CHAPTER 37

Configuring WebVPN

This chapter includes the following sections:

- Getting Started with WebVPN, page 37-1
- Creating and Applying WebVPN Policies, page 37-15
- Configuring WebVPN Tunnel Group Attributes, page 37-17
- Configuring WebVPN Group Policy and User Attributes, page 37-17
- Configuring Application Access, page 37-18
- Configuring File Access, page 37-22
- Configuring Access to Citrix MetaFrame Services, page 37-24
- Using WebVPN with PDAs, page 37-25
- Using E-Mail over WebVPN, page 37-26
- Optimizing WebVPN Performance, page 37-28
- WebVPN End User Setup, page 37-33
- Capturing WebVPN Data, page 37-51

Getting Started with WebVPN

WebVPN lets users establish a secure, remote-access VPN tunnel to a security appliance using a web browser. Users do not need a software or hardware client.

WebVPN provides secure and easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. They include:

- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS
- MS Outlook Web Access
- MAPI
- Application Access (that is, port forwarding for access to other TCP-based applications)

WebVPN uses Secure Sockets Layer Protocol and its successor, Transport Layer Security to provide the 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.

The following sections address getting started with the configuration of WebVPN access:

- Observing WebVPN Security Precautions
- Understanding Features Not Supported for WebVPN
- Using SSL to Access the Central Site
- Authenticating with Digital Certificates
- Enabling Cookies on Browsers for WebVPN
- Managing Passwords
- Using Single Sign-on with WebVPN
- Authenticating with Digital Certificates

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:

- DSA certificates; the ASA does support RSA certificates.
- 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
- Configuring WebVPN and ASDM on the Same Interface
- Setting WebVPN HTTP/HTTPS Proxy
- Configuring SSL/TLS Encryption Protocols

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
```

Configuring WebVPN and ASDM on the Same Interface

The security appliance can support both WebVPN connections and HTTPS connections for ASDM administrative sessions simultaneously on the same interface. Both HTTPS and WebVPN use port 443 by default. Therefore, to enable both HTTPS and WebVPN on the same interface, you must specify a different port number for either HTTPS or WebVPN. An alternative is to configure WebVPN and HTTPS on different interfaces.

To specify a port for HTTPS, use the *port* argument of the **http server enable** command. The following example specifies that HTTPS ASDM sessions use port 444 on the outside interface. WebVPN is also enabled on the outside interface and uses the default port (443). With this configuration, remote users initiate ASDM sessions by entering https://<outside_ip>:444 in the browser.

```
hostname(config)# http server enable 444
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

To specify a port for WebVPN, use the **port** command from webvpn configuration mode. The next example enables WebVPN on port 444 of the outside interface. HTTPS for ASDM is also configured on the outside interface and uses the default port (443). With this configuration, remote users initiating WebVPN sessions enter https://<outside_ip>:444 in the browser.

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside
```

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, use the **http-proxy** and **https-proxy** commands in webvpn mode. These commands let you identify HTTP and HTTPS proxy servers and ports.

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 e-mail 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:

- Application Access 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.
- E-mail proxy supports certificate authentication with Netscape 7.x e-mail clients only. Other e-mail clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

For more information on authentication and authorization using digital certificates, see "Using Certificates and User Login Credentials" in the "Configuring AAA Servers and the Local Database" chapter.

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.

Managing Passwords

You can configure the security appliance to warn end users when their passwords are about to expire. To do this, you specify the **password-management** command in tunnel-group general-attributes mode.

When you configure this command, the security appliance notifies the remote user at login that the user's current password is about to expire or has expired. The security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. This command is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this does not change the number of days before the password expires, but rather specifies the number of days ahead of expiration that the security appliance starts warning the user that the password is about to expire. The default value is 14 days.

For LDAP server authentication only, you can use the **password-expire-in-days** keyword to specify a specific number of days. If you specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The security appliance then does not notify the user of the pending expiration, but the user can change the password after it expires.

The following example sets the days before password expiration to begin warning the user of the pending expiration to 90 for the tunnel group "testgroup":

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
```

```
hostname(config-general)# password-management password-expire-in-days 90
```

Using Single Sign-on with WebVPN

Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and web servers. In general, the SSO mechanism either starts as part of the AAA process or just after successful user authentication to a AAA server. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

This section describes the three SSO authentication methods supported by WebVPN: HTTP Basic and NTLMv1 (NT LAN Manager) authentication, the Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder), and the HTTP Form protocol.

This section includes:

- Configuring SSO with HTTP Basic or NTLM Authentication
- Configuring SSO Authentication Using SiteMinder
- Configuring SSO with the HTTP Form Protocol

Configuring SSO with HTTP Basic or NTLM Authentication

This section describes single sign-on with HTTP Basic or NTLM authentication. You can configure the security appliance to implement SSO using either or both of these methods. The **auto-signon** command configures the security appliance to automatically pass WebVPN user login credentials (username and password) on to internal servers. You can enter multiple **auto-signon** commands. The security appliance processes them according to the input order (early commands take precedence). You specify the servers to receive the login credentials using either IP address and IP mask, or URI mask.

Use the **auto-signon** command in any of three modes: webvpn configuration, webvpn group-policy mode, or webvpn username mode. Username supersedes group, and group supersedes global. The mode you choose depends upon scope of authentication you want:

Mode	Scope
Webvpn configuration	All WebVPN users globally
Webvpn group configuration	A subset of WebVPN users defined by a group policy
Webvpn username configuration	An individual WebVPN user

The following example commands present various possible combinations of modes and arguments.

All Users, IP Address Range, NTLM

To configure **auto-signon** for all WebVPN users to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255 using NTLM authentication, for example, enter the following commands:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type ntlm
```

All Users, URI Range, HTTP Basic

To configure **auto-signon** for all WebVPN users, using basic HTTP authentication, to servers defined by the URI mask https://*.example.com/*, for example, enter the following commands:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

Group, URI Range, HTTP Basic and NTLM

To configure **auto-signon** for WebVPN users ExamplePolicy group policy, using either basic or NTLM authentication, to servers defined by the URI mask https://*.example.com/*, for example, enter the following commands:

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

Specific User, IP Address Range, HTTP Basic

To configure **auto-signon** for a user named Anyuser to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255 using HTTP Basic authentication, for example, enter the following commands:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type
basic
```

Configuring SSO Authentication Using SiteMinder

This section describes configuring the security appliance to support SSO with SiteMinder. You would typically choose to implement SSO with SiteMinder if your website security infrastucture already incorporates SiteMinder. With this method, SSO authentication is separate from AAA and happens once the AAA process completes. If you want to configure SSO for a WebVPN user or group, you must first configure a AAA server, such as a RADIUS or LDAP server. You can then setup SSO support for WebVPN. This section includes:

- Task Overview: Configuring SSO with Siteminder
- Detailed Tasks: Configuring SSO with Siteminder
- Adding the Cisco Authentication Scheme to SiteMinder

Task Overview: Configuring SSO with Siteminder

This section presents an overview of the tasks necessary to configure SSO with SiteMinder SSO. These tasks are:

- Specifying the SSO server.
- Specifying the URL of the SSO server to which the security appliance makes SSO authentication requests.
- Specifying a secret key to secure the communication between the security appliance and the SSO server. This key is similar to a password: you create it, save it, and enter it on both the security appliance and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

In addition to these required tasks, you can optionally do the following configuration tasks:

- Configuring the authentication request timeout.

- Configuring the number of authentication request retries.

After you have completed the configuration tasks, you assign an SSO server to a user or group policy.

Detailed Tasks: Configuring SSO with Siteminder

This section presents specific steps for configuring the security appliance to support SSO authentication with CA SiteMinder. To configure SSO with SiteMinder, perform the following steps:

Step 1 In webvpn configuration mode, enter the **sso-server** command with the **type** option to create an SSO server. For example, to create an SSO server named Example of type siteminder, enter the following:

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server Example type siteminder
hostname(config-webvpn-sso-siteminder)#
```

Note The security appliance currently supports only the SSO server type siteminder.

Step 2 Enter the **web-agent-url** command in webvpn-sso-siteminder configuration mode to specify the authentication URL of the SSO server. For example, to send authentication requests to the URL http://www.Example.com/webvpn, enter the following:

```
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.Example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

Step 3 Specify a secret key to secure the authentication communications between the security appliance and SiteMinder using the **policy-server-secret** command in webvpn-sso-siteminder configuration mode. You can create a key of any length using any regular or shifted alphanumeric character, but you must enter the same key on both the security appliance and the SSO server.

