SSL VPN–WebVPN

First Published: February 27, 2006
Last Updated: August 3, 2006

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

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for SSL VPN–WebVPN" section on page 195.

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

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

Prerequisites for WebVPN

- To securely access resources on a private network behind a WebVPN gateway, the remote user of a WebVPN service must have the following:
  - An account (login name and password)
  - An SSL-enabled browser (for example, Internet Explorer, Netscape, Mozilla, or FireFox)
  - E-mail client, such as Eudora, Microsoft Outlook, or Netscape Mail.
  - The Microsoft Windows 2000 or Windows XP operating system with either the Sun MicroSystems Java Runtime Environment (JRE) for Windows version 1.4 or later or a browser that supports Active X control.

  or

  - The Linux operating system with Sun MicroSystems JRE for Linux version 1.4 or later. To access Microsoft file shares from Linux in clientless remote access mode, Samba must also be installed.
- "Thin Client" support used for TCP port-forwarding applications requires administrative privileges on the computer of the remote user.
- "Tunnel mode" support used for Cisco SSL VPN access requires administrative privileges on the computer of the remote user.
- The remote user must have local administrative privileges to use thin client or full tunnel client features.
- The WebVPN gateway and context configuration must be completed before a remote user can access resources on a private network behind a WebVPN. This configuration is shown in the section "How to Configure WebVPN Services on a Router."

Restrictions for WebVPN

- URLs referred by the Macromedia Flash player cannot be modified for secure retrieval by the WebVPN gateway.

Information About WebVPN

To configure WebVPN, you should understand the following concepts:

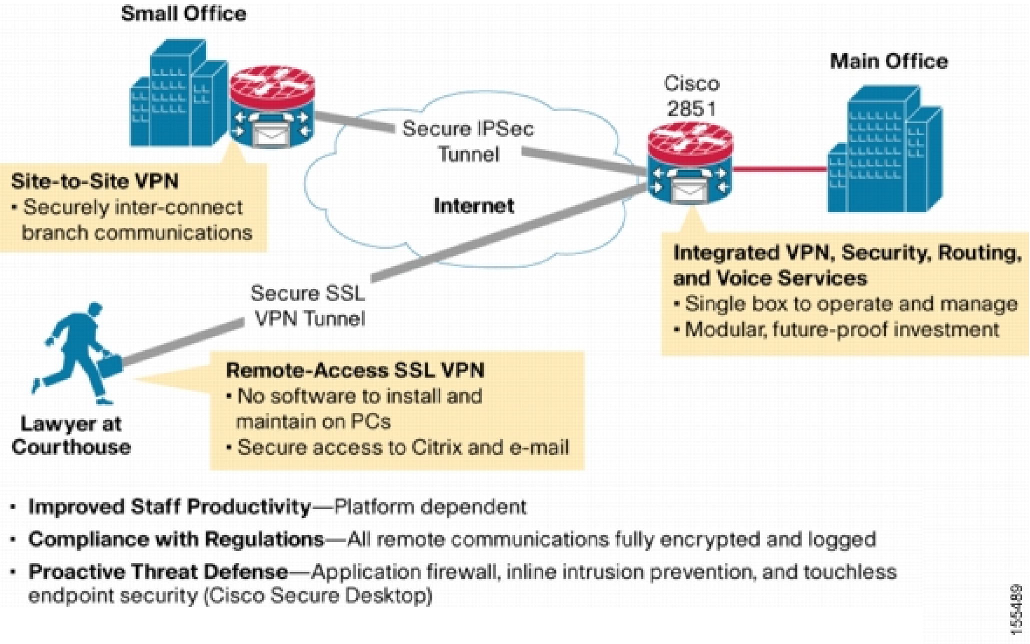
WebVPN Overview

Cisco IOS WebVPN provides SSL VPN remote-access connectivity from almost any Internet-enabled location using only a web browser that natively supports SSL encryption. This feature allows your company to extend access to its secure enterprise network to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS WebVPN can also support access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hotspots. These locations are difficult places to deploy and manage VPN client software and remote configuration required to support IPsec VPN connections.

Figure 1 shows how a mobile worker (the lawyer at the courthouse) can access protected resources from the main office and branch offices. Site-to-site IPsec connectivity between the main and remote sites is unaltered. The mobile worker needs only Internet access and supported software (web browser and operating system) to securely access the corporate network.

