SSL VPN Remote User Guide

First Published: February 27, 2006
Last Updated: March 6, 2008

The SSL VPN feature (also known as WebVPN) provides support, in Cisco IOS software, for remote user access to enterprise networks from anywhere on the Internet. Remote access is provided through a Secure Socket Layer- (SSL-) enabled SSL Virtual Private Network (VPN) gateway. The SSL VPN gateway allows remote users to establish a secure VPN tunnel using a web browser. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support.

This document describes how a remote user, whose enterprise network is configured for SSL VPN, can access the network by launching a browser and connecting to the SSL VPN gateway.

For information about SSL VPN from the point of view of a system administrator, see the document *SSL VPN*.

Note The Cisco AnyConnect VPN Client is introduced in Cisco IOS Release 12.4(15)T. This feature is the next-generation SSL VPN Client. If you are using Cisco software before Cisco IOS Release 12.4(15)T, you should use SSL VPN Client and see GUI for the SSL VPN Client when you are web browsing. However, if you are using Cisco software Release 12.4(15)T or later, you should use Cisco AnyConnect VPN Client and see GUI for Cisco AnyConnect VPN Client when you are web browsing.

For "What's New" information about SSL VPN features by release, see the "Feature Information for SSL VPN for Remote Users" section on page 23.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for SSL VPN for Remote Users" section on page 23.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents:

SSL VPN Prerequisites for the Remote User

The following prerequisites are required to start SSL VPN on a PC or device:

- Connection to the Internet—Any Internet connection is supported, including:
  - Home DSL, cable, or dial-ups
  - Public kiosks
  - Hotel connections
  - Airport wireless nodes
  - Internet cafes
- Operating system support

Note Later versions of the following software are also supported.

  - Microsoft Windows 2000, Windows XP, or Windows Vista
  - Macintosh OS X 10.4.6
  - Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)
- SSL VPN-supported browser—The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.

Note Later versions of the following software are also supported.

  - Internet Explorer 6.0 or 7.0
  - Firefox 2.0 (Windows and Linux)
  - Safari 2.0.3
- Cookies enabled—Cookies must be enabled on the browser to access applications through port forwarding.

- Pop-ups enabled—Pop-ups should be enabled on the browser to display the floating SSL VPN toolbar and timeout warnings. If pop-ups are blocked, change the browser setting and click the SSL VPN floating toolbar icon on the in-page toolbar to display the floating toolbar.

  If pop-ups are disabled on the browser, SSL VPN does not warn you before disconnecting because of an idle timeout or a maximum connect time.
- URL for SSL VPN—An HTTPS address in the following form:

  https://*address*

  where *address* is the IP address or Domain Name System (DNS) hostname of an interface of the SSL VPN gateway, for example https://10.89.192.163 or https://vpn.company.com.
- SSL VPN username and password

Restrictions for SSL VPN Remote User Guide

Cisco AnyConnect VPN Client

CiscoAnyConnect VPN Client does not support the following:

- Adaptive Security Appliance (ASA) and Adaptive Security Device Manager (ASDM) and any command-line interface (CLI) associated with the them
- Adjusting Maximum Transmission Unit (MTU) size
- Client-side authentication
- Compression support
- Datagram Transport Layer Security (DTLS) with SSL connections
- IPv6 VPN access
- Language Translation (localization)
- (Optional) Local printer—SSL VPN does not support printing in clientless mode from a web browser to a network printer. However, printing to a local printer is supported.
- Sequencing
- Standalone Mode

Usernames and Passwords

Table 1 lists the type of usernames and passwords that SSL VPN users might have to know.

Table 1 Usernames and Passwords for SSL VPN Users

Login Username/ Password Type	Purpose	Entered When
Computer	Access the computer	Starting the computer
Internet Provider	Access the Internet	Connecting to an Internet provider
SSL VPN	Access the remote network	Starting SSL VPN
File Server	Access the remote file server	Using the SSL VPN file browsing feature to access a remote file server

Table 1 Usernames and Passwords for SSL VPN Users (continued)

Login Username/ Password Type	Purpose	Entered When
Corporate Application Login	Access the firewall-protected internal server	Using the SSL VPN web browsing feature to access an internal protected website
Mail Server	Access the remote mail server via SSL VPN	Sending or receiving e-mail messages

Remote User Interface

If your enterprise network has been configured for SSL VPN, you can access the network by launching a browser and connecting to the SSL VPN gateway. Present your credentials and authenticate, and then a portal page (home page) of the enterprise site is displayed. The portal page displays SSL VPN features (for example, e-mail and web browsing) to which you have access on the basis of your credentials. If you have access to all features enabled on the SSL VPN gateway, the home page will provide access links.

The following sections explain the remote user interface in more detail:

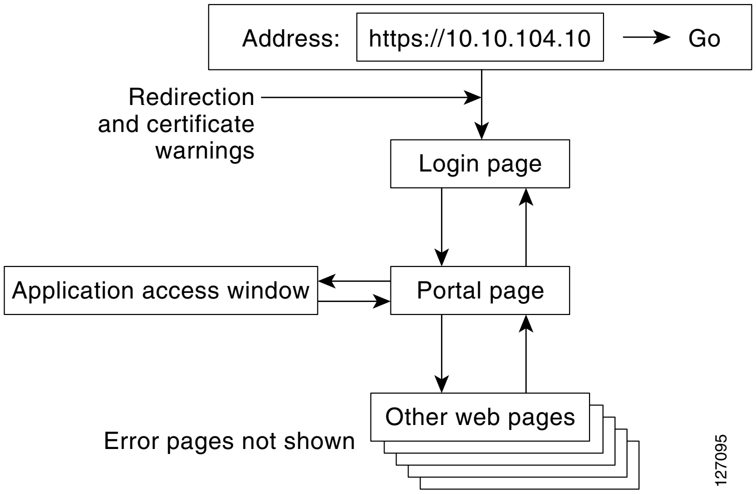
- Page Flow, page 4
- Initial Connection, page 5
- Login Page, page 5
- Certificate Authentication, page 6
- Logout Page, page 6
- Portal Page, page 7
- Remote Servers, page 9
- Toolbar, page 9
- Session Timeout, page 12
- TCP Port Forwarding and Thin Client, page 13
- Tunnel Connection, page 15
- User-Level Bookmarking, page 15

Page Flow

This section describes the page flow process (see Figure 1) for a SSL VPN session. When you enter the HTTPS URL (https://*address*) into your browser, you are then redirected to https://*address*/index.html, where the login page is located.

Note Depending on the configuration of the browser, this redirection may display a warning message in your browser, which indicates that you are being redirected to a secure connection.