For example, to create the secret key AtaL8rD8!, enter the following:

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret AtaL8rD8!
hostname(config-webvpn-sso-siteminder)#
```

Step 4 Optionally, you can configure the number of seconds before a failed SSO authentication attempt times out using the **request-timeout** command in webvpn-sso-siteminder configuration mode. The default number of seconds is 5 seconds and the possible range is 1 to 30 seconds. To change the number of seconds before a request times out to 8, for example, enter the following:

```
hostname(config-webvpn-sso-siteminder)# request-timeout 8
hostname(config-webvpn-sso-siteminder)#
```

Step 5 Optionally, you can configure the number of times the security appliance retries a failed SSO authentication attempt before the authentication times-out using the **max-retry-attempts** command in webvpn-sso-siteminder configuration mode. The default is 3 retry attempts and the possible range is 1 to 5 attempts. To configure the number of retries to be 4, for example, enter the following:

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

Step 6 After you configure the SSO server, you must specify SSO authentication for either a group or user. To specify SSO for a group, assign an SSO server to a group policy using the **sso-server value** command in group-policy-webvpn configuration mode. To specify SSO for a user, assign an SSO server to a user policy using the same command, **sso-server value**, but in username-webvpn configuration mode. For example, to assign the SSO server named Example to the user named Anyuser, enter the following:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
```

```
hostname(config-username-webvpn)# sso-server value Example
hostname(config-group-webvpn)#
```

Step 7 Finally, you can test the SSO server configuration using the **test sso-server** command in privileged EXEC mode. For example, to test the SSO server named Example using the username Anyuser, enter the following:

```
hostname# test sso-server Example username Anyuser
INFO: Attempting authentication request to sso-server Example for user Anyuser
INFO: STATUS: Success
hostname#
```

Adding the Cisco Authentication Scheme to SiteMinder

Besides configuring the security appliance for SSO with SiteMinder, you must also configure your CA SiteMinder Policy Server with the Cisco authentication scheme, provided as a Java plug-in.

Note

- Configuring the SiteMinder Policy Server requires experience with SiteMinder.
- This section presents general tasks, not a complete procedure.
- Refer to the CA SiteMinder documentation for the complete procedure for adding a custom authentication scheme.

To configure the Cisco authentication scheme on your SiteMinder Policy Server, perform these following tasks:

Step 1 With the Siteminder Administration utility, create a custom authentication scheme being sure to use the following specific arguments:

- In the Library field, enter **smjavaapi**.
- In the Secret field, enter the same secret configured on the security appliance.

  You configure this on the security appliance with either the **policy-server-secret** command at the command line interface or in the Secret Key field of the Add SSO Server dialog in ASDM.
- In the Parameter field, enter **CiscoAuthAPI**.

Step 2 Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from http://www.cisco.com/cisco/software/navigator.html and copy it to the default library directory for the SiteMinder server.

Configuring SSO with the HTTP Form Protocol

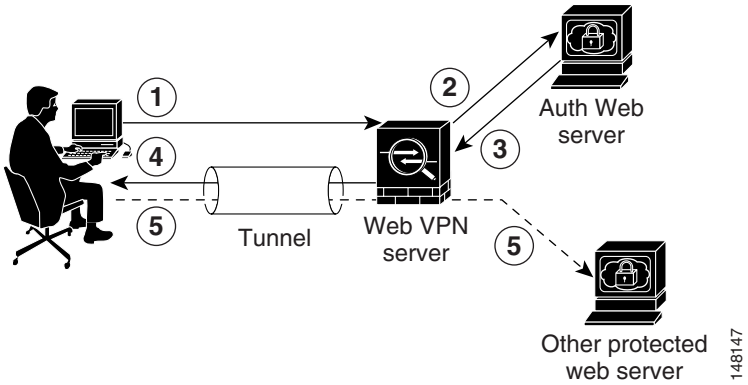
This section describes using the HTTP Form protocol for SSO. HTTP Form protocol is a common approach to SSO authentication that can also qualify as a AAA method. It provides a secure method for exchanging authentication information between WebVPN users and authenticating web servers. As a common protocol, it is highly compatible with web servers and web-based SSO products, and you can use it in conjunction with other AAA servers such as RADIUS or LDAP servers.

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

The security appliance again serves as a proxy for WebVPN users to an authenticating web server but, in this case, it uses HTTP Form protocol and the POST method for requests. You must configure the security appliance to send and receive form data. Figure 37-1 illustrates the following SSO authentication steps:

1. A WebVPN user first enters a username and password to log into the WebVPN server on the security appliance.
2. The WebVPN server acts as a proxy for the user and forwards the form data (username and password) to an authenticating web server using a POST authentication request.
3. If the authenticating web server approves the user data, it returns an authentication cookie to the WebVPN server where it is stored on behalf of the user.
4. The WebVPN server establishes a tunnel to the user.
5. The user can now access other websites within the protected SSO environment without reentering a username and password.

Figure 37-1 SSO Authentication Using HTTP Forms



While you would expect to configure form parameters that let the security appliance include POST data such as the username and password, you initially might not be aware of additional hidden parameters that the web server requires. Some authentication applications expect hidden data which is neither visible to nor entered by the user. You can, however, discover hidden parameters the authenticating web server expects by making a direct authentication request to the web server from your browser without the security appliance in the middle acting as a proxy. Analyzing the web server response using an HTTP header analyzer reveals hidden parameters in a format similar to the following:

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

Some hidden parameters are mandatory and some are optional. If the web server requires data for a hidden parameter, it rejects any authentication POST request that omits that data. Because a header analyzer does not tell you if a hidden parameter is mandatory or not, we recommend that you include all hidden parameters until you determine which are mandatory.

This section describes:

- Gathering HTTP Form Data
- Task Overview: Configuring SSO with HTTP Form Protocol
- Detailed Tasks: Configuring SSO with HTTP Form Protocol

Gathering HTTP Form Data

This section presents the steps for discovering and gathering necessary HTTP Form data. If you do not know what parameters the authenticating web server requires, you can gather parameter data by analyzing an authentication exchange using the following steps:

Note These steps require a browser and an HTTP header analyzer.

Step 1 Start your browser and HTTP header analyzer, and connect directly to the web server login page without going through the security appliance.

Step 2 After the web server login page has loaded in your browser, examine the login sequence to determine if a cookie is being set during the exchange. If the web server has loaded a cookie with the login page, configure this login page URL as the *start-URL*.

Step 3 Enter the username and password to log in to the web server, and press Enter. This action generates the authentication POST request that you examine using the HTTP header analyzer.

An example POST request—with host HTTP header and body—follows:

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac05-83
846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2b
J0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F
HTTP/1.1
Host: www.example.com
(BODY)
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F%2F
www.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

Step 4 Examine the POST request and copy the protocol, host, and the complete URL to configure the action-uri parameter.

Step 5 Examine the POST request body and copy the following:

a. Username parameter. In the preceding example, this parameter is USERID, not the value anyuser.

b. Password parameter. In the preceding example, this parameter is USER_PASSWORD.

c. Hidden parameter. This parameter is everything in the POST body except the username and password parameters. In the preceding example, the hidden parameter is: SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0

Figure 37-2 highlights the action URI, hidden, username and password parameters within sample output from an HTTP analyzer. This is only an example; output varies widely across different websites.

Figure 37-2 Action-uri, hidden, username and password parameters

1	Action URI parameter
2	Hidden parameters
3	Username and password parameters

Step 6 If you successfully log in to the web server, examine the server response with the HTTP header analyzer to locate the name of the session cookie set by the server in your browser. This is the **auth-cookie-name** parameter.

In the following server response header, the name of the session cookie is SMSESSION. You just need the name, not the value.

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQzxwfEz2cl7Ef5iMr8LgGcDK7qvMcvrgUqx68
JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V7flBqecH7+kVrU01
F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtPK6t1gFJyOn0s7QdNQ7q9
knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYzVu7EmzMQ+UefYxh4cF2gYD8R
ZL2RwmP9JV5l48I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyxjzMd88DVzM41LxxaUDhbcmkoHT9I
mzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4MlHGH+0CPscZXqoi/kon9YmGauHyRs+0m
6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5SxbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReW
```

```
J6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6RM6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8Vb
aR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefS
QTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;
Domain=.example.com;Path=/
```

Figure 37-3 shows an example of authorization cookies in HTTP analyzer output. This is only an example; output varies widely across different websites.

Figure 37-3 Authorization cookies in sample HTTP analyzer output

1	Authorization cookies

Step 7 In some cases, the server may set the same cookie regardless of whether the authentication was successful or not, and such a cookie is unacceptable for SSO purposes. To confirm that the cookies are different, repeat Step 1 through Step 6 using invalid login credentials and then compare the "failure" cookie with the "success" cookie.

You now have the necessary parameter data to configure the security appliance for SSO with HTTP Form protocol.

Task Overview: Configuring SSO with HTTP Form Protocol

This section presents an overview of configuring SSO with the HTTP Form protocol.To enable SSO using HTTP Forms, perform the following tasks:

- Configure the uniform resource identifier on the authenticating web server to receive and process the form data (**action-uri**).
- Configure the username parameter (**user-parameter**).
- Configure the user password parameter (**password-parameter**).

You might also need to do the following tasks depending upon the requirements of authenticating web server:

- Configure a starting URL if the authenticating web server requires a pre-login cookie exchange (**start-url**).
- Configure any hidden authentication parameters required by the authenticating web server (**hidden-parameter**).
- Configure the name of an authentication cookie set by the authenticating web server (**auth-cookie-name**).

Detailed Tasks: Configuring SSO with HTTP Form Protocol

This section presents the detailed tasks required to configure SSO with the HTTP Form protocol. Perform the following steps to configure the security appliance to use HTTP Form protocol for SSO:

Step 1 If the authenticating web server requires it, enter the **start-url** command in aaa-server-host configuration mode to specify the URL from which to retrieve a pre-login cookie from the authenticating web server. For example, to specify the authenticating web server URL http://example.com/east/Area.do?Page-Grp1 in the testgrp1 server group with an IP address of 10.0.0.2, enter the following:

```
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
hostname(config-aaa-server-host)#
```

Step 2 To specify a URI for an authentication program on the authenticating web server, enter the **action-uri** command in aaa-server- host configuration mode. A URI can be entered on multiple, sequential lines. The maximum number of characters per line is 255. The maximum number of characters for a complete URI is 2048. An example action URI follows:

```
http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALM
OID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$S
M$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth
.example.com
```

To specify this action URI, enter the following commands:

```
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these appear at the start of the URI in http://www.example.com.