Figure 1 Secure WebVPN Access Model


Small Office
Main Office
Cisco 2851
Secure IPSec Tunnel
Internet
Site-to-Site VPN
• Securely inter-connect branch communications
Integrated VPN, Security, Routing, and Voice Services
• Single box to operate and manage
• Modular, future-proof investment
Secure SSL VPN Tunnel
Lawyer at Courthouse
Remote-Access SSL VPN
• No software to install and maintain on PCs
• Secure access to Citrix and e-mail
• Improved Staff Productivity—Platform dependent
• Compliance with Regulations—All remote communications fully encrypted and logged
• Proactive Threat Defense—Application firewall, inline intrusion prevention, and touchless endpoint security (Cisco Secure Desktop)
155489

SSL VPN–WebVPN delivers the following three modes of SSL VPN access:

- *Clientless*—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to access in a web browser, such as Internet access, databases, and online tools that employ a web interface.
- *Thin Client* (port-forwarding Java applet)—Thin client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).

- *Tunnel Mode*—Full tunnel client mode offers extensive application support through its dynamically downloaded SSL VPN Client for WebVPN. Full tunnel client mode delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application.

SSL VPN application accessibility is somewhat constrained relative to IPsec VPNs; however, SSL-based VPNs provide access to a growing set of common software applications, including web page access, web-enabled services such as file access, e-mail, and TCP-based applications (by way of a downloadable thin-client applet). SSL-based VPN requires slight changes to user workflow because some applications are presented through a web browser interface, not through their native GUI. The advantage for SSL VPN comes from accessibility from almost any Internet-connected system without needing to install additional desktop software.

Modes of Remote Access

End-user login and authentication is performed by the web browser to the secure gateway using an HTTP request. This process creates a session that is referenced by a cookie. After authentication, the remote user is shown a portal page that allows access to the WebVPN networks. All requests sent by the browser include the authentication cookie. The portal page provides all the resources available on the internal networks. For example, the portal page could provide a link to allow the remote user to download and install a thin-client Java applet (for TCP port forwarding) or a tunneling client.

Figure 2 shows an overview of the remote access modes.

Figure 2 Modes of Remote Access Overview

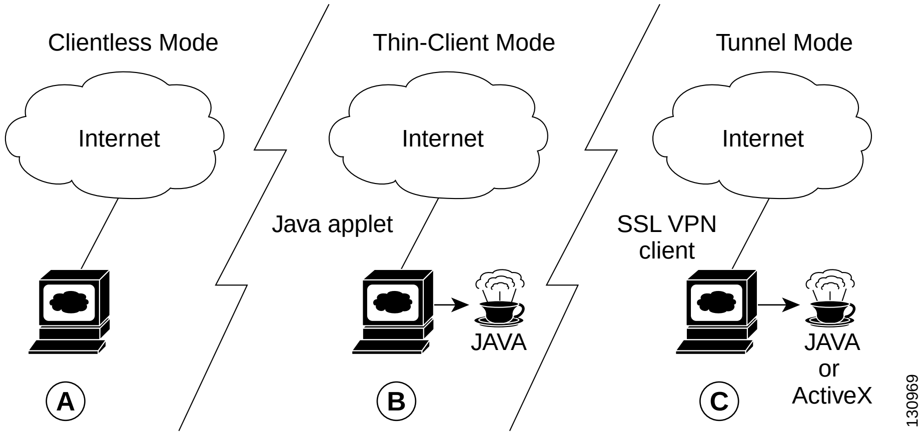


Table 1 summarizes the level of SSL VPN support that is provided by each access mode.

Table 1 Access Mode Summary

A	Clientless Mode	B	Thin-Client Mode	C	Tunnel Mode
	• Browser-based (clientless) • Microsoft Windows or Linux • Web-enabled applications, file sharing, Outlook Web Access • Gateway performs address or protocol conversion and content parsing and rewriting		• TCP port forwarding • Uses Java Applet • Extends application support • Telnet, e-mail, SSH, Meeting Maker, Sametime Connect • Static port-based applications		• Works like “clientless” IPsec VPN • Tunnel client loaded through Java or ActiveX (approximately 500 kB) • Application agnostic—supports all IP-based applications • Scalable • Local administrative permissions required for installation

Clientless Mode

In clientless mode, the remote user accesses the internal or corporate network using the web browser on the client machine. The PC of the remote user must run the Windows 2000, Windows XP, or Linux operating systems.

