Configuring WebVPN

This chapter describes WebVPN. WebVPN lets users establish a secure, remote-access VPN tunnel to a security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. These include secure access to the following resources:

- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- Email proxies, including POP3S, IMAP4S, and SMTPS
- MS Outlook Web Access
- MAPI
- Port forwarding for access to other TCP-based applications.

WebVPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to WebVPN resources to users on a group basis. Users have no direct access to resources on the internal network.

This chapter includes the following sections:

Observing WebVPN Security Precautions

WebVPN connections on the security appliance are very different from remote access IPSec connections, particularly with respect to how they interact with SSL-enabled servers, and precautions to reduce security risks.

In a WebVPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When a WebVPN user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore cannot examine and validate the certificate.

The current implementation of WebVPN on the security appliance does not permit communication with sites that present expired certificates. Nor does the security appliance perform trusted CA certificate validation. Therefore, WebVPN users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To minimize the risks involved with SSL certificates:

1. Configure a group policy that consists of all users who need WebVPN access and enable the WebVPN feature only for that group policy.
2. Limit Internet access for WebVPN users. One way to do this is to disable URL entry. Then configure links to specific targets within the private network that you want WebVPN users to be able to access.
3. Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a WebVPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

Understanding Features Not Supported for WebVPN

The security appliance does not support the following features for WebVPN connections:

- Active/Active or Active/Standby Stateful Failover, letting you configure two security appliances so that one takes over operation if the first one fails.
- Inspection features under the Modular Policy Framework, inspecting configuration control.
- Functionality the filter configuration commands provide, including the **vpn-filter** command.
- NAT, reducing the need for globally unique IP addresses.
- PAT, permitting multiple outbound sessions appear to originate from a single IP address.
- QoS, rate limiting using the **police** command and **priority-queue** command.
- Connection limits, checking either via the static or the Modular Policy Framework **set connection** command.
- The **established** command, allowing return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

Using SSL to Access the Central Site

WebVPN uses SSL and its successor, TLS1 to provide a secure connection between remote users and specific, supported internal resources at a central site. This section includes the following topics:

Using HTTPS for WebVPN Sessions

Establishing WebVPN sessions requires the following:

- Using HTTPS to access the security appliance or load balancing cluster. In a web browser, users enter the security appliance IP address in the format *https:// address* where *address* is the IP address or DNS hostname of the security appliance interface.
- Enabling WebVPN sessions on the security appliance interface that users connect to.

To permit WebVPN sessions on an interface, perform the following steps:

Step 1 In global configuration mode, enter the **webvpn** command to enter webvpn mode.

Step 2 Enter the **enable** command with the name of the interface that you want to use for WebVPN sessions.

For example, to enable WebVPN sessions on the interface called outside, enter the following:

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

Note ASA supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.

Setting WebVPN HTTP/HTTPS Proxy

The security appliance can terminate HTTPS connections and forward HTTP/HTTPS requests to HTTP and HTTPS proxy servers. These servers act as intermediaries between users and the Internet. Requiring all Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

To set values for HTTP and HTTPS proxy, enter the **http-proxy** and **https-proxy** commands in webvpn mode.

Configuring SSL/TLS Encryption Protocols

When you set SSL/TLS encryption protocols, be aware of the following:

- Make sure that the security appliance and the browser you use allow the same SSL/TLS encryption protocols.
- If you configure email proxy, do not set the security appliance SSL version to TLSv1 Only. MS Outlook and MS Outlook Express do not support TLS.
- TCP Port Forwarding requires Sun Microsystems Java Runtime Environment (JRE) version 1.4.x and 1.5.x. Port forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

• Negotiate SSLv3	• Java downloads
• Negotiate SSLv3/TLSv1	• Java downloads
• Negotiate TLSv1	• Java does NOT download
• TLSv1Only	• Java does NOT download
• SSLv3Only	• Java does NOT download

Authenticating with Digital Certificates

SSL uses digital certificates for authentication. The security appliance creates a self-signed SSL server certificate when it boots; or you can install in the security appliance an SSL certificate that has been issued in a PKI context. For HTTPS, this certificate must then be installed on the client. You need to install the certificate from a given security appliance only once.

Restrictions for authenticating users with digital certificates include the following:

- Port forwarding does not work for WebVPN users who authenticate using digital certificates. JRE does not have the ability to access the web browser keystore. Therefore JAVA cannot use a certificate that the browser uses to authenticate a user, so it cannot start.
- Email proxy supports certificate authentication with Netscape 7.x email clients only. Other email clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

Enabling Cookies on Browsers for WebVPN

Browser cookies are required for the proper operation of WebVPN. When cookies are disabled on the web browser, the links from the web portal home page open a new window prompting the user to log in once more.