Step 3 To configure a username parameter for the HTTP POST request, enter the **user-parameter** command in aaa-server-host configuration mode. For example, the following command configures the username parameter userid:

```
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

Step 4 To configure a user password parameter for the HTTP POST request, use the **password-parameter** command in aaa-server-host configuration mode. For example, the following command configures a user password parameter named user_password:

```
hostname(config-aaa-server-host)# password-parameter user_password
```

```
hostname(config-aaa-server-host)#
```

Step 5 To specify hidden parameters for exchange with the authenticating web server, use the **hidden-parameter** command in aaa-server-host configuration mode. An example hidden parameter excerpted from a POST request follows:

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

This hidden parameter includes four form entries and their values, separated by &. The four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason with a value of 0

To specify this hidden parameter, enter the following commands:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Fwww.example.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

Step 6 To specify the name for the authentication cookie, enter the **auth-cookie-name** command in aaa-server-host configuration mode. This command is optional. The following example specifies the authentication cookie name of SsoAuthCookie:

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
hostname(config-aaa-server-host)#
```

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. For more information on authentication and authorization using digital certificates, see "Using Certificates and User Login Credentials" in the "Configuring AAA Servers and the Local Database" chapter.

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

Chapter 30, "Configuring Tunnel Groups, Group Policies, and Users" includes step-by-step instructions for all of these tasks.

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. See

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 the configuration by letting you apply policies to many users. You can use an internal authentication server or a RADIUS server to assign users to group policies. See Chapter 30, "Configuring Tunnel Groups, Group Policies, and Users"for a thorough explanation of ways to simplify configuration with group policies.

Using the Security Appliance Authentication Server

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

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.)

Configuring WebVPN Tunnel Group Attributes

Table 37-1 provides a list of tunnel group attributes that are specific to WebVPN. In addition to these attributes, you configure general tunnel group attributes common to all VPN connections. For step-by-step information on configuring tunnel groups, see "Configuring WebVPN Tunnel Groups" in Chapter 30, "Configuring Tunnel Groups, Group Policies, and Users."

Table 37-1 WebVPN Tunnel Group Attributes

Command	Function
authentication	Sets the authentication method.
customization	Identifies the name of a previously defined customization to apply.
nbns-server	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
group-alias	Specifies the alternate names by which the server can refer to a tunnel group
group-url	Identifies one or more group URLs. If you configure this attribute, users coming in on a specified URL need not select a group at login
dns-group	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values
hic-fail-group-policy	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to "Use Failure Group-Policy" or "Use Success Group-Policy, if criteria match."

Configuring WebVPN Group Policy and User Attributes

Table 37-2 provides a list of WebVPN group policy and user attributes. For step-by-step instructions on configuring group policy and user attributes, see "Configuring Group Policies" and "Configuring Attributes for Specific Users"in Chapter 30, "Configuring Tunnel Groups, Group Policies, and Users."

Table 37-2 WebVPN Group Policy and User Attributes

Command	Function
auto-signon	Sets values for auto signon, which requires only that s user enter username and password credentials only once for a WebVPN connection.
customization	Assigns a customization object to a group-policy or user.
deny-message	Specifies the message delivered to a remote user who logs into WebVPN successfully, but has no VPN privileges.
filter	Sets the name of the webtype access list.
functions	Enables some or all of these WebVPN features: auto-download, Citrix, file access, file browsing, file entry, filter, http-proxy, URL entry, MAPI proxy, port forwarding.
homepage	Sets the URL of the web page that displays upon login.
html-content-filter	Configures the content and objects to filter from the HTML for this group policy.
http-comp	Configures compression.

Table 37-2 WebVPN Group Policy and User Attributes

Command	Function
keep-alive-ignore	Sets the maximum object size to ignore for updating the session timer.
port-forward	Applies a list of WebVPN TCP ports to forward. The user interface displays the applications on this list.
port-forward-name	Configures the name of the port forwarding applet.
sso-server	Sets the name of the SSO server.
svc	Configures SSL VPN Client attributes.
url-list	Applies a list of WebVPN servers and URLs that the user interface displays for end user access.

Configuring Application Access

The following sections provide information about configuring application access:

Downloading the Port-Forwarding Applet Automatically

Closing Application Access to Prevent hosts File Errors

Recovering from hosts File Errors When Using Application Access

Downloading the Port-Forwarding Applet Automatically

To run a remote application over WebVPN, a user clicks **Start Application Access** on the WebVPN homepage to download and start a port-forwarding Java applet. To simplify application access and shorten start time, you can configure WebVPN to automatically download this port-forwarding applet when the user first logs in to WebVPN.

To enable automatic download of the port-forwarding applet, enter the **functions** command in webvpn mode using the **auto-download** option.

Note Before you configure the auto-download feature, you must first enable an application that uses the applet: port forwarding, Outlook/Exchange proxy, or HTTP proxy.

Closing Application Access to Prevent hosts File Errors

To prevent hosts file errors that can interfere with Application Access, close the Application Access window properly when you finish using Application Access. To do so, click the close icon.

Recovering from hosts File Errors When Using Application Access

The following errors can occur if you do not close the Application Access 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
- Stopping Application Access Improperly
- Reconfiguring a hosts File

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

When Application Access terminates abnormally, the `hosts` file remains in a WebVPN-customized state. WebVPN checks the state the next time you start Application Access by searching for a hosts.webvpn file. If it finds one, a `Backup HOSTS File Found` error message (Figure 37-4) appears, 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 a hosts File

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 a 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."

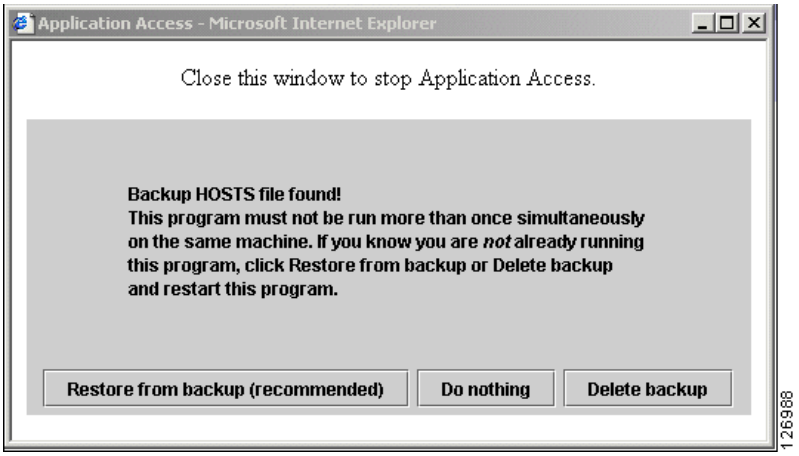
Reconfiguring a hosts File Automatically Using WebVPN

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 appears. (See Figure 37-4.)

Figure 37-4 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. The remote access home page reappears.
- **Delete backup** — WebVPN deletes the hosts.webvpn file, leaving the hosts file in its WebVPN-customized state. The original `hosts` file settings are lost. Application Access then 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. The most common location is c:\windows\sysem32\drivers\etc\hosts.

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.

Configuring File Access

The Common Internet File System (CIFS) protocol provides users with network access to files, printers, and other machine resources. Microsoft implemented CIFS for networks of Windows computers, however, open source implementations of CIFS provide file access to servers running other operating systems, such as Linux, UNIX, and Mac OS X.

WebVPN serves remote users with HTTPS portal pages that interface with a proxy CIFS client running on the security appliance. Using this client, WebVPN provides users with network access to the files on the network, to the extent that the users meet user authentication requirements and the file properties do not restrict access. The client is transparent; the portal pages delivered by WebVPN provide the appearance of direct access to the file systems.