The following applications are supported in clientless mode:

- Web browsing (using HTTP and secure HTTP [HTTPS])—provides a URL box and a list of web server links in the portal page that allows the remote user to browse the web.
- File sharing (using common Internet file system [CIFS])—provides a list of file server links in the portal page that allows the remote user to do the following operations:
  - Browse a network (listing of domains)
  - Browse a domain (listing of servers)
  - Browse a server (listing of shares)
  - List the files in a share
  - Create a new file
  - Create a directory
  - Rename a directory
  - Update a file
  - Download a file
  - Remove a file
  - Rename a file

Note Linux requires that the Samba application is installed before CIF file shares can be remotely accessed.

- Web-based e-mail, such as Microsoft Outlook Web Access (OWA) 2003 (using HTTP and HTTPS) with Web Distributed Authoring and Versioning (WebDAV) extensions—provides a link that allows the remote user to connect to the exchange server and read web-based e-mail.

Thin-Client Mode

Thin-client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port. In thin-client mode, the remote user downloads a Java applet by clicking the link provided on the portal page. The Java applet acts as a TCP proxy on the client machine for the services that you configure on the gateway.

The applications that are supported in thin-client mode are mainly e-mail-based (SMTP, POP3, and Internet Map Access Protocol version 4 [IMAP4] applications.

Note The TCP port-forwarding proxy works only with the Sun MicroSystems (JRE) version 1.4 or later versions. A Java applet is loaded through the browser that verifies the JRE version. The Java applet will refuse to run if a compatible JRE version is not detected.

The Java applet initiates an HTTP request from the remote user client to the WebVPN gateway. The name and port number of the internal e-mail server is included in the HTTP request (POST or CONNECT). The WebVPN gateway creates a TCP connection to that internal e-mail server and port.

The Java applet starts a new SSL connection for every client connection.

You should observe the following restrictions when using thin-client mode:

- The remote user must allow the Java applet to download and install.
- You cannot use thin-client mode for applications such as FTP, where the ports are negotiated dynamically. You can use TCP port forwarding only with static ports.
- For applications to work seamlessly, you should give administrative privileges to remote users. If you do not give administrative privileges to remote users, remote users may need to manually change the client program settings so that applications work properly.

Note There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, remove the line from the webvpn gateway subconfiguration.

Automatic Applet Download

Effective with Cisco IOS Release 12.4(9)T, administrators have the option of automatically downloading the port-forwarding Java applet. This feature must be configured on a group policy basis.

Note Users still have to allow the Java applet to be downloaded. The dialog box pops up, asking for permission.

To configure the automatic download, see the section “Configuring a WebVPN Policy Group.”

Tunnel Mode

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

The tunnel connection is determined by the group policy configuration. The SSL VPN client (SVC) is downloaded and installed to the remote user PC, and the tunnel connection is established when the remote user logs into the WebVPN gateway.

By default, the SVC is removed from the client PC after the connection is closed. However, you have the option to keep the SVC installed on the client PC.

WebVPN RADIUS Accounting

Effective with Cisco IOS Release 12.4(9)T, this feature provides for RADIUS accounting of SSL VPN user sessions.

For information about configuring WebVPN RADIUS accounting for SSL VPN user sessions, see the section "Configuring RADIUS Accounting for SSL VPN User Sessions."

For more information about configuring RADIUS accounting, see the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part10/ch05/index.htm

