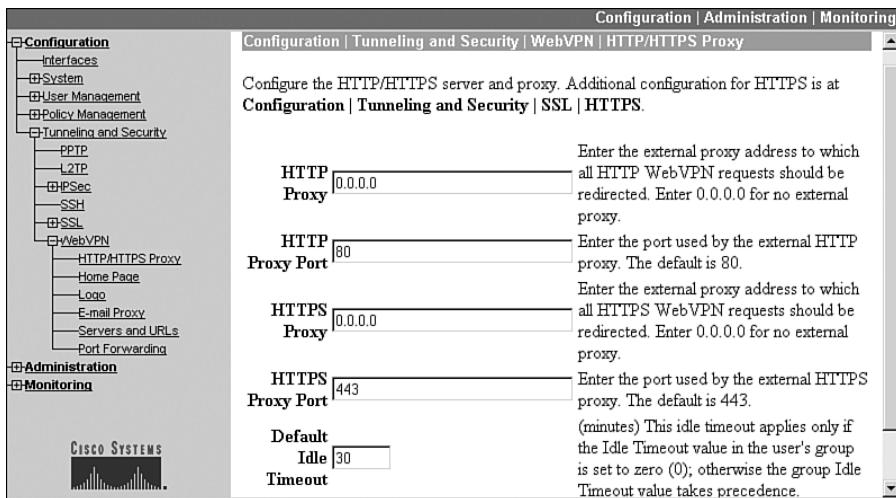
- **Default Idle Timeout**—This text box allows you to enter the number of minutes that a WebVPN session can be idle before the concentrator terminates it. The default is 30 minutes. The group timeout in **Configuration > User Management** overrides this global timeout value.

TIP

I recommend using a short timeout for the *Default Idle Timeout* parameter. If a user's browser is set to cookies disabled, or the user is prompted for a cookie and denies it, these denied sessions still would appear in the **Administration > Administer Sessions** and **Monitoring > Sessions** screen (they're basically nonexistent or "ghost" sessions), which can be confusing when trying to troubleshoot problems. Using a low idle timeout quickly removes the ghost sessions from the monitoring screens and, more important, from the license limit!

Click the **Apply** button at the bottom to activate your changes.

Figure 8-3 WebVPN HTTP/HTTPS Proxy



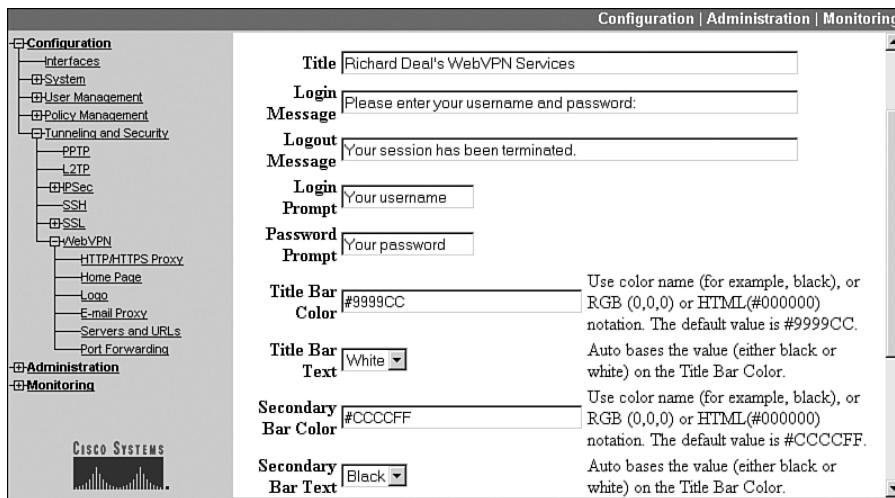
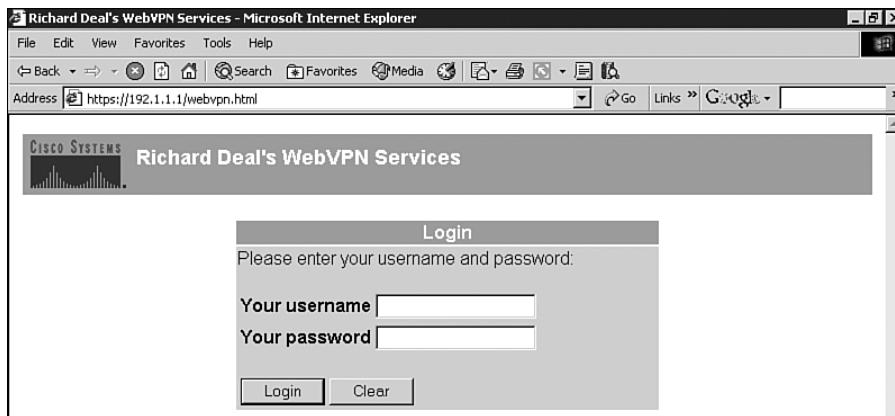
Home Page

Clicking the **Home Page** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to configure the web page that the WebVPN users initially will see: the concentrator's home page. This is a web page sitting on a concentrator that you build through the concentrator's GUI interface. The top part of the home page building

screen is shown in Figure 8-4. Here are the parameters you can configure that will affect the appearance of your concentrator's home page:

- **Title**— You can enter up to 255 characters, including spaces and the ENTER key, for the title that appears at the top of your screen.
- **Login Message**— This message is displayed above your login credentials; it can be up to 255 characters in length.
- **Logout Message**— This message is displayed when a user terminates a WebVPN session; it can be up to 255 characters in length.
- **Login Prompt**— You can specify up to 16 characters for the username login prompt.
- **Password Prompt**— You can specify up to 16 characters for the password login prompt.
- **Title Bar Color**— You can change the color of the title bar either by entering the name of an RGB color (“red,” “green,” “blue”), the range of decimal numbers from 0–255 (“x,x,x,” where “x” is the decimal color number), or a hexadecimal number representing the RGB color (#000000, where the first two numbers represent red, the second two green, and the third two blue). I commonly use this site to access RGB color coding schemes: <http://www.hypersolutions.org/rgb.html>. But you can easily do a search for “RGB table” or “RGB color” to find other tables.
- **Title Bar Text**— This is the color of the text in the title bar. Your options are “Black,” “White,” or “Auto”; choosing “Auto” causes the concentrator to choose the color depending on the color of the *Title Bar Color* parameter.
- **Secondary Bar Color**— This text box allows you to enter the RGB color code for the bar below the title bar.
- **Secondary Bar Text**— This drop-down selector allows you to chose the color of the text appearing in the secondary bar (below the title bar). Your options are the same as with the *Title Bar Text* parameter.
- **Sample Display**— At the bottom is a sample display based on the parameters you entered on this screen (you can't see this in Figure 8-4). Every time you change a color component, this sample coloring section will be updated automatically; this allows you to easily determine if the color schemes you've chosen are easy to comprehend, especially the text coloring.

You can test your changes easily by accessing the concentrator's public IP address externally using HTTPS. Figure 8-5 shows an example of a home page login screen. Before this screen appears, you must accept the concentrator's certificate by clicking the **Yes** button in the pop-up certificate window. Users can be authenticated using RADIUS or via the concentrator. Please note that if you are using Cisco Secure ACS, you can have the ACS server perform the user authentication using other external resources, such as Active Directory, NT Domain, NDS, and others; however, the concentrator itself supports only the two authentication methods I mentioned for WebVPN.

Figure 8-4 WebVPN Home Page Creation**Figure 8-5** WebVPN Home Page Login Screen Example**NOTE**

If you still want to manage the concentrator on the WebVPN interface, enter the following in your web browser's URL address bar: **http://concentrator's_IP_address/access.html**; or you can use **admin.html** at the end. Anything else causes the concentrator to redirect your web browser to the WebVPN login/home page.

Home Page Logo

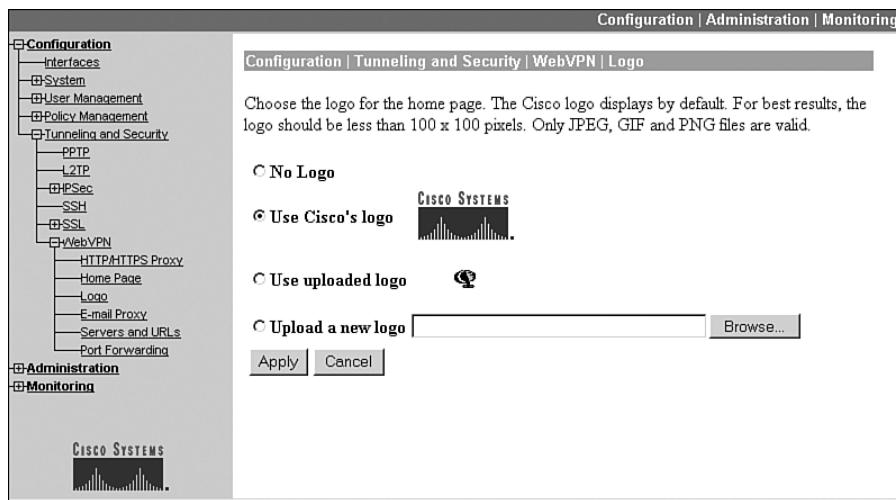
As you can see in Figure 8-5, you can add a logo to the home page; in this example, it's the Cisco logo. Clicking the **Logo** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to configure the logo on the WebVPN home

page. Figure 8-6 shows you this configuration screen. Here are the configuration parameters on this screen:

- **No Logo**—Don't put a logo on the WebVPN home page.
- **Use the Cisco Logo**—Use the Cisco logo on the home page.
- **Upload a new logo**—Upload a logo from your hard drive to use on the home page. Click the **Browse** button to find your logos. For logos to display correctly, they shouldn't exceed 100x100 pixels. They also must be in a JPEG, GIF, or PNG format. If you choose this option and click the **Apply** button at the bottom, the screen will be redisplayed, where you'll see a new option: *Use uploaded logo*. As you can see in Figure 8-6, I uploaded a logo—it's not very legible because I exceeded the Cisco 100x100 rule (it's really a picture of a globe).

The top left corners of Figure 8-5 and Figure 8-9 show the Cisco logo on the concentrator's home page.

Figure 8-6 WebVPN Home Page Logo



E-mail Proxy

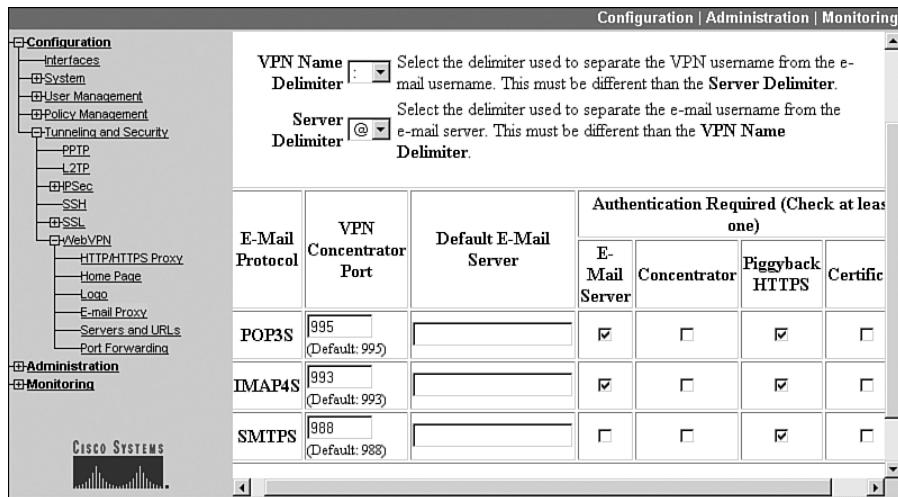
Clicking the **E-mail Proxy** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to configure e-mail proxy servers for WebVPN users; this screen is shown in Figure 8-7. The e-mail proxy services supported include POP3S (downloading e-mail), IMAP4S (downloading e-mail), and SMTPS (sending e-mail). Notice that these use an encrypted connection to interact with an e-mail server. Here are the configuration options on the screen:

- **VPN Name Delimiter**—This drop-down selector allows you to choose the delimiter that will be used to differentiate the user's VPN username from the e-mail username.

