



# WebVPN

---

The Cisco WebVPN feature provides remote access to enterprise sites by users from anywhere on the Internet. The Secure Socket Layer (SSL) Virtual Private Network (VPN) provides users with secure access to specific enterprise applications, such as e-mail and web browsing, without requiring them to have VPN client software installed on their end-user devices.



## Note

The WebVPN Enhancements feature, released in Cisco IOS Release 12.4(6)T, obsoletes the commands and configuration described in this document. If you are using a platform that is not supported in 12.4(6)T, you can continue to use 12.3T and 12.4 mainline images. The WebVPN Enhancements feature expands SSLVPN functionality in Cisco IOS Software. For more information about Cisco IOS WebVPN Enhancements, see the following document:

[http://www.cisco.com/en/US/customer/products/ps6441/products\\_feature\\_guide09186a00805eeaea.html](http://www.cisco.com/en/US/customer/products/ps6441/products_feature_guide09186a00805eeaea.html)

---

## Feature History for WebVPN

Release	Modification
12.3(14)T	This feature was introduced.
12.4(6)T	This feature was replaced by the WebVPN Enhancements feature.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

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

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for WebVPN, page 2](#)
- [Restrictions for WebVPN, page 2](#)
- [Information About WebVPN, page 2](#)
- [How to Configure WebVPN, page 11](#)
- [Configuration Examples for WebVPN, page 24](#)
- [Additional References, page 25](#)
- [Command Reference, page 26](#)

## Prerequisites for WebVPN

- To securely access resources on a private network behind a WebVPN gateway, the user of a WebVPN service must have the following:
  - An account (login name and password)
  - An SSL-enabled browser (for example, Internet Explorer, Netscape, Mozilla, or FireFox)
  - Operating system, such as Windows 2000 or Windows XP with Sun Microsystems Java Runtime.
  - E-mail client, such as Eudora, Microsoft Outlook, or Netscape Mail.
- Before a user can access resources on a private network behind a web VPN, the administrator of a web VPN service has to configure basic WebVPN functionality on a router as shown in the section [“Configuring WebVPN.”](#)

## Restrictions for WebVPN

- If WebVPN has to be enabled on a router that is running HTTP Secure Server, the administrator must configure an IP address for WebVPN using the **gateway-addr** keyword option of the **webvpn enable** command.
- The browsing of URLs that are referred by Macromedia Flash are not modified for the secure retrieval by the WebVPN gateway.
- In Cisco IOS Release 12.3(14)T, this feature supports SSL Version 3. Transport Layer Security (TLS) is not supported.
- “Thin Client” used for TCP port-forwarding applications requires administrative privileges on the computer of the end user.

## Information About WebVPN

To configure the WebVPN feature, you should understand the following concept:

- [WebVPN, page 3](#)

# WebVPN

The WebVPN feature provides end users with unrestricted, secure remote access to enterprise sites without having VPN installed on their end devices. Users can access the enterprise sites from anywhere on the Internet and can access enterprise applications such as e-mail and web browsing.

This feature provides for an administrator interface and an end-user interface.

## Administrator Interface

Enterprise administrators can enable WebVPN functionality for their end users through the command-line-interface (CLI) on their Cisco IOS routers. See the section “Configuring WebVPN.”

## End User Interface

A user whose enterprise has configured WebVPN can access the enterprise network by launching a browser and connecting to the WebVPN gateway that is hosted by the enterprise network. The user will present his or her credentials, be authenticated, and see the portal page (home page) of the enterprise site. The portal page will display those functionalities (for example, e-mail and Web browsing) to which the user has access on the basis of his or her credentials. If the user has access to all functionalities of the WebVPN gateway, the home page will provide links to all those functionalities.



---

**Note**

The user interface is primarily an HTML interface.

---

The following sections explain the user interface in more detail:

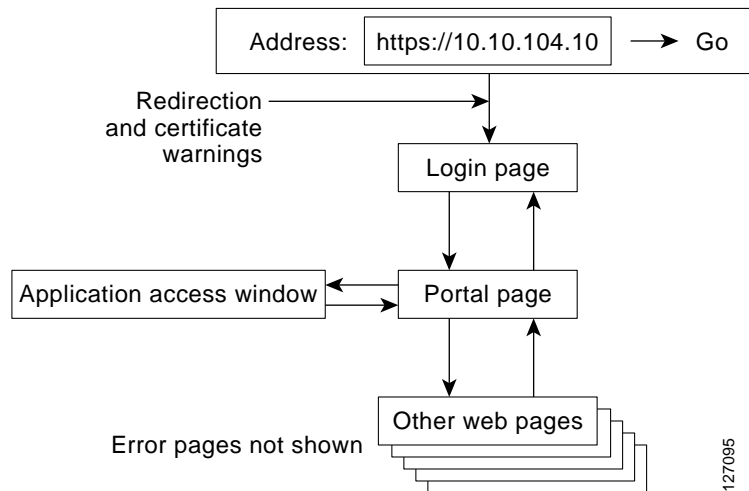
- [Page Flow, page 4](#)
- [Initial Connection, page 4](#)
- [Login Page, page 5](#)
- [Certificate Authentication, page 5](#)
- [Logout Page, page 6](#)
- [Portal Page, page 7](#)
- [Remote Servers, page 8](#)
- [DNS and Connection Errors, page 9](#)
- [Session Timeout, page 10](#)
- [TCP Port Forwarding and Application Access, page 10](#)

## Page Flow

This section describes the page flow that an end user will see as he or she uses a WebVPN session. The user first enters the Hypertext Transfer Protocol Secure (HTTPS) URL (`https://address`) into his or her browser. The user is redirected to `https://address/index.html`, where the login page is located.

Figure 1 illustrates the flow of pages that the user may expect to see.

**Figure 1** Page Flow



## Initial Connection

If the user enters the HTTP URL, the browser will be redirected to the equivalent HTTPS URL. Depending on the configuration of the browser, this redirection may cause a warning in the browser of the user indicating that he or she is being redirected to a secure connection.

On establishment of the HTTPS connection, the user may receive a warning about the SSL/TLS certificate. The user should install this certificate. The user does not receive a warning if the administrator has installed a certificate that the browser of the user trusts or if the user had previously installed the certificate.

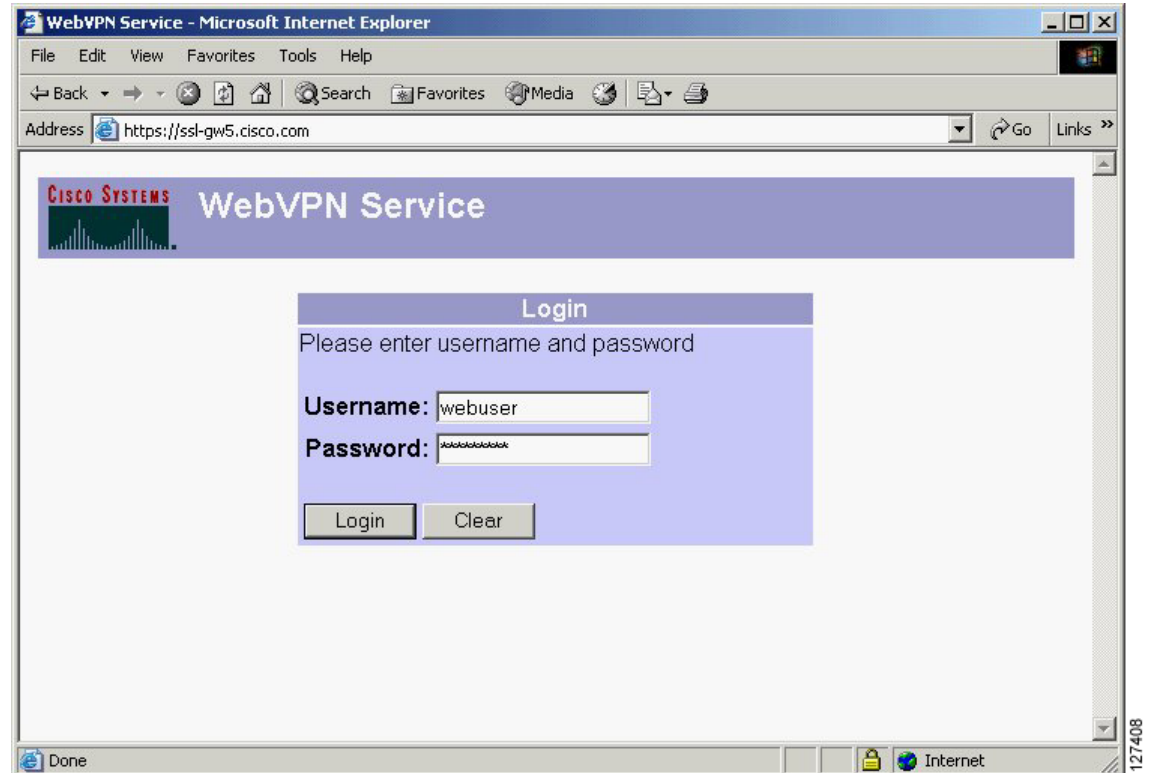
The user will then be connected to the login page.

## Login Page

The login page is where the user will be prompted to enter his or her credentials. The credentials consist of a username and password, which are entered into an HTML form. If an authentication failure occurs, the user will be presented with the login page again but with an error message.

Figure 2 illustrates a default login page.

**Figure 2**      *Default Login Page*



**Note**

Only the fields that are necessary for the challenge are presented on the login page.

The login page has logos, titles, messages, and colors that may be customized by administrators.