Understanding WebVPN Global and Group Policy Settings

In general, the tunnel group and group policy commands for IPSec sessions do not apply for WebVPN. For WebVPN, use these same commands in global webvpn mode. The exceptions to this are:

- WebVPN commands from the group policy WebVPN mode apply.
- The banner, if any, that the client applies to WebVPN sessions.
- The **vpn-idletimeou**t, **vpn-tunnel-protocol**, and **vpn-session-timeout** commands apply.

Web VPN uses authentication, authorization, and accounting settings specific to WebVPN, which you configure with the **global webvpn** commands. Table 29-1 lists the commands specific to WebVPN for these features:

Table 29-1 Commands Specific to WebVPN

Command
accounting-server-group
authentication-server-group
authorization-server-group
authorization-dn-attributes
authoriziation-required

Note In Version 7.0.x, WebVPN does not support RADIUS with Expiry authentication.

Authenticating with Digital Certificates

WebVPN users that authenticate using digital certificates do not use global authentication and authorization settings. Instead, they use an authorization server to authenticate once the certificate validation occurs.

Configuring DNS Globally

WebVPN does not use the DNS settings of the group policy with which it has connected. WebVPN follows the security appliance global DNS settings. Ensure that the global DNS settings of the security appliance are configured properly.

Configuring Global WebVPN Attributes

Table 29-2 lists WebVPN attributes that apply globally to WebVPN users:

Table 29-2 Global WebVPN Attributes

Function	Command	Default Value
Specifies the previously configured accounting servers to use with WebVPN.	**accounting-server-group**	None
Specifies the authentication method(s) for WebVPN users.	**authentication**	AAA
Specifies the previously configured authentication servers to use with WebVPN.	**authentication-server-group**	LOCAL
Specifies the previously configured authorization servers to use with WebVPN.	**authorization-server-group**	None
Requires users to authorize successfully to connect.	**authorization-required**	Disabled
Identifies the DN of the peer certificate to use as a username for authorization.	**authorization-dn-attributes**	Primary attribute: CN Secondary attribute: OU
Specifies the name of the group policy to use.	**default-group-policy**	DfltGrpPolicy
Specifies the default idle timeout (in seconds).	**default-idle-timeout**	1800 seconds (30 minutes)
Enables WebVPN on the specified interface.	**enable**	Disabled
Identifies the proxy server for HTTP requests.	**http-proxy**	None
Identifies the proxy server for HTTPS requests.	**https-proxy**	None
Configures the HTML text that prompts a user to log in.	**login-message**	“Please enter your username and password.”
Specifies the logo image that displays on the WebVPN login and home pages.	**logo**	Cisco logo
Configures the HTML text the security appliance presents to a user logging out.	**logout-message**	“Goodbye.”
Identifies the NetBIOS Name Service server for CIFS name resolution.	**nbns-server**	None
Configures the prompt for a username at initial login to WebVPN.	**username-prompt**	“Login:”
Configures the prompt for the password at initial login to WebVPN.	**password-prompt**	“Password:”
Configures the HTML title string that is in the WebVPN browser title and on the title bar.	**title**	“WebVPN Service”
Configures the color of the title bars on the login, home and file access pages.	**title-color**	HTML #999CC, a lavender color
Configures the color of the text bars on the login, home, and file access pages.	**text-color**	White

Table 29-2 Global WebVPN Attributes (continued)

Function	Command	Default Value
Configures the color of the secondary title bars on the login, home and file access pages.	**secondary-color**	HTML #CCCCFF, a lavender color
Configures the color of the secondary text bars on the login, home and file access pages.	**secondary-text-color**	Black

You enter these WebVPN commands in webvpn mode. To enter webvpn mode, in global configuration mode, enter the **webvpn** command.

To reset all commands entered with the **webvpn** command to default values, use the **no webvpn** command.

Creating and Applying WebVPN Policies

Creating and applying WebVPN policies that govern access to resources at the central site includes the following tasks:

- Creating Port Forwarding, URL, and Access Lists in Global Configuration Mode
- Assigning Lists to Group Policies and Users in Group-Policy or User Mode
- Enabling Features for Group Policies and Users
- Assigning Users to Group Policies

Creating Port Forwarding, URL, and Access Lists in Global Configuration Mode

Use the **port forward**, **url-list,** and **access-list** commands in global configuration mode to configure the lists of ports to forward and URLs to present to WebVPN users, and their level of access.

Assigning Lists to Group Policies and Users in Group-Policy or User Mode

After you configure port forwarding and URL lists, use the **port forward** and **url-list,** and **filter** commands in webvpn group-policy or user mode to assign lists to group policies and/or users.