Delimiters can be “;,” “!,” “@,” “#,” or “!.” When using the proxy service, the user would need to configure something like *vpn_username:e-mail_username@e-mail_server_name* for a user account name if the VPN delimiter was “;.” Please note that passwords for e-mail proxy users cannot contain the VPN delimiter within their password.

- **Server Delimiter**—This drop-down selector chooses the delimiter that separates the user’s e-mail username from the e-mail server’s name. Typically this is an “@” but it also can be any of the ones mentioned in the *VPN Delimiter Name* parameter.
- **E-mail Protocol**—Only the three e-mail protocols listed are supported by WebVPN. You must enable access for these protocols on the concentrator in the **Configuration > Interfaces** area, described earlier in the “WebVPN Interface Configuration” section.
- **VPN Concentrator Port**—This text box allows you to change the port number the e-mail proxy server is listening on for protected e-mail connections—both the e-mail server and client must be configured for this port number.
- **Default E-mail Server**—This text box allows you to enter the name or IP address of the e-mail server handling the e-mail for the protocol to the left of it.
- **Authentication Required**—You must choose one or more of the authentication options for your e-mail users using the proxy. These include:
 - **E-Mail Server**—The e-mail server performs authentication.
 - **Concentrator**—The concentrator performs authentication; if the VPN username and e-mail username are different, they both must be specified and separated by the delimiter in the *VPN Name Delimiter* parameter.
 - **Piggyback HTTPS**—This option requires the WebVPN user to have an HTTPS session established to the concentrator already; in this case, the user still must supply a username, but no password is required (authentication already has been done). This option often is used with SMTPS, because most SMTPS servers don’t allow users to log in.
 - **Certificate**—The user must have a certificate that the concentrator can validate during the SSL negotiation. The concentrator also needs a root certificate and an identity certificate. This can be the only method of authentication for SMTPS connections, but other proxy connections require at least two methods of authentication, like *E-mail Server* or *Concentrator*. Internet Explorer 6.0 doesn’t support this option, but the newest versions of Mozilla, including FireFox, and Netscape Navigator do.

When you are done, click the **Apply** button at the bottom to activate your changes.

Figure 8-7 WebVPN E-mail Proxy Configuration**TIP**

When using IMAP, a number of sessions can be generated by a user; each of these sessions counts against the simultaneous logins allowed for a user (group configuration in the General tab). To overcome this problem you can increase the number of simultaneous logins allowed per user, have the user close the IMAP application to clear the sessions, or disable the *Piggyback HTTPS* option for IMAP e-mail proxies.

NOTE

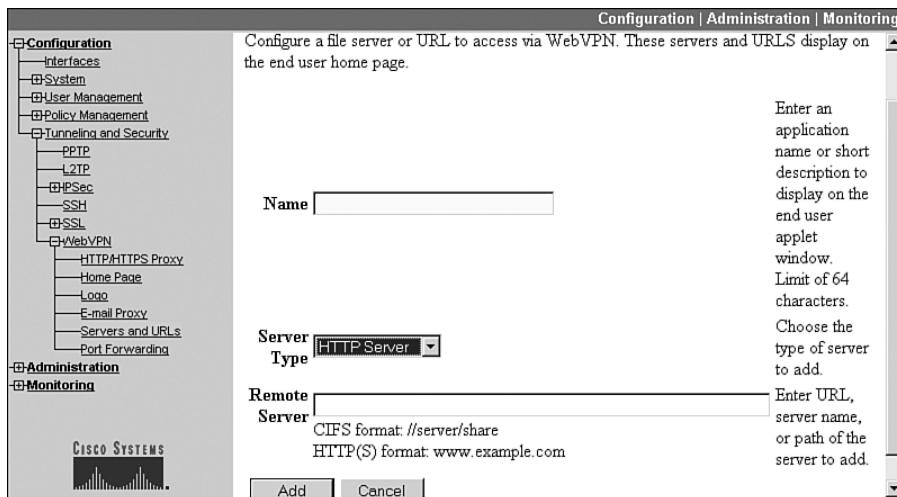
You don't have to have the concentrator proxy secure e-mail connections if you feel safe in letting outside users access them directly through the concentrator; however, if you do this, you'll need to add e-mail proxy rules to your public interfaces filter to allow the proxy e-mail traffic. My personal preference is to set up the proxy, because it adds an extra level of security.

Servers and URLs

Clicking the **Servers and URLs** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to configure file (CIFS), web (HTTP and HTTPS servers and URLs), and e-mail server proxies for WebVPN users that will appear on the concentrator's home page once a user has authenticated; this screen lists the current entries you've created.

To add a new URL entry, click the **Add** button, which takes you to the screen shown in Figure 8-8. The entries you create here will show up on the WebVPN home page once a user authenticates; however, only these entries show up for users who are not members of a specific group. In other words, this is a generic listing of hyperlinks. You can create hyperlinks for file shares, internal web sites, e-mail proxies, and e-mail servers.

Figure 8-8 Adding Servers to the Home Page



At the top of the screen you need to enter a descriptive name for the hyperlink in the *Name* text box. The *Server Type* hyperlink allows you to choose the type of server: “CIFS” for file servers using NETBIOS names, and “HTTP” or “HTTPS” for web servers. The *Remote Server* field contains the actual URL, DNS name, or network path (CIFS) for the server. For a web server, you would enter something like “www.richard-deal.com”; you can even enter a specific URL like “http://www.richard-deal.com/index.html.” For a CIFS file share, it would be something like “//dealserver/sharedfiles” when adding the entry. When done, click the **Add** button to add the hyperlink to the home page.

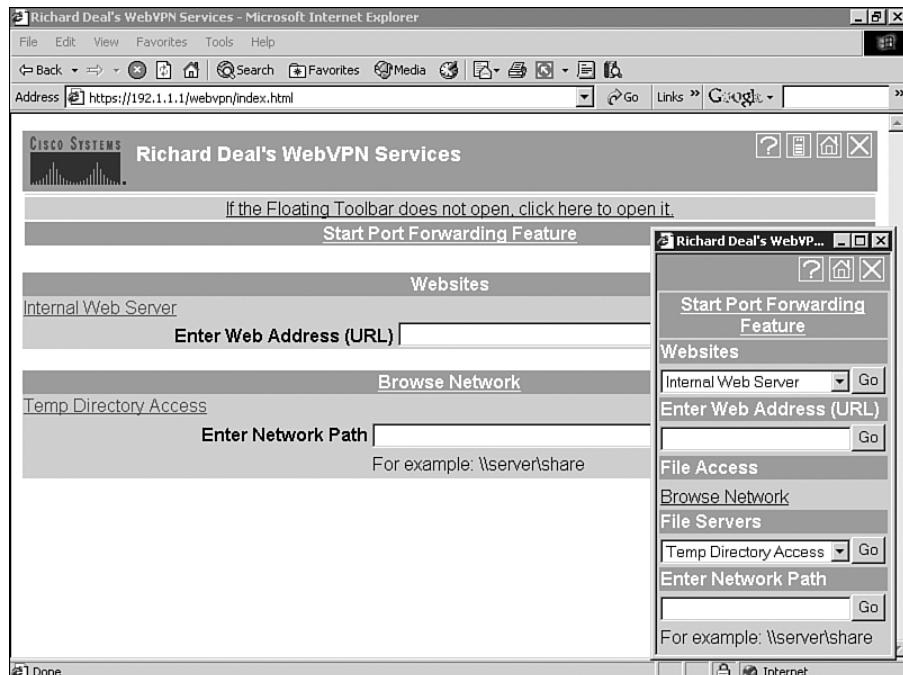
NOTE

If you are using names for Windows file servers, you’ll need to define a WINS server on the concentrator so that the concentrator can resolve the name to an address. To add a WINS server to the concentrator, go to **Configuration > System > Servers > NBNS Servers**. You’ll need to enable WINS and can then specify up to three WINS servers for name resolution.

Figure 8-9 shows an example home page of what you see once you have authenticated from the screen in Figure 8-5. At the top right is a set of icons: clicking the ? icon brings up help;

clicking the icon that looks like a file server brings up a smaller web browser window (this is shown in the bottom right-hand side of the screen); clicking the house icon takes you back to the home page, and clicking the X icon logs you out of your WebVPN session.

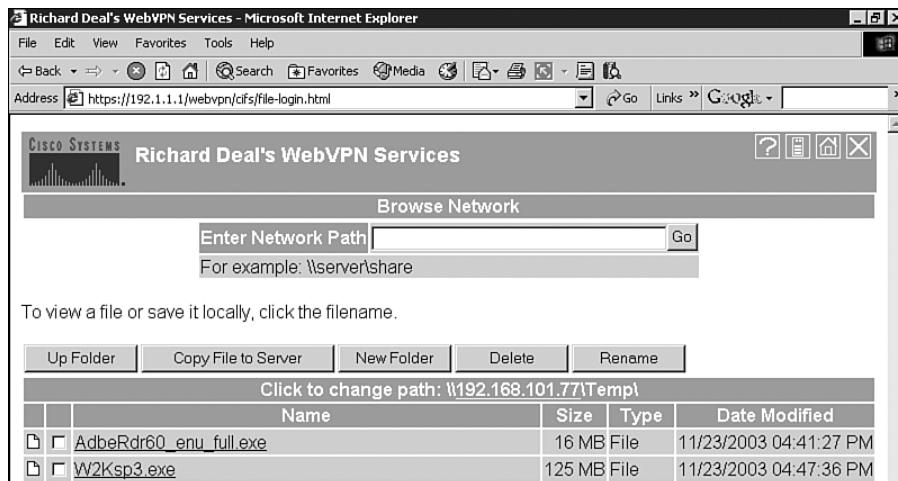
Figure 8-9 Example WebVPN Home Page



Below the title and icon toolbar at the top of the concentrator's home page are the WebVPN options available to you. The screen is broken into three sections:

- *Start Port Forwarding Feature* (this is discussed in the next section)
- *Web Sites*
- *Browse Networks* (these are file shares)

In this screen, you can see the hyperlink, “Internal Web Server” that I’ve added through the screen in Figure 8-8. You also can see a file share hyperlink: “Temp Directory Access.” Clicking either of these will take you to the respective location (assuming that the directory or file is shared on the server). For Windows file shares, the user might have to authenticate first before being able to access the remote file share. Figure 8-10 shows an example where I clicked the “Temp Directory” file access hyperlink. If you haven’t authenticated to the Windows file share already, you’ll be prompted to do so; once authenticated, you’ll see the screen shown in Figure 8-10.

Figure 8-10 Network File Access

To download a file, just click the file name. To upload a file, click the **Upload** button. When an upload is in process, do not navigate to a different screen or shut down the web browser window until the upload is complete—failure to do this can cause an incomplete or corrupted file to be stored on the server. You can use the other buttons at the top to perform actions on the file server. As you can see from this screen, interaction with files is different than when using Microsoft’s Windows Explorer program.

You can use the web browser **Back** button to take you back to the WebVPN home page or you can click the home icon to take you back (see Figure 8-9). I’ll discuss the other options on the WebVPN home page later in this chapter.

NOTE

For WebVPN access to operate correctly, the user’s web browser must have cookies enabled; otherwise, any hyperlinks the user clicks from the home page will open a new window, prompting the user to log in once again.