Figure 1 *Page Flow*



Initial Connection

When you connect for the first time, you might be presented with one of the following scenarios:

- 503 Service Unavailable Message, page 5
- SSL/TLS Certificate, page 5
- Web Browsing, page 10

503 Service Unavailable Message

You might see a "503 Service Unavailable" message if the gateway is experiencing high traffic loads. If you receive this message, try to connect again later.

SSL/TLS Certificate

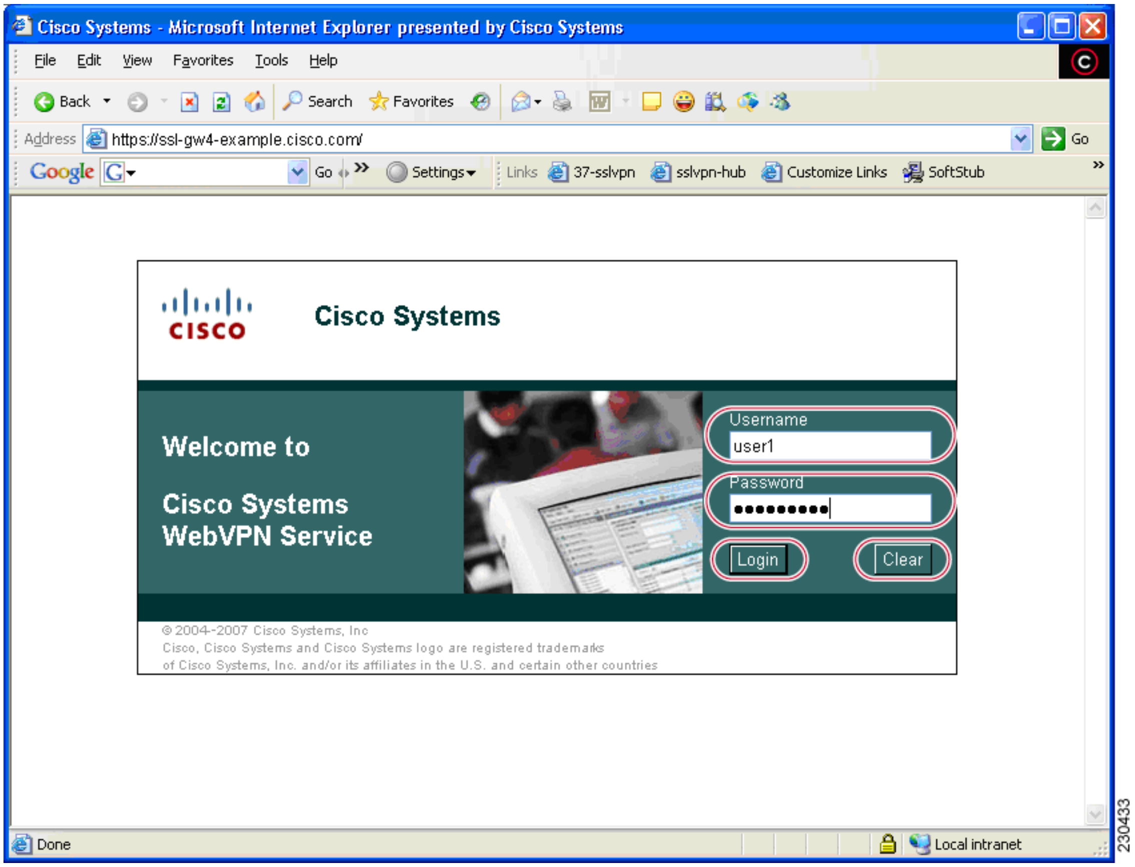
When the HTTPS connection is established, a warning about the SSL/Transport Layer Security (TLS) certificate may display. If the warning displays, you should install this certificate. If the warning does not display, the system already has a certificate that the browser trusts.

You are then connected to the login page.

Login Page

The default login page (Figure 2) prompts you to enter your username and password, which are entered into an HTML form. If an authentication failure occurs, the login page displays an error message.