Enabling Features for Group Policies and Users

To enable features for group policies and users, issue the **functions** command in group-policy or user configuration mode.

Assigning Users to Group Policies

Assigning users to group policies simplifies configuration, by letting you apply policies to many users, rather than configuring policies for each user individually.There are two ways to assign users to group policies:

Using a RADIUS Server

Using a RADIUS server to authenticate users, assign users to group policies by following these steps:

Step 1 Authenticate the user with RADIUS and use the Class attribute to assign that user to a particular group policy.

Step 2 Set the class attribute to the group policy name in the format OU=group_name

For example, to set a WebVPN user to the SSL_VPN group, set the RADIUS Class Attribute to a value of *OU=SSL_VPN;* (Do not omit the semicolon.)

Using the Security Appliance Authentication Server

You can also configure users to authenticate to the security appliance internal authentication server, and assign these users to a group policy on the security appliance.

Configuring WebVPN Group Policy and User Attributes

Table 29-3 lists all WebVPN group policy and user attributes:

Table 29-3 WebVPN Group Policy Attributes

Function	Command	Default Value
Configures the name of the webtype access list.	**filter**	The security appliance does not enforce WebVPN access lists until you enter this command
Enables some or all of these WebVPN features: file access, file browsing, file entry, URL entry, port forwardng, MAPI proxy.	**functions**	Disabled
Sets the URL of the web page that displays upon login.	**homepage**	None
Configures the content and objects to filter from the HTML for this group policy.	**html-content-filter**	No filtering
Applies a list of WebVPN TCP ports to forward. The user interface displays the applications on this list.	**port-forward**	None
Configures the name of the port forwarding applet.	**port-forward-name**	“Application Access”
Applies a list of WebVPN servers and URLs that the user interface displays for end user access.	**url-list**	None

Configuring Email

WebVPN supports several ways to access email. This section includes the following methods:

- Configuring Email Proxies
- Configuring MAPI

- Configuring Web Email: MS Outlook Web Access

Configuring Email Proxies

WebVPN supportsIMAP4S, POP3S, and SMTPS email proxies. Table 29-4 lists attributes that apply globally to Email proxy users:

Table 29-4 Global Email proxy Attributes

Function	Command	Default Value
Specifies the previously configured accounting servers to use with Email proxy.	**accounting-server-group**	None
Specifies the authentication method(s) for Email proxy users.	**authentication**	IMAP4S: Mailhost (required) POP3S Mailhost (required) SMTPS: AAA
Specifies the previously configured authentication servers to use with Email proxy.	**authentication-server-group**	LOCAL
Specifies the previously configured authorization servers to use with WebVPN.	**authorization-server-group**	None
Requires users to authorize successfully to connect.	**authorization-required**	Disabled
Identifies the DN of the peer certificate to use as a username for authorization.	**authorization-dn-attributes**	Primary attribute: CN Secondary attribute: OU
Specifies the name of the group policy to use.	**default-group-policy**	DfltGrpPolicy
Enables Email proxy on the specified interface.	**enable**	Disabled
Defines the separator between the email and VPN usernames and passwords.	**name-separator**	":" (colon)
Configures the maximum number of outstanding non-authenticated sessions.	**outstanding**	20
Sets the port the email proxy listens to.	**port**	IMAP4S:993 POP3S: 995 SMTPS: 988
Specifies the default email server.	**server**	None.
Defines the separator between the email and server names.	**server-separator**	"@"

Note With the Eudora email client, SMTPS works only on port 465, even though the default port for SMTPS connections is 988.

Email Proxy Certificate Authentication

Certificate authentication for email proxy connections works with Netscape 7x email clients. Other email clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

Configuring MAPI

MAPI, also called MS Outlook Exchange proxy, has the following requirements:

- MS Outlook Exchange must be installed on the remote computer.
- You must enable MS Outlook Exchange Proxy on a security appliance interface. You do this by entering the **functions** command, which is a group-policy web vpn command. For example:

```
hostname(config)# group-policy group_policy_name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions mapi
```

- Provide the Exchange server NetBIOS name. The Exchange server must be on the same domain as the security appliance DNS server. For example:

```
hostname(config)# domain domain_name
hostname(config)#
```

Note An open MS Outlook client connected via MS Outlook Exchange Mail Proxy is always checking for mail on the Exchange Server, which keeps the connection open. As long as Outlook is open, the connection never times out, regardless of the settings.

Configuring Web Email: MS Outlook Web Access

Web email is MS Outlook Web Access for Exchange 2000, Exchange 5.5, and Exchange 2003. It requires an MS Outlook Exchange Server at the central site. It also requires that users perform the following tasks:

- Enter the URL of the mail server in a browser in your WebVPN session.
- When prompted, enter the email server username in the format *domain\username*.
- Enter the email password.