All user interaction needs to take place within the WebVPN web browser screens. You’ll need to train your users to **not** enter information in the URL bar in the web browser when interacting with WebVPN components: everything should be done **within** the web browser page presented to the user; otherwise, the traffic will not be sent through the SSL VPN session. By having the user use the hyperlink information within the home page, the concentrator can proxy the connections.

Port Forwarding

The Cisco WebVPN Port Forwarding feature allows for non-web-based applications to use the SSL VPN connection (thin client access). If you recall from Chapter 5, “SSL VPNs,” Cisco has tested the following applications for their thin client implementation: Lotus

Notes, Outlook and Outlook Express, Perforce, Sametime Instant Messaging, Secure FTP (FTP over SSH), SSH, Telnet, Windows Terminal Services, and XDDTS. Other TCP-based applications might work, but Cisco hasn't tested them.

NOTE

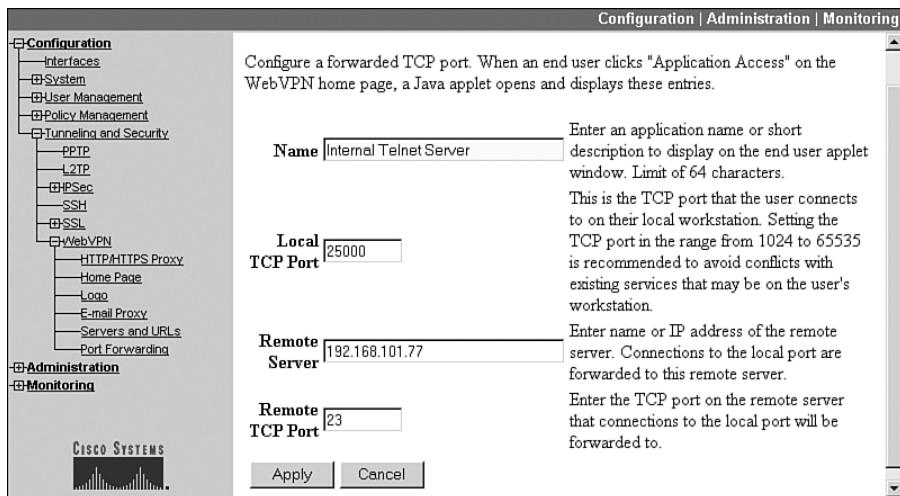
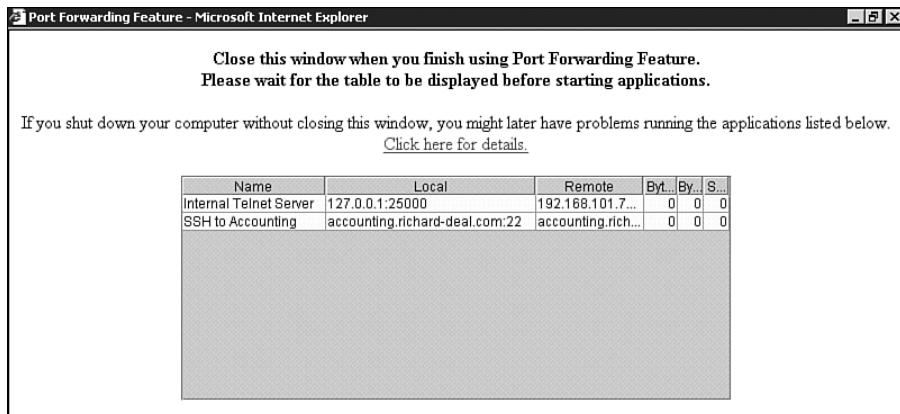
Remember that for the client to use the Port Forwarding feature, Sun Microsystems' Java Runtime Environment (JRE) must be installed: Microsoft's Java will *not* work. WebVPN automatically checks to see if JRE is installed on a user's PC; if it isn't, a window pops up and directs the user to a web site where it can be downloaded and installed.

Clicking the **Port Forwarding** hyperlink from the **Configuration > Tunneling and Security > WebVPN** screen allows you to configure TCP-based applications that you want to tunnel through the user's SSL VPN session. You'll be presented with a list of Port Forwarding applications you've already added, if any. Just click the **Add** button to add a new application. This will bring you to the screen in Figure 8-11. Here are the parameters you need to configure:

- **Name**—This will become the name of the port forwarding process you're defining; give it a descriptive name, like "Telnet to the Accounting Server." This name will appear in the list of port forwarding applications within the concentrator's web pages.
- **Local TCP Port**—This is the port number that must be used on the user's PC when making the connection to the application; it should be a number from 1,024 to 65,535 that is *not* going to be used on the user's PC. This number is used by Java to identify the application uniquely on the user's computer.
- **Remote Server**—This is the fully qualified domain name (FQDN) or IP address of the remote server; if you're using DNS mapping, this must be the FQDN of the remote server.
- **Remote TCP Port**—This is the port number of the application that is to be forwarded; for example, if you wanted to enable port forwarding for Telnet, you would enter "23" for this parameter.

When you are done with your Port Forwarding entry, click the **Add** button at the bottom of the screen to add the entry. You can create up to 252 port forwarding entries for your users.

Once you've authenticated as a user for WebVPN and are brought to the screen in Figure 8-9, click the **Start Port Forwarding Feature** hyperlink on the concentrator's home page. A pop-up window states that both secure and unsecured information will appear in the Port Forwarding window; click **OK** to accept this. Next, you must accept two SSL certificates: one for the concentrator and one for Java. After this the window shown in Figure 8-12 will be displayed. This is a display-only window and will require you to train your users on how this information should be used to establish Port Forwarding connections.

Figure 8-11 Adding Port Forwarding Applications**Figure 8-12** WebVPN Port Forwarding Screen

If you used an IP address for the *Remote Server* parameter in Figure 8-11, you'll see something like the first line in the web browser box in Figure 8-12. First you see the name you created, followed by the *Local* information: 127.0.0.1:25000 for a telnet to 192.168.101.77 (this is cut off). Your users, when wanting to telnet to this device, must telnet to 127.0.0.1 and port 25000; by doing this, the Java script will intercept the TCP connection and forward it across the SSL VPN to the actual server (192.168.101.77 on port 23). The Java script is redirecting the connection to the correct server and port.

If you use a hostname to identify a remote server for port forwarding, the WebVPN Java script will back up the user PC's local host file first and then modify it by adding the port forwarding entry. The Windows hosts file is located here: C:\Windows\system32\drivers\

etc\hosts or C:\WINNT\system32\drivers\etc\hosts. Here's an example of a hosts file Java created based on what I set up for the second example in Figure 8-12 (which uses SSH) :

```
127.0.0.3 accounting.richard-deal.com # added by WebVpnPortForward  
at Mon Nov 29 17:58:44 EST 2004
```

In this example, when a user would use SSH to access "accounting.richard-deal.com," the traffic would be directed to the loopback address of "127.0.0.3," which the Java applet would intercept and redirect through the WebVPN session to the concentrator. The concentrator then would redirect the traffic to the actual accounting server. The user *doesn't* have to know about the port to use—this information was already updated, behind the user's back, in the local hosts file.

CAUTION

It is very important that users *correctly exit* the Port Forwarding screen by closing it down—click the X in the top right corner of the web browser window; failing to do this can corrupt the user's hosts file by keeping the modified hosts file and not replacing it with the backup file. If the user closes the Port Forwarding screen correctly, Java removes the updated file and replaces it with the backup file (the one before Java made its changes). So, if the user doesn't shut this down correctly, their hosts file will still have the Java information in it. To rectify this, have the user manually delete the "hosts" file and then rename the "hosts.WebVPN" file (in the same directory) to "hosts." If for whatever reason this file doesn't exist, the lines at the beginning of the hosts file (ending in "added by WebVPN...") will need to be removed manually with a text editor. I would send this information out in an e-mail to reduce the amount of time you'll have to spend explaining to your users how to fix this problem. Or you might even want to put a hyperlink on the WebVPN page that points to instructions to do this!

Group Configuration

What I've discussed so far affects all users that access your concentrator via WebVPN. Now I'll discuss how to fine-tune this using base and specific groups. With both, you must enable WebVPN access first by going into the group and clicking the **General** tab. For the *Tunneling Protocols* parameter, you need to make sure the "WebVPN" check box is checked; if this is not done, members of the specific group will not be allowed WebVPN access.

TIP

My recommendation is to disable WebVPN in the base group and then enable it on a specific group-by-group basis, giving you more control over who uses the WebVPN remote access feature.

Because the configuration is almost the same with the base and specific groups, I'll focus only on customizing a specific group's WebVPN access configuration. To make WebVPN

changes on a group-by-group basis, go to **Configuration > User Management > Groups**. There are three areas in a specific group where you can enforce WebVPN policies:

- WebVPN tab within a group's configuration
- WebVPN Servers and URLs group button on the group screen
- WebVPN Port Forwarding group button on the group screen

The remaining sections will discuss the configuration of these options.

NOTE

The Cisco clientless WebVPN feature does not use the DNS configuration of the group that a user belongs to; only the concentrator's global DNS settings are used. Remember that the concentrator is acting as a proxy, and thus the concentrator uses its own defined DNS server to perform DNS resolution. The concentrator's DNS server is defined on the **Configuration > System > Servers > DNS Servers** screen. You must click the *Enable* check box and enter the IP address of at least one (but up to three) DNS server(s).

WebVPN Tab

To access the WebVPN tab for a group, from the screen in group screen (**Configuration > User Management > Groups**), click the name of the group, click the **Modify** button, and then click the **WebVPN** tab. The top, middle, and bottom parts of this screen are shown in Figures 8-13, 8-14, and 8-15. The WebVPN tab is broken into three sections: *WebVPN Parameters*, *Content Filter Parameters*, and *WebVPN ACLs*. Here's an explanation of the parameters found in the three sections.