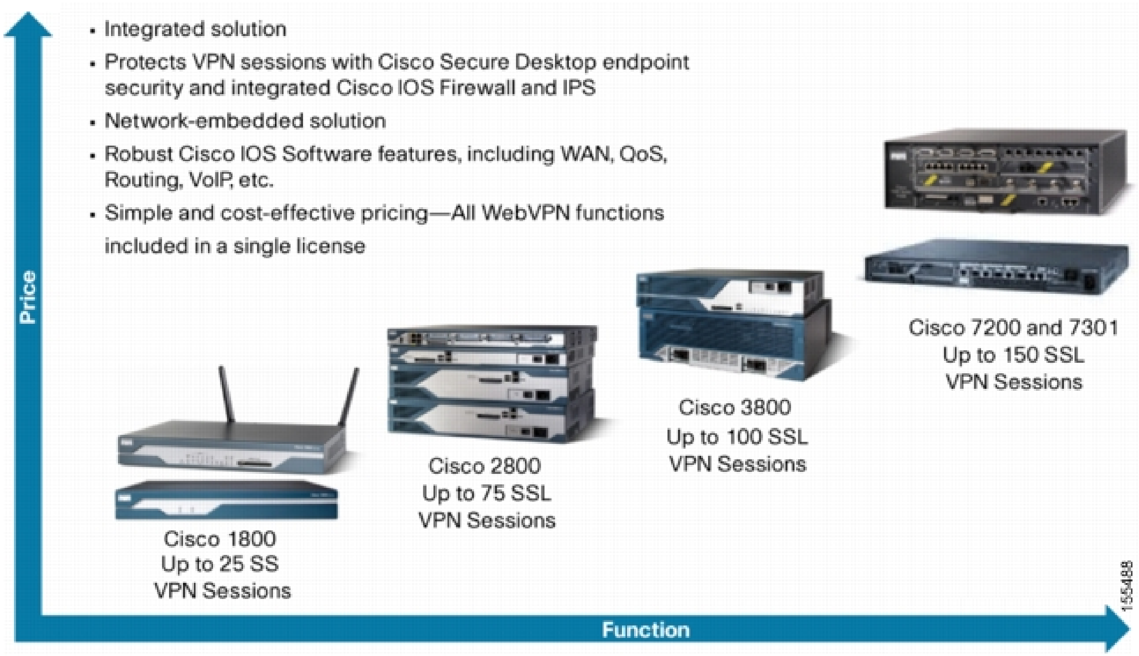
WebVPN NTLM Authentication

NT LAN Manager (NTLM) is supported for SSLVPN–WebVPN effective with Cisco IOS Release 12.4(9)T. The feature is configured by default. If you have to disable this feature, see the section "Disabling NTLM Authentication."

Platform Support

Figure 3 shows WebVPN platform support in Cisco IOS Release 12.4(6)T. Support for SSL VPN–WebVPN is provided in advanced enterprise, advanced IP services, and advanced security images that run on Integrated Service Routers, Cisco 7200 series routers, and Cisco 7301 series routers. These platforms can be deployed in a small office/home office (SOHO) networks, remote branch offices, and main corporate sites.

Figure 3 SSL VPN–WebVPN Platform Support



- Integrated solution
- Protects VPN sessions with Cisco Secure Desktop endpoint security and integrated Cisco IOS Firewall and IPS
- Network-embedded solution
- Robust Cisco IOS Software features, including WAN, QoS, Routing, VoIP, etc.
- Simple and cost-effective pricing—All WebVPN functions included in a single license

Cisco IOS WebVPN licenses can be purchased with or for the following platforms:

- Cisco 870 Series Integrated Services Routers for Small Offices
- Cisco 1800 Series Integrated Services Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Integrated Services Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7200 Series Routers
- Cisco 7301 Series Router

How to Configure WebVPN Services on a Router

This section contains the following tasks:

Configuring and Enabling WebVPN Services

- Configuring a WebVPN Gateway, page 9 (required)
- Configuring a WebVPN Context, page 12 (required)
- Configuring a WebVPN Policy Group, page 17 (required)

Configuring AAA-Related Features for WebVPN

- Configuring Local AAA Authentication for SSL VPN User Sessions, page 19 (optional)
- Configuring AAA for SSL VPN Users Using a Secure Access Control Server, page 21 (optional)
- Configuring RADIUS Accounting for SSL VPN User Sessions, page 23 (optional)
- Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session, page 25 (optional)
- Configuring RADIUS Attribute Support for WebVPN, page 25 (optional)