Figure 2 Default Login Page



Cisco Systems - Microsoft Internet Explorer presented by Cisco Systems

Address: https://ssl-gw4-example.cisco.com/

Cisco Systems

Welcome to

Cisco Systems WebVPN Service

Username: user1

Password: ●●●●●●●●●

© 2004-2007 Cisco Systems, Inc

Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

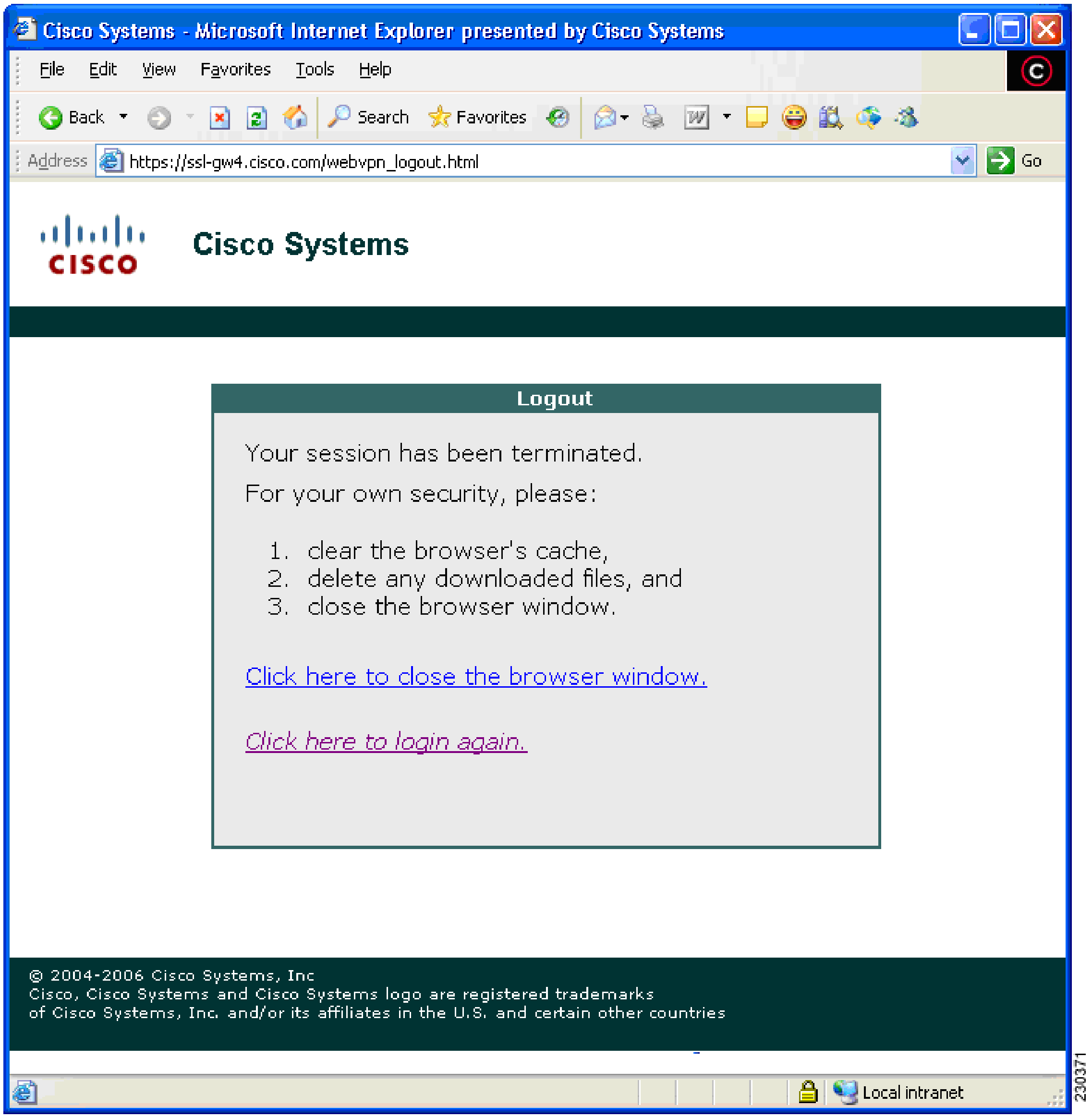
Certificate Authentication

Client certificate authentication is not supported. Only username and password authentication is supported.

Logout Page

The logout page (Figure 3) displays if you click the logout link or if the session terminates because of an idle timeout or a maximum connection time.

Figure 3 Logout Page


Cisco Systems - Microsoft Internet Explorer presented by Cisco Systems
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ssl-gw4.cisco.com/webvpn_logout.html Go
CISCO
Cisco Systems
Local intranet
230371

Logout

Your session has been terminated.

For your own security, please:

1. clear the browser's cache,
2. delete any downloaded files, and
3. close the browser window.

Click here to close the browser window.

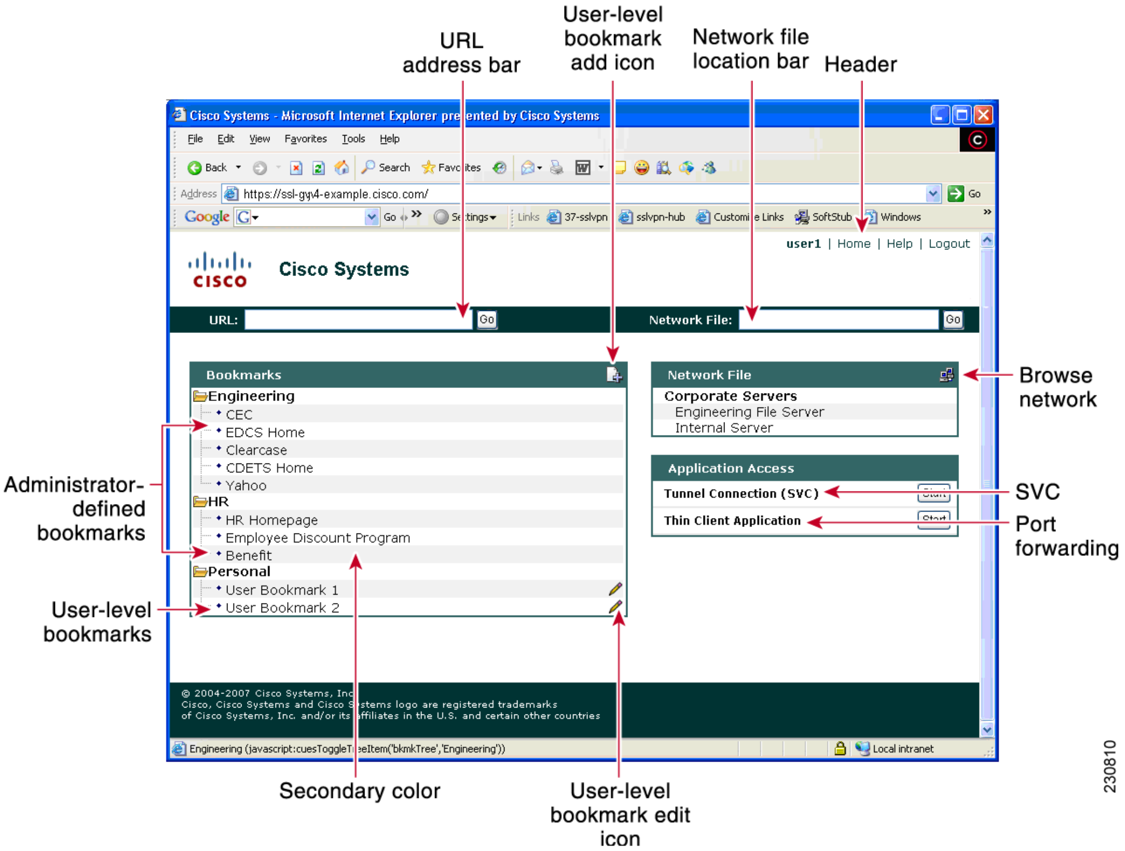
Click here to login again.

© 2004-2006 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

Portal Page

The portal page (Figure 4) is the main page for the SSL VPN functionality. See the callouts for functions that exist for administrators and users.

Figure 4 Portal Page


URL address bar
User-level bookmark add icon
Network file location bar
Header
Browse network
SVC
Port forwarding
Administrator-defined bookmarks
User-level bookmarks
Secondary color
User-level bookmark edit icon
230810

Cisco Systems - Microsoft Internet Explorer presented by Cisco Systems

File Edit View Favorites Tools Help

Address https://ssl-gyy4-example.cisco.com/

user1 | Home | Help | Logout

Cisco Systems

URL: Go Network File: Go

Bookmarks
- Engineering
  - CEC
  - EDCS Home
  - Clearcase
  - CDETS Home
  - Yahoo
- HR
  - HR Homepage
  - Employee Discount Program
  - Benefit
- Personal
  - User Bookmark 1
  - User Bookmark 2

Network File
- Corporate Servers
  - Engineering File Server
  - Internal Server

Application Access
- Tunnel Connection (SVC) Start
- Thin Client Application Start

© 2004-2007 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

Engineering (javascript:cuesToggleTreeItem('bkmkTree','Engineering')) Local intranet

Table 2 provides information about various fields on the portal page.