Figure 8-13 Group WebVPN Tab: Top Part

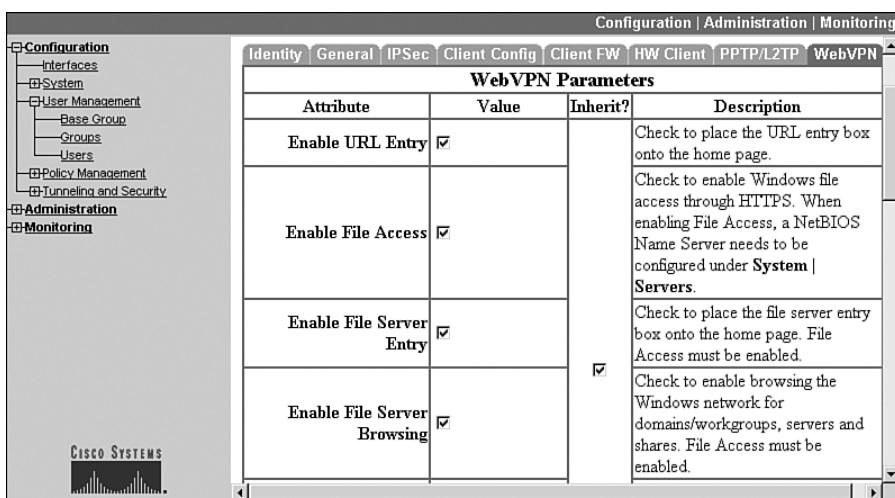
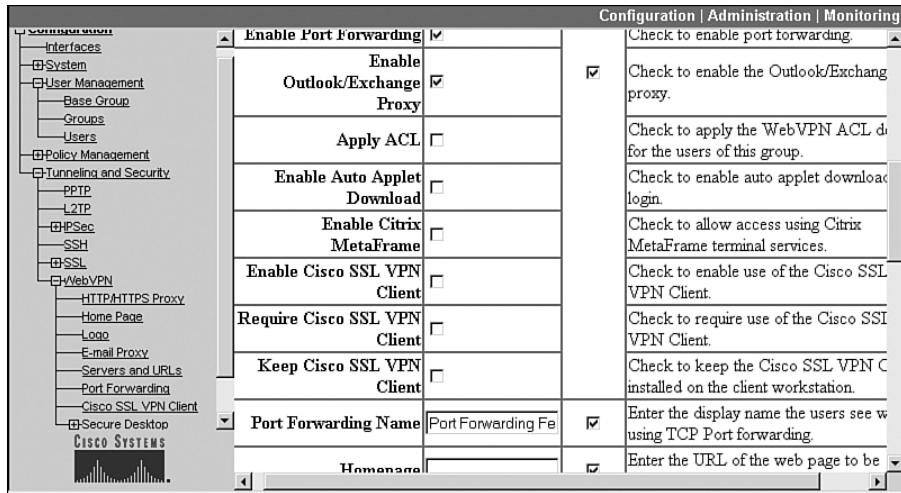
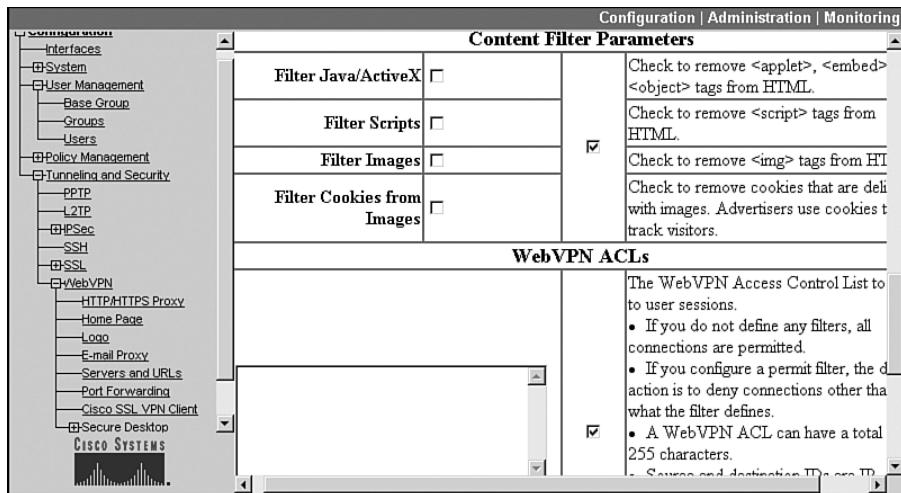


Figure 8-14 Group WebVPN Tab: Middle Part**Figure 8-15** Group WebVPN Tab: Bottom Part

WebVPN Parameters

The information in the *WebVPN* parameters section affects the kinds of information found on the WebVPN home page shown previously in Figure 8-9. Here are the parameters you can configure:

- **Enable URL Entry**—If you want users to be able to enter their own URLs on the WebVPN home page, check this check box. If you look back to Figure 8-9, you'll see that this has been enabled in the *Websites* section for the group. Please note that

the concentrator is acting as a web proxy for the user when the user accesses URLs with this feature. If the user is trying to access a secure, remote site, the concentrator will establish an SSL connection from itself to the remote server on behalf of the user; in the current software version, with an SSL proxy connection, the concentrator will not establish an SSL connection to a remote server if the remote server's certificate is expired.

- **Enable File Access**—This check box, when checked, allows WebVPN users to access SMB/CIFS file structures through the WebVPN connection. When this option is enabled, users can edit, download, upload, and rename files. They also can create, delete, and rename folders. For this feature to work, you must specify a WINS or Master Browser server on the concentrator. I discussed this previously in the “Servers and URLs” section.
- **Enable File Server Entry**—If the above check box and this check box are enabled, a file server entry text box appears on the WebVPN home page, allowing users to enter their own entries to access remote file resources. Figure 8-9 shows that the home page has this option enabled for the group (look below the **Browse Network** hyperlink).
- **Enable File Server Browsing**—If this and the *Enable File Access* check boxes are checked, the **Browse Network** hyperlink appears on the group’s WebVPN home page (you can see this in Figure 8-9). When you click this, it functions like the Network Neighborhood on a Windows device.
- **Enable Port Forwarding**—This check box allows the user to use the Port Forwarding feature on the WebVPN home page. As you can see in the top part of Figure 8-9, I’ve enabled this feature because the *Start Port Forwarding Feature* hyperlink appears.
- **Enable Outlook/Exchange Proxy**—This check box enables the Outlook/Exchange mail forwarding proxy (MAPI). Users get their information about the Outlook/Exchange mail proxy by what you enter in a Java applet; users then launch this applet by clicking the *Application Access* section of the WebVPN home page. To use this feature, the WebVPN user first must make a connection to the Exchange server before making one through WebVPN.
- **Apply ACL**—This check box allows you to apply a WebVPN ACL to the group’s access; the ACL itself is defined at the bottom of the *WebVPN* tab. I highly recommend the configuration of ACLs for additional security. Normally I’ll allow users access to a small set of services and then deny everything else.
- **Enable Auto Applet Download** (new in 4.7)—This check box allows you to start port forwarding or an Outlook/Exchange Proxy Java applet download when WebVPN users log in.
- **Enable Citrix Metaframe** (new in 4.7)—This check box enables support for Citrix Metaframe. On your Metaframe web software, you must configure it for “Normal Address” mode. You also must install an SSL certificate on the concentrator using

an FQDN for the CN in the SSL certificate—using an IP address in this field will not work.

- **Enable Cisco SSL VPN Client** (new in 4.7)—This check box enables the Cisco SSL VPN Client (SVC), which supports a broader range of more complex services not supported across a normal web browser connection. SVC doesn’t support WebVPN ACLs, discussed in a later bullet; however, it does support IP-based ACLs, like with the Cisco VPN Client (IPsec). I discuss this in more depth later in the “SSL VPN Client (SVC)” section.
- **Require Cisco SSL VPN Client** (new in 4.7)—This check box, when selected, requires that members of this group use SVC for their WebVPN sessions—the concentrator will verify this upon the client’s WebVPN connection attempt. Because SVC is supported for only Windows 2000 and XP systems, don’t enable this for a group that contains other client operating systems.
- **Keep Cisco SSL VPN Client** (new in 4.7)—When checked, this allows users to keep the SVC software installed on their computers versus downloading it from the concentrator each time a WebVPN session is made. When not checked (the default), the SVC software is uninstalled each time the client disconnects. If this option is selected and a new SVC client version is installed on the concentrator, the client will download and install it automatically instead of using the currently installed older version.
- **Port Forwarding Name**—This text box allows you to change the name of the hyperlink that appears on the WebVPN home page for the Port Forwarding feature. This defaults to “Port Forwarding Feature.”
- **Home Page**—This text box allows you to display a different home page than the one the concentrator builds. This is useful if you want to take your users directly to one web server with a specific web application on it; if users need to access more than one service, I would present the user with the concentrator’s home page and add the necessary web links to this page.

CAUTION

If you are concerned about security, especially regarding users accessing remote resources that you have no control over (like Internet web surfing), I would not enable the *Enable URL Entry, Enable File Server Entry, and Enable File Server Browsing* parameters unless you configure ACLs to limit your users’ access to internal resources.

Content Filter Parameters

The *Content Filter Parameters* section of the *WebVPN* tab allows you to filter certain kinds of web downloads, including Java/ActiveX applets (remove the “`<applet>`,” “`<embed>`,” and “`<object>`” tags), scripts (remove the “`<script>`” tags), images (remove the “``”

tags), and cookies delivered with images from HTTP downloads. Here are the parameters you can enable for content filtering of your WebVPN users:

- **Filter Java/ActiveX**—Enabling this might cause some web pages to break.
- **Filter Scripts**—Enabling this might cause some web pages to break.
- **Filter Images**—Enabling this might increase download speeds for your users.
- **Filter Cookies from Images**—Enabling this increases security by preventing web sites from keeping track of your users.

WebVPN ACLs

The last section from the group's WebVPN tab screen, shown at the bottom of Figure 8-15, allows you to configure access control lists (ACLs) to filter users' access to web servers. If you don't configure any WebVPN ACLs, all web access is permitted to your users; however, as soon as you configure one WebVPN ACL, if no match is found in a configured ACL, the user is denied the web access. Therefore, you'll need to configure at least one **permit** statement in an ACL when configuring WebVPN ACLs.

Here's the syntax for creating an ACL that filters protocol information:

```
{permit | deny} {ip | smtp | pop3 | imap4 | http | https | cifs}  
    src_address src_wildcard_mask  
    dst_address dst_wildcard_mask
```

When creating a protocol ACL, the statement can have a maximum of 255 characters. You start out with an action: either **permit** or **deny**. This is followed by the name of the protocol you want to filter; you must use a protocol from the list of supported ones shown in the above command syntax. Following this are the source and destination addresses and wildcard masks. As you can see, this is a very similar syntax to configuring a named ACL entry on a Cisco IOS router. If you are filtering on a specific device, like 192.1.1.1, you can enter the addressing information as **192.1.1.1 0.0.0.0** or **host 192.1.1.1**; likewise, if you want to match on any address, you can use either **0.0.0.0 255.255.255.255** for the address information (source or destination) or the keyword **any**. Each ACL statement needs to be on a separate line.

You can also do rudimentary URL filtering by using the following syntax:

```
{permit | deny} URL url_definition
```

An example of a URL definition would be **http://www.richard-deal.com**. Any URL style syntax is supported, including HTTP, HTTPS, CIFS, IMAP4S, POP3S, SMTPS, and so on.

Here's a simple ACL configuration:

```
permit URL http://www.richard-deal.com  
permit smtp any host 192.168.101.77  
permit pop3 any host 192.168.101.77
```

In this example, only URL access to the internal web server (www.richard-deal.com) and e-mail access (SMTP and POP3) to the internal e-mail server (192.168.101.77) are allowed—all other traffic will be dropped for the users' WebVPN sessions.

Once you've completed the configuration of your Web ACLs, be sure to check the *Apply ACL* check box in the *WebVPN Parameters* under the WebVPN tab. After completing the WebVPN tab configuration, click the **Apply** button at the bottom to activate your changes for the group.

NOTE

Remember that a specific group's WebVPN configuration overrides the base group's configuration. Also, if you are using specific groups, each user must be associated with a group. This is accomplished from the **Configuration > User Management > Users** screen discussed previously in the "User Configuration" section in the last chapter.

WebVPN Group Buttons

With the specific groups configuration screen (**Configuration > User Management > Groups**), you have two buttons you can click to add additional URLs and Port Forwarding applications to the selected group that are not available for users that access WebVPN using the base group: the **WebVPN Servers and URLs** and **WebVPN Port Forwarding** buttons. The next two sections will discuss these two group buttons.

WebVPN Servers and URL Button

When you click a group name from the group screen (**Configuration > User Management > Groups**) and click the **WebVPN Servers and URLs** button, you are taken to a screen where you can see the servers and URLs that this group can access through the WebVPN home page. To add a server or URL, click the **Add** button. This takes you to the screen shown previously in Figure 8-6. The difference between the two screens is that the screen from **Configuration > Tunneling and Security > WebVPN > Servers and URLs** and the group screen is that the previous screen adds servers and URLs for only the base group users, and this screen adds servers and URLs for the specific group. In other words, if a user logs in via WebVPN belonging to a specific group, that user will see only the servers and URLs created for the specific group through the group's **WebVPN Servers and URLs** button—the user won't see the base group servers and URLs created from the **Configuration > Tunneling and Security > WebVPN > Servers and URLs** screen.