## Certificate Authentication

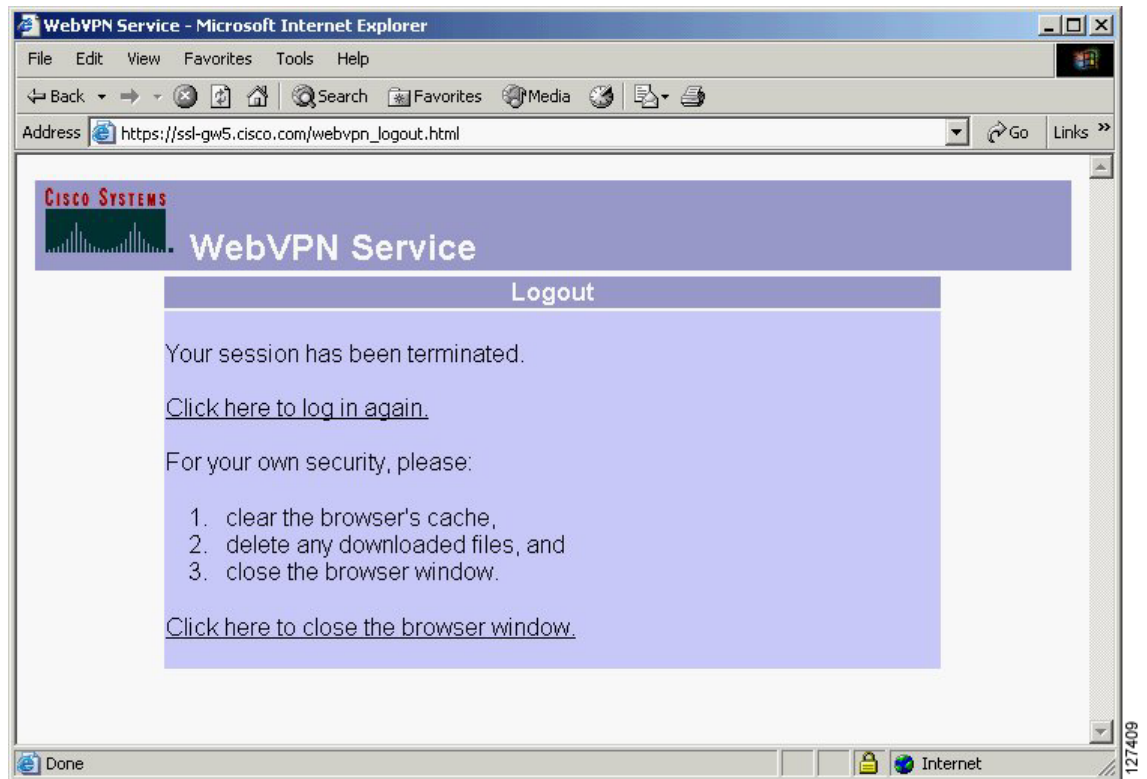
Client certificate authentication is not supported. Only username and password authentication is needed.

## Logout Page

If the user clicks the logout link, or if his or her session terminates because of an idle timeout or maximum connection time, the user is presented with the logout page.

Figure 3 illustrates a logout page.

**Figure 3** Logout Page



## Portal Page

The portal page is the main page for the WebVPN functionality. This page is a customizable page that contains the following:

- Custom logo (the default is the Cisco bridge logo)
- Custom title (the default is “WebVPN Services”)
- Custom banner (the default is an empty string)
- Custom colors (the default is a combination of white and purples)
- List of web server links (customizable)
- URL entry box (always present)
- Application access link (always present)
- Icon links for Help, Home (that is, the portal page), and Logout
- Link to popup, floating toolbar

Items that have not been configured will not be displayed on the portal page.

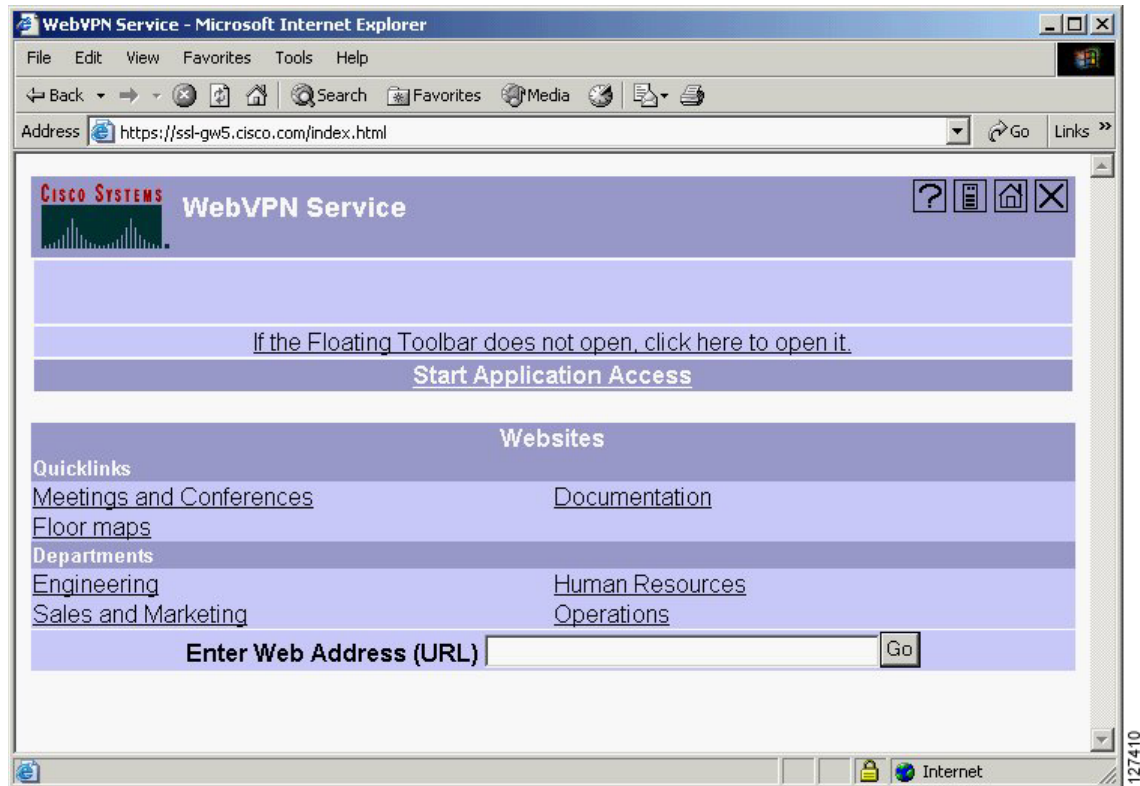


### Note

E-mail access is supported by “thin client,” which is downloaded using the application access link.

Figure 4 illustrates a portal page.

**Figure 4** Portal Page



## Remote Servers

An end user may enter an address or URL path of a website to which he or she wants to visit either in the text box on the portal page or in the text box on the floating toolbar. Pages from the remote server will be displayed in the browser window. The user can then browse to other links on the page normally.

Figure 5 illustrates the portal page of a typical website. By clicking the home icon button on the floating toolbar (see Figure 6), the user can go back to the portal page.