Table 2 Information About Fields on the Portal Page

Field	Description
Administrator-defined bookmarks	Administrator-defined URL lists that cannot be edited by the user.
Browse network	Allows you to browse the file network.
Header	Shares the same color value as the “Title.” Set by the administrator.
Network File location bar	Allows you to access the network share or folder directly by entering \\server\share\folder.
Port forwarding	Downloads the applet and starts port forwarding.
Tunnel connection	Allows you to download the tunnel client and to install tunnel connect.
URL address bar	A new window is opened when you click **Go**.
User-level bookmark add icon	Clicking the icon opens a dialog box so you can add a new bookmark to the Personal folder.

Table 2 Information About Fields on the Portal Page (continued)

Field	Description
User-level bookmark edit icon	Allows you to edit or delete an existing bookmark.
User-level bookmarks	You can add a bookmark by using the plus icon (see below) on the bookmark panel or toolbar. See the "Toolbar" section on page 9 for information about the toolbar. A new window is opened when the link is clicked.

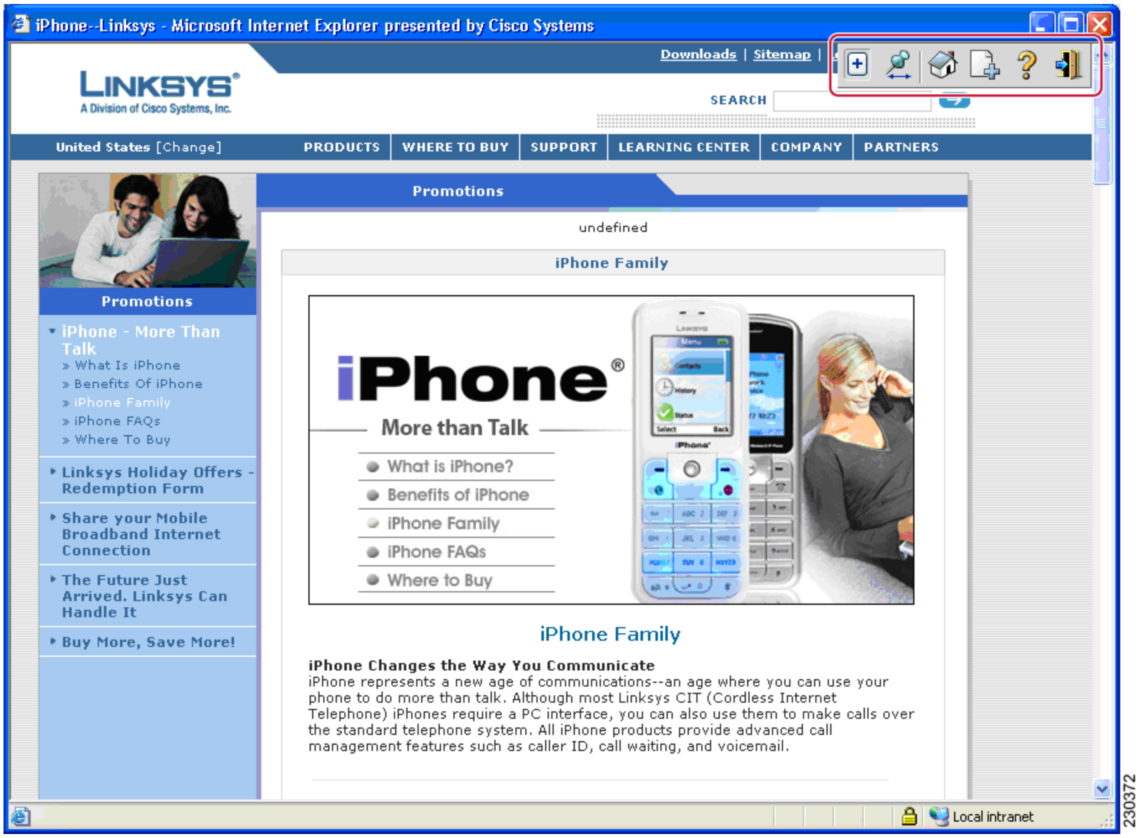
Remote Servers

You may enter an address or URL path of a website that you want to visit in the text box on the portal page. Pages from the remote server are displayed in the browser window. You can then browse to other links on the page.

Toolbar

A toolbar has been introduced to help you access the SSL VPN functionalities that are outside the portal page. The toolbar is in the upper right corner of Figure 5 and is outlined in red.

Figure 5 Website with a Toolbar

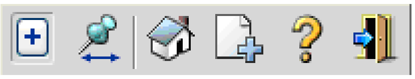


iPhone Changes the Way You Communicate

iPhone represents a new age of communications--an age where you can use your phone to do more than talk. Although most Linksys CIT (Cordless Internet Telephone) iPhones require a PC interface, you can also use them to make calls over the standard telephone system. All iPhone products provide advanced call management features such as caller ID, call waiting, and voicemail.

The toolbar is expanded below in Figure 6. The sections that follow it explain how to use the toolbar icons.

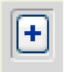
Figure 6 Toolbar



Web Browsing

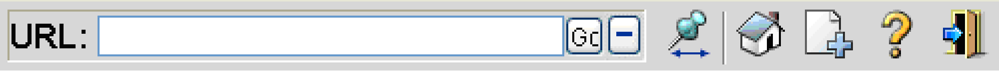
The web browser is the plus icon (see Figure 7).

Figure 7 Web Browsing Icon



If you click the web browsing icon (see Figure 7), the toolbar expands so that you can enter a URL (see Figure 8).

Figure 8 URL Bar

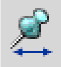


When a remote user goes to a URL through the URL address bar, the window that is already open is used for display.

Moving the Toolbar

The push-pin icon (see Figure 9) allows you to move the toolbar to the right or left side of the portal page.

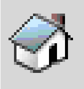
Figure 9 Toolbar Repositioning



Returning to the Portal Page

The house icon allows you to return to the portal page (see Figure 10).

Figure 10 Return to the Portal Page

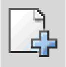


If the portal page is present in the parent window and you click to return to the portal page, your screen jumps back (sets the focus) to that window; otherwise, the current page is loaded with the portal page.

Adding the Current Page to the Personal Bookmark Folder

You can add the current page to your personal bookmark folder by clicking the page-with-a-plus icon (see Figure 11).

Figure 11 Adding Current Page to Personal Bookmark Folder



Displaying the Help Page

You can display the help page by clicking the question mark icon (see Figure 12).