NOTE

Please note that the group **WebVPN Servers and URLs** button is available only for specific groups; to add servers and URLs for the base group, you need to go to the **Configuration > Tunneling and Security > WebVPN > Servers and URLs** screen.

WebVPN Port Forwarding Button

When you click a group name from the group screen (**Configuration > User Management > Groups**) and click the **WebVPN Port Forwarding button**, you are taken to a screen where you can see the port forwarding applications that only this group can access through the WebVPN home page. To add a server or URL, click the **Add** button. This takes you to the screen shown previously in Figure 8-11. The difference between the two screens is that the screen from **Configuration > Tunneling and Security > WebVPN > Port Forwarding** and this group screen is that the previous screen adds Port Forwarding applications for only the base group users and this screen adds Port Forwarding applications for only the selected specific group. Please see the note in the previous section about the appearance difference on the WebVPN home page concerning the setup of the base group and the specific groups.

SSL VPN Client (SVC)

The SVC client is new in software Version 4.7. SVC works only with Windows 2000 and Windows XP clients. It provides an alternative to using an IPsec VPN client. SVC has one main advantage over a normal HTTPS WebVPN connection: it supports many additional functions, policies, and applications, more than the Cisco clientless and thin client WebVPN implementations. Plus, unlike the IPsec VPN client, SVC is downloaded and installed on the user's desktop automatically, reducing any additional configuration the user has to perform.

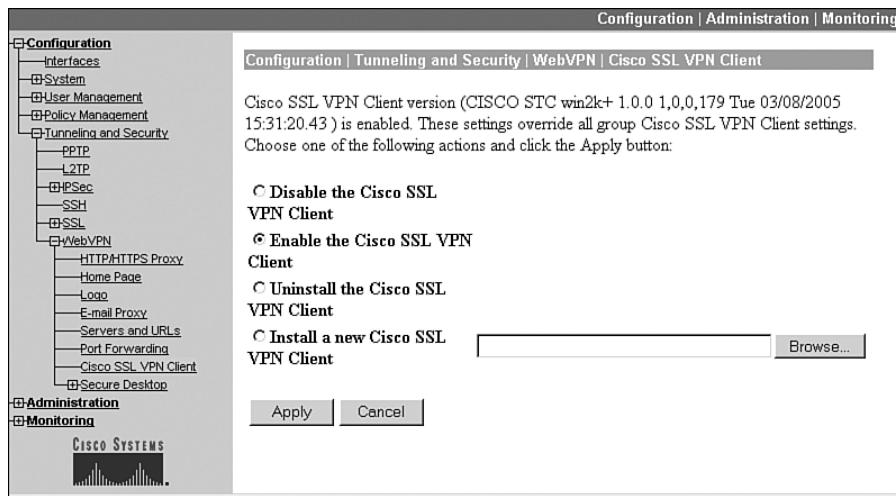
To help you with installing and using the SVC, the following sections cover these topics:

- Installing SVC on the Concentrator
- Using the SVC Software
- Non-Administrator Users

Installing SVC on the Concentrator

The SVC software is installed on the concentrator and downloaded by the client during its initial WebVPN connection. To install the SVC software on the concentrator, go to **Configuration > Tunneling and Security > WebVPN > Cisco SSL VPN Client**. Click the **Browse** button to find the client software on your desktop (assuming you've downloaded this from the Cisco site) and then click the **Apply** button to download the SVC software to the concentrator, which stores it locally in Flash memory. The package name you download from Cisco will be something like this: `sslclient-win-1.0.0.179.pkg`—it's important that you download the file ending in “.pkg” because this is used by the concentrator.

Once installed, if you return to the above screen, you'll see the screen shown in Figure 8-16; here you can see which SVC client version is installed (at the top) and enable (enabled by default), disable, install, or uninstall the SVC client on the concentrator.

Figure 8-16 SVC Software Screen

Using the SVC Software

When the user makes the initial connection via HTTPS to the concentrator's public interface, the user will log in normally (see Figure 8-5). Upon successfully logging in, the web browser window will indicate that the SVC software will be installed (see Figure 8-17). The user must accept the SVC certificate by clicking the **Yes** button in the pop-up window. If the concentrator is using a self-signed certificate, you'll receive a couple of warnings regarding this, which the user can click to ignore. If you are concerned about the amount of interaction the user has to perform, install an SSL certificate on concentrator. The SVC software is downloaded and installed on the user's computer automatically. The user is given the option to access the local LAN, and resources behind the VPN 3000 concentrator (a limited form of split tunneling).

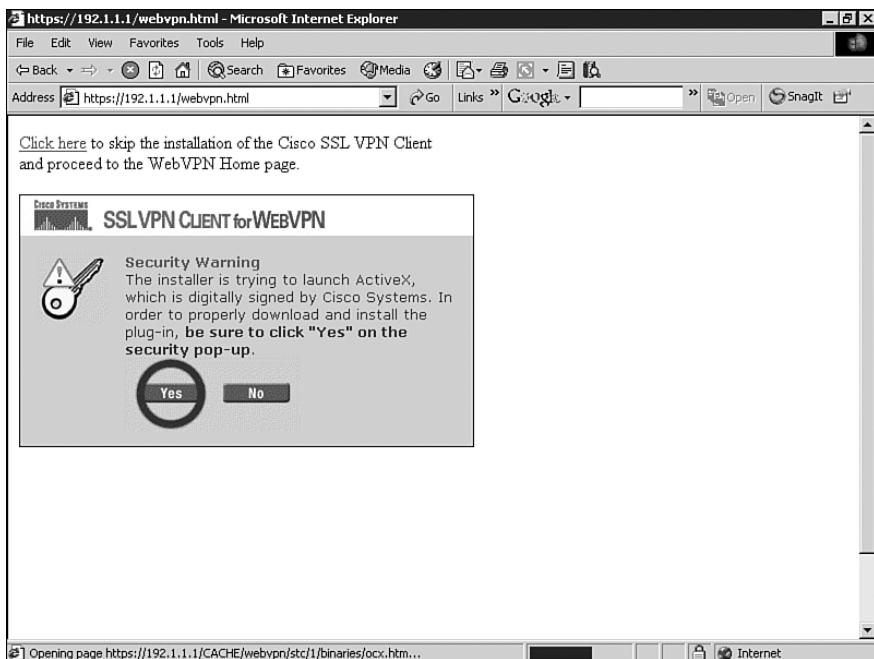
NOTE

For the SVC software to be installed on the user's desktop, the user must be logged in with Administrator privileges; otherwise, the install will fail. However, once installed, the use of the software does not require Administrator privileges. Also, for cases where Administrator permissions are not available to the user, an installer helper (stub installer) can be used to install the Administrator piece.

Once a connection has been established, a yellow key icon will appear in the bottom right-hand corner of the Windows taskbar (the bottom right-hand corner of the user's desktop). If you right-click and choose any of the options, the screen in Figure 8-18 appears. The Status tab is in the foreground, displaying protected traffic statistics. The Route Details tab displays what traffic is protected. The About tab displays the SVC software version. To disconnect, either click the **Disconnect** button on the screen in Figure 8-18 or right-click the yellow key icon in the taskbar and choose **Disconnect**. Upon disconnecting, the SVC

software is uninstalled from the user's desktop automatically unless you've chosen the *Keep Cisco SSL VPN Client* option under the group WebVPN tab.

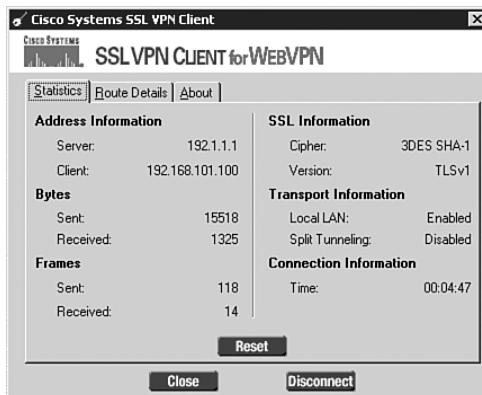
Figure 8-17 Initial SVC User Screen



TIP

For users in a group that use dialup for accessing the Internet, I would highly recommend that you choose the *Keep Cisco SSL VPN Client* option, because the downloaded software (SVC) is about 300 KB in size.

Figure 8-18 SVC Status Window



Non-Administrator Users

One limitation of SVC is that for the initial automatic download and install process to work, the users must have Administrator privileges on their 2000 or XP PCs. If they don't, you still can use SVC, but it requires that you give the user a special installation package from Cisco. When you download the SVC software from Cisco, you'll need to look for the file ending in ".zip," like this: sslclient-win-1.0.0.179.zip. Inside this zipped archive are two files: stc.pkg and stcie.exe. Have the user unzip the files and run the stcie.exe file to perform the installation. Some command options may be viewed by executing "stcie.exe /?". This option might be necessary if the user needs to use SVC but is accessing the concentrator from a PC in a controlled environment.

Cisco Secure Desktop for WebVPN Access

Cisco Secure Desktop (CSD) for WebVPN connections was added in Version 4.7. CSD allows you to verify the basic security setup of a PC before it connects to the concentrator, while it is connected, and after it disconnects. This control can include the operating system version installed, including service packs, the installation of antivirus software and its version, the installation of personal firewall software and its version, and the device's IP address.

CSD is responsible for obtaining this information from the client's machine when the client is using WebVPN. The CSD software is installed on the user's computer and will encrypt all CSD queries to and from the concentrator. It isolates the connection information in a Secure Desktop space. Any data downloaded to CSD is encrypted using RC4 or 3DES. Once the client device disconnects from the concentrator, the CSD software automatically erases and overwrites all data obtained from the secured WebVPN session, which meets one of the U.S. Department of Defense standards for security. This includes data downloaded, inserted, or created within the client, such as web browsing information (passwords, auto-completed information, configuration changes, downloaded files, cached browser information, and so on).

CSD is fully supported on Microsoft Windows (2000 and XP) and has limited functionality on Windows 95, 98, ME, MacOS X, and Linux (only the Cache Cleaner). Table 8-1 displays the antivirus products supported by CSD, and Table 8-2 displays the personal firewall products supported by CSD.

Table 8-1 *CSD-Supported Antivirus Packages*

Product	Version
eTrust Antivirus	7.0+
F-Secure Antivirus	2003+
McAfee VirusScan	8.0–9.0 and Enterprise 7.0–8.0
Norton Antivirus for Windows	Professional 2004+ and Corporate 8.0–9.0
Panda Antivirus	Platinum 7.0–8.0 and Titanium 2004

continues

Table 8-1 CSD-Supported Antivirus Packages (Continued)

Product	Version
PC-cillin	2003–2004
Trend Micro PC-cillin Internet Security	2004
Microsoft Windows AntiSpyware	Beta v1

Table 8-2 CSD-Supported Personal Firewall Packages

Product	Version
Cisco Security Agent (CSA)	4.0+
Internet Connection Firewall	Windows XP–XP SP2
ISS BlackICE PC Protection	3.6
McAfee Personal Firewall	4.0–5.0
Norton Personal Firewall	2003+
Sygate Personal Firewall	5.0–5.5
ZoneAlarm Personal Firewall	4.0–5.0

Installing the Secure Desktop Software on Your Concentrator

The CSD software must be installed on the concentrator and downloaded by the client during its initial WebVPN session connection. To install the CSD software on the concentrator, go to **Configuration > Tunneling and Security > WebVPN > Secure Desktop > Secure Desktop Setup**. Click the **Browse** button to find the CSD client software on your desktop (assuming you've already downloaded this from the Cisco web site). The package name you download from Cisco will be something like this: securedesktop-3.0.1.260-k9.pkg. Then click the **Apply** button to download the software to the concentrator, which stores the CSD software locally in Flash memory. Once CSD is installed, a hyperlink will appear that if you click it, it will take you automatically to the **Configuration > Tunneling and Security > WebVPN > Secure Desktop > Secure Desktop Manager** screen (if you go back to the **Configuration > Tunneling and Security > WebVPN > Secure Desktop > Secure Desktop Setup** screen, you can disable, enable, uninstall, or install the CSD software).