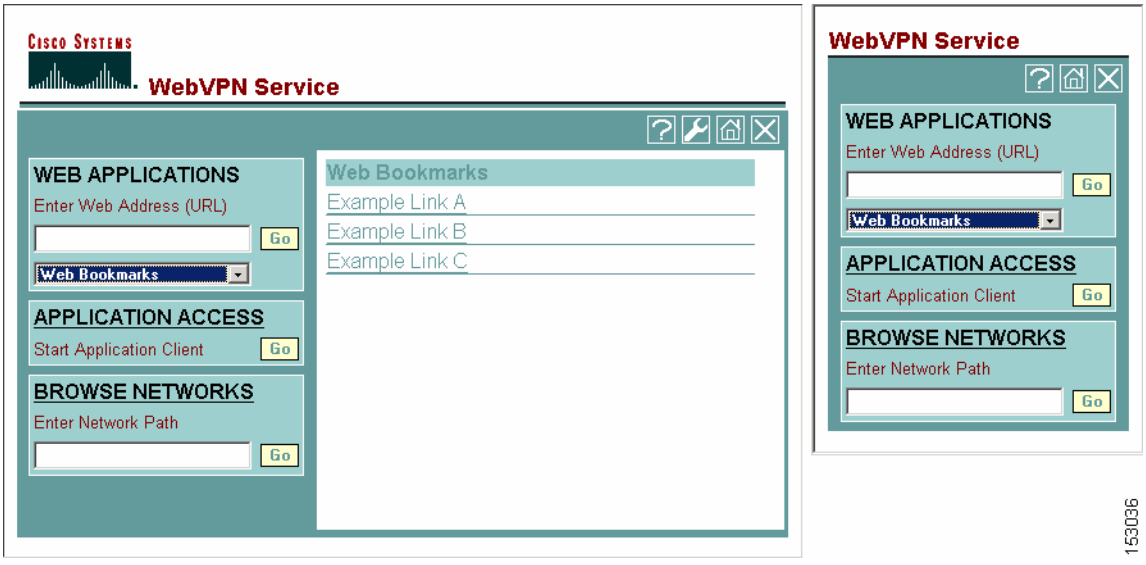
When a user requests a list of files, WebVPN queries the server designated as the master browser for the IP address of the server containing the list. The security appliance gets the list and delivers it to the remote user on a portal page.

WebVPN lets the user invoke the following CIFS functions, depending on user authentication requirements and file properties:

- Navigate and list domains and workgroups, servers within a domain or workgroup, shares within a server, and files within a share or directory
- Create directories
- Download, upload, rename, move, and delete files

The security appliance requires a master browser or WINS server, typically on the same network as the security appliance or reachable from that network, to query the network for a list of servers when the remote user clicks Browse Networks on the WebVPN home page or toolbar (Figure 37-5).

Figure 37-5 Browse Networks on the WebVPN Home Page and Floating Toolbar



The master browser provides the CIFS client on the security appliance with a list of the resources on the network, which WebVPN serves to the remote user. You cannot use a DNS server for a master browser. WebVPN supports file access in an Active Native Directory environment using a WINS server, but not a Dynamic DNS server.

Step 1 of the following procedure describes how to specify the master browser and WINS servers. As an alternative to following the instructions Step 1, you can use the **url-list** command in global configuration mode or in webvpn mode, which you enter from group-policy or username mode, to configure a server share in the File Folder Bookmarks. For example:

url-list *listname displayname* **cifs://***ServerA/ShareX/*

Using this method (adding a share) does not require a master browser or a WINS server, however, it does not provide support for the Browse Networks link. You can use a hostname or an IP address to refer to ServerA when entering this command. If you use a hostname, the security appliance requires a DNS server to resolve it to an IP address.

Note Before configuring file access, you must configure the shares on the servers for user access.

Add support for CIFS access to files as follows:

Step 1 Use the **nbns-server** command in tunnel-group webvpn configuration mode once for each NetBIOS Name Server (NBNS).

nbns-server {*IPaddress* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

master is the computer designated as the master browser. The master browser maintains the list of computers and shared resources. Any NBNS server you identify with this command without entering the master portion of the command must be a Windows Internet Naming Server (WINS). Specify the master browser first, then specify the WINS servers. You can specify up to three servers, including the master browser, for a tunnel group.

retries is the number of times to retry queries to the NBNS server. The security appliance recycles through the list of servers this number of times before sending an error message. The default value is 2; the range is 1 through 10.

timeout is the number of seconds the security appliance waits before sending the query again, to the same server if it is the only one, or another server if there are more than one. The default timeout is 2 seconds; the range is 1 to 30 seconds.

For example,

```
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.20 master
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.41
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.47
```

Note Use the **tunnel-group webvpn-attributes** command if you want to display the NBNS servers already present in the tunnel group configuration.

Step 2 (Optional) Use the **character-encoding** command to specify the character set to encode in WebVPN portal pages to be delivered to remote users. By default, the encoding type set on the remote browser determines the character set for WebVPN portal pages, so you need to set the character encoding only if it is necessary to ensure proper encoding on the browser.

character-encoding *charset*

Charset is a string consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
hostname(config-webvpn-custom)#
```

Step 3 (Optional) Use the **file-encoding** command to specify the encoding for WebVPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings.

file-encoding {server-name | server-ip-address} *charset*

The following example sets the file-encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias "CP860") characters:

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

Step 4 To configure security appliance support for file access, file browsing, and file server entry, use the **functions** command in webvpn mode, which you enter from group-policy or username mode.

functions file-access file-browsing file-entry

For example:

```
hostname(config-group-webvpn)# functions file-access file-browsing file-entry
hostname(config-group-policy)#
```

For a complete description of these commands, see the *Cisco Security Appliance Command Reference*.

Configuring Access to Citrix MetaFrame Services

WebVPN users can use a connection to the security appliance to access Citrix MetaFrame services. In this configuration, the security appliance functions as the Citrix secure gateway. Complete the following steps to configure support for Citrix MetaFrame services:

Step 1 Configure the Citrix Web Interface software to operate in a mode that does not use the secure gateway.

Step 2 Install an SSL certificate onto the security appliance interface to which remote users use a fully-qualified domain name (FQDN) to connect.

Note Do not specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN.

Step 3 Use the **functions citrix** command once for each group policy or user for which you want to enable Citrix support.

The following example shows how to configure Citrix for a group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup internal
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions citrix
hostname(config-group-webvpn)#
```

Using WebVPN with PDAs

You can access WebVPN from your Pocket PC or other certified personal digital assistant device. Neither the security appliance administrator nor the WebVPN user need do anything special to use WebVPN with a certified PDA.

Cisco has certified the following PDA platform:

HP iPaq H4150
Pocket PC 2003
Windows CE 4.20.0, build 14053
Pocket Internet Explorer (PIE)
ROM version 1.10.03ENG
ROM Date: 7/16/2004

Some differences in the PDA version of WebVPN exist:

- A banner web page replaces the popup WebVPN window.
- An icon bar replaces the standard WebVPN floating toolbar. This bar displays the Go, Home and Logout buttons.
- The Show Toolbar icon is not included on the main WebVPN portal page.
- Upon WebVPN logout, a warning message provides instructions for closing the PIE browser properly. If you do not follow these instructions and you close the browser window in the common way, PIE does not disconnect from WebVPN or any secure website that uses HTTPS.
- WebVPN supports OWA 2000 and OWA 2003 Basic Authentication. If Basic Authentication is not configured on an OWA server and a WebVPN user attempts to access that server, access is denied.
- Unsupported WebVPN features:
  - Application Access (port forwarding) and other Java-dependent features
  - MAPI proxy
  - HTTP proxy
  - Cisco Secure Desktop (CSD does provide limited support for Microsoft Windows CE)
  - Microsoft Outlook Web Access (OWA) 5.5

– The Citrix Metaframe feature (if the PDA does not have the corresponding Citrix ICA client software)

Using E-Mail over WebVPN

WebVPN supports several ways to access e-mail. This section includes the following methods:

- Configuring E-mail Proxies
- Configuring MAPI
- Configuring Web E-mail: MS Outlook Web Access

Configuring E-mail Proxies

WebVPN supports IMAP4S, POP3S, and SMTPS e-mail proxies. Table 37-3 lists attributes that apply globally to e-mail proxy users:

Table 37-3 WebVPN Attributes for E-mail Proxy Users

Function	Command	Default Value
Specifies the previously configured accounting servers to use with e-mail proxy.	**accounting-server-group**	None
Specifies the authentication method(s) for e-mail proxy users.	**authentication**	IMAP4S: Mailhost (required) POP3S Mailhost (required) SMTPS: AAA
Specifies the previously configured authentication servers to use with e-mail 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 e-mail proxy on the specified interface.	**enable**	Disabled
Defines the separator between the e-mail and VPN usernames and passwords.	**name-separator**	":" (colon)
Configures the maximum number of outstanding non-authenticated sessions.	**outstanding**	20
Sets the port the e-mail proxy listens to.	**port**	IMAP4S:993 POP3S: 995 SMTPS: 988[1]

Table 37-3 WebVPN Attributes for E-mail Proxy Users

Function	Command	Default Value
Specifies the default e-mail server.	**server**	None.
Defines the separator between the e-mail and server names.	**server-separator**	"@"

1. With the Eudora e-mail client, SMTPS works only on port 465, even though the default port for SMTPS connections is 988.

E-mail Proxy Certificate Authentication

Certificate authentication for e-mail proxy connections works with Netscape 7x e-mail clients. Other e-mail 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 webvpn 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 checks continually 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 E-mail: MS Outlook Web Access

The adaptive security appliance supports Microsoft Outlook Web Access to Exchange Server 2000, 2003, and 2007. It 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 e-mail server username in the format *domain\username*.
- Enter the e-mail password.