Figure 12 Help Page

Logging Out

The door icon (see Figure 13) allows you to log out.

Figure 13 Log Out

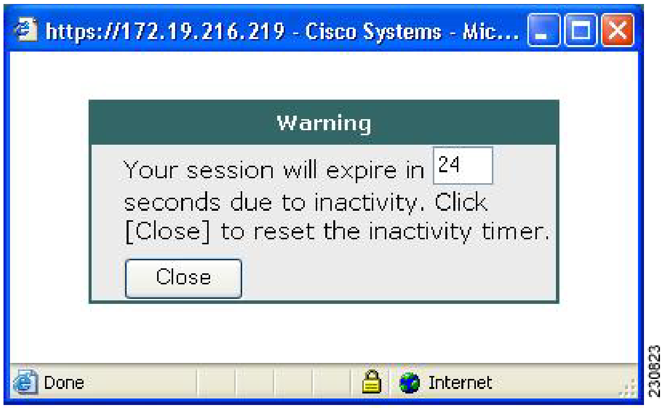
Session Timeout

You receive a warning message approximately 1 minute before the session is set to expire, and you receive another message when the session expires. On the workstation, the local time indicates when the message was displayed.

The first message will be similar to the following:

"Your session will expire in *x* seconds due to inactivity. Click Close to reset the inactivity timer. (browser time and date)" (See Figure 14 below.)

Figure 14 Session Expiration Message



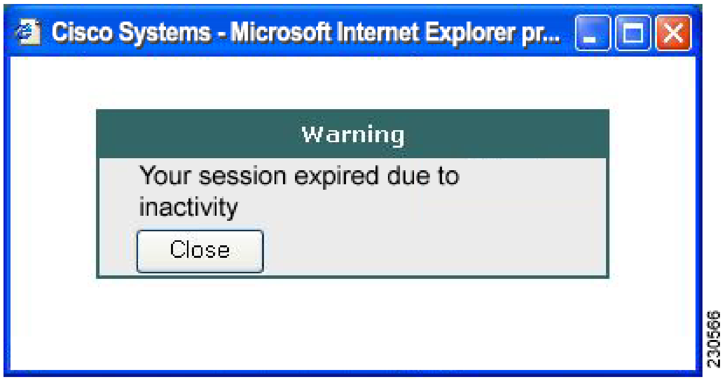
https://172.19.216.219 - Cisco Systems - Mic...

Warning

Your session will expire in 24 seconds due to inactivity. Click [Close] to reset the inactivity timer.

The last message, as shown below in Figure 15, displays when the time runs out (depending on whether the reason of the session termination is known):

Figure 15 Session Inactivity or Timeout Window



Cisco Systems - Microsoft Internet Explorer pr...

Warning

Your session expired due to inactivity

TCP Port Forwarding and Thin Client

Note This feature requires the Java Runtime Environment (JRE) version 1.4 or later releases to properly support SSL connections.

Note Because this feature requires installing JRE and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that you can use applications when you connect from public remote systems.

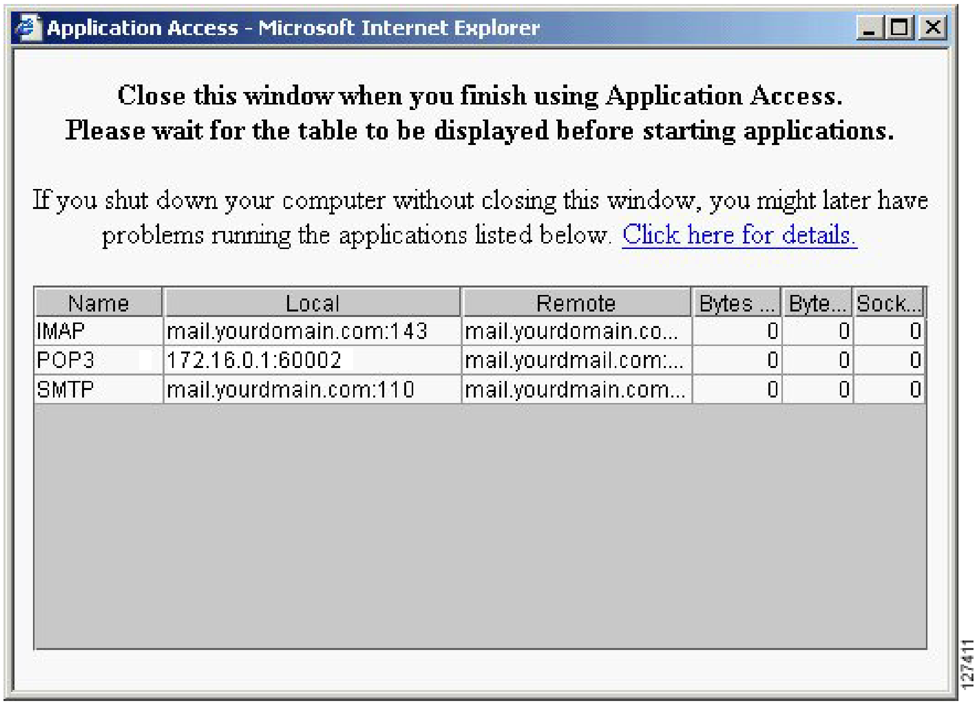
When you click the Start button of the Thin Client application (under Application Access), a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks you to verify the certificate with which this applet is signed. When you accept the certificate, the applet starts running, and port-forwarding entries are displayed (see Figure 16). The number of active connections and bytes that are sent and received is also listed on this window.

Note When you click the Thin Client link, your system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If your connection hangs, minimize the browser windows to find this dialog box.

The administrator should have configured IP addresses, DNS names, and port numbers for the e-mail servers. If they are configured, you can launch the e-mail client, which is configured to contact these e-mail servers and send and receive e-mails. Point of Presence3 (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP) protocols are supported.

The window attempts to close automatically if you are logged out using JavaScript. If the session terminated and a new port forwarding connection is established, the applet displays an error message.

Figure 16 TCP Port Forwarding Page



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

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

Name	Local	Remote	Bytes ...	Byte...	Sock...
IMAP	mail.yourdomain.com:143	mail.yourdomain.co...	0	0	0
POP3	172.16.0.1:60002	mail.yourdmail.com:...	0	0	0
SMTP	mail.yourdmain.com:110	mail.yourdmain.com...	0	0	0

Caution You should always close the Thin Client window when you finish using applications by clicking the close icon. Failure to quit the window properly can cause Thin Client or the applications to be disabled. See the "Thin Client—Recovering from Hosts File Error" section on page 18 for details.