Understanding WebVPN End User Set-up

This section is for the system administrator who sets up WebVPN for end users. It describes how to customize the end-user interface.

This section summarizes configuration requirements and tasks for a remote system. It specifies information to communicate to users to get them started using WebVPN. It includes the following topics:

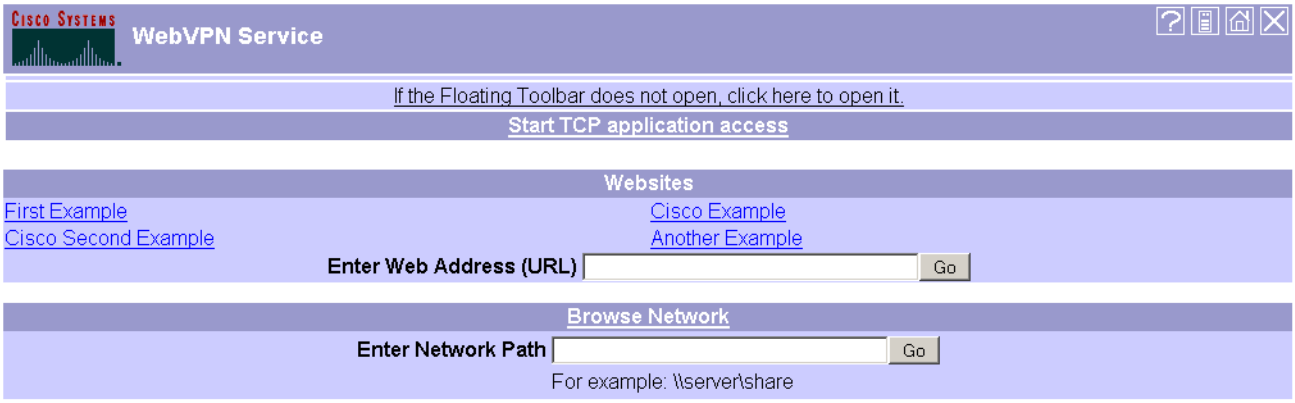
Defining the End User Interface

The WebVPN end user interface is a series of html panels. A user logs on to WebVPN by entering the IP address of a security appliance interface in the format https://*address*. The first panel that displays is the login screen.

Viewing the WebVPN Home Page

After the user logs in, the WebVPN home page displays (Figure 29-1).

Figure 29-1 WebVPN Home Page

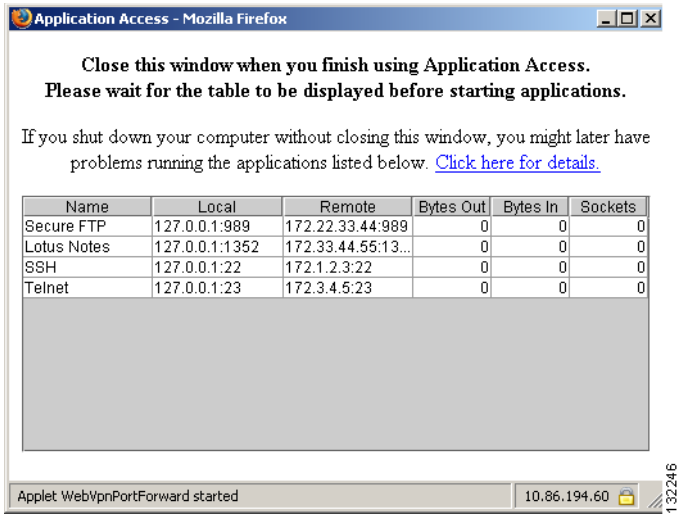


The home page displays all of the WebVPN features you have configured, and its appearance reflects the logo, text, and colors you have selected. This sample home page includes all available WebVPN features with the exception of identifying specific file shares. It lets users browse the network, enter URLs, access specific websites, and use port forwarding to access TCP applications.

Viewing the WebVPN Application Access Panel

To start port forwarding, also called application access, a user clicks the "Start TCP application access" link. The Application Access Panel opens (Figure 29-2).

Figure 29-2 WebVPN Application Access Panel

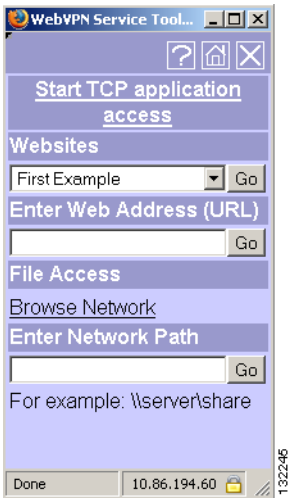


This panel displays the TCP applications configured for this WebVPN connection. To use an application, with this panel open, the user starts the application in the normal way.