Customizing and Enabling WebVPN Features

- Configuring a URL List for Clientless Remote Access, page 28 (optional)
- Configuring Microsoft Files Shares for Clientless Remote Access, page 30 (optional)
- Configuring Citrix Application Support for Clientless Remote Access, page 33 (optional)
- Configuring Application Port Forwarding, page 35 (optional)
- Configuring the WebVPN Gateway to Distribute CSD and SVC Package Files, page 37 (optional)
- Configuring Cisco Secure Desktop Support, page 39 (optional)
- Configuring SSL VPN Client Full Tunnel Support, page 40 (optional)
- Configuring Advanced SSL VPN Tunnel Features, page 45 (optional)
- Configuring VRF Virtualization, page 48 (optional)
- Disabling NTLM Authentication, page 49 (optional)

Monitoring and Maintaining WebVPN Features

- Using WebVPN Clear Commands, page 50 (optional)
- Verifying WebVPN Configuration, page 51 (optional)
- Using WebVPN Debug Commands, page 58 (optional)

Configuring a WebVPN Gateway

The WebVPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through an SSL-encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer. Entering the **webvpn gateway** command places the router in SSLVPN Gateway configuration mode. The following configuration steps are completed in this task:

- The gateway is configured with an IP address
- A port number is configured to carry HTTPS traffic (443 is default)
- A hostname is configured for the gateway

- Crypto encryption and trust points are configured
- The gateway is configured to redirect HTTP traffic (port 80) over HTTPS
- The gateway is enabled

SSL VPN Encryption

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. The **ssl encryption** command is configured to restrict the encryption algorithms that SSL uses in Cisco IOS software.

Note There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, remove the line from the webvpn gateway subconfiguration.

SSL VPN Trustpoints

The configuration of the **ssl trustpoint** command is required only if you need to configure a specific CA certificate. A self-signed certificate is automatically generated when a WebVPN gateway is put in service.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn gateway** *name*
4. **hostname** *name*
5. **http-redirect** [**port** *number*]
6. **inservice**
7. **ip address** *number* [**port** *number*] [**secondary**]
8. **ssl encryption** [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]
9. **ssl trustpoint** *name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**webvpn gateway** *name* **Example:** `Router(config)# webvpn gateway GW_1`	Enters SSLVPN Gateway configuration mode to configure a WebVPN gateway. • Only one gateway is configured in a WebVPN-enabled network.
Step 4	**hostname** *name* **Example:** `Router(config-webvpn-gateway)# hostname VPN_1`	Configures the hostname for a WebVPN gateway.
Step 5	**http-redirect** [**port** *number*] **Example:** `Router(config-webvpn-gateway)# http-redirect`	Configures HTTP traffic to be carried over secure HTTP (HTTPS). • When this command is enabled, the WebVPN gateway listens on port 80 and redirects HTTP traffic over port 443 or the port number specified with the **port** keyword.
Step 6	**inservice** **Example:** `Router(config-webvpn-gateway)# inservice`	Enables a WebVPN gateway. • A gateway cannot enabled or put "in service" until a proxy IP address has been configured.
Step 7	**ip address** *number* [**port** *number*] [**secondary**] **Example:** `Router(config-webvpn-gateway)# ip address 10.1.1.1`	Configures a proxy IP address on a WebVPN gateway. • A secondary address must be configured if the proxy IP address is not on a directly connected network. • A secondary address does not reply to Address Resolution Protocol (ARP) or Internet Control Message Protocol (ICMP) messages.
Step 8	**ssl encryption** [**3des-sha1**] [**aes-sha1**] [**rc4-md5**] **Example:** `Router(config-webvpn-gateway)# ssl encryption rc4-md5`	Specifies the encryption algorithm that the SSL protocol uses for SSL Virtual Private Network (SSLVPN) connections. • The ordering of the algorithms specifies the preference.
Step 9	**ssl trustpoint** *name* **Example:** `Router(config-webvpn-gateway)# ssl trustpoint CA_CERT`	Configures the certificate trust point on a WebVPN Gateway. **Tip** Entering the **no** form of this command configures the WebVPN gateway to revert to using an autogenerated self-signed certificate.