Table 3 lists the requirements for Thin Client (Port Forwarding) on your PC or device.

Table 3 SSL VPN Remote System Thin Client Requirements

Remote User System Requirements	Specifications or Use Suggestions
Client applications installed	—
Cookies enabled on browser	—
Administrator priviliges	You must be the local administrator on your PC.
Sun Microsystems JRE version 1.4 or later installed	SSL VPN automatically checks for JRE whenever you start Thin Client. If it is necessary to install JRE, a pop-up window displays, directing you to a site where it is available.

Table 3 SSL VPN Remote System Thin Client Requirements (continued)

Remote User System Requirements	Specifications or Use Suggestions
Client applications configured, if necessary **Note** The Microsoft Outlook client does not require this configuration step.	To configure the client application, use the locally mapped IP address and port number of the server. To find this information, do the following: • Start SSL VPN on the remote system and click the Thin Client link on the SSL VPN home page. The Thin Client window is displayed. • In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column). • Use this IP address and port number to configure the client application. The configuration steps vary for each client application.
Windows XP SP2 patch	If you are running Windows XP SP2, you must install a patch from Microsoft that is available at the following address: http://support.microsoft.com/?kbid=884020 This problem is a known Microsoft issue.

Tunnel Connection

In a typical clientless remote access scenario, you establish an SSL tunnel to move data to and from the internal networks at the application layer (for example, web and e-mail). In tunnel mode, you use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications (for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet).

The tunnel connection is determined by the group policy configuration. The Cisco AnyConnect VPN Client (next-generation SSL VPN Client) is downloaded and installed on your PC, and the tunnel connection is established after the installation.

By default, Cisco AnyConnect VPN Client is removed from your PC after the connection is closed. However, you have the option to keep the Cisco AnyConnect VPN Client installed on your PC.

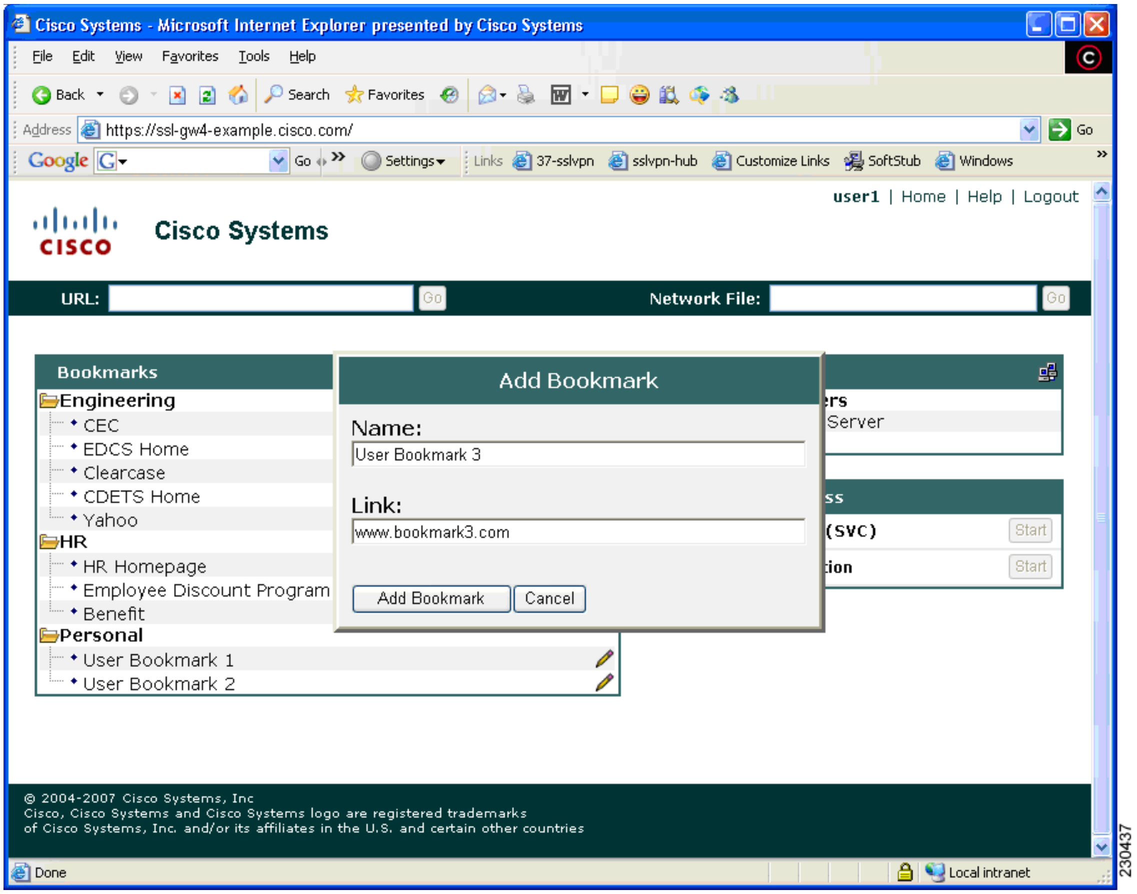
User-Level Bookmarking

Effective with Cisco IOS Release 12.4(15)T, you can bookmark URLs while connected through an SSL VPN tunnel. You can access the bookmarked URLs by clicking the URL.

Adding a Bookmark

Figure 17 shows a typical web page to which a bookmark can be added.

Figure 17 Add Bookmark



Cisco Systems - Microsoft Internet Explorer presented by Cisco Systems
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ssl-gw4-example.cisco.com/ Go
Google Go Settings Links 37-sslvpn sslvpn-hub Customize Links SoftStub Windows
user1 | Home | Help | Logout
Cisco Systems
URL: Go Network File: Go
Bookmarks
Engineering
CEC
EDCS Home
Clearcase
CDETS Home
Yahoo
HR
HR Homepage
Employee Discount Program
Benefit
Personal
User Bookmark 1
User Bookmark 2
ers
Server
ss
(SVC) Start
ion Start
Add Bookmark
Add Bookmark Cancel
© 2004-2007 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries
Done Local intranet
230437