Optimizing WebVPN Performance

The security appliance provides several ways to optimize WebVPN performance and functionality. Performance improvements include caching and compressing web objects. Functionality tuning includes setting limits on content transformation and proxy-bypass. APCF provides an additional method of tuning content transformation. The following sections explain these features:

- Configuring Caching
- Configuring Content Transformation

Configuring Caching

Caching enhances WebVPN performance. It stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and the remote servers, with the result that many applications run much more efficiently.

By default, caching is enabled. You can customize the way caching works for your environment by using the caching commands in cache mode, which you enter from webvpn mode, as in the following example.

```
hostname(config)#
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

A list of caching commands and their functions follows:

Cache Command	Function
cache-compressed	Caches compressed content.
disable	Disables caching.
expiry-time	Configures an expiration time for caching objects.
lmfactor	Configures terms for revalidating cached objects.
max-object-size	Sets a maximum size for objects to cache.
min-object-size	Sets a minimum size for objects to cache.

Configuring Content Transformation

By default, the security appliance processes all WebVPN traffic through a content transformation/rewriting engine that includes advanced elements such as JavaScript and Java to proxy HTTP traffic that may have different semantics and access control rules depending on whether the user is accessing an application within or independently of an SSL VPN device.

Some web resources require highly individualized treatment. The following sections describe functionality that provides such treatment:

- Configuring a Certificate for Signing Rewritten Java Content
- Disabling Content Rewrite
- Using Proxy Bypass
- Configuring Application Profile Customization Framework

Subject to the requirements of your organization and the web content involved, you might use one of these features.

Configuring a Certificate for Signing Rewritten Java Content

Java objects which have been transformed by WebVPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. You import and employ the certificate using a combination of the **crypto ca import** and **java-trustpoint** commands.

The following example commands show the creation of a trustpoint named mytrustpoint and its assignment to signing Java objects:

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

Disabling Content Rewrite

You might not want some applications and web resources, for example, public websites, to go through the security appliance. The security appliance therefore lets you create rewrite rules that let users browse certain sites and applications without going through the security appliance. This is similar to split-tunneling in an IPSec VPN connection.

Use the **rewrite** command with the **disable** option in webvpn mode to specify applications and resources to access outside a WebVPN tunnel.

You can use the rewrite command multiple times. The order number of rules is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

Using Proxy Bypass

You can configure the security appliance to use proxy bypass when applications and web resources work better with the special content rewriting this feature provides. Proxy bypass is an alternative method of content rewriting that makes minimal changes to the original content. It is often useful with custom web applications.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the security appliance. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.mycompany.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.mycompany.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

To configure proxy bypass, use the **proxy-bypass** command in webvpn mode.

Configuring Application Profile Customization Framework

An APCF profile for WebVPN lets the security appliance handle non-standard applications and web resources so that they display correctly over a WebVPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application. The script is in XML and uses sed (stream editor) syntax for string/text transformation. Multiple APCF profiles can run in parallel on a security appliance. Within an APCF profile script, multiple APCF rules can apply. In this case, the security appliance processes the oldest rule first (based on configuration history), then the next oldest rule, and so forth.

You can store APCF profiles on the security appliance flash memory, or on an HTTP, HTTPS, or TFTP server. Use the **apcf** command in webvpn mode to identify and locate an APCF profile that you want to load on the security appliance.

The following example shows how to enable an APCF profile named apcf1.xml, located on flash memory.

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

This example shows how to enable an APCF profile named apcf2.xml, located on an https server called myserver, port 1440 with the path being /apcf.

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

APCF Syntax

The following sections describe APCF syntax.

Caution Misuse of an APCF profile can result in reduced performance and undesired rendering of content. In most cases, Cisco Engineering supplies APCF profiles to solve specific application rendering issues.

APCF profiles use XML format, and sed script syntax, with the XML tags in Table 37-4

Table 37-4 APCF XML Tags

Tag	Use
<APCF>...</APCF>	The mandatory root element that opens any APCF XML file.
<version>1.0</version>	The mandatory tag that specifies the APCF implementation version. Currently the only version is 1.0.
<application>...</application>	The mandatory tag that wraps the body of the XML description.
<id> text </id>	The mandatory tag that describes this particular APCF functionality.
<apcf-entities>...</apcf-entities>	The mandatory tag that wraps a single or multiple APCF entities.

Table 37-4 APCF XML Tags (continued)

Tag	Use
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</process-request-header> <process-response-header>...</process-response-header> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	One of theses tags specifying type of content or the stage at which the APCF processing should take place is required.
<conditions>… </conditions>	A child element of the pre/post-process tags that specifies criteria for processing such as: http-version (such as 1.1, 1.0, 0.9) http-method (get, put, post, webdav) http-scheme (http, https, other) server-regexp regular expression containing ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?")) server-fnmatch (regular expression containing ("a".."z" | "A".."Z" | "0".."9" | ".-_*[]?+()\{},")), user-agent-regexp user-agent-fnmatch request-uri-regexp request-uri-fnmatch If more than one of condition tags is present, the security appliance performs a logical AND for all tags.
<action> … </action>	Wraps one or more actions to perform on the content under specified conditions; you can use the following tags to define these actions (shown below): <do>, <sed-script>, <rewrite-header>, <add-header>, <delete-header>.
<do>…</do>	Child element of the action tag used to define one of the following actions: <no-rewrite/>—Do not mangle the content received from the remote server. <no-toolbar/>—Do not insert the toolbar. <no-gzip/>—Do not compress the content. <force-cache/>—Preserve the original caching instructions. <force-no-cache/>—Make object non-cacheable. < downgrade-http-version-on-backend>—Use HTTP/1.0 when sending the request to remote server.

Table 37-4 APCF XML Tags (continued)

Tag	Use
<sed-script> TEXT </sed-script>	Child element of the action tag used to change the content of text-based objects. The Text must be a valid Sed script. The <sed-script> applies to the <conditions> tag defined before it.
<rewrite-header></rewrite-header>	Child element of the action tag. Changes the value of the HTTP header specified in the child element <header> tag shown below.
<add-header></add-header>	Child element of the action tag used to add a new HTTP header specified in the child element <header> tag shown below.
<delete-header></delete-header>	Child element of the action tag used to delete the specified HTTP header specified by the child element <header> tag shownbelow.

<header></header>	Specifies the name HTTP header to be rewritten, added, or deleted. For example, the following tag changes the value of the HTTP header named Connection:
	`<rewrite-header>`
	`<header>Connection</header>`
	`<value>close</value>`
	`</rewrite-header>`

APCF Example 1

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from notsogood.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.notsogood.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

APCF Example 2

```
<APCF>
<version>1.0</version>
<application>
 <id>Change MIME type for all .xyz objects</id>
 <apcf-entities>
      <process-response-header>
        <conditions>
            <request-uri-fnmatch>*.xyz</request-uri-fnmatch>
        </conditions>
         <action>
```