**Figure 5** Website with a Toolbar

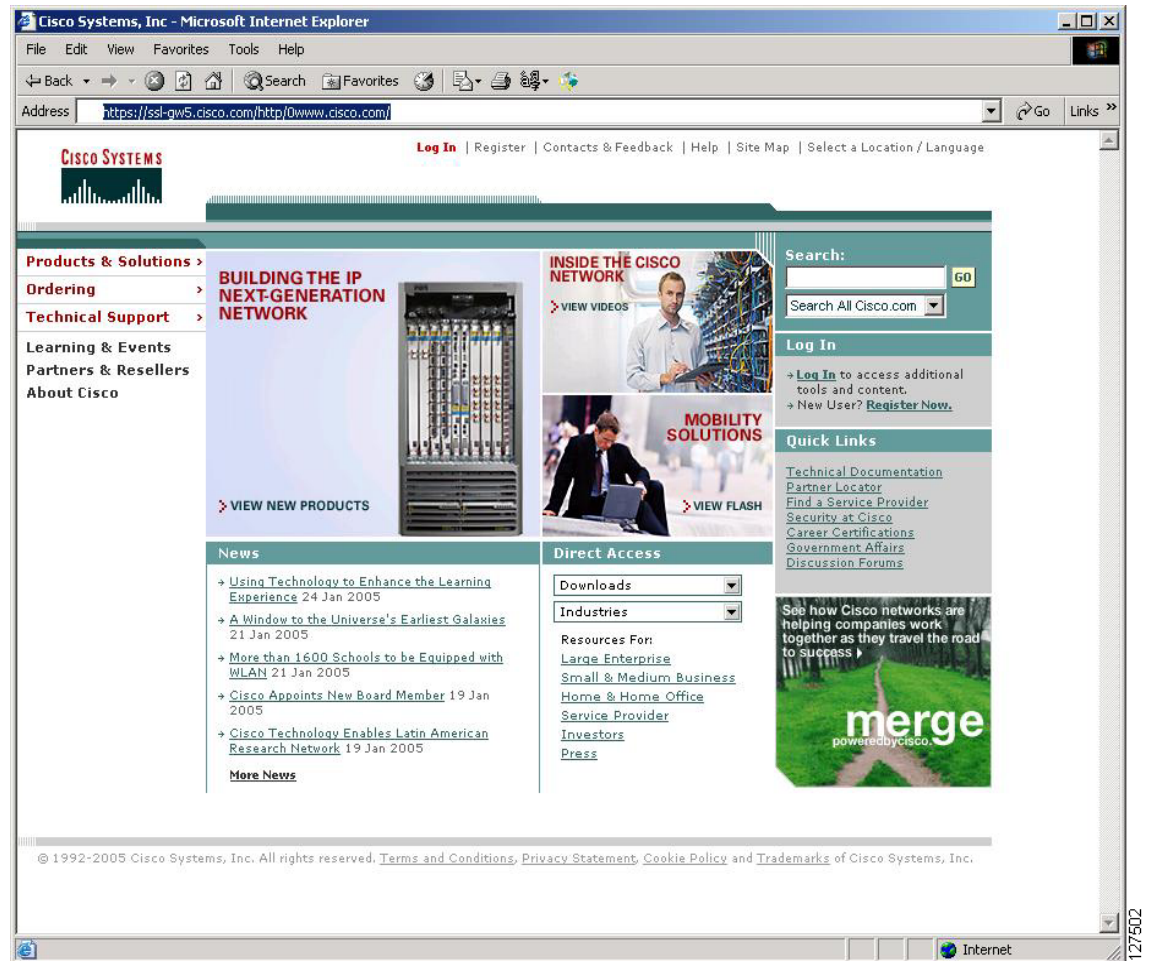


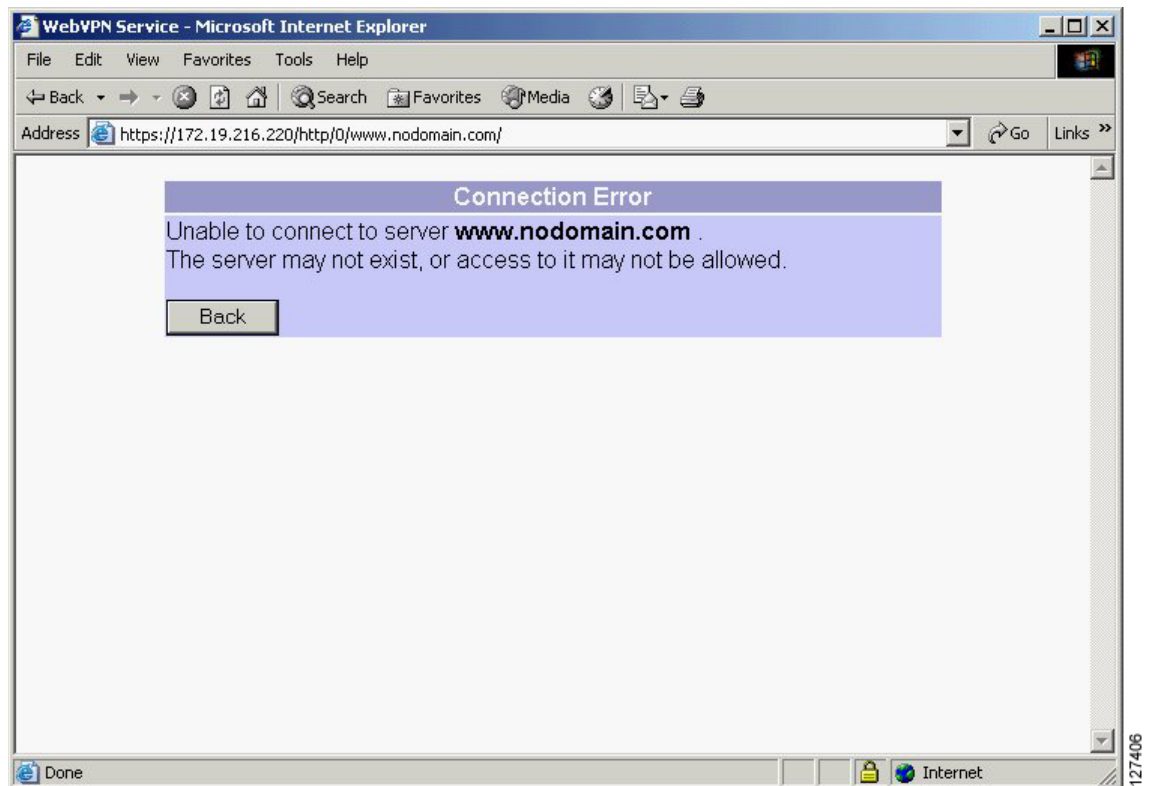
Figure 6 Floating Toolbar



## DNS and Connection Errors

If a user specifies a remote server to which he or she cannot connect because of domain naming system (DNS) or other connection errors, the user is presented with a friendly error, as shown in Figure 7. Because of TCP timeouts, it may take a while for connection errors to be returned to the user.

Figure 7 DNS Errors



## Session Timeout

Users will be warned when their sessions are about to expire because of inactivity. The user will be presented with a small, centered window as shown in [Figure 8](#). The user will receive a warning approximately 1 minute before the session expires and another warning when the session expires. The time of the workstation will be displayed to indicate when the message was displayed.

The first message will be one of the following:

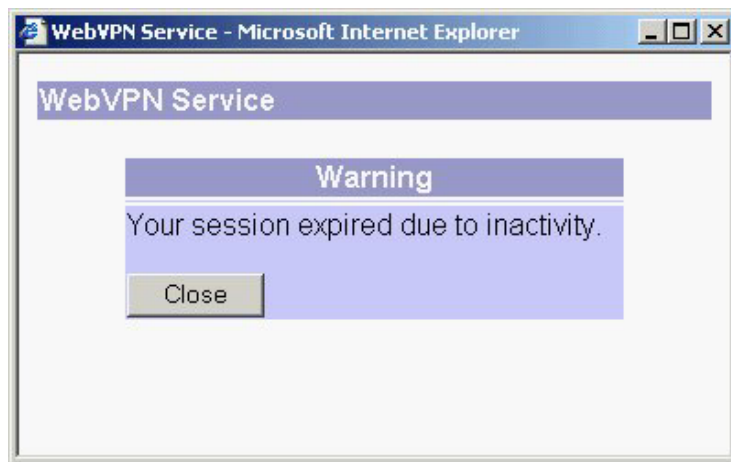
- “Your session will expire in  $x$  seconds due to inactivity. Click [Close] to reset the inactivity timer. (browser time and date)”

Clicking the [Close] button on the idle warning message will reset the inactivity timer.

The last message, as shown below, will be displayed when time runs out (depending on whether the reason of the session termination is known):

- “Your session has expired due to inactivity.”

**Figure 8**      *Session Inactivity or Timeout Window*



## TCP Port Forwarding and Application Access

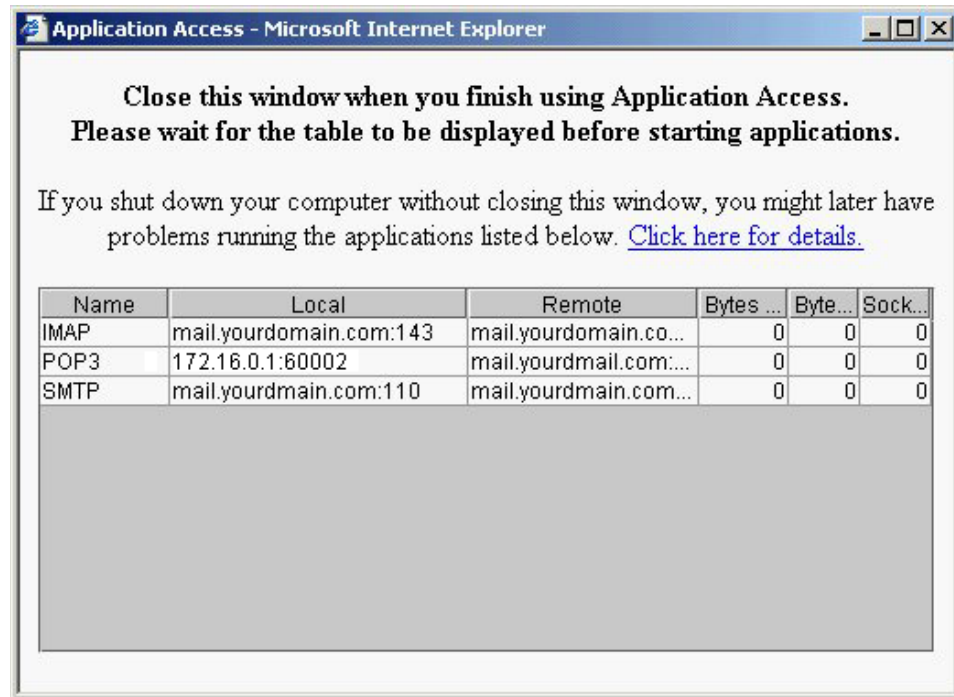
When the Application Access link is clicked, a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks the user to verify the certificate with which this applet is signed. When the user accepts the certificate, the applet starts running, and port-forwarding entries are displayed. The administrator should have configured IP addresses, DNS names, and port numbers for the e-mail servers. The user can then launch Email Client, which is configured to contact the above e-mail servers and have them send and receive e-mails. Point of Presence3 (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP) protocols are supported.

This feature will require the Java 1.4 Java Virtual Machine (JVM) to properly support SSL connections. The number of active connections and bytes that are sent and received is also listed on this window. The user may then open the client programs and connect to the local port. This window should not be subject to advertisement or popup blockers.

An attempt will be made to have this window close automatically if the user is logged out using JavaScript. If the session of the user is terminated and a new port forwarding connection is established, the applet will indicate the error.

Figure 9 illustrates a typical port forwarding page.