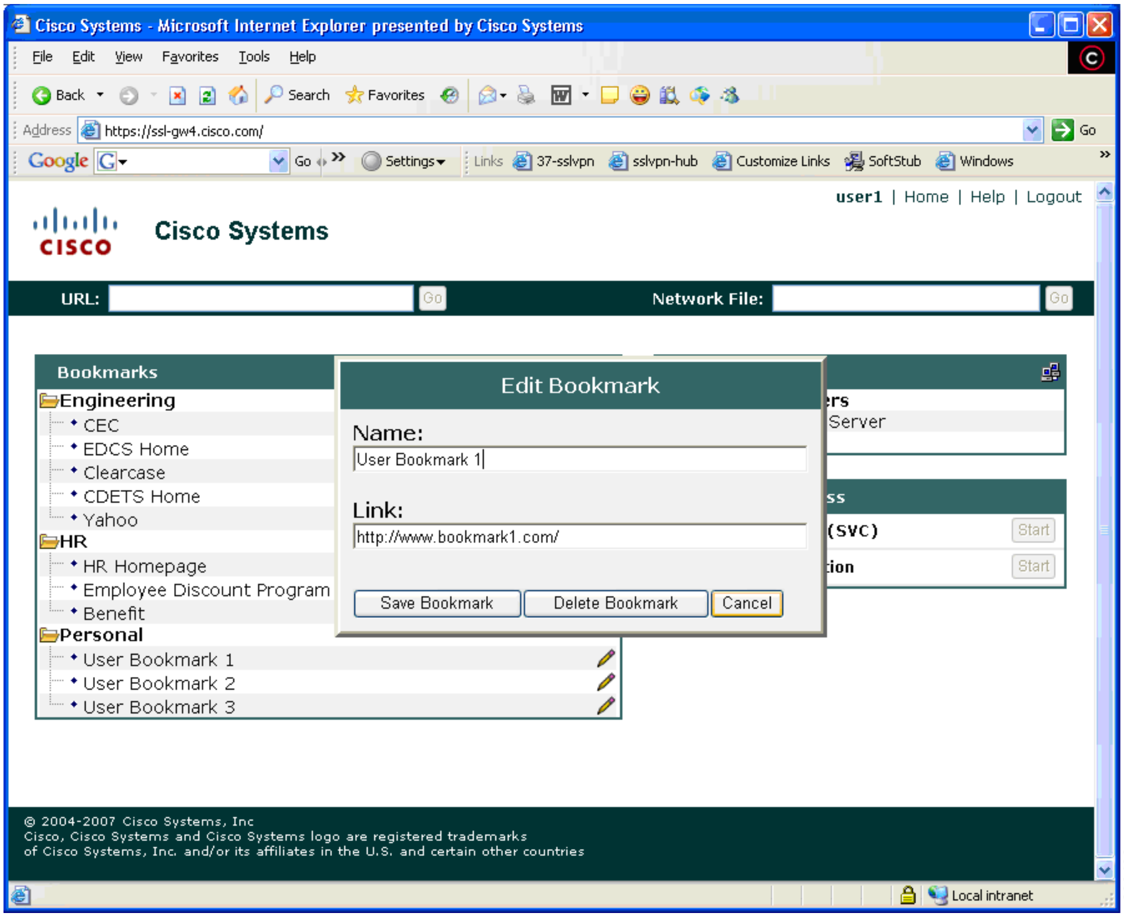
Name: User Bookmark 3

Link: www.bookmark3.com

Editing a Bookmark

Figure 18 shows a typical web page to which a bookmark can be edited.

Figure 18 Edit Bookmark



Cisco Systems - Microsoft Internet Explorer presented by Cisco Systems
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ssl-gw4.cisco.com/
Go
Google G Go Settings Links 37-sslvpn sslvpn-hub Customize Links SoftStub Windows
user1 | Home | Help | Logout
CISCO
Cisco Systems
URL: Go
Network File: Go
Bookmarks
rs
Server
ss
(SVC) Start
ion Start
Local intranet
230438

Edit Bookmark

Name: User Bookmark 1

Link: http://www.bookmark1.com/

Save Bookmark
Delete Bookmark
Cancel

Engineering
- CEC
- EDCS Home
- Clearcase
- CDETS Home
- Yahoo

HR
- HR Homepage
- Employee Discount Program
- Benefit

Personal
- User Bookmark 1
- User Bookmark 2
- User Bookmark 3

© 2004-2007 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

Security Tips

You should always log out from the SSL VPN session when you are finished. (To log out of SSL VPN, click the logout icon on the SSL VPN toolbar or quit the browser.)

Using SSL VPN does not ensure that communication with every site is secure. SSL VPN ensures the security of data transmission between your PC or workstation and the SSL VPN gateway on the corporate network. If you then access a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate SSL VPN gateway to the destination web server is not secured.

Browser Caching and Security Implications

If you access SSL VPN through a public or shared Internet system, such as an Internet cafe or kiosk, to ensure the security of your information after terminating or logging out of the SSL VPN session, you must delete all files that you have saved on the PC during the SSL VPN session. These files are not removed automatically upon disconnect.

Note SSL VPN does not save the content of web pages viewed during the session. However, for additional security, we recommend that you clear your browser cache. Deleting content from a PC does not ensure that it cannot be recovered; keep this fact in mind when downloading sensitive data.

Thin Client—Recovering from Hosts File Error

It is important that you close the Thin Client window properly by clicking the close icon. If you do not close the window properly, the following could occur:

- The next time you try to start Thin Client, it might be disabled; you will receive a "Backup HOSTS File Found" error message.
- The applications might be disabled or might malfunction even when you are running them locally.

These errors can result if you terminate the Thin Client window in any improper way:

- The browser crashes while using Thin Client.
- A power outage or system shutdown occurs while using Thin Client.
- You minimize the Thin Client window and then shut down the computer with the window active (but minimized).

How SSL VPN Uses the Hosts File

The hosts file on your system maps IP addresses to hostnames. When you start Thin Client, SSL VPN modifies the hosts file by adding SSL VPN-specific entries. When you stop Thin Client by properly closing the Thin Client window, SSL VPN returns the hosts file to its original state. The hosts file goes through the following states:

- Before invoking Thin Client, the hosts file is in its original state.
- When Thin Client starts, SSL VPN does the following:
  1. Copies the hosts file to hosts.webvpn and creates a backup.
  2. Edits the hosts file, inserting SSL VPN-specific information.
- When Thin Client stops, SSL VPN does the following:
  1. Copies the backup file to the hosts file, restoring the hosts file to its original state.
  2. Deletes hosts.webvpn.
- After finishing Thin Client, the hosts file is in its original state.

What Happens If You Stop Thin Client Improperly

If you improperly terminate Thin Client, the hosts file is left in the SSL VPN-customized state. SSL VPN checks for this possibility the next time you start Thin Client by searching for a hosts.webvpn file. If SSL VPN finds the file, you receive a "Backup HOSTS File Found" error message, and Thin Client is temporarily disabled.