Viewing the Floating Toolbar

WebVPN also includes a floating toolbar (Figure 29-3).

Figure 29-3 WebVPN Floating Toolbar



Be aware of the following characteristics of the floating toolbar:

- The toolbar lets you enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.
- If you configure your browser to block popups, the floating toolbar cannot display.
- The floating toolbar represents the current WebVPN session. If you click the **Close** button, the security appliance prompts you to confirm that you want to end the WebVPN session.

See Table 29-6 on page 15 for detailed information about using WebVPN.

Requiring Usernames and Passwords

Depending on your network, during a remote session users might have to log in to any or all of the following: the computer itself, an Internet servicde provider, WebVPN, mail or file servers, or corporate applications. Users might have to authenticate in many different contexts, requiring different information, such as a unique username, password, or pincode.

Table 29-5 lists the type of usernames and passwords that WebVPN users might need to know.

Table 29-5 Usernames and Passwords to Tell WebVPN Users

Login Username/ Password Type	Purpose	Entered When
Computer	Access the computer	Starting the computer
Internet Service Provider	Access the Internet	Connecting to an Internet service provider
WebVPN	Access remote network	Starting WebVPN
File Server	Access remote file server	Using the WebVPN file browsing feature to access a remote file server
Corporate Application Login	Access firewall-protected internal server	Using the WebVPN web browsing feature to access an internal protected website
Mail Server	Access remote mail server via WebVPN	Sending or receiving email messages

Communicating Security Tips

Advise users always to log out from the WebVPN session. (To log out of WebVPN, click the logout icon on the WebVPN toolbar or close the browser.)

Advise users that using WebVPN does not ensure that communication with every site is secure. WebVPN ensures the security of data transmission between the remote PC or workstation and the security appliance on the corporate network. If the user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate security appliance to the destination web server is not secure.

Configuring Remote Systems to Use WebVPN Features

Table 29-6 includes information about setting up remote systems to use WebVPN. It includes the following tasks:

- Starting WebVPN
- Using the WebVPN Floating Toolbar
- Web Browsing
- Network Browsing and File Management
- Using Applications (Port Forwarding)
- Using Email via Port Forwarding

- Using Email via Web Access
- Using Email via email proxy

Table 29-6 also provides information about the following:

- WebVPN requirements, by feature
- WebVPN supported applications
- Client application installation and configuration requirements
- Information you might need to provide end users
- Tips and use suggestions for end users

It is possible you have configured user accounts differently and that different WebVPN features are available to each user. We have organized the information in Table 29-6 by feature, so you can skip over the information for unavailable features.

Table 29-6 WebVPN Remote System Configuration and End User Requirements

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Starting WebVPN	A connection to the Internet	Any Internet connection is supported, including: • Home DSL, cable, or dial-ups • Public kiosks • Hotel hook-ups • Airport wireless nodes • Internet cafes
	A WebVPN-supported browser	We recommend the following browsers for WebVPN. Other browsers might not fully support WebVPN features. On Microsoft Windows: • Internet Explorer version 6.0 • Netscape version 7.2 • Mozilla version 1.7 and above • Firefox 1.x On Linux: • Mozilla version 1.7 • Netscape version 7.2 • Firefox 1.x On Solaris: • Netscape version 7.2 On Macintosh OS X: • Safari version 1.0 • Firefox 1.x
	Cookies enabled on browser	Cookies must be enabled on the browser in order to access applications via port forwarding.
	The URL for WebVPN	An https address in the following form: https://*address* where *address* is the IP address or DNS hostname of an interface of the security appliance (or load balancing cluster) on which WebVPN is enabled. For example: https://10.89.192.163 or https://cisco.example.com.
	A WebVPN username and password	
	[Optional] A local printer	WebVPN does not support printing from a web browser to a network printer. Printing to a local printer is supported.

Table 29-6 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Using the WebVPN Floating Toolbar		A floating toolbar is available to simplify the use of WebVPN. The toolbar lets you enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window. If you configure your browser to block popups, the floating toolbar cannot display. The floating toolbar represents the current WebVPN session. If you click the **Close** button, the security appliance prompts you to confirm that you want to close the WebVPN session. **Tip** TIP: To paste text into a text field, use Ctrl-V. Right-clicking is disabled on the WebVPN toolbar.
Web Browsing	Usernames and passwords for protected websites	Using WebVPN does not ensure that communication with every site is secure. See the Communicating Security Tips section. The look and feel of web browsing with WebVPN might be different from what users are accustomed to. For example, when using WebVPN: • The WebVPN title bar appears above each web page • You access websites by: – Entering the URL in the Enter Web Address field on the WebVPN home page – Clicking on a preconfigured website link on the WebVPN home page – Clicking a link on a webpage accessed via one of the previous two methods Also, depending on how you configured a particular account, it might be that: • Some websites are blocked • Only the websites that appear as links on the WebVPN home page are available