Figure 9 TCP Port Forwarding Page



## How to Configure WebVPN

This section contains the following procedures:

- [Configuring WebVPN: Prerequisites, page 11](#) (required)
- [Configuring WebVPN, page 15](#) (required)
- [Defining Encryption Algorithms for the SSL Protocol, page 17](#) (optional)
- [Displaying URL Entries on the Portal Page, page 18](#) (optional)
- [Maintaining and Monitoring Your WebVPN Functionality, page 19](#) (optional)
- [Troubleshooting WebVPN, page 23](#) (optional)

### Configuring WebVPN: Prerequisites

Before configuring WebVPN, an administrator must configure and install the following:

- [AAA-Related Configuration, page 12](#)
- [DNS-Related Configuration, page 13](#)
- [Certificates and Trustpoints, page 13](#)

## AAA-Related Configuration

Before configuring WebVPN for a AAA-related configuration, an administrator must create user accounts using either local authentication or authentication via AAA (RADIUS and TACACS+ servers) and configure AAA-related commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
5. **exit**
6. **aaa authentication login** {**default** | **list-name**} *method*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa group server radius</b> <i>group-name</i>  <b>Example:</b> Router# aaa group server radius EMAIL-AUTH	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 4	<b>server</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ]  <b>Example:</b> Router (config-server-group)# server 10.1.1.1 auth-port 2 acct-port 3	Configures the IP address of the RADIUS server for the group server.
Step 5	<b>exit</b>  <b>Example:</b> Router (config-server-group)# exit	Exits server-group configuration mode.
Step 6	<b>aaa authentication login</b> { <b>default</b>   <b>list-name</b> } <i>method</i>  <b>Example:</b> Router (config)# aaa authentication login default EMAIL-AUTH	Sets AAA authentication at login.

## DNS-Related Configuration

Before configuring WebVPN, an administrator must configure DNS-related commands, such as the following.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain name** *name*
4. **ip name server** *server-address*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip domain name</b> <i>name</i>  <b>Example:</b> Router (config)# ip domain name cisco.com	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 4	<b>ip name server</b> <i>server-address</i>  <b>Example:</b> Router (config)# ip name server 172.16.1.111	Specifies the address of one or more name servers to use for name and address resolution.

## Certificates and Trustpoints

Before configuring WebVPN, an administrator must install certificates and configure trustpoints. To load the certificate, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki import** *trustpointname* **pkcs12** *source url passphrase*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki import trustpointname pkcs12 source url passphrase</b>  <b>Example:</b> Router# crypto pki import SSLVPN pkcs12 tftp:cisco	Imports Rivest, Shamir, and Adelman (RSA) keys.

## Examples

After configuring the **crypto pki import pkcs** command, an administrator will see something like the following on his or her console:

```
Router(config)# crypto pki import SSLVPN pkcs12 tftp: cisco
      Address or name of remote host []? 10.1.1.1
      Source filename [SSLVPN]? cert/SSLVPN.cert
      Loading cert/SSLVPN.cert from 10.1.1.1 (via Ethernet1/0):
      !
Router(config)#
```

The above would generate the crypto-specific commands, as shown in the following sample **show running-config** command output:

```
crypto pki trustpoint SSLVPN
      revocation-check crl
      rsakeypair SSLVPN

crypto pki certificate chain SSLVPN
      certificate 77220E6A00000000130E
.
.
.
```

## Configuring WebVPN

To configure WebVPN functionality on your router, perform the following steps. All steps except Step 1 and Step 2 are optional.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn enable** [*gateway-addr ip-address*]
4. **webvpn**
5. **title** *title-string*
6. **login-message** *message-string*
7. **title-color** *color*
8. **secondary-color** *color*
9. **text-color** [**black** | **white**]
10. **secondary-text-color** [**black** | **white**]
11. **idle-timeout** *seconds*
12. **ssl encryption** [**3des-sha1**] [**des-sha-1**] [**rc4-md5**]
13. **ssl trustpoint** *trustpoint-name*
14. **port-forward** {*list list-name*} {**local-port** *port-number*} {**remote-server** *server-name-or-ip-address*} {**remote-port** *port-number*}
15. **url-list** *list-name*
16. **logo** [**file** *filename* | **none**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>webvpn enable [gateway-addr ip-address]</code>  <b>Example:</b> <code>Router (config)# webvpn enable</code>	Enables WebVPN in the system. <ul style="list-style-type: none"><li>• The <b>gateway-addr</b> keyword and <i>ip-address</i> argument enable WebVPN on only the IP address that is specified.</li></ul>
Step 4	<code>webvpn</code>  <b>Example:</b> <code>Router (config)# webvpn</code>	Enters the WebVPN configuration mode.
Step 5	<code>title title-string</code>  <b>Example:</b> <code>Router (config-webvpn)# title "Secure Corporate Access: Unauthorized users prohibited"</code>	(Optional) Enters the HTML title string that is shown in the browser title and on the title bar (also known as the banner).
Step 6	<code>login-message message-string</code>  <b>Example:</b> <code>Router (config-webvpn)# login-message "Please enter your username and password"</code>	(Optional) Configures the HTML that prompts the user to log in to a web VPN.
Step 7	<code>title-color color</code>  <b>Example:</b> <code>Router (config-webvpn)# title-color green</code>	(Optional) Specifies the color of the title bars on the login, home, and file access pages.
Step 8	<code>secondary-color color</code>  <b>Example:</b> <code>Router (config-webvpn)# secondary-color yellow</code>	(Optional) Specifies the color of the secondary title bars on the login, home, and file access pages.
Step 9	<code>text-color [black   white]</code>  <b>Example:</b> <code>Router (config-webvpn)# text-color black</code>	(Optional) Sets the color of the text on the title bars.
Step 10	<code>secondary-text-color [black   white]</code>  <b>Example:</b> <code>Router (config-webvpn)# secondary-text-color black</code>	(Optional) Specifies the color of the text on the secondary bars.

	Command or Action	Purpose
Step 11	<code>idle-timeout seconds</code>  <b>Example:</b> Router (config-webvpn)# idle-timeout 60	(Optional) Sets the default idle timeout.
Step 12	<code>ssl encryption [3des-sha1] [des-sha-1] [rc4-md5]</code>  <b>Example:</b> Router (config-webvpn)# ssl encryption 3des-sha1	Specifies the encryption algorithms that the SSL protocol will use for a SSL Virtual Private Network (SSLVPN).
Step 13	<code>ssl trustpoint trustpoint-name</code>  <b>Example:</b> Router (config-webvpn)# ssl trustpoint Trustpoint1	Specifies the certificate trustpoint.
Step 14	<code>port-forward {list list-name} {local-port port-number} {remote-server server-name-or-ip-address} {remote-port port-number}</code>  <b>Example:</b> Router (config-webvpn)# port-forward list POP3 local-port 60002 remote-server mail.youremail.com remote-port 25	Lists the set of forwarded ports to which a user has access.
Step 15	<code>url-list list-name</code>  <b>Example:</b> Router (config-webvpn)# url-list My List	Configures the list of URLs to which a user has access on the portal page of a SSL VPN and enters URL configuration mode.
Step 16	<code>logo [file filename   none]</code>  <b>Example:</b> Router (config-webvpn-url)# logo file flash://webvpn/company-logo.gif.	(Optional) Specifies the custom logo image that is displayed on the login and portal pages.

## Defining Encryption Algorithms for the SSL Protocol

To define the encryption algorithms that the SSL protocol will use, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn enable [gateway-addr ip-address]**
4. **webvpn**
5. **ssl encryption [3des-sha1] [des-sha1] [rc4-md5]**
6. **ssl trustpoint trustpoint-name**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>webvpn enable [gateway-addr ip-address]</code>  <b>Example:</b> <code>Router (config)# webvpn enable</code>	Enables WebVPN in the system.
Step 4	<code>webvpn</code>  <b>Example:</b> <code>Router (config)# webvpn</code>	Enters WebVPN configuration mode.
Step 5	<code>ssl encryption [3des-sha1] [des-sha1] [rc4-md5]</code>  <b>Example:</b> <code>Router (config-webvpn)# ssl encryption 3des-sha1</code>	Specifies the encryption algorithms.
Step 6	<code>ssl trustpoint trustpoint-name</code>  <b>Example:</b> <code>Router (config-webvpn)# ssl trustpoint Trustpoint1</code>	Specifies the certificate trustpoint.

## Displaying URL Entries on the Portal Page

To display a list of URLs on the portal page from which users may access common resources, perform the following steps.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `webvpn enable [gateway-addr ip-address]`
4. `webvpn`
5. `url-list list-name`
6. `heading heading-name`
7. `url-text text url-value URL`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>webvpn enable [gateway-addr ip-address]</code>  <b>Example:</b> Router (config)# <code>webvpn enable</code>	Enables WebVPN in the system.
Step 4	<code>webvpn</code>  <b>Example:</b> Router (config)# <code>webvpn</code>	Enters WebVPN configuration mode.
Step 5	<code>url-list list-name</code>  <b>Example:</b> Router (config-webvpn)# <code>url-list englist</code>	Configures the list of URLs to which a user has access on the portal page.
Step 6	<code>heading heading-name</code>  <b>Example:</b> Router (config-webvpn-url)# <code>heading Engineering</code>	Sets the heading that is displayed above all URLs on the portal page.
Step 7	<code>url-text text url-value URL</code>  <b>Example:</b> Router (config-webvpn-url)# <code>url-text ENG</code> <code>url-value http://www.eng.mycompany.com</code>	Sets the text of the link to be displayed on the home page and the URL that is under the link.

## Maintaining and Monitoring Your WebVPN Functionality

To maintain and monitor your WebVPN functionality, you may use the following **debug** and **show** commands. The **enable** command is required for each **debug** and **show** command.

## SUMMARY STEPS

1. `enable`
2. `debug webvpn [aaa | cookie | dns | http | port-forward | webservice]`
3. `show webvpn sessions`
4. `show webvpn statistics`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<code>debug webvpn [aaa   cookie   dns   http   port-forward   webservice]</code>  <b>Example:</b> Router# debug webvpn port-forward	Enables web VPN session monitoring.
Step 3	<code>show webvpn sessions</code>  <b>Example:</b> Router# show webvpn sessions	Displays information about WebVPN sessions.
Step 4	<code>show webvpn statistics</code>  <b>Example:</b> Router# show webvpn statistics	Displays WebVPN statistics.