Step 10	**end**
	Example:
	`Router(config-webvpn-gateway)# end`
		Exits SSLVPN Gateway configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, configures a WebVPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# ip address 10.1.1.1
Router(config-webvpn-gateway)# hostname VPN_1
Router(config-webvpn-gateway)# http redirect
Router(config-webvpn-gateway)# ssl encryption rc4-md5
Router(config-webvpn-gateway)# ssl trustpoint CA_CERT
Router(config-webvpn-gateway)# inservice
Router(config-webvpn-gateway)# end
```

What to Do Next

WebVPN context and policy group configurations must be configured before a WebVPN gateway can be operationally deployed. Proceed to the next section to see information on WebVPN context configuration.

Configuring a WebVPN Context

The WebVPN context defines the virtual configuration of the SSL VPN. Entering the **webvpn context** command places the router in SSLVPN configuration mode. The following configuration steps are completed in this task:

- A gateway and domain is associated
- The AAA authentication method is specified
- A group policy is associated
- The remote user portal (web page) is customized
- A limit on the number users sessions is configured
- The context is enabled

Context Defaults

The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration, while a WebVPN gateway is in an enabled state (in service).

Configuring a Virtual Host

A virtual hostname is specified when multiple virtual hosts are mapped to the same IP address on the WebVPN gateway (similar to the operation of a canonical domain name). The virtual hostname differentiates host requests on the gateway. The host header in the HTTP message is modified to direct traffic to the virtual host. The virtual hostname is configured with the **gateway** command in SSLVPN configuration mode.

Prerequisites

The WebVPN gateway configuration has been completed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **webvpn context** *name*
4. **aaa authentication** {**domain** *name* | **list** *name*}
5. **default-group-policy** *name*
6. **gateway** *name* [**domain** *name* | **virtual-host** *name*]
7. **inservice**
8. **login-message** [*message-string*]
9. **logo** [**file** *filename* | **none**]
10. **max-users** *number*
11. **secondary-color** *color*
12. **secondary-text-color** {**black** | **white**}
13. **title** [*title-string*]
14. **title-color** *color*
15. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`webvpn context`** *`name`*
	Example:
	`Router(config)# webvpn context SSLVPN`
		Enters SSLVPN configuration mode to configure the WebVPN context.
		Tip The context can be optionally named using the domain or virtual hostname. This is recommended as a best practice. It simplifies the management of multiple context configurations.

Step 4	**`aaa authentication`** {**`domain`** *`name`* | **`list`** *`name`*}
	Example:
	`Router(config-webvpn-context)# aaa authentication domain SERVER_GROUP`
		Specifies a list or method for SSL VPN remote-user authentication.
		Tip If this command is not configured, the WebVPN gateway will use global AAA parameters (if configured) for remote-user authentication.

	Command or Action	Purpose
Step 5	**default-group-policy** *name* **Example:** `Router(config-webvpn-context)# default-group-policy ONE`	Associates a a group policy with a WebVPN context configuration. • This command is configured to attach the policy group to the WebVPN context when multiple group policies are defined under the context. • This policy will be used as default, unless a AAA server pushes an attribute that specifically requests another group policy.
Step 6	**gateway** *name* [**domain** *name* | **virtual-host** *name*] **Example:** `Router(config-webvpn-context)# gateway GW_1 domain cisco.com`	Associates a WebVPN gateway with a WebVPN context. • The gateway configured in the first configuration task table is associated with the WebVPN context in this configuration step.
Step 7	**inservice** **Example:** `Router(config-webvpn-gateway)# inservice`	Enables a WebVPN context configuration. • The context is put “in service” by entering this command. However, the context is not operational until it is associated with an enabled WebVPN gateway.
Step 8	**login-message** [*message-string*] **Example:** `Router(config-webvpn-context)# login-message “Please enter your login credentials”`	Configures a message for the user login text box displayed on the login page.
Step 9	**logo** [**file** *filename* | **none**] **Example:** `Router(config-webvpn-context)# logo file flash:/mylogo.gif`	Configures a custom logo to be displayed on the login and portal pages of a SSL VPN. • The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. • The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. • No logo will be displayed if the image file is removed from the local file system.
Step 10	**max-users** *number* **Example:** `Router(config-webvpn-context)# max-users 500`	Limits the number of connections to a SSL VPN that will be permitted.

	Command or Action	Purpose

Step 11	**`secondary-color`** *`color`*
	
	Example:
	`Router(config-webvpn-context)# secondary-color darkseagreen`
	`Router(config-webvpn-context)# secondary-color #8FBC8F`
	`Router(config-webvpn-context)# secondary-color 143,188,143`
		Configures the color of the secondary title bars on the login and portal pages of a SSLVPN.
		• The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):
		– \#/x{6}
		– \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)
		– \w+
		• The default color is purple.
		• The example shows the three forms that the color can be configured.

Step 12	**`secondary-text-color`** {**`black`** | **`white`**}
	
	Example:
	`Router(config-webvpn-context)# secondary-text-color white`
		Configures the color of the text on the secondary bars of a SSLVPN.
		• The color of the text on the secondary bars must be aligned with the color of the text on the title bar.
		• The default color is black.

Step 13	**`title`** [*`title-string`*] **Example:** `Router(config-webvpn-context)# title “Secure Access: Unauthorized users prohibited”`	Configures the HTML title string that is shown in the browser title and on the title bar of a SSLVPN. • The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string “WebVPN Service” is displayed.

	Command or Action	Purpose

Step 14	**title-color** *color*
	Example:
	`Router(config-webvpn-context)# title-color darkseagreen`
	`Router(config-webvpn-context)# title-color #8FBC8F`
	`Router(config-webvpn-context)# title-color 143,188,143`
		Specifies the color of the title bars on the login and portal pages of a SSLVPN.
		• The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):
		– \#/x{6}
		– \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)
		– \w+
		• The default color is purple.
		• The example shows the three forms that can be used to configure the title color.

Step 15	**end**
	Example:
	`Router(config-webvpn-context)# end`
		Exits SSLVPN configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, configures a WebVPN context:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# aaa authentication domain SERVER_GROUP
Router(config-webvpn-context)# default-group-policy ONE
Router(config-webvpn-context)# gateway GW_1 domain cisco.com
Router(config-webvpn-context)# login-message “Please enter your login credentials”
Router(config-webvpn-context)# logo file flash:/mylogo.gif
Router(config-webvpn-context)# max-users 500
Router(config-webvpn-context)# secondary-color darkseagreen
Router(config-webvpn-context)# secondary-text-color white
Router(config-webvpn-context)# title “Secure Access: Unauthorized users prohibited”
Router(config-webvpn-context)# title-color yellow
Router(config-webvpn-gateway)# inservice
Router(config-webvpn-context)# end
```