Configuring the Secure Desktop Parameters for Windows

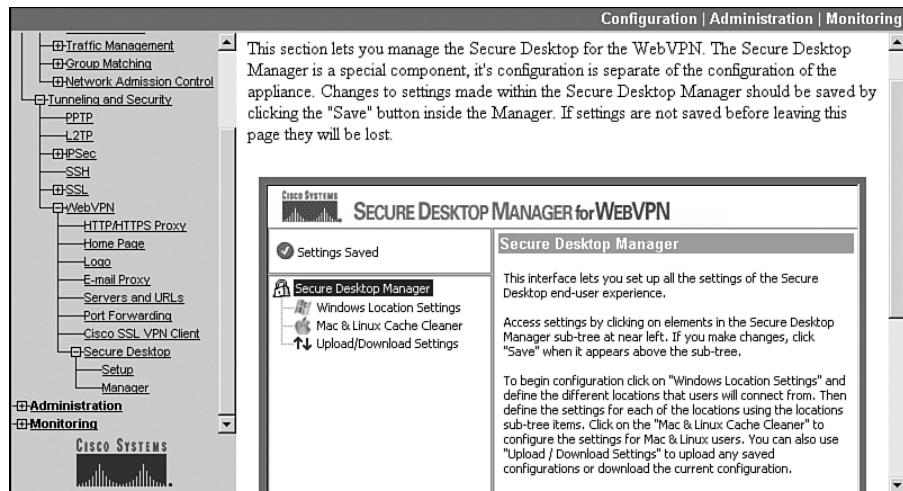
Once the CSD software is installed, you can go to the Secure Desktop Manager screen (**Configuration > Tunneling and Security > WebVPN > Secure Desktop > Secure Desktop Manager**), shown in Figure 8-19, to configure CSD parameters. This is an HTML and JavaScript-based utility that works within your web browser and allows you to build and manage the following components:

- **Locations**—A location from which Microsoft Windows users connect. You can define location settings for these users, like operating system version and VPN feature policies.

Common locations would include Work, Home, and Insecure or Internet, where you can define different policies for different locations. Locations are discussed in more depth in the “Windows Location Settings” and “Windows Location Identification” sections.

- **VPN Feature Policy**—A VPN feature policy can check the following items before allowing access to the network behind the concentrator: SSL VPN Client installation, web browsing, file access, and port forwarding. It also can verify the installation and operation of the operating system and its version, antivirus software, and personal firewall software. VPN Feature Policies are discussed in more depth in the “VPN Feature Policy” section.
- **Cache Cleaner**—The cache cleaner disables or erases all data that a user downloads and creates, or is inserted into a web browser session; it is supported with the following web browsers: Microsoft IE 5.0+, Netscape Navigator 7.1+, Mozilla 1.7+, or Firefox 1.0+ on Windows platforms, Safari 1.0+ on Mac OS X, and Mozilla 1.1+ on Red Hat Linux v9. The Cache Cleaner is discussed in more depth in the “Windows Cache Cleaner” section later.
- **CSD Settings**—The CSD settings feature allows you to have CSD start up automatically after its installation on a user’s computer, check for keystroke logging programs, switch between the local desktop and the Secure Desktop, restrict Windows registry access, cmd.exe access, and printing access, local browser settings, and many others. CSD Settings will be discussed in more depth in the “Secure Desktop General Settings for Windows,” “Secure Desktop Settings for Windows,” and “Secure Desktop Browser for Windows” sections later.

Figure 8-19 CSD Software Screen



Windows Location Settings

Once you access the CSD Manager HTML/JavaScript utility, if you have Windows clients, the first thing you'll do is set up your locations by clicking the **Windows Location Settings** hyperlink in Figure 8-19. For each different group of users you have that have different policies, you'll create a separate location. Once you've created a location, you can determine how users are assigned to a location, in addition to configuring the Cache Cleaner, VPN Feature Policy, and Secure Desktop features for that location.

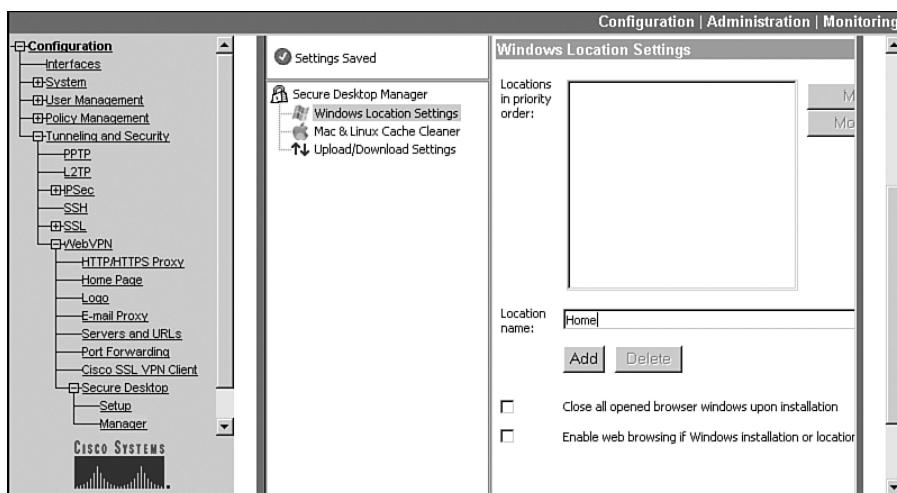
For example, if you have wireless LAN users who have an IP address assigned from 10.10.x.x, which is part of the central office network, you might define a policy that disables both the Cache Cleaner and Secure Desktop function for these devices; however, for SOHO users, such as remote access WebVPN clients, you'll enable both of these features, requiring additional software on these PCs such as antivirus and personal firewall software. And finally, for remote access users who access the concentrator via Internet Café or other such locations, you might add additional policies, like a much shorter timeout period, to prevent unauthorized access.

NOTE

The Windows Location Settings feature works with only Windows-based clients.

Once you've clicked the **Windows Location Settings** hyperlink, enter the name of the location, like "Home," in the *Location Name* text box shown in Figure 8-20, and click the **Add** button.

Figure 8-20 Adding a Windows Location

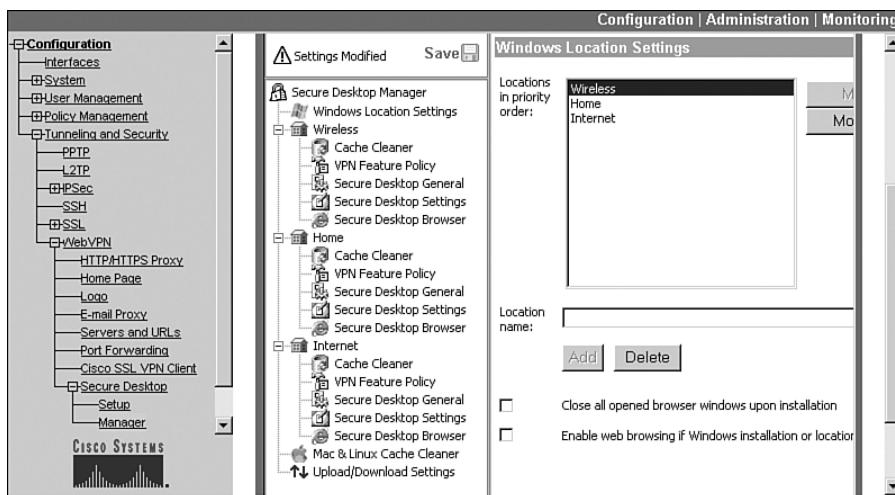


Once you have added your locations, you can move the locations up or down in the list. The order is important because CSD checks to see if a user belongs to a location by processing the locations in the order they're listed on this screen. For all locations, you have two check boxes you can select:

- **Close all opened browser windows upon installation**—Closes unsecured web browser windows once CSD has been installed on the user's desktop upon their Windows WebVPN connection to the concentrator.
- **Enable web browsing if Windows installation or location matching fails**—If the user doesn't match a listed location, enabling this check box allows Windows clients to browse the Internet minimally via a web browser. Cisco recommends enabling this option for PocketPC devices, because CSD isn't supported on this platform.

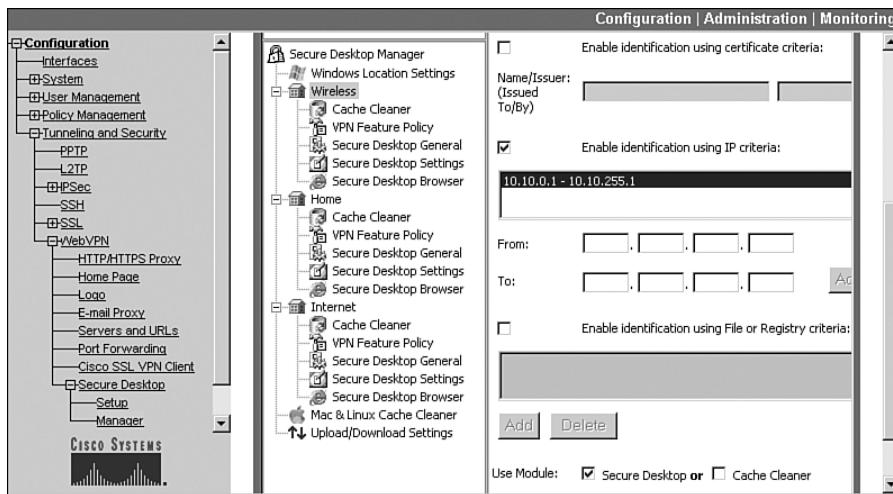
Figure 8-21 shows a list of three locations. Notice in the left JavaScript window pane that there are additional entries for the three locations you've added.

Figure 8-21 Using Multiple Windows Locations



Windows Location Identification

To specify who belongs to a location, click the name of the location in the left HTML/JavaScript window pane. In Figure 8-22, I clicked "Wireless" for local LAN users. Membership of a location can be based on information found on a user's certificate, the user's IP address, or a particular file or registry entry found on the user's Windows device. If you specify more than one type, like certificate and IP addressing information, the concentrator uses a logical "AND" to match on the criteria.

Figure 8-22 Specifying Members of a Windows Location

To match on a user's certificate information, click the check box labeled *Enable identification using certificate criteria*. In the first text box enter the CN on the user's certificate. Or, you can enter the CN of the issuer (Certificate Authority) in the second text box.

To match on a user's IP address, select the *Enable identification using IP criteria* check box and enter the range of IP addresses and click **Add**—you can add multiple ranges for a location. In Figure 8-22 for the Wireless location, I specified the IP addresses assigned to them via DHCP. If a client device has more than one IP address on a NIC, or multiple NICs, CSD on the desktop will use only the IP address of the first NIC detected on the PC.

To match on a user's file or registry information, click the *Enable identification using File or Registry criteria* check box. When you click the **Add** button to add an entry, a small window will pop up asking you for the file (like the location and name) or registry key information.

At the bottom of the screen is the *Use Module* section. Only one option out of the following can be selected:

- “Secure Desktop,” when selected, specifies that the Secure Desktop Settings are used.
- “Cache Cleaner” specifies that the Cache Cleaner settings are used.
- If neither are selected, the VPN Feature Policy is used.