```
            <rewrite-header>
                 <header>Content-Type</header>
                 <value>text/html</value>
            </rewrite-header>
          </action>
       </process-response-header>
 </apcf-entities>
</application>
</APCF>
```

WebVPN End User Setup

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

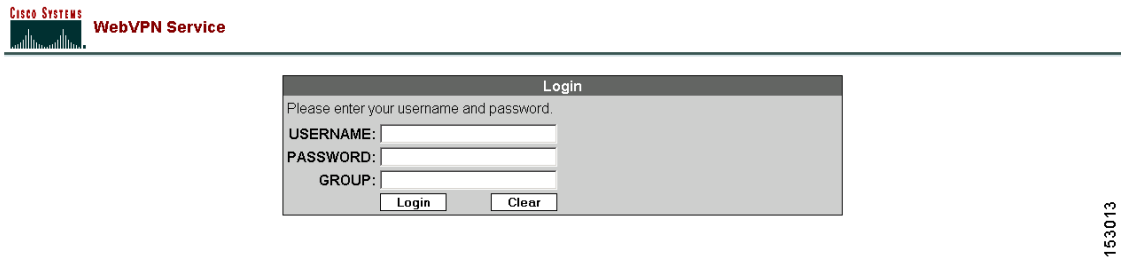
This section summarizes configuration requirements and tasks for a remote system. It specifies information to communicate to users to get them started using WebVPN. It includes the following topics:

- Defining the End User Interface
- Customizing WebVPN Pages, page 37-36
- Requiring Usernames and Passwords
- Communicating Security Tips
- Configuring Remote Systems to Use WebVPN Features

Defining the End User Interface

The WebVPN end user interface consists of 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 (Figure 37-6).

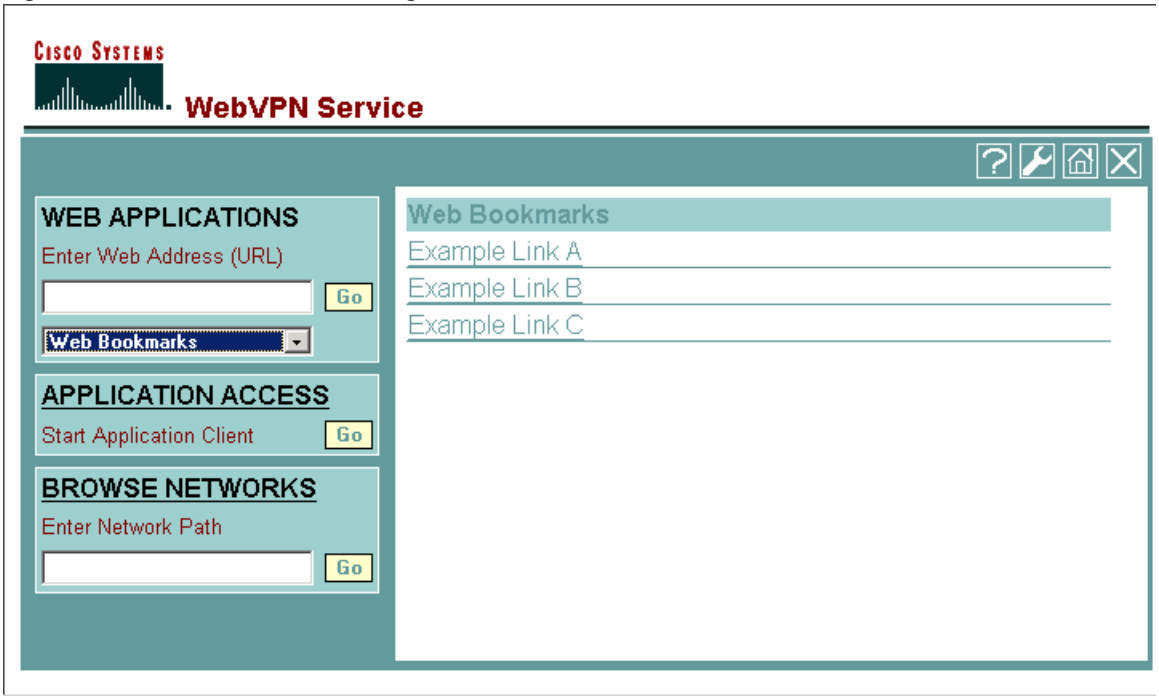
Figure 37-6 WebVPN Login Screen



Viewing the WebVPN Home Page

After the user logs in, the WebVPN Home page opens (Figure 37-7).

Figure 37-7 WebVPN Home Page

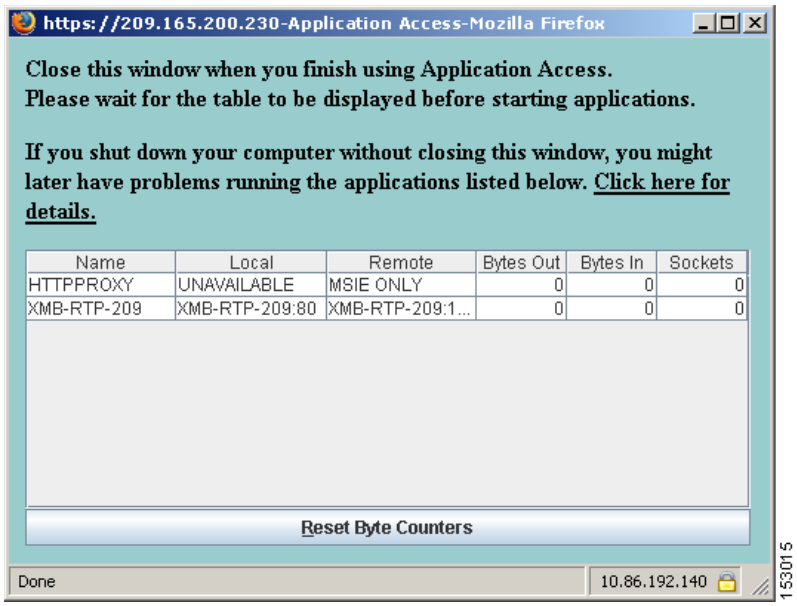


The home page displays all of the WebVPN features you have configured, and its appearance reflects the logo, text, and colors you have selected. This sample home page includes all available WebVPN features with the exception of identifying specific file shares. It lets users browse the network, enter 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 Go button in the Application Access box. The Application Access window opens (Figure 37-8).

Figure 37-8 WebVPN Application Access Windowl



This window 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

The floating toolbar shown in Figure 37-9 represents the current WebVPN session.

Figure 37-9 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.
- If you close the toolbar, the security appliance prompts you to confirm that you want to end the WebVPN session.

See Table 37-6 on page 37-47 for detailed information about using WebVPN.

Customizing WebVPN Pages

You can change the appearance of WebVPN pages displayed to WebVPN users. This includes the Login page displayed to users when they connect to the security appliance, the Home page displayed to users after the security appliance authenticates them, the Application Access window displayed when users launch an application, and the Logout page displayed when users logout of WebVPN service.

After you customize the WebVPN pages, you can save your customization and apply it to a specific tunnel group, group, or user. You can create and save many customizations, enabling the security appliance to change the appearance of WebVPN pages for individual users, or group of users.

This section contains the following topics and tasks:

- Using Cascading Style Sheet Parameters, page 37-36
- Customizing the WebVPN Login Page, page 37-37
- Customizing the WebVPN Logout Page, page 37-38
- Customizing the WebVPN Home Page, page 37-39
- Customizing the Application Access Window, page 37-41
- Customizing the Prompt Dialogs, page 37-42
- Applying Customizations to Tunnel Groups, Groups and Users, page 37-43

Using Cascading Style Sheet Parameters

Many WebVPN customization commands contain the **style** option. The value is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

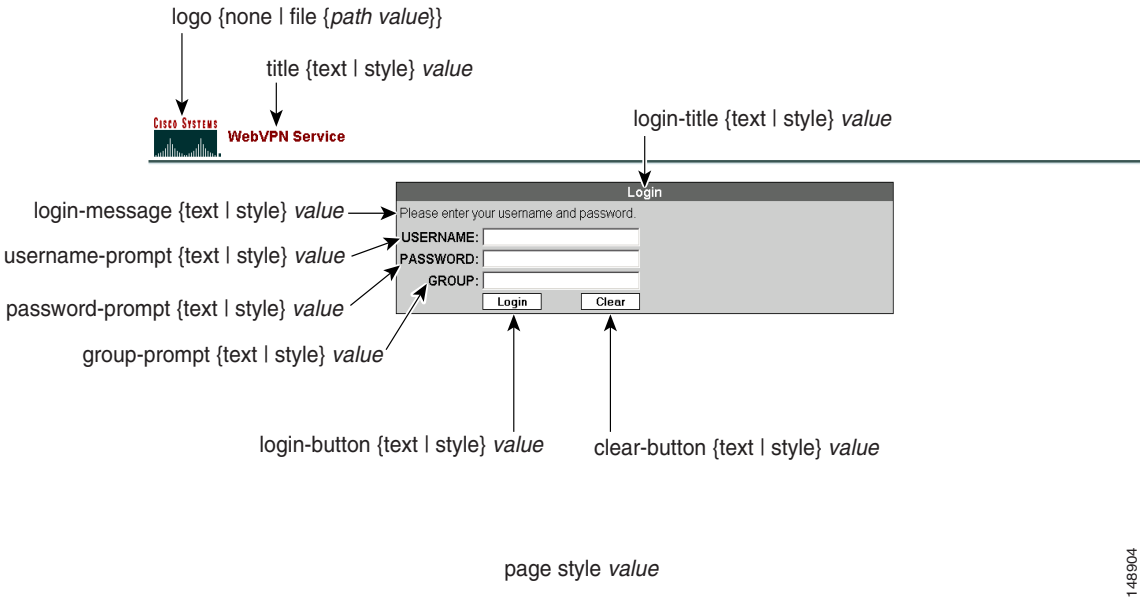
- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Customizing the WebVPN Login Page

Figure 37-10 shows the WebVPN Login page and associated CLI commands that you can use to customize the page.

Figure 37-10 WebVPN Login Page and Associated CLI Commands



The following procedure guides you through customizing every element of the WebVPN Login page using CLI commands and includes examples of the commands:

Step 1 Enter WebVPN customization mode using the **customization** command from webvpn mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

Step 2 Change the CSS style of the WebVPN Login page using the **page style** command:

[no] page style *value*

```
hostname(config-webvpn-custom)# page style font-size:large
```

Step 3 Change the title using the **title** command:

[no] title {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

Step 4 Change the logo with a logo residing in flash memory using the **logo** command:

[no] logo {none | file {*path value***}}**

To disallow a logo and prevent inheriting a logo, **use the none** option to set a null value.