Table 29-6 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Network Browsing and File Management	File permissions configured for shared remote access	Only shared folders and files are accessible via WebVPN.
	Server name and passwords for protected file servers	
	Domain, workgroup, and server names where folders and files reside	Users might not be familiar with how to locate their files through your organization network.
	Patience	Do not interrupt the **Copy File to Server** command or navigate to a different screen while the copying is in progress. Interrupting the operation can cause an incomplete file to be saved on the server.

Table 29-6 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Using Applications	**Note** On Macintosh OS X, only the Safari browser supports this feature.	
(called Port Forwarding or Application Access)	**Note** Because this feature requires installing Sun Microsystems Java™ Runtime Environment and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.	
	Caution Users should always close the Application Access window when they finish using applications by clicking the**Close** icon. Failure to quit the window properly can cause Application Access or the applications themselves to be disabled. See Recovering from hosts File Errors in Application Access for details.	
	Client applications installed	
	Cookies enabled on browser	
	Administrator privileges	User must be local administrator on the PC if you use DNS names to specify servers. This is because modifying the hosts file requires administrator privileges.
	Sun Microsystems Java Runtime Environment (JRE) version 1.4.x and 1.5.x installed. Javascript must be enabled on the browser. By default, it is enabled.	If JRE is not installed, a pop-up window displays, directing users to a site where it is available. On rare occasions, the WebVPN port forwarding applet fails with JAVA exception errors. If this happens, do the following: 1. Clear the browser cache and close the browser. 2. Verify that no JAVA icons are in the computer task bar. Close all instances of JAVA. 3. Establish a WebVPN session and launch the port forwarding JAVA applet.
	Client applications configured, if necessary. **Note** The Microsoft Outlook client does not require this configuration step. All non-Windows client applications require configuration. To see if configuration is necessary for a Windows application, check the value of the Remote Server. • If the Remote Server contains the server hostname, you do not need to configure the client application. • If the Remote Server field contains an IP address, you must configure the client application.	To configure the client application, use the server's locally mapped IP address and port number. To find this information: 1. Start WebVPN on the remote system and click the Application Access link on the WebVPN home page. The Application Access window displays. 2. In the Name column, find the name of the server you want to use, then identify its corresponding client IP address and port number (in the Local column). 3. Use this IP address and port number to configure the client application. Configuration steps vary for each client application.
	Note When you use an application over WebVPN, for example Outlook over Port Forwarding, if the application presents a URL, for example a URL within an email, clicking the URL does not open the site over WebVPN. You must cut and paste the URL into the **Enter WebVPN (URL) Address** box on the WebVPN home page to open the site in WebVPN.	

Table 29-6 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Using Email via Application Access	Fulfill requirements for Application Access (See Using Applications)	To use mail, start Application Access from the WebVPN home page. The mail client is then available for use.
	Note If you are using an IMAP client and you lose your mail server connection or are unable to make a new connection, close the IMAP application and restart WebVPN.	
	Other mail clients	We have tested Microsoft Outlook Express versions 5.5 and 6.0. WebVPN should support other SMTPS, POP3S, or IMAP4S email programs via port forwarding, such as Netscape Mail, Lotus Notes, and Eudora, but we have not verified them.
Using Email via Web Access	Web-based email product installed	Supported: • Outlook Web Access For best results, use OWA on Internet Explorer 6.x or higher, Mozilla 1.7, or Firefox 1.x. • Louts iNotes Other web-based email products should also work, but we have not verified them.
Using Email via Email Proxy	SSL-enabled mail application installed Do not set the security appliance SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.	Supported mail applications: • Microsoft Outlook • Microsoft Outlook Express versions 5.5 and 6.0 • Netscape Mail version 7 • Eudora 4.2 for Windows 2000 Other SSL-enabled mail clients should also work, but we have not verified them.
	Mail application configured	See instructions and examples for your mail application in the "Configuring Email" section.

Recovering from hosts File Errors in Application Access

It is very important to close the Application Access window properly. When you finish using Application Access, click the close icon. If you do not close the window properly:

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

These errors can result from terminating the Application Access window in any improper way. For example:

- Your browser crashes while you are using Application Access.
- A power outage or system shutdown occurs while you are using Application Access.
- You minimize the Application Access window while you are working, then shut down your computer with the window active (but minimized).