As to which you should use, you can use the following guidelines:

- For internal users, typically the VPN Feature Policy is used, where you want to ensure that users have the correct security software installed on their PCs.
- For remote access home users, either the VPN Feature Policy, Secure Desktop, or Cache Cleaner (for non-Windows systems).

- For remote access users using public PCs, either Secure Desktop or Cache Cleaner; in some cases, because of restricted access to the computer, they might not be able to use CSD.

TIP

Some older implementations of Windows, like 98, don't support CSD functionality fully; therefore, if you select the "Secure Desktop" option to the right of *Use Module*, you should configure both the Secure Desktop Settings and the Cache Cleaner, where the latter will serve as a fallback security solution.

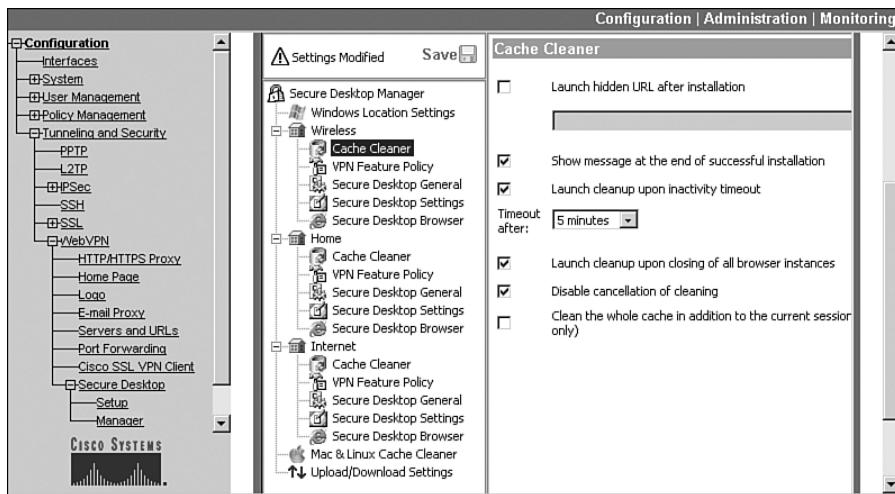
NOTE

If you only want to configure a location where you want everyone to match, then don't specify any matching criteria; however, make sure that this location is listed at the *bottom* of the locations you've added, because they are processed in order (top-down).

Windows Cache Cleaner

If you selected "Cache Cleaner" from the *Use Module* section in the Identification window in Figure 8-22, you can click the **Cache Cleaner** hyperlink under the name of the location (like "Wireless"), which will take you to the screen in Figure 8-23. Normally this is used for users for whom CSD can't be installed on their desktops, like in an Internet Café, or for non-Windows 2000/XP systems. Here are your options:

- **Launch hidden URL after installation**—Specifies a hidden URL to launch so that you know that the Cache Cleaner was installed; as an example, you might place a cookie file on the user's computer and then later check for the existence of the cookie.
- **Show message at the end of successful installation**—Displays a window showing that the Cache Cleaner was installed successfully on the user's desktop.
- **Launch cleanup upon inactivity timeout**—Specifies that the idle timer should be used, and when the idle timer expires, causes cache cleaning to begin. You can then change the *Timeout after* drop-down selector to specify what the idle timer should be (the smallest is 1 minute and the largest is 60 minutes).
- **Launch cleanup upon closing of all browser instances**—Specifies that cache cleaning begins once all web browser windows are closed.
- **Disable cancellation of cleaning**—Removes the cancellation feature from the user's desktop when performing cache cleaning. I highly recommend that you leave this disabled, because this does not allow the user to cancel a cache cleaning; enabling this can create a security risk.
- **Clean the whole cache in addition to . . .**—Removes all data from the user's web browser cache upon activation, including any web browser files that existed before the user's session began. I highly recommend that you enable this; however, this feature works only with Microsoft's Internet Explorer web browser.

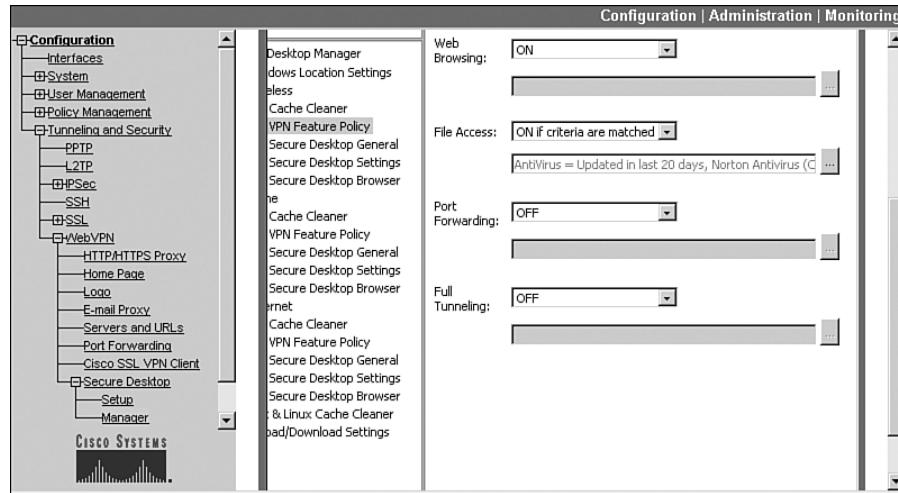
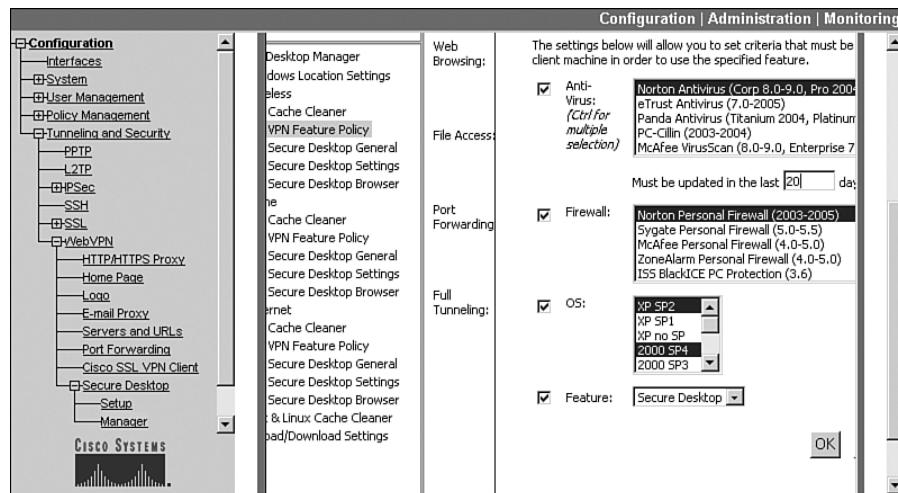
Figure 8-23 Configuring Cache Cleaning for a Windows Location

VPN Feature Policy

If you selected neither “Secure Desktop” nor “Cache Cleaner” from the *Use Module* section in the Identification window in Figure 8-22, you can click the **VPN Feature Policy** hyperlink under the name of the location, taking you to the screen in Figure 8-24. There are four features you can configure: Web Browsing, File Access, Port Forwarding, and Full Tunneling.

Here are the options you can specify for each:

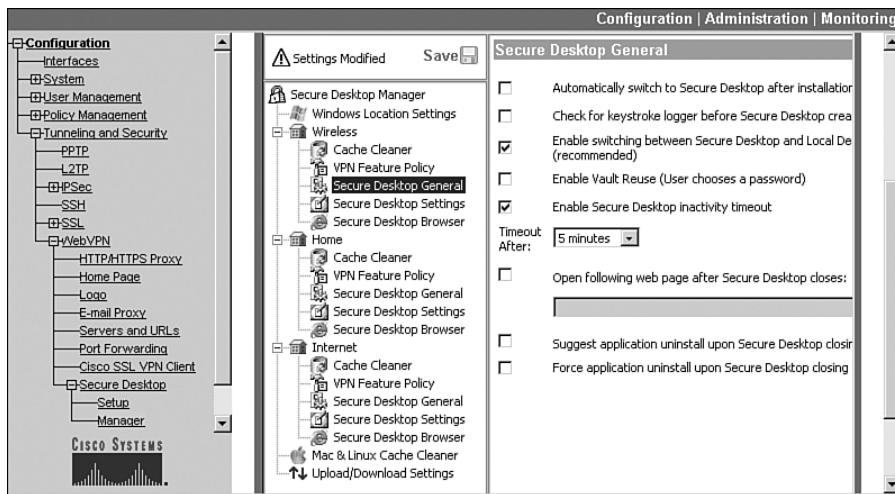
- If you specify “ON” in the drop-down selector, the corresponding feature is unconditionally *allowed*.
- If you specify “OFF” in the drop-down selector, the corresponding feature is unconditionally *denied*.
- If you specify “ON if criteria are matched” in the drop-down selector, the corresponding feature is enabled if the corresponding criteria are matched. Click the ... button to the right (hidden in Figure 8-24) and you’ll see the criteria screen in Figure 8-25. Choose the criteria that must match and then click the **OK** button to accept them. From a category, you can CNTRL-click to select multiple options. Within a category, only one option needs to match. If you select multiple categories, at least one option in each category must match for the user to be allowed access to the corresponding feature in Figure 8-24. One additional point to make: at the bottom of the screen you can select either “Secure Desktop” or “Cache Cleaner” as the feature to use for the client; if you choose the former and CSD is not active on the client, the VPN Feature Policy fails and the user is denied access to the corresponding feature in Figure 8-24. Choosing this option might create problems for older Windows systems and non-Windows systems.

Figure 8-24 Enabling VPN Feature Policies for Windows**Figure 8-25** Configuring VPN Feature Policies

Secure Desktop General Settings for Windows

If you selected “Secure Desktop” from the *Use Module* section in the Identification window in Figure 8-22, you can click the **Secure Desktop General** hyperlink under the name of the location, taking you to the screen in Figure 8-26. Here are your options:

- **Automatically switch to Secure Desktop after installation**—When selected, specifies that CSD is loaded automatically after being installed on the user’s PC, forcing the user to use it.
- **Check for keystroke logger before Secure Desktop creation**—When selected, verifies that no keystroke logging application is running on the PC before CSD is installed (the user needs Administrator privileges for this option to work).
- **Enable switching between Secure Desktop and Local Desktop**—When selected, allows users to switch between CSD and the local desktop (their normal desktop). Cisco highly recommends that you enable this feature, because it allows a user to respond to prompts from other running applications. As an example, Microsoft’s AntiSpyware application might prompt you to allow CSD to be installed, in addition to other anti-spyware or antivirus software. However, by unchecking it, you are creating a more secure environment: you’ll have to weigh the advantages of both choices before enabling or disabling this option.
- **Enable Vault Re-use**—When selected, allows a user to close CSD and open it later, creating a persistent desktop that’s available from one session to the next. When you enable this option, users will have to enter a password to re-access CSD. Choose this option for users that use the same computer, like wireless office workers or SOHO users, or for laptop users.
- **Enable Secure Desktop inactivity timeout**—When selected, specifies an idle timeout that causes CSD to close down once the idle timer in the *Timeout After* drop-down selector parameter is reached. This parameter is used only if you also have enabled the *Enable switching between Secure Desktop and Local Desktop* parameter.
- **Open following web page after Secure Desktop closes**—When selected, causes the specified web page to open automatically upon the closing of CSD on the user’s desktop.
- **Suggest application uninstall upon Secure Desktop closing**—When selected, prompts the user to uninstall CSD when it closes. For users that always use the same PC, don’t enable this option; this will allow the users from this location to use the Vault feature.
- **Force Uninstall of application when Secure Desktop closes**—When selected, prompts the user to uninstall CSD when it closes; this is recommended for locations like Internet Cafés where the user doesn’t own the desktop. For users (in the same location) that always use the same PC, don’t enable this option; this will allow the users from this location to use the Vault feature.