```
hostname(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Step 5 Change the title of the Login box using the **login-title** command:

[**no**] **login-title** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Step 6 Change the message of the Login box using the **login-message** command:

[**no**] **login-message** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-message text username and password
```

Step 7 Change the username prompt of the Login box using the **username-prompt** command:

[**no**] **username-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# username-prompt text Corporate Username:
hostname(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Step 8 Change the password prompt of the Login box using the **password-prompt** command:

[**no**] **password-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# password-prompt text Corporate Username:
hostname(config-webvpn-custom)# password-prompt style font-weight:bolder
```

Step 9 Change the group prompt of the Login box using the **group-prompt** command:

[**no**] **group-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# group-prompt text Corporate Group:
hostname(config-webvpn-custom)# group-prompt style font-weight:bolder
```

Step 10 Change the content or appearance of the Login button of the Login box using the **login-button** command:

[**no**] **login-button** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-button text OK
```

Step 11 Change the content or appearance of the Clear button of the Login box using the **clear-button** command:

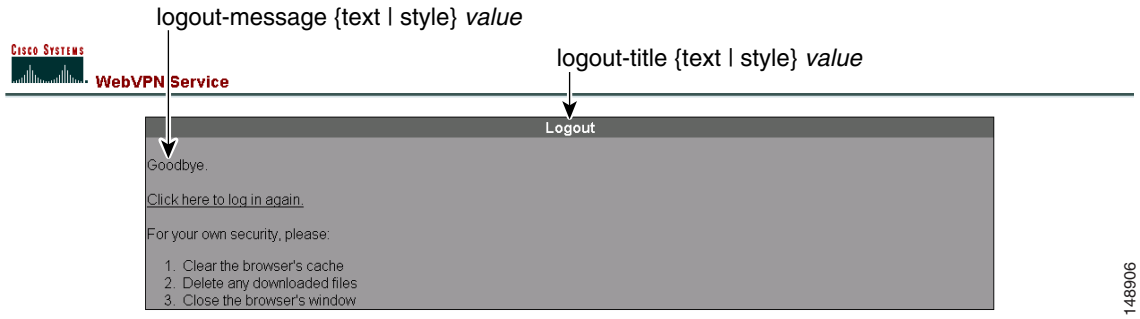
[**no**] **clear-button** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# clear-button background-color:blue
```

Customizing the WebVPN Logout Page

The security appliance displays the WebVPN Logout page when WebVPN users log out of WebVPN service. Figure 37-11 shows the WebVPN Logout page and the associated CLI commands that you can use to customize the page.

Figure 37-11 WebVPN Logout Page



The following procedure guides you through customizing the WebVPN Logout page using CLI commands and includes examples of the commands:

Step 1 Enter WebVPN customization mode using the **customization** command from webvpn mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

Step 2 Change the title of the Logout box using the **logout-title** command:

[no] logout-title {text | style} *value*

```
hostname(config-webvpn-custom)# logout-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Step 3 Change the message of the Logout box using the **logout-message** command:

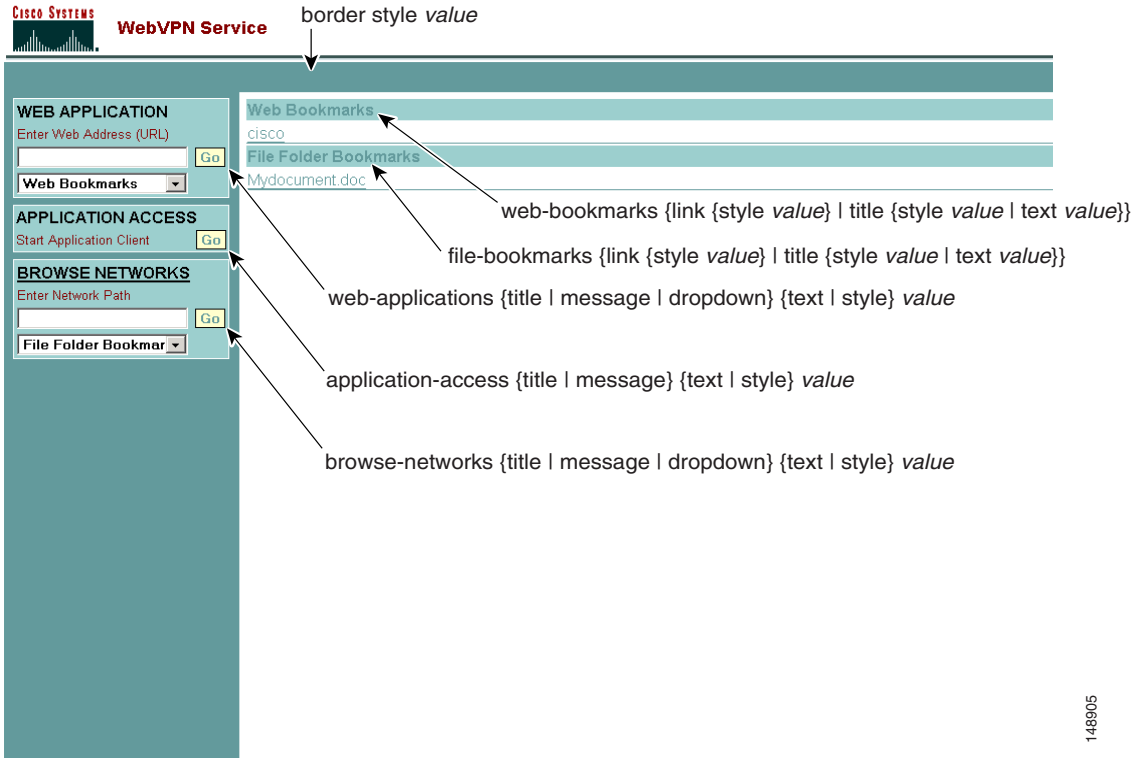
[no] logout-message {text | style} *value*

```
hostname(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Customizing the WebVPN Home Page

You can customize the appearance of the WebVPN Home page that the security appliance displays to authenticated WebVPN users. Figure 37-12 shows the WebVPN Home page and associated CLI commands that you can use to customize the page.

Figure 37-12 WebVPN Home Page and Associated CLI Commands



The following procedure guides you through customizing every element of the WebVPN Home page using CLI commands and includes examples of the commands:

Step 1 Enter WebVPN customization mode using the **customization** command from webvpn mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

Step 2 Change the border of the WebVPN page using the **border style** command and CSS parameters:

[no] border style *value*

```
hostname(config-webvpn-custom)# border style background-color:66FFFF
```

Step 3 Change the appearance of the Web Applications box using the **web-applications** command:

[no] web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# web-applications title text WWW Applications
hostname(config-webvpn-custom)# web-applications title style color:blue
hostname(config-webvpn-custom)# web-applications message text Enter URL
hostname(config-webvpn-custom)# web-applications message style color:blue
hostname(config-webvpn-custom)# web-applications dropdown text URLs to Browse
hostname(config-webvpn-custom)# web-applications dropdown style color:red
```

Step 4 Change the appearance of the Application Access box using the **application-access** command**:**

[no] application-access {**title** | **message**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# application-access title text Applications
hostname(config-webvpn-custom)# application-access title style color:blue
hostname(config-webvpn-custom)# application-access message text Start Application
```

```
hostname(config-webvpn-custom)# application-access message style color:blue
```

Step 5 Change the appearance of the Browse Networks box using the **browse-networks** command:

[**no**] **browse-networks** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# browse-networks title text Corporate Nets
hostname(config-webvpn-custom)# browse-networks title style color:blue
hostname(config-webvpn-custom)# browse-networks message text Enter URL
hostname(config-webvpn-custom)# browse-networks message style color:blue
hostname(config-webvpn-custom)# browse-networks dropdown text URLs to Browse
hostname(config-webvpn-custom)# browse-networks dropdown style color:red
```

Step 6 Change the Web Bookmarks title or links using the **web-bookmarks** command:

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

```
hostname(config-webvpn-custom)# web-bookmarks link style color:black
hostname(config-webvpn-custom)# web-bookmarks title style color:black
hostname(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

Step 7 Change the File Bookmarks title or the File Bookmarks links using the **file-bookmarks** command:

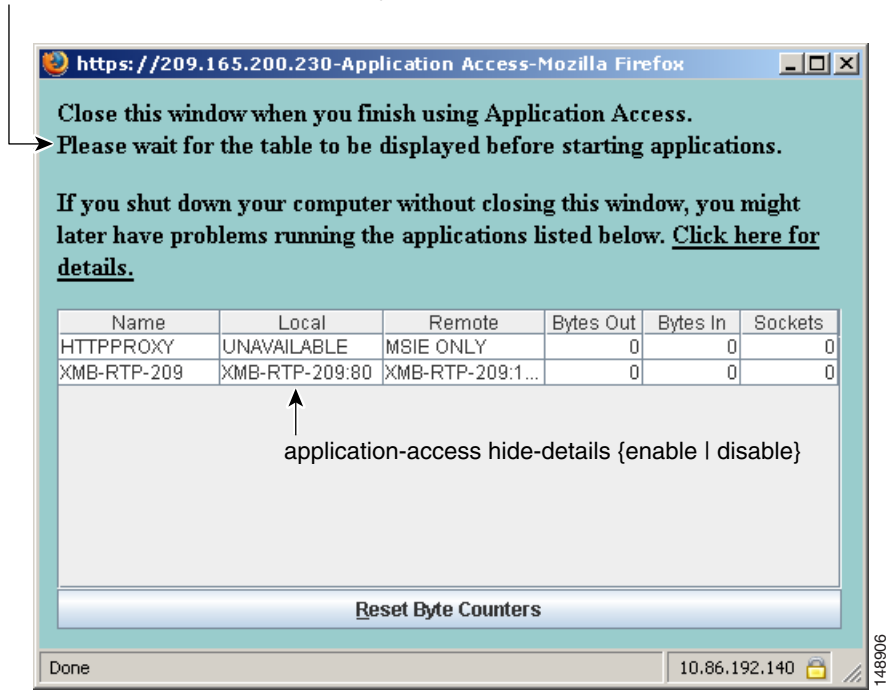
[**no**] **file-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

```
hostname(config-webvpn-custom)# file-bookmarks link style color:blue
hostname(config-webvpn-custom)# file-bookmarks title style color:blue
hostname(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

Customizing the Application Access Window

You can customize the Application Access window that launches when the remote user selects an application. Figure 37-13 shows the Application Access window and the associated CLI commands that you can use to customize it.