This section includes the following topics:

Understanding the hosts File

The hosts file on your local system maps IP addresses to host names. When you start Application Access, WebVPN modifies the hosts file, adding WebVPN-specific entries. Stopping Application Access by properly closing the Application Access window returns the file to its original state.

Before invoking Application Access...	hosts file is in original state.
When Application Access starts....	• WebVPN copies the hosts file to hosts.webvpn, thus creating a backup. • WebVPN then edits the hosts file, inserting WebVPN-specific information.
When Application Access stops...	• WebVPN copies the backup file to the `hosts` file, thus restoring the hosts file to its original state. • WebVPN deletes hosts.webvpn.
After finishing Application Access...	hosts file is in original state.

Note Microsoft anti-spyware software blocks changes that the port forwarding JAVA applet makes to the hosts file. See www.microsoft.com for information on how to allow hosts file changes when using anti-spyware software.

Stopping Application Access Improperly

Once Application Access terminates abnormally, the `hosts` file is left in a WebVPN-customized state. WebVPN checks for this possibility the next time you start Application Access by searching for a hosts.webvpn file. If it finds one, you receive a `Backup HOSTS File Found` error message(see Figure 29-4), and Application Access is temporarily disabled.

Once you shut down Application Access improperly, you leave your remote access client/server applications in limbo. If you try to start these applications without using WebVPN, they 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 Application Access window before shutting down the computer, then try to run the applications later from the office.

Reconfiguring hosts Files

To reenable Application Access or malfunctioning applications:

- If you are able to connect to your remote access server, follow the steps in the section "Reconfiguring hosts File Automatically Using WebVPN."
- If you are unable to connect to your remote access server from your current location or if you have made custom edits to the hosts file, follow the steps in the section "Reconfiguring hosts File Manually."

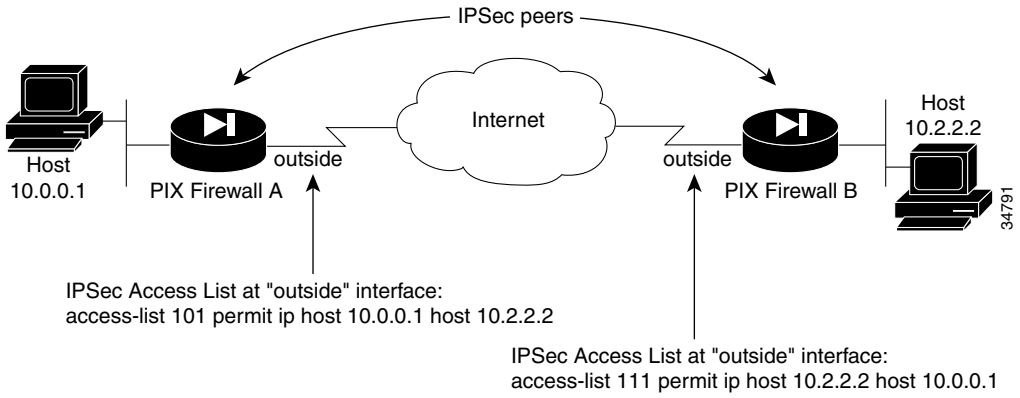
Reconfiguring hosts File Automatically Using WebVPN

If you are able to connect to your remote access server, follow these steps to reconfigure the hosts file and reenable both Application Access and the applications.

Step 1 Start WebVPN and log in. The home page opens.

Step 2 Click the **Applications Access** link. A `Backup HOSTS File Found` message displays. (See Figure 29-4.)

Figure 29-4 Backup HOSTS File Found Message



Step 3 Choose one of the following options:

- **Restore from backup** = WebVPN forces a proper shutdown. WebVPN copies the hosts.webvpn backup file to the `hosts` file, restoring it to its original state, then deletes hosts.webvpn. You then have to restart Application Access.
- **Do nothing** = Application Access does not start. You return to your remote access home page.
- **Delete backup** = WebVPN deletes the hosts.webvpn file, leaving the hosts file in its WebVPN-customized state. The original `hosts` file settings are lost. Then Application Access starts, using the WebVPN-customized hosts file as the new original. Choose this option only if you are

unconcerned about losing hosts file settings. If you or a program you use might have edited the hosts file after Application Access has shut down improperly, choose one of the other options, or edit the hosts file manually. (See the "Reconfiguring hosts File Manually" section.)

Reconfiguring hosts File Manually

If you are not able to 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, follow these steps to reconfigure the hosts file and reenable both Application Access and the applications.

Step 1 Locate and edit your hosts file.