Figure 8-26 Configuring Secure Desktop General Settings

Secure Desktop Settings for Windows

If you selected “Secure Desktop” from the *Use Module* section in the Identification window in Figure 8-22, you can click the **Secure Desktop Settings** hyperlink under the name of the location, where your options are:

- **Put Secure Desktop in restricted mode**—When selected, only the originating web browser that starts CSD can be used; all other applications are denied.
- **Restrict Registry tools on Secure Desktop**—When selected, users are prevented from modifying the registry from within CSD. Cisco recommends enabling this feature to provide for optimum security.
- **Restrict DOS-CMD tools on Secure Desktop**—When selected, users are prevented from accessing a DOS command prompt. Cisco recommends enabling this feature to provide for optimum security.
- **Restrict Printing on Secure Desktop**—When selected, users are prevented from printing while CSD is active. If you have sensitive data being downloaded to the users’ computers, you might want to enable this feature to prevent them from printing the sensitive information.

Secure Desktop Browser for Windows

If you selected “Secure Desktop” from the *Use Module* section in the Identification window in Figure 8-22, you can click the **Secure Desktop Browser** hyperlink under the name of the location, where your options are:

- Specifying the home page of the user’s web browser
- Specifying bookmarks and folders for the user’s web browser

This feature is useful for public PCs where you don't want users to be using any web pages already bookmarked in the web browser.

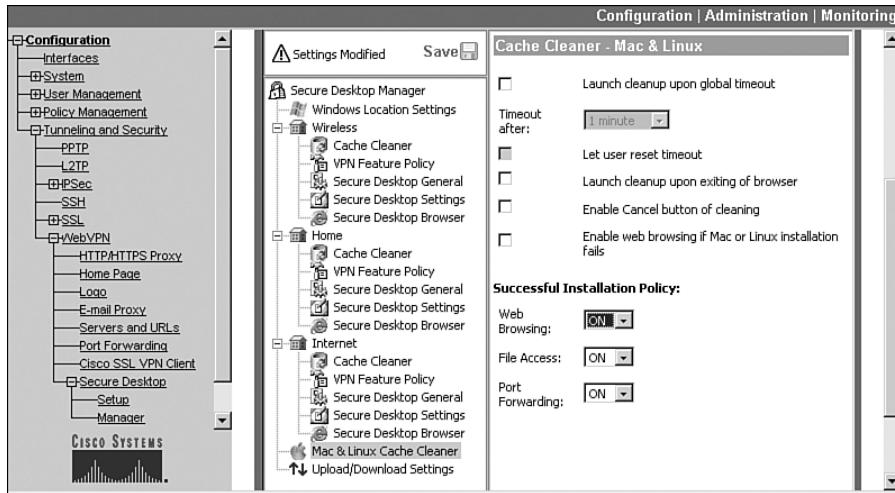
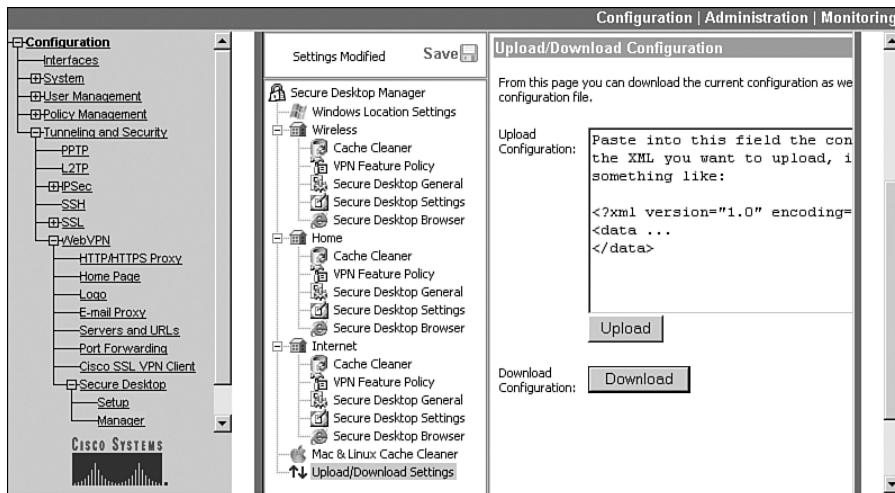
Configuring the Cache Cleaner for Mac & Linux Systems

Unfortunately, CSD is not available for non-Windows systems; however, the Cache Cleaner feature is. This feature is available for Windows, MacOS X, and Linux systems. To access the configuration screen for non-Windows systems, click the **Mac & Linux Cache Cleaner** hyperlink under the Secure Desktop column on the left-hand side of the screen. With this option, you can't specify a location; therefore, all your configuration options are defined globally for these devices. When you click this hyperlink, you'll be shown the screen in Figure 8-27, where you have the following options:

- **Launch cleanup upon global timeout**—When checked, specifies that the Cache Cleaner is run after the specified timeout in the *Timeout after* drop-down selector is reached.
- **Let user reset timeout**—When checked, allows the user to reset the timeout period.
- **Launch cleanup upon exiting of browser**—When checked, causes the Cache Cleaner to run when all web browser windows have closed.
- **Enabled Cancel button of cleaning**—When checked, allows the user to cancel cache cleaning. I highly recommend that you do *not* enable this feature, because it can create a security risk for sensitive data downloaded during a web session.
- **Enable web browsing if Mac or Linux installation fails**—When checked, allows the user to access the network using a web browser if the Cache Cleaner fails to install; all other remote access applications are denied, though.
- **Web Browsing, File Access, Port Forwarding**—For these three features, you can choose either “ON” to enable them or “OFF” to disable them. This is similar to configuring the same policies for Windows users, but there is not an option to specify additional matching criteria, like antivirus or personal firewall software.

Configuring Upload/Download Settings

The **Upload/Download Settings** hyperlink shown under the “Secure Desktop Manager” column allows you to back up or reload your CSD settings. This is shown at the very bottom of Figure 8-28 in the left-hand column of the CSD manager. This is a handy feature if you have configured VCA load balancing or VRRP redundancy and want to duplicate your configurations across multiple VPN 3000 concentrators easily. When you click this hyperlink, you are taken to the screen shown in Figure 8-28. Click the **Download** button to back up your CSD configuration. A new web browser window will open, displaying the configuration in an XML format. Log in to a secondary concentrator and go to this screen and paste in the configuration in the text box above the **Upload** button; click the **Upload** button to load the CSD settings.

Figure 8-27 Configuring Cache Cleaning for Non-Windows Systems**Figure 8-28** Backing Up and Restoring CSD Settings

Saving Settings and Enabling CSD

The configuration you create within the CSD manager on the concentrator is not saved automatically. To determine if you need to save your configuration, look for the yellow triangular warning icon indicating “Settings Modified” in the upper left-hand corner of the HTML/JavaScript window; if you see this information, the current configuration hasn’t been saved. Click the **Save** floppy icon (to the right of the warning icon) to save the CSD settings to the concentrator’s Flash memory.

CAUTION The **Save** button in the concentrator's CSD manager window and the **Save As Needed** button in the concentrator's GUI are *not* the same; both save different things! If you navigate to another part of the concentrator's GUI (leaving the concentrator's CSD manager application), then you'll lose your CSD settings. So make sure you save your CSD settings before leaving the CSD Manager screen!

After you've installed and configured CSD, it is not enabled automatically. You'll need to go to the **Configuration > Tunneling and Security > WebVPN > Secure Desktop > Secure Desktop Setup** screen and choose the "Enable Secure Desktop" radio button.

Using the Secure Desktop Client

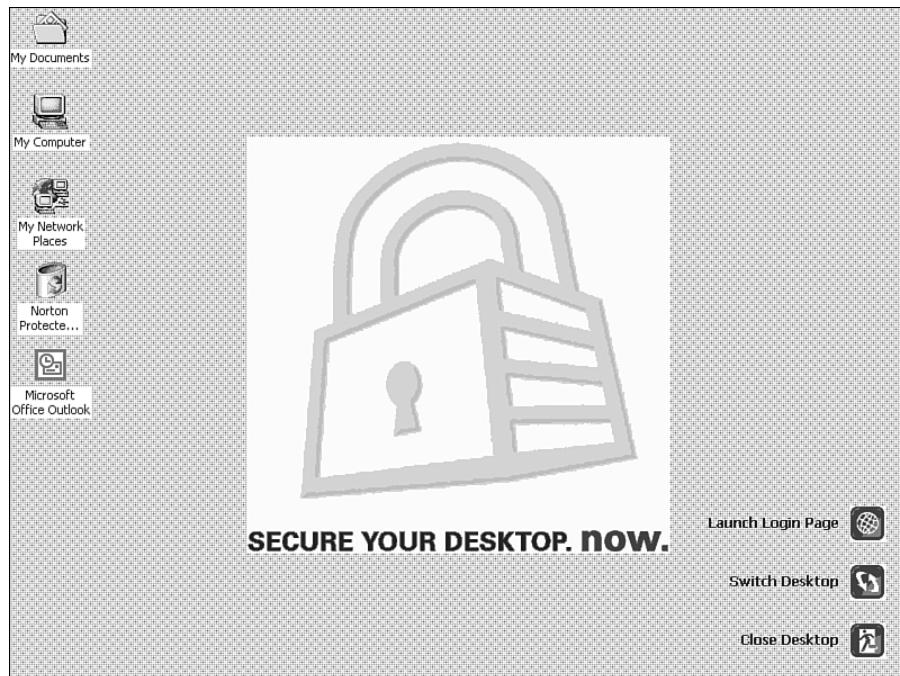
To run CSD on a user's desktop optimally, Cisco recommends using Windows 2000 or XP. On these computers, you should, at a minimum, meet these specifications:

- Pentium 633MHz processor
- 128MB of RAM
- 25MB of disk space
- A supported web browser (IE 6.0, Netscape 7.1, Mozilla 1.7, or Firefox 1.0).

A WebVPN user normally will access the concentrator as if CSD wasn't being used. Before the user is prompted for a username and password, the CSD software (an ActiveX script, Javascript, or EXE program) is downloaded and installed on the user's computer. Once this has been accomplished, the user is presented with the username and password prompt, and WebVPN proceeds as normal if using the VPN Feature Policy. If you're using the Secure Desktop feature, you'll be presented with the screen shown in Figure 8-29. Based on your concentrator's CSD configuration, a web browser might open automatically to start the WebVPN user login process. You can always start this process manually by clicking the **Launch Login Page** hyperlink in the bottom right-hand corner of the screen. And assuming you've set up CSD to allow the user to switch between the CSD and local desktops, you can click the **Switch Desktop** hyperlink to go to the local desktop. When in the local desktop, the Secure Desktop is still running, and you can access it and go back to the Secure Desktop.

CSD can be run separately from the Cisco SSL VPN Client or in conjunction. When both options are configured on the concentrator, CSD is installed first, user authentication is performed, and then SVC is installed. If you have enabled desktop switching, SVC is available in both the CSD *and* on local desktops.

Figure 8-29 Backing Up and Restoring CSD Settings



Summary

This chapter introduced you to configuring remote access sessions: PPTP L2TP/IPsec, and WebVPN. In regard to PPTP and L2TP/IPsec, I'll spend more time on how these are configured on the concentrator when I discuss the Microsoft software client in Chapter 13, "Windows Software Client."

Next up is Chapter 9, "Concentrator Site-to-Site Connections," where I show you how to use your VPN 3000 concentrator to terminate site-to-site, or LAN-to-LAN (L2L), sessions.