Figure 37-13 Application Access Window



The following procedure guides you through customizing the Application Access window using CLI commands and includes examples of the commands:

Step 1 Enter WebVPN customization mode using the **customization** command from webvpn mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

Step 2 Change the Application Access window using the **application-access window** command**:**

[no] application-access window {text | style} *value*

```
hostname(config-webvpn-custom)# application-access window text URLs to Browse
hostname(config-webvpn-custom)# application-access window style color:red
```

Step 3 Enable or disable the Hiding of application details displayed in the WebVPN Applications Access window using the **application-access hide-details** command:

[no] application-access hide-details {enable | disable}

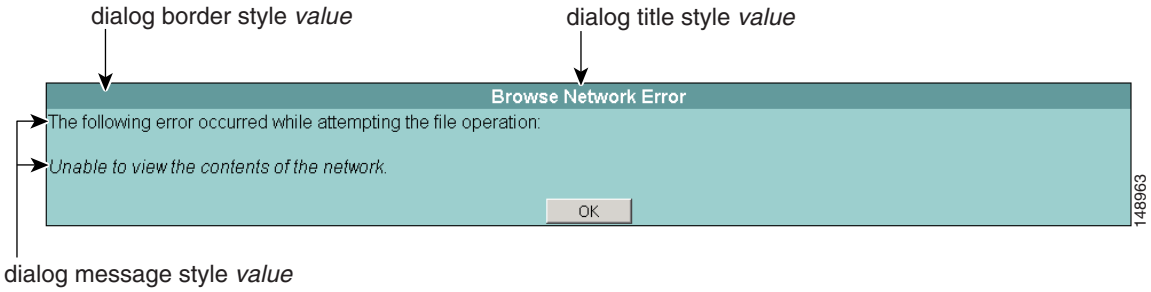
The default is disabled. Application details are not hidden—they display in the Application Access window.

```
hostname(config-webvpn-custom)# application-access hide-details enable
```

Customizing the Prompt Dialogs

The security appliance may send WebVPN users various prompt dialog messages as notices or warnings. Figure 37-14 shows a sample dialog message and the associated CLI commands you can use to customize the appearance of these messages.

Figure 37-14 Dialog Message and Associated CLI Command



The following procedure customizes every element of the dialog message and includes examples of the commands:

Step 1 Enter WebVPN customization mode using the **customization** command from webvpn mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

Step 2 Customize the border of the dialog messages with the **dialog border** command:

[no] dialog border style *value*

```
hostname(config-webvpn-custom)# dialog border style color:blue
```

Step 3 Change the appearance of the title using the **dialog title** command:

[no] dialog title style *value*

```
hostname(config-webvpn-custom)# dialog title style font:bolder
```

Step 4 Change the appearance of the message using the **dialog message** command:

[no] dialog message style *value*

```
hostname(config-webvpn-custom)# dialog message style font:italic
```

Applying Customizations to Tunnel Groups, Groups and Users

After you create a customization, you can apply the customization to a tunnel group, a group, or a user, with the **customization** command. The options displayed with this command are different depending on the mode you are in.

For more information about configuring tunnel groups, group policies, and users, see Chapter 30, "Configuring Tunnel Groups, Group Policies, and Users".

Applying Customizations to Tunnel Groups

To apply a customization to a tunnel group, use the **customization** command from tunnel group webvpn mode:

[no] customization *name*

name is the name of a customization to apply to the tunnel group.

To remove the command from the configuration, and remove a customization from the tunnel group, use the **no** form of the command.

Enter the **customization command followed by a question mark (?)** to view a list of existing customizations.

In the following example, the user enters tunnel group webvpn mode and enables the customization *cisco* for the tunnel group *cisco_telecommuters*:

```
hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes
hostname(tunnel-group-webvpn)# customization cisco
```

Applying Customizations to Groups and Users

To apply a customization to a group or user, use the **customization** command from group policy webvpn mode or username webvpn mode. In these modes, the **none** and **value** options are included:

[**no**] **customization {none | value** *name*}

none disables the customization for the group or user, prevents the value from being inherited, and displays the default WebVPN pages.

value *name* is the name of a customization to apply to the group or user.

To remove the command from the configuration, and cause the value to be inherited, use the **no** form of the command.

Enter the **customization value command followed by a question mark (?)** to view a list of existing customizations.

In the following example, the user enters group policy webvpn mode, queries the security appliance for a list of customizations, and enables the customization *cisco* for the group policy *cisco_sales*:

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# customization value ?

config-username-webvpn mode commands/options:
Available configured customization profiles:
    DfltCustomization
    cisco
hostname(config-group-webvpn)# customization value cisco
```

In the next example, the user enters username webvpn mode and enables the customization *cisco* for the user *cisco_employee*:

```
hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value cisco
```

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 service 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 PIN.

Table 37-5 lists the type of usernames and passwords that WebVPN users might need to know.

Table 37-5 Usernames and Passwords to Give to 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 e-mail messages

Communicating Security Tips

Advise users always to click the logout icon on the WebVPN toolbar to log out from the WebVPN session. (Closing the browser window does not close the session.)

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 a 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 37-6 includes the following information about setting up remote systems to use WebVPN:

- Starting WebVPN
- Using the WebVPN Floating Toolbar
- Web Browsing
- Network Browsing and File Management
- Using Applications (Port Forwarding)
- Using E-mail via Port Forwarding
- Using E-mail via Web Access
- Using E-mail via e-mail proxy

Table 37-6 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. Table 37-6 organizes information by feature, so you can skip over the information for unavailable features.

Table 37-6 WebVPN Remote System Configuration and End User Requirements

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Starting WebVPN	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
	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 later • 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.
	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.
	WebVPN username and password	
	[Optional] Local printer	WebVPN does not support printing from a web browser to a network printer. Printing to a local printer is supported.

Table 37-6 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 "Communicating Security Tips." The look and feel of web browsing with WebVPN might be different from what users are accustomed to. For example: • 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 37-6 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.
	—	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 37-6 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 or full control of C:\windows\System32\drivers\etc, 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 When Using Application Access for details.	
	Client applications installed	—
	Cookies enabled on browser	—
	Administrator privileges	User must have administrator access on the PC if you use DNS names to specify servers because modifying the hosts file requires it.
	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 appears. 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 Clicking a URL (such as one in an -e-mail message) in an application running over WebVPN does not open the site over WebVPN. To open a site over WebVPN, cut and paste the URL into the Enter WebVPN (URL) Address field.	

Table 37-6 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Using E-mail 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 e-mail programs via port forwarding, such as Netscape Mail, Lotus Notes, and Eudora, but we have not verified them.
Using E-mail via Web Access	Web-based e-mail product installed	Supported: • Microsoft Outlook Web Access to Exchange Server 2000, 2003, and 2007. For best results, use OWA on Internet Explorer 6.x or higher, Mozilla 1.7, or Firefox 1.x. • Lotus iNotes Other web-based e-mail products should also work, but we have not verified them.
Using E-mail via E-mail 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 "Using E-Mail over WebVPN."

Capturing WebVPN Data

The CLI capture command lets you log information about websites that do not display properly over a WebVPN connection. This data can help your Cisco customer support engineer troubleshoot problems. The following sections describe how to use the capture command:

- Creating a Capture File
- Using a Browser to Display Capture Data

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

Creating a Capture File

Perform the following steps to capture data about a WebVPN session to a file.

Step 1 To start the WebVPN capture utility, use the **capture** command from privileged EXEC mode.

capture *capture_name* **type webvpn user** *webvpn_username*

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.

The capture utility starts.

Step 2 A WebVPN user logs in to begin a WebVPN session. The capture utility is capturing packets.

Stop the capture by using the **no** version of the command.

no capture *capture_name*

The capture utility creates a *capture_name*.zip file, which is encrypted with the password **koleso**.

Step 3 Send the .zip file to Cisco Systems, or attach it to a Cisco TAC service request.

Step 4 To look at the contents of the .zip file, unzip it using the password **koleso**.

The following example creates a capture named *hr*, which captures WebVPN traffic for user2 to a file:

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

Using a Browser to Display Capture Data

Perform the following steps to capture data about a WebVPN session and view it in a browser.

Step 1 To start the WebVPN capture utility, use the **capture** command from privileged EXEC mode.

capture *capture_name* **type webvpn user** *webvpn_username*

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.

The capture utility starts.

Step 2 A WebVPN user logs in to begin a WebVPN session. The capture utility is capturing packets.

Stop the capture by using the **no** version of the command.

Step 3 Open a browser and in the address box enter

https://*IP_address or hostname of the security appliance***/webvpn_capture.html**

The captured content displays in a sniffer format.

Step 4 When you finish examining the capture content, stop the capture by using the **no** version of the command.