Step 2 Check to see if any lines contain the string: `# added by WebVpnPortForward`
If any lines contain this string, your hosts file is WebVPN-customized. If your hosts file is WebVPN-customized, it looks similar to the following example:

```
123.0.0.3 server1 # added by WebVpnPortForward
123.0.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.4 server2 # added by WebVpnPortForward
123.0.0.4 server2.example.com.vpn3000.com # added by WebVpnPortForward
123.0.0.5 server3 # added by WebVpnPortForward
123.0.0.5 server3.example.com vpn3000.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 host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name 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:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

Step 3 Delete the lines that contain the string: `# added by WebVpnPortForward`

Step 4 Save and close the file.

Step 5 Start WebVPN and log in. The home page appears.

Step 6 Click the Application Access link. The Application Access window appears. Application Access is now enabled.

Capturing WebVPN Data

WebVPN capture lets you log information about websites that do not display properly over a WebVPN connection. The data recorded can help your Cisco customer support engineer troubleshoot problems.

Note Enabling WebVPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

WebVPN Capture Files

When you enable WebVPN capture using the **capture** command, the security appliance stores the data from the first URL visited in the following files:

- *capture name*_ORIGINAL.000—Contains the data exchanged between the security appliance and the web server.
- *capture name*_MANGLED.000—Contains the data exchanged between the security appliance and the browser.

For each subsequent capture, the security appliance generates additional pairs of matching *capture name*_ORIGINAL.<nnn> and *capture name*_MANGLED.<nnn> files and increments the file extensions. In the following example, the capture name *sales* was assigned to the capture, and the output of the **dir** command displays three sets of files from three URL captures:

```
hostname# dir
Directory of disk0:/
2952    -rw-    10931      10:38:32 Jan 19 2005 config
6       -rw-    5124096    19:43:32 Jan 01 2003 cdisk.bin
3397    -rw-    5157       08:30:56 Feb 14 2005 sales_ORIGINAL.000
3398    -rw-    6396       08:30:56 Feb 14 2005 sales_MANGLED.000
3399    -rw-    4928       08:32:51 Feb 14 2005 sales_ORIGINAL.001
3400    -rw-    6167       08:32:51 Feb 14 2005 sales_MANGLED.001
3401    -rw-    5264       08:35:23 Feb 14 2005 sales_ORIGINAL.002
3402    -rw-    6503       08:35:23 Feb 14 2005 sales_MANGLED.002
hostname#
```

Activating the WebVPN Capture Tool

Note When you activate WebVPN capture, the icon appears in the WebVPN window.

To activate WebVPN capture, use the **capture** command from privileged EXEC mode.

capture *capture-name* **type webvpn user** *webvpn-user* [**url** *url*]

no capture *capture-name*

where:

- *capture-name* is a name you assign to the capture, which is also prepended to the name of the capture files.
- *webvpn-user* is the username to match for capture.
- *url* is the URL prefix to match for data capture. Use one of the following two URL formats:

- Use http://*server*/*path* to capture HTTP traffic to the server identified by *server*/*path*.
- Use https://*server*/*path* to capture HTTPS traffic to the server identified by *server*/*path.*

If no URL is specified, all traffic is logged.

The following example creates a capture designated *hr*, which is configured to capture HTTP traffic for user2 visiting website wwwin.abcd.com/hr/people:

```
hostname# capture hr type webvpn user user2 url http://wwwin.abcd.com/hr/people
WebVPN capture started.
   capture name   hr
   user name      user2
   url            /http/0/wwwin.abcd.com/hr/people
hostname#
```

Locating and Uploading the WebVPN Capture Tool Output Files

To locate the WebVPN capture tool output files, use the **dir** command. The following example shows the output of the **dir** command including the ORIGINAL.000 and MANGLED.000 files that were generated:

```
hostname# dir
Directory of disk0:/
2952    -rw-    10931       10:38:32 Jan 19 2005 config
6       -rw-    5124096     19:43:32 Jan 01 2003 cdisk.bin
3397    -rw-    5157        08:30:56 Feb 14 2005 hr_ORIGINAL.000
3398    -rw-    6396        08:30:56 Feb 14 2005 hr_MANGLED.000
hostname#
```

You can upload the WebVPN capture tool output files to another computer using the **copy flash** command. In the following example, the **copy flash** command is used to upload the hr_ORIGINAL.000 and hr_MANGLED.000 files via tftp:

```
hostname# copy flash:/hr_original.000 tftp://10.86.194.191/hr_original.000
Source filename [hr_original.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [hr_original.000]?
!!!!!!
21601 bytes copied in 0.370 secs

hostname# copy flash:/hr_mangled.000 tftp://10.86.194.191/hr_mangled.000
Source filename [hr_mangled.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [hr_mangled.000]?
!!!!!!
23526 bytes copied in 0.380 secs

hostname#
```

Note To conserve flash memory, delete the capture files from the security appliance when you no longer need them.