## Examples

The following examples show **debug webvpn** output for various WebVPN sessions:

```
Router# debug webvpn
```

```
*Jan 19 03:05:22.796: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
    Data buffer(buffer: 0x0D2EF888, data: 0x1A7E756C, len: 335, offset: 0, domain:
0)
*Jan 19 03:05:22.796: SSLVPN: http request: / with domain cookie
*Jan 19 03:05:22.796: SSLVPN: [Q]Client side Chunk data written..
    buffer=0x0D2EF748 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.796: SSLVPN: Client side Chunk data written..
    buffer=0x0D2EF8A8 total_len=1167 bytes=1167 tcb=0x0C5920C8
*Jan 19 03:05:22.836: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
    Data buffer(buffer: 0x0D2EF888, data: 0x1A7E836C, len: 383, offset: 0, domain:
0)
*Jan 19 03:05:22.836: SSLVPN: http request: /paramdef.js with domain cookie
*Jan 19 03:05:22.836: SSLVPN: Created 323 byte content data to send to external client
*Jan 19 03:05:22.836: SSLVPN: Client side Chunk data written..
    buffer=0x0D2EF8A8 total_len=440 bytes=440 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
    Data buffer(buffer: 0x0D2EF888, data: 0x1A7E916C, len: 381, offset: 0, domain:
0)
*Jan 19 03:05:22.860: SSLVPN: http request: /shared.js with domain cookie
*Jan 19 03:05:22.860: SSLVPN: [Q]Client side Chunk data written..
    buffer=0x0D2EF8A8 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Client side Chunk data written..
    buffer=0x0D2EF748 total_len=986 bytes=986 tcb=0x0C5920C8
*Jan 19 03:05:22.896: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
    Data buffer(buffer: 0x0D2EF888, data: 0x1A7E9F6C, len: 384, offset: 0, domain:
0)
*Jan 19 03:05:22.896: SSLVPN: http request: /img/logo.gif with domain cookie
*Jan 19 03:05:22.896: SSLVPN: Created 552 byte content data to send to external client
```

```
*Jan 19 03:05:22.896: SSLVPN: Client side Chunk data written..
  buffer=0x0D2EF748 total_len=669 bytes=669 tcb=0x0C5920C8
```

The following is sample output when authentication has failed and when authentication has passed:

```
Router# debug webvpn
```

```
*Jan 19 03:08:28.428: SSLVPN: AAA authentication request sent for user: "cisco"
*Jan 19 03:08:28.428: SSLVPN: AAA Authentication Failed !

*Jan 19 03:08:42.148: SSLVPN: AAA authentication request sent for user: "cisco"
*Jan 19 03:08:42.148: SSLVPN: AAA Authentication Passed !
```

The following sample output displays WebVPN cookie output during login:

```
Router# debug webvpn cookie
```

```
*Jan 19 03:10:38.880: SSLVPN: ipaddr: 172.107.163.142, index: 11, time: 3315093038,
random: 210936245
*Jan 19 03:10:38.880: SSLVPN: Created gateway cookie:
2154537870@11@3315093038@210936245@ssl-vpn
*Jan 19 03:10:38.900: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 128.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn
*Jan 19 03:10:39.348: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 172.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn
```

The following sample output displays WebVPN cookie information during the browsing of a website that is serving cookies:

```
Router# debug webvpn cookie
```

```
*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
  buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
  cookie: 0x1A8BBFB5, length: 152
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Set-Cookie
*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
  buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
  cookie: 0x1A8BBFC1, length: 140
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: expires
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Sun, 17-Jan-2038
19:14:07 GMT
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: path
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: /
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: domain
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: .google.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .google.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .google.com
*Jan 19 03:12:10.484: SSLVPN: Enter Cookie unmangler with Context: 0x0D2B1EB0,
  buffer: 0x0D2EF728, buffer->data: 0x1A8BCD6C, buffer->len: 589,
  cookie: 0x1A8BCEA3, length: 276
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: Cookie
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
11@73@3315093130@3318152330
```

```

*Jan 19 03:12:10.484: SSLVPN: Received internal cookie 11@73@3315093130@3318152330 is
converted to gw-index: 11, int-index: 73, time: 3315093130, rand: 3318152330
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: .google.com
*Jan 19 03:12:10.484: SSLVPN: Cookie domain- unmangled request matched
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.488: SSLVPN: Unlimited cookie parser element display:
CP_GUTC=128.107.163.142.1100045930344008
*Jan 19 03:12:10.488: SSLVPN: Not a mangled internal cookie - ignore
*Jan 19 03:12:10.488: SSLVPN: Limited cookie parser element display:
2154537870@11@3315093038@210936245@ssl-vpn
*Jan 19 03:12:10.488: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 128.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn

```

The following sample output displays WebVPN HTTP during browsing:

```
Router# debug webvpn http
```

```

*Jan 19 03:16:15.164: Original client request
*Jan 19 03:16:15.164: GET /http/0/gmail.google.com/gmail/help/about.html HTTP/1.1
*Jan 19 03:16:15.164:
*Jan 19 03:16:15.164: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.164: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.200: Original server response

*Jan 19 03:16:15.200: HTTP/1.1 200 OK
*Jan 19 03:16:15.200:
*Jan 19 03:16:15.200: SSLVPN: Content type requires mangling
*Jan 19 03:16:15.236: Original client request

*Jan 19 03:16:15.236: GET /http/0/gmail.google.com/gmail/help/images/logo.gif HTTP/1.1
*Jan 19 03:16:15.236:
*Jan 19 03:16:15.236: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.236: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.264: Original server response

*Jan 19 03:16:15.264: HTTP/1.1 200 OK
*Jan 19 03:16:15.264:
*Jan 19 03:16:15.264: SSLVPN: Contents need no mangling, parse no more
*Jan 19 03:16:15.264: All contents seen in HTTP_RES_PARSE_NOMORE
*Jan 19 03:16:15.264: SSLVPN: Deallocating HTTP info
*Jan 19 03:16:15.276: Original client request

*Jan 19 03:16:15.276: GET
/http/0/gmail.google.com/gmail/help/images/corner_tl_sharp.gif HTTP/1.1 *Jan 19
03:16:15.276:
*Jan 19 03:16:15.276: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.276: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.296: Original server response

*Jan 19 03:16:15.296: HTTP/1.1 200 OK
*Jan 19 03:16:15.296:
*Jan 19 03:16:15.296: SSLVPN: Contents need no mangling, parse no more
*Jan 19 03:16:15.296: *** Parsing of response body over
*Jan 19 03:16:15.296: SSLVPN: Deallocating HTTP info

```

The following sample output displays WebVPN web service information:

```
Router# debug webvpn webservice
```

```

*Jan 19 03:18:39.060: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT

```

```

*Jan 19 03:18:39.060: SSLVPN: Created 2608 byte content data to send to external client
for requested file: /webvpn.html
*Jan 19 03:18:39.100: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Created 2459 byte content data to send to external client
for requested file: /shared.js
*Jan 19 03:18:39.152: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:47.496: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:47.496: SSLVPN: Created 1375 byte content data to send to external client
for requested file: /logon.html
*Jan 19 03:18:47.516: SSLVPN: HTTP request: 0, path: /paramdef.js
*Jan 19 03:18:47.516: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:48.036: SSLVPN: HTTP request: 0, path: /index.html
*Jan 19 03:18:48.036: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.036: SSLVPN: Created 8269 byte content data to send to external client
for requested file: /index.html
*Jan 19 03:18:48.220: SSLVPN: HTTP request: 0, path: /toolbarframe.html
*Jan 19 03:18:48.220: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.220: SSLVPN: Created 1312 byte content data to send to external client
for requested file: /toolbarframe.html
*Jan 19 03:18:48.256: SSLVPN: HTTP request: 0, path: /img/logo.gif
*Jan 19 03:18:48.256: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: HTTP request: 0, path: /test.html
*Jan 19 03:18:48.268: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: Created 684 byte content data to send to external client for
requested file: /test.html
*Jan 19 03:18:48.316: SSLVPN: HTTP request: 0, path: /toolbar.html
*Jan 19 03:18:48.316: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.316: SSLVPN: Created 2618 byte content data to send to external client
for requested file: /toolbar.html
*Jan 19 03:18:48.364: SSLVPN: HTTP request: 0, path: /tools.html
*Jan 19 03:18:48.364: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.364: SSLVPN: Created 2284 byte content data to send to external client
for requested file: /tools.html

```

## Troubleshooting WebVPN

The following situations may occur when using the WebVPN feature:

The user is unable to establish an SSL connection to the WebVPN gateway. Verify whether the TCP listeners are correctly created using the **show tcp brief all** command. The listener on port 80 is used for redirecting HTTP connections to HTTPS connections. The listener on port 443 is an HTTPS listener.

```
Router# show tcp brief all
```

TCB	Local Address	Foreign Address	(state)
652998D8	*.80	*.*	LISTEN
64CDDE00	*.443	*.*	LISTEN
6548B37C	*.5060	*.*	LISTEN
652D3928	*.1723	*.*	LISTEN

If services that use an HTTP secure server are enabled along with WebVPN on the same router, WebVPN must be enabled with the **gateway-addr** keyword option of the **webvpn enable** command by specifying the IP address to enable web VPN service. Two TCP listeners can be seen in the output of the **show tcp brief all** command as follows:

```
Router# show tcp brief all

TCB                Local Address      Foreign Address    (state)
652998D8           *.80               *.*               LISTEN
64CDDE00           *.443              *.*               LISTEN
6548B37C           *.5060             *.*               LISTEN
652D3928           *.1723             *.*               LISTEN
632988C8           10.1.1.1.80       *.*               LISTEN
63CDDE1F           10.1.1.1.443     *.*               LISTEN
```

In the above example, TCP traffic for port 443, which is destined for this router and not on IP address 10.1.1.1, is handled by TCB listener 64CDDE00. Web VPN traffic is handled by TCB listener 63CDDE1F.