If you improperly shut down Thin Client, you leave the remote access client or server applications in a suspended state. If you start these applications without using SSL VPN, the applications might malfunction. You might find that hosts that you normally connect to are unavailable. This situation could commonly occur if you run applications remotely from home, fail to quit the Thin Client window before shutting down the computer, and then try to run the applications later from the office.

What to Do

To reenable Thin Client or malfunctioning applications, you should do the following:

- If you can connect to your remote access server, you should follow the steps in the "Reconfiguring the Hosts File Automatically Using SSL VPN" section on page 19.
- If you cannot connect to your remote access server from your current location or if you have made custom edits to the hosts file, you should follow the steps in the "Reconfiguring the Hosts File Manually" section on page 19.

Reconfiguring the Hosts File Automatically Using SSL VPN

If you can connect to your remote access server, you should follow these steps to reconfigure the hosts file and reenable both Thin Client and the applications:

Step 1 Start SSL VPN and log in. The portal page opens.

Step 2 Click the Applications Access link. A "Backup HOSTS File Found" message displays.

Step 3 Choose one of the following options:

- Restore from backup—SSL VPN forces a proper shutdown. SSL VPN copies the hosts.webvpn backup file to the hosts file, restoring it to its original state, and then deletes the hosts.webvpn backup file. You then have to restart Thin Client.
- Do nothing—Thin Client does not start. You are returned to the remote access home page.
- Delete backup—SSL VPN deletes the hosts.webvpn file, leaving the hosts file in its SSL VPN-customized state. The original hosts file settings are lost. Then Thin Client starts, using the SSL VPN-customized hosts file as the new original. Choose this option only if you are unconcerned about losing hosts file settings. If you edited the hosts file after Thin Client has shut down improperly, choose one of the other options, or edit the hosts file manually. (See the "Reconfiguring the Hosts File Manually" section on page 19.)

Reconfiguring the Hosts File Manually

If you cannot connect to your remote access server from your current location, or if you have customized the hosts file and do not want to lose your edits, you should follow these steps to reconfigure the hosts file and reenable both Thin Client and the applications:

Step 1 Locate and edit your hosts file.

Step 2 Check to see if any lines contain the "added by WebVpnPortForward" string.

If any lines contain this string, your hosts file is customized for SSL VPN. If your hosts file is customized, it looks similar to the following example:

```
10.23.0.3 server1 # added by WebVpnPortForward
10.23.0.3 server1.example.com emailxyz.com # added by WebVpnPortForward
10.23.0.4 server2 # added by WebVpnPortForward
10.23.0.4 server2.example.com.emailxyz.com # added by WebVpnPortForward
10.23.0.5 server3 # added by WebVpnPortForward
10.23.0.5 server3.example.com emailxyz.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      172.16.102.97     rhino.acme.com          # source server
#      192.168.63.10     x.acme.com              # x client host

10.23.0.1       localhost
```

Step 3 Delete the lines that contain the "# added by WebVpnPortForward" string.

Step 4 Save and close the file.

Step 5 Start SSL VPN and log in. Your home page appears.

Step 6 Click the Thin Client link. The Thin Client window appears. Thin Client is now enabled.

Troubleshooting Guidelines

Table 4 provides a list of messages notifying you of various problems, causes, and fixes.

Table 4 Troubleshooting Guidelines

Message	Cause	Fix
The request to {*url*} is not allowed. WebVPN has dropped the request. If you have any questions, please ask {...}.	The administrator does not allow you to access a particular URL.	Contact the administrator.
Unable to connect to server {*server name*}. The server may not exist, or access to it may not be allowed.	Problem with the server.	Check the server name or contact the administrator if it persists.
Unable to find the server {*server or url*} The server may not exist, or access to it may not be allowed.	DNS cannot resolve the server name or URL location.	Check the URL address or contact the administrator if it persists.
This (client) machine does not match any identification of a WebVPN user. Please contact your WebVPN provider for assistance.	The client computer does not match any profile of Cisco Secure Desktop (CSD).	Contact the administrator.
This (client) machine does not have the web access privilege. Please contact your WebVPN provider for assistance.	The client computer does not meet the security criteria of having web access functionality through the SSL VPN gateway.	Check the URL to the gateway or contact the administrator if it persists.

Table 4 Troubleshooting Guidelines (continued)

Message	Cause	Fix
CSD is enabled, but not installed. Please contact your WebVPN provider for assistance.	The CSD has been enabled on the gateway, but it is not available.	Contact the administrator.
The requested information is not available.	Various causes.	Contact the administrator.

Additional References

The following sections provide references related to SSL VPN.

Related Documents

Related Topic	Document Title
Security configurations	*Cisco IOS Security Configuration Guide*, Release 12.4 http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html
Security commands	*Cisco IOS Security Command Reference*, Release 12.4T http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html
Cisco Secure Desktop	Cisco Secure Desktop Home Page http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html
Cisco AnyConnect VPN Client	• *Cisco AnyConnect VPN Client Administrator Guide* • *Release Notes for Cisco AnyConnect VPN Client, Version 2.0*
SSL VPN (administrator guide)	*SSL VPN*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for SSL VPN for Remote Users

Table 5 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for SSL VPN Remote User Guide

Feature Name	Releases	Feature Information
SSL VPN Remote User Guide	12.4(6)T	This section was originally included in the *SSL VPN* feature document.
Cisco AnyConnect VPN Client	12.4(15)T	This feature is the next-generation SSL VPN Client. The feature provides remote users with secure VPN connections to the router platforms supported by SSL VPN and to the Cisco 5500 Series Adaptive Security Appliances. **Note** Users who are using Cisco IOS software releases before Release 12.4(15)T see the SSL VPN Client GUI interface when they are web browsing. Users who are using Cisco IOS software Release 12.4(15)T and later see the Cisco AnyConnect VPN Client GUI when they are web browsing. **Note** See the restrictions in the "Cisco AnyConnect VPN Client" section on page 3 for features not currently supported by Cisco AnyConnect VPN Client on platforms other than the Cisco ASA 5500 series Adaptive Security Appliance.

Table 5 Feature Information for SSL VPN Remote User Guide (continued)

Feature Name	Releases	Feature Information
GUI Enhancements	12.4(15)T	These enhancements provide updated examples and explanation of the Web VPN GUIs. The following sections provide information about these updates: • Page Flow, page 4 • Initial Connection, page 5 • Login Page, page 5 • Certificate Authentication, page 6 • Logout Page, page 6 • Portal Page, page 7 • Remote Servers, page 9 • Toolbar, page 9 • Session Timeout, page 12 • TCP Port Forwarding and Thin Client, page 13 • Tunnel Connection, page 15 • User-Level Bookmarking, page 15

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.