If a cookie is not enabled properly on a browser, WebVPN may not work. For example, if a cookie is set to "High" in Internet Explorer (at Tools>Internet Options>Privacy), a user cannot log into WebVPN. In this situation, the cookie has to be set no higher than "Medium High."

## Configuration Examples for WebVPN

This section provides the following configuration examples:

- [WebVPN Enabled Globally: Example, page 24](#)
- [WebVPN Enabled on a Specific IP Address: Example, page 25](#)

### WebVPN Enabled Globally: Example

The following is sample running configuration for WebVPN that is enabled globally (on all IP addresses in the system).

```
Router# show running-config

webvpn enable
!
webvpn
 logo file flash:/mylogo.gif
 title-color #FF9933
 text-color black
 ssl encryption 3des-sha1 rc4-md5
 ssl trustpoint WebVPN
 url-list "quicklinks"
   heading "Quicklinks"
   url-text "Meetings and Conferences" url-value
"http://www.mydomain.com/resources/meetings.html"
 url-text "Floor maps" url-value "http://www.mydomain.com/resources/floormaps.html"
 url-text "Documentation" url-value "http://www.mydomain.com/eng/documents"
 url-list "Departments"
   url-text "Engineering" url-value "http://www.mydomain.com/eng"
   url-text "Human Resources" url-value "http://www.mydomain.com/HR"
```

```

url-text "Sales and Marketing" url-value "http://www.mydomain.com/sandm"
url-text "Operations" url-value "http://www.mydomain.com/ops"

login-message "Enter your email-id and password"
!
```

## WebVPN Enabled on a Specific IP Address: Example

The following is sample output from a running configuration for WebVPN that is enabled on IP address 10.1.1.1. This configuration also enables e-mail.

```
Router# show running-config
```

```

access via port-forwarding.

!
webvpn enable gateway-addr 10.1.1.1
!
webvpn
 logo file flash:/mylogo.gif
 title-color #FF9933
 text-color black
 ssl encryption 3des-sha1 rc4-md5
 ssl trustpoint WebVPN
 url-list "Search"
   heading "Search Engines"
   url-text "Google" url-value "http://www.google.com"
   url-text "Altavista" url-value "http://www.altavista.com"
   url-text "Ask Jeeves" url-value "http://www.askjeeves.com"
 login-message "Enter your email-id and password"
 port-forward list IMAP local-port 60013 remote-server mail.yourdomain.com remote-port 143
 port-forward list POP3 local-port 60014 remote-server mail.yourdomain.com remote-port 25
 port-forward list SMTP local-port 60015 remote-server mail.yourdomain.com remote-port 110
```

## Additional References

The following sections provide references related to WebVPN.

### Related Documents

Related Topic	Document Title
Cisco IOS security commands	<a href="#">Cisco IOS Security Command Reference</a> , Release 12.3T
Other Cisco IOS commands	<a href="#">Cisco IOS Command Reference</a> , Release 12.3T

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

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

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3T command reference publications.

- [debug webvpn](#)
- [heading](#)
- [idle-timeout](#)
- [login-message](#)
- [logo](#)
- [port-forward](#)
- [secondary-color](#)
- [secondary-text-color](#)
- [show webvpn sessions](#)
- [show webvpn statistics](#)
- [ssl encryption](#)
- [ssl trustpoint](#)

- [text-color](#)
- [title](#)
- [title-color](#)
- [url-list](#)
- [url-text](#)
- [webvpn](#)
- [webvpn enable](#)

# debug webvpn

To enable Web VPN session monitoring, use the **debug webvpn** command in privileged EXEC mode. To disable the Web VPN session monitoring, use the **no** form of this command.

**debug webvpn** [**aaa** | **cookie** | **dns** | **http** | **port-forward** | **webservice**]

**no debug webvpn** [**aaa** | **cookie** | **dns** | **http** | **port-forward** | **webservice**]

## Syntax Description

<b>aaa</b>	(Optional) Displays authentication, authorization, and accounting (AAA) debug messages.
<b>cookie</b>	(Optional) Displays cookie debug messages.
<b>http</b>	(Optional) Displays domain name system (DNS) messages.
<b>port-forward</b>	(Optional) Displays port-forwarding debug messages.
<b>webservice</b>	(Optional) Displays web service debug messages.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Examples

The following examples show **debug webvpn** output for various WebVPN sessions:

```
Router# debug webvpn

*Jan 19 03:05:22.796: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
      Data buffer(buffer: 0x0D2EF888, data: 0x1A7E756C, len: 335, offset: 0, domain:
0)
*Jan 19 03:05:22.796: SSLVPN: http request: / with domain cookie
*Jan 19 03:05:22.796: SSLVPN: [Q]Client side Chunk data written..
      buffer=0x0D2EF748 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.796: SSLVPN: Client side Chunk data written..
      buffer=0x0D2EF8A8 total_len=1167 bytes=1167 tcb=0x0C5920C8
*Jan 19 03:05:22.836: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
      Data buffer(buffer: 0x0D2EF888, data: 0x1A7E836C, len: 383, offset: 0, domain:
0)
*Jan 19 03:05:22.836: SSLVPN: http request: /paramdef.js with domain cookie
*Jan 19 03:05:22.836: SSLVPN: Created 323 byte content data to send to external client
*Jan 19 03:05:22.836: SSLVPN: Client side Chunk data written..
      buffer=0x0D2EF8A8 total_len=440 bytes=440 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
      Data buffer(buffer: 0x0D2EF888, data: 0x1A7E916C, len: 381, offset: 0, domain:
0)
*Jan 19 03:05:22.860: SSLVPN: http request: /shared.js with domain cookie
*Jan 19 03:05:22.860: SSLVPN: [Q]Client side Chunk data written..
      buffer=0x0D2EF8A8 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Client side Chunk data written..
      buffer=0x0D2EF748 total_len=986 bytes=986 tcb=0x0C5920C8
*Jan 19 03:05:22.896: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
```

```

    Data buffer(buffer: 0x0D2EF888, data: 0x1A7E9F6C, len: 384, offset: 0, domain:
0)
*Jan 19 03:05:22.896: SSLVPN: http request: /img/logo.gif with domain cookie
*Jan 19 03:05:22.896: SSLVPN: Created 552 byte content data to send to external client
*Jan 19 03:05:22.896: SSLVPN: Client side Chunk data written..
    buffer=0x0D2EF748 total_len=669 bytes=669 tcb=0x0C5920C8

```

The following is sample output when authentication has failed and when authentication has passed:

```
Router# debug webvpn
```

```

*Jan 19 03:08:28.428: SSLVPN: AAA authentication request sent for user: "cisco"
*Jan 19 03:08:28.428: SSLVPN: AAA Authentication Failed !

*Jan 19 03:08:42.148: SSLVPN: AAA authentication request sent for user: "cisco"
*Jan 19 03:08:42.148: SSLVPN: AAA Authentication Passed !

```

The following sample output displays WebVPN cookie output during login:

```
Router# debug webvpn cookie
```

```

*Jan 19 03:10:38.880: SSLVPN: ipaddr: 172.107.163.142, index: 11, time: 3315093038,
random: 210936245
*Jan 19 03:10:38.880: SSLVPN: Created gateway cookie:
2154537870@11@3315093038@210936245@ssl-vpn
*Jan 19 03:10:38.900: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 128.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn
*Jan 19 03:10:39.348: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 172.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn

```

The following sample output displays WebVPN cookie information during the browsing of a website that is serving cookies:

```
Router# debug webvpn cookie
```

```

*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
    buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
    cookie: 0x1A8BBFB5, length: 152
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Set-Cookie
*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
    buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
    cookie: 0x1A8BBFC1, length: 140
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: expires
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Sun, 17-Jan-2038
19:14:07 GMT
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: path
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: /
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: domain
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: .google.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .google.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .google.com
*Jan 19 03:12:10.484: SSLVPN: Enter Cookie unmangler with Context: 0x0D2B1EB0,
    buffer: 0x0D2EF728, buffer->data: 0x1A8BCD6C, buffer->len: 589,
    cookie: 0x1A8BCEA3, length: 276
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: Cookie

```

```

*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
11@73@3315093130@3318152330
*Jan 19 03:12:10.484: SSLVPN: Received internal cookie 11@73@3315093130@3318152330 is
converted to gw-index: 11, int-index: 73, time: 3315093130, rand: 3318152330
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: .google.com
*Jan 19 03:12:10.484: SSLVPN: Cookie domain- unmangled request matched
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.488: SSLVPN: Unlimited cookie parser element display:
CP_GUTC=128.107.163.142.1100045930344008
*Jan 19 03:12:10.488: SSLVPN: Not a mangled internal cookie - ignore
*Jan 19 03:12:10.488: SSLVPN: Limited cookie parser element display:
2154537870@11@3315093038@210936245@ssl-vpn
*Jan 19 03:12:10.488: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 128.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn

```

The following sample output displays WebVPN HTTP during browsing:

```
Router# debug webvpn http
```

```

*Jan 19 03:16:15.164: Original client request
*Jan 19 03:16:15.164: GET /http/0/gmail.google.com/gmail/help/about.html HTTP/1.1
*Jan 19 03:16:15.164:
*Jan 19 03:16:15.164: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.164: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.200: Original server response

*Jan 19 03:16:15.200: HTTP/1.1 200 OK
*Jan 19 03:16:15.200:
*Jan 19 03:16:15.200: SSLVPN: Content type requires mangling
*Jan 19 03:16:15.236: Original client request

*Jan 19 03:16:15.236: GET /http/0/gmail.google.com/gmail/help/images/logo.gif HTTP/1.1
*Jan 19 03:16:15.236:
*Jan 19 03:16:15.236: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.236: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.264: Original server response

*Jan 19 03:16:15.264: HTTP/1.1 200 OK
*Jan 19 03:16:15.264:
*Jan 19 03:16:15.264: SSLVPN: Contents need no mangling, parse no more
*Jan 19 03:16:15.264: All contents seen in HTTP_RES_PARSE_NOMORE
*Jan 19 03:16:15.264: SSLVPN: Deallocating HTTP info
*Jan 19 03:16:15.276: Original client request

*Jan 19 03:16:15.276: GET
/http/0/gmail.google.com/gmail/help/images/corner_tl_sharp.gif HTTP/1.1 *Jan 19
03:16:15.276:
*Jan 19 03:16:15.276: SSLVPN: HTTP Header parsing complete
*Jan 19 03:16:15.276: SSLVPN: * HTTP request complete
*Jan 19 03:16:15.296: Original server response

*Jan 19 03:16:15.296: HTTP/1.1 200 OK
*Jan 19 03:16:15.296:
*Jan 19 03:16:15.296: SSLVPN: Contents need no mangling, parse no more
*Jan 19 03:16:15.296: *** Parsing of response body over
*Jan 19 03:16:15.296: SSLVPN: Deallocating HTTP info

```

The following sample output displays WebVPN web service information:

Router# **debug webvpn webservice**

```
*Jan 19 03:18:39.060: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.060: SSLVPN: Created 2608 byte content data to send to external client
for requested file: /webvpn.html
*Jan 19 03:18:39.100: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Created 2459 byte content data to send to external client
for requested file: /shared.js
*Jan 19 03:18:39.152: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:47.496: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:47.496: SSLVPN: Created 1375 byte content data to send to external client
for requested file: /logon.html
*Jan 19 03:18:47.516: SSLVPN: HTTP request: 0, path: /paramdef.js
*Jan 19 03:18:47.516: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:48.036: SSLVPN: HTTP request: 0, path: /index.html
*Jan 19 03:18:48.036: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.036: SSLVPN: Created 8269 byte content data to send to external client
for requested file: /index.html
*Jan 19 03:18:48.220: SSLVPN: HTTP request: 0, path: /toolbarframe.html
*Jan 19 03:18:48.220: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.220: SSLVPN: Created 1312 byte content data to send to external client
for requested file: /toolbarframe.html
*Jan 19 03:18:48.256: SSLVPN: HTTP request: 0, path: /img/logo.gif
*Jan 19 03:18:48.256: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: HTTP request: 0, path: /test.html
*Jan 19 03:18:48.268: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: Created 684 byte content data to send to external client for
requested file: /test.html
*Jan 19 03:18:48.316: SSLVPN: HTTP request: 0, path: /toolbar.html
*Jan 19 03:18:48.316: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.316: SSLVPN: Created 2618 byte content data to send to external client
for requested file: /toolbar.html
*Jan 19 03:18:48.364: SSLVPN: HTTP request: 0, path: /tools.html
*Jan 19 03:18:48.364: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.364: SSLVPN: Created 2284 byte content data to send to external client
for requested file: /tools.html
```

The field descriptions in the above displays are self-explanatory.

#### Related Commands

Command	Description
<b>webvpn</b>	Enters WebVPN configuration mode.

# heading

To set the heading that is displayed above all URLs on the portal page of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **heading** command in Web VPN URL configuration mode. To remove the heading, use the **no** form of this command.

**heading** *heading-name*

**no heading** *heading-name*

Syntax Description	<i>heading-name</i>	Name of the heading.
--------------------	---------------------	----------------------

Defaults	A URL list is not configured.
----------	-------------------------------

Command Modes	Web VPN URL configuration
---------------	---------------------------

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines	This command sets the headings that are displayed above all URLs on the portal page.
------------------	--

Examples	The following example shows that the heading has been set to “Engineering”:
----------	---

```
Router (config) webvpn
Router (config-webvpn)# url-list englist
Router (config-webvpn-url)# heading Engineering
```

Related Commands	Command	Description
	<b>url-list</b>	Configures the list of URLs to which a user has access on the portal page of a SSLVPN and enters URL configuration mode
	<b>webvpn</b>	Enters Web VPN configuration mode.

# idle-timeout

To set the default idle timeout for a Secure Sockets Layer Virtual Private Network (SSLVPN) if no idle timeout has been defined or if the idle timeout is zero (0), use the **idle-timeout** command in Web VPN configuration mode. To revert to the default value, use the **no** form of this command.

**idle-timeout** [**never** | *seconds*]

**no idle-timeout** [**never** | *seconds*]

Syntax Description	never	(Optional) The idle timeout function is disabled.
	<i>seconds</i>	(Optional) Idle timeout in seconds. The values are from 180 seconds (3 minutes) to 86400 seconds (24 hours).

**Defaults** If command is not configured, the default idle timeout is 1800 seconds (30 minutes).

**Command Modes** Web VPN configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** Configuring this command prevents stale sessions.

**Examples** The following example shows that the idle timeout has been set for 1200 seconds:

```
Router (config)# webvpn
Router (config-webvpn)# idle-timeout 1200
```

The following example shows that the idle timeout function is disabled:

```
Router (config)# webvpn
Router (config-webvpn)# idle-timeout never
```

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

# login-message

To configure a message for a user login text box on the login page, use the **login-message** command in Web VPN configuration mode. To reset the value to the default, use the **no** form of this command.

**login-message** *message-string*

**no login-message** *message-string*

<b>Syntax Description</b>	<i>message-string</i>	Limited to 255 characters. The default is “Please enter your username and password.” The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. To have no login message, the <b>login-message</b> command is issued without a string.
---------------------------	-----------------------	---

<b>Defaults</b>	Message will be “Please enter your username and password.”
-----------------	--

<b>Command Modes</b>	Web VPN configuration
----------------------	-----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

<b>Usage Guidelines</b>	If you type the <b>login-message</b> command and then press the <b>Enter</b> key, no login message will be displayed.
-------------------------	---

<b>Examples</b>	The following example shows that the login message to be displayed is “Please enter your login credentials.”
-----------------	--

```
Router (config-webvpn)# login-message "Please enter your login credentials."
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>webvpn</b>	Enters Web VPN configuration mode.

# logo

To specify the custom logo image that is displayed on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **logo** command in Web VPN configuration mode. To remove the logo, use the **no** form of this command.

**logo** [*file filename* | **none**]

**no logo** [*file filename* | **none**]

Syntax Description	file <i>filename</i>	(Optional) Limited to 255 characters. The logo must be a GIF, JPG, or PNG file and must be less than 100 kilobytes (KBs). An error will occur if the file does not exist. If the logo file is subsequently deleted, no logo is displayed. The default is to use the Cisco logo.
	<b>none</b>	(Optional) No logo will be displayed.

**Defaults** No logo is displayed.

**Command Modes** Web VPN configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Examples** The following example shows that a logo file (mylogo.gif) is being configured in flash: media:

```
logo file flash:/mylogo.gif
```

The following example shows that no logo is to be displayed in the login or portal pages:

```
logo none
```

The following example shows that the logo is set to the default logo, which is the Cisco logo:

```
no logo
```

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

# port-forward

To list the set of forwarded ports to which a user has access, use the **port-forward** command in Web VPN configuration mode. To remove ports, use the **no** form of this command.

**port-forward** {**list** *list-name*} {**local-port** *port-number*} {**remote-server** *server-name-or-IP-address*} {**remote-port** *port-number*}

**no port-forward** {**list** *list-name*} {**local-port** *port-number*} {**remote-server** *server-name-or-IP-address*} {**remote-port** *port-number*}

Syntax Description		
<b>list</b> <i>list-name</i>		Used to group port-forwarding entries into a list that can be applied to a username or group policy. Multiple entries may be specified for a given list name.
<b>local-port</b> <i>port-number</i>		Specifies the local port that is listened upon. A local port value may be used only once within a given list name. Values may be from 1 through 65535.
<b>remote-server</b> <i>server-name-or-IP-address</i>		Specifies the domain name system (DNS) name or IP address of the remote server to which the user will connect (usually the name or IP address of an e-mail server).
<b>remote-port</b> <i>port-number</i>		Specifies the port on the remote server to which the user will connect. The port value may be from 1 through 65535.

**Defaults** None

**Command Modes** Web VPN configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** This command is used for TCP port forwarding.

**Examples** The following example shows that the list name is POP3, the local port is 60002, the remote server is mail.youremail.com, and the remote port number is 25:

```
Router (config)# webvpn
Router (config-webvpn)# port-forward list POP3 local-port 60002 remote-server
mail.youremail.com remote-port 25
```

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

# secondary-color

To specify the color of the secondary title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **secondary-color** command in Web VPN configuration mode. To remove the color, use the **no** form of this command.

**secondary-color** *color*

**no secondary-color** *color*

## Syntax Description

*color*

The value can be a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a “#”), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):

- `\#/x{6}`
- `\d{1,3},\d{1,3},\d{1,3}` (and each number is from 1 to 255)
- `\w+`

The default is purple.

## Defaults

Purple

## Command Modes

Web VPN configuration

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Usage Guidelines

If a new color is configured, it will override the color that was already configured.

## Examples

The following examples show three ways that a secondary color may be configured:

```
secondary-color darkseagreen
```

```
secondary-color #8FBC8F
```

```
secondary-color 143,188,143
```

## Related Commands

Command	Description
<b>webvpn</b>	Enters Web VPN configuration mode.

## secondary-text-color

To specify the color of the text on the secondary bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **secondary-text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

**secondary-text-color** [**black** | **white**]

**no secondary-text-color** [**black** | **white**]

Syntax Description	<b>black</b>	(Optional) Color of the text is black. This is the default value.
	<b>white</b>	(Optional) Color of the text is white.

**Defaults** Color of the text is black.

**Command Modes** Web VPN configuration

Command History	Release	Modification
	12.3(14)T	

**Usage Guidelines** The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

**Examples** The following example shows that the secondary text color has been set to white:

```
secondary-text-color white
```

Related Commands	Command	Description
	<b>webvpn</b>	

# show webvpn sessions

To display information about Web VPN sessions, use the **show webvpn sessions** command in privileged EXEC mode.

## show webvpn sessions

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.3(14)T	This command was introduced.

### Examples

The following output example displays information about a WebVPN session:

```
Router# show webvpn sessions

WebVPN domain name: cisco.com
Client Login Name      Client IP Address      Number of Connections
webuser                172.107.163.142       4
    Created 00:14:25, Last-used 00:00:10
    Client Port: 2366
    Client Port: 2386
    Client Port: 2396
    Client Port: 2486
browseruser           172.107.163.142       2
    Created 00:00:09, Last-used 00:00:08
    Client Port: 2431
    Client Port: 2432
```

[Table 1](#) describes the significant fields shown in the display.

**Table 1** show webvpn sessions Command Field Descriptions

Field	Description
Client Login Name	Username used to log in to the WebVPN gateway.
Client IP Address	IP address of the host from which the user is connecting.
Number of Connections	Number of active TCP connections by the user at this point.
Created	Provides the time that has elapsed since the user logged in (in HH:MM:SS format).
Client Port	Local TCP port used on the client host.

### Related Commands

Command	Description
<b>show webvpn statistics</b>	Displays WebVPN statistics.

# show webvpn statistics

To display WebVPN statistics, use the **show webvpn statistics** command in privileged EXEC mode.

## show webvpn statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Examples** The following is sample output using the **show webvpn statistics** command:

```
Router# show webvpn statistics

Active user sessions: 2
Active user TCP connections: 6
Authentication failures: 3
Terminated user sessions: 0
```

[Table 2](#) describes the significant fields shown in the display.

**Table 2** *show webvpn statistics Command Field Descriptions*

Field	Description
Active user sessions	Number of users who are logged into the system.
Active user TCP connections	Number of TCP user connections that are used by the user session.
Authentication failures	Number of authentication failures to the gateway.
Terminated user sessions	Number of users who logged in and logged out after the statistics were cleared.

Related Commands	Command	Description
	<b>show webvpn sessions</b>	Displays information about WebVPN sessions.

# ssl encryption

To specify the encryption algorithms that the Secure Sockets Layer (SSL) protocol will use for a SSL Virtual Private Network (SSLVPN), use the **ssl encryption** command in Web VPN configuration mode. To remove an algorithm, use the **no** form of this command.

```
ssl encryption [3des-sha1] [des-sha-1] [rc4-md5]
```

```
no ssl encryption [3des-sha1] [des-sha-1] [rc4-md5]
```

## Syntax Description

<b>3des-sha1</b>	(Optional) Encryption algorithm type is 3 DES-SHA1.
<b>des-sha-1</b>	(Optional) Encryption algorithm type is DES-SHA-1.
<b>rc4-md5</b>	(Optional) Encryption algorithm type is RC4-MD5.

## Defaults

All algorithms are available in the order shown above.

## Command Modes

Web VPN configuration

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Usage Guidelines

Configuring this command allows administrators to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

## Examples

The following example shows that 3 DES-SHA1 has been specified as the encryption algorithm:

```
ssl encryption 3des-sha1
```

## Related Commands

Command	Description
<b>webvpn</b>	Enters Web VPN configuration mode.

# ssl trustpoint

To specify the certificate trustpoint, use the **ssl trustpoint** command in Web VPN configuration mode. To remove the trustpoint association, use the **no** form of this command.

**ssl trustpoint** *trustpoint-name*

**no ssl trustpoint** *trustpoint-name*

Syntax Description	<i>trustpoint-name</i>	Name of the trustpoint.

Defaults	The trustpoint name is SSLVPN.

Command Modes	Web VPN configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

Usage Guidelines	No configuration is required if the trustpoint name is SSLVPN.

Examples	The following example shows that the trustpoint name is Mytrustpoint: <pre>ssl trustpoint Mytrustpoint</pre>

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

# text-color

To set the color of the text on the title bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

**text-color** [**black** | **white**]

**no text-color** [**black** | **white**]

Syntax Description	black	(Optional) Color of the text is black. This is the default value
	white	(Optional) Color of the text is white.

**Defaults** Color of the text is black.

**Command Modes** Web VPN configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Usage Guidelines** This command is limited to only two values to limit the number of icons that are on the toolbar.

**Examples** The following example shows that the text color will be white:

```
text-color white
```

Related Commands	Command	Description
	<b>webvpn</b>	Enters Web VPN configuration mode.

# title

To enter the HTML title string that is shown in the browser title and on the title bar for a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **title** command in Web VPN configuration mode. To remove the title, use the **no title** form of this command.

**title** [*title-string*]

**no title** [*title-string*]

<b>Syntax Description</b>	<i>title-string</i>	(Optional) Title string to be displayed in the browser of the user. Limited to 255 characters. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. The default is “WebVPN Service.” If this argument is not configured, a title will not be displayed in the browser of the user.
---------------------------	---------------------	---

**Defaults** If the **title** command is not configured, “WebVPN Service” is displayed in the browser of the user.

**Command Modes** Web VPN configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines** If you type the **title** command and then press the **Enter** key, a title will not be displayed on the browser. If the **no** form of this command is used, the default title string “WebVPN Service” is displayed in the browser of the user.

**Examples** The following example shows the title will be “Secure Corporate Access: Unauthorized users prohibited.”

```
Router (config)# webvpn
Router (config-webvpn)# title "Secure Corporate Access: Unauthorized users prohibited."
```

<b>Syntax Description</b>	<b>Command</b>	<b>Description</b>
	<b>webvpn</b>	Enters Web VPN configuration mode.

# title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **title-color** command in Web VPN configuration mode. To remove the color, use the **no** form of this command.

**title-color** *color*

**no title-color** *color*

## Syntax Description

*color*

The value can be a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a “#”), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):

- \#/x{6}
- \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)
- \w+

The default is purple.

## Defaults

Purple

## Command Modes

Web VPN configuration

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Usage Guidelines

If a new color is configured, it will override the color that was already configured.

## Examples

The following examples show three ways to configure the title color.

```
title-color darkseagreen
```

```
title-color #8FBC8F
```

```
title-color 143,188,143
```

## Related Commands

Command	Description
<b>webvpn</b>	Enters Web VPN configuration mode.

# url-list

To configure the list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSLVPN) and to enter URL configuration mode, use the **url-list** command in Web VPN configuration mode. To remove a URL, use the **no** form of this command.

**url-list** *list-name*

**no url-list** *list-name*

<b>Syntax Description</b>	<i>list-name</i>	URL list name.
---------------------------	------------------	----------------

<b>Defaults</b>	A URL is not shown on the portal page.
-----------------	--

<b>Command Modes</b>	Web VPN configuration
----------------------	-----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Examples** The following example shows that the URL list name is Mylist:

```
url-list Mylist
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>heading</b>	Sets the heading that is displayed above all URLs on the portal page of a SSLVPN.
	<b>url-text</b>	Sets the text of the link to be displayed on the portal page and the URL that is under the link.
	<b>webvpn</b>	Enters Web VPN configuration mode.

# url-text

To set the text of the link that is to be displayed on the portal page and the URL that is under the link, use the **url-text** command in Web VPN URL configuration mode. To remove the text and URL or the text or URL, use the **no** form of this command.

**url-text** *text* **url-value** *URL*

**no url-text** *text* **url-value** *URL*

## Syntax Description

<i>text</i>	Text of the link.
<b>url-value</b> <i>URL</i>	URL of the link.

## Command Modes

Web VPN URL configuration

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Usage Guidelines

There is no checking performed on the URL text or URL value before it is added to the URL list. It is up to the administrator to verify the effect of this command on the portal page.

## Examples

The following example shows that the text for the link to be displayed on the portal page is “ENG” and that the URL is “Mycompany.com”:

```
Router (config)# webvpn
Router (config-webvpn)# url-list englist
Router (config-webvpn-url)# heading Engineering
Router (config-webvpn-url)# url-text ENG url-value http://www.Mycompany.com
```

## Related Commands

Command	Description
<b>heading</b>	Sets the heading that is displayed above all URLs on the portal page of a SSLVPN.
<b>url-list</b>	Configures the list of URLs to which a user has access on the portal page of a SSLVPN and enters URL configuration mode.
<b>webvpn</b>	Enters Web VPN configuration mode.

# webvpn

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

**webvpn**

**no webvpn**

**Syntax Description** This command has no arguments or keywords.

**Defaults** WebVPN configuration mode is not entered.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Examples** The following example shows that Web VPN configuration mode has been entered:

```
Router (config)# webvpn
Router (config-webvpn)#
```

Related Commands	Command	Description
	<b>webvpn enable</b>	Enables WebVPN in the system.

# webvpn enable

To enable WebVPN in the system, use the **webvpn enable** command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

**webvpn enable** [**gateway-addr** *ip-address*]

**no webvpn enable** [**gateway-addr** *ip-address*]

<b>Syntax Description</b>	<b>gateway-addr</b> <i>ip-address</i>	(Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses.
---------------------------	--	--

**Defaults** WebVPN is disabled in the system.

**Command Modes** Web VPN configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines** This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

**Examples** The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>webvpn</b>	Enters Web VPN configuration mode.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.