What to Do Next

A WebVPN policy group configuration must be defined before a WebVPN gateway can be operationally deployed. Proceed to the next section to see information on WebVPN policy group configuration.

Configuring a WebVPN Policy Group

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the **policy group** command places the router in SSLVPN Group Policy Configuration mode. After it is configured, the group policy is attached to the WebVPN context configuration by configuring the **default-group-policy** command. The following configuration steps are completed in this task:

- The presentation of the SSL VPN portal page is configured
- A NetBIOS server list is referenced
- A port-forwarding list is referenced
- The idle and session timers are configured
- A URL list is referenced

Outlook Web Access 2003

Outlook Web Access 2003 (OWA 2003) is supported by the WebVPN gateway upon competition of this task. The Outlook Exchange Server must be reachable by the WebVPN gateway via TCP/IP.

URL-List Configuration

A URL list can be configured under the WebVPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **banner** *string*
6. **hide-url-bar**
7. **nbns-list** *name*
8. **port-forward** *name* [**auto-download**]
9. **timeout** {**idle** *seconds* | **session** *seconds*}
10. **url-list** *name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`webvpn context`** *`name`*
	Example:
	`Router(config)# webvpn context SSLVPN`
		Enters SSLVPN configuration mode to configure the WebVPN context.

Step 4	**`policy group`** *`name`*
	Example:
	`Router(config-webvpn-context)# policy group ONE`
		Enters SSLVPN Group Policy Configuration mode to configure a group policy.

Step 5	**`banner`** *`string`*
	Example:
	`Router(config-webvpn-group)# banner “Login Successful”`
		Configures a banner to be displayed after a successful login.

Step 6	**`hide-url-bar`**
	Example:
	`Router(config-webvpn-group)# hide-url-bar`
		Prevents the URL bar from being displayed on the SSL VPN portal page.

Step 7	**`nbns-list`** *`name`*
	Example:
	`Router(config-webvpn-group)# nbns-list SERVER_LIST`
		Attaches a NetBIOS Name Service (NBNS) server list to a policy group configuration.
		• The NBNS server list is first defined in SSLVPN NBNS list configuration mode.

Step 8	**`port-forward`** *`name`* `[`**`auto-download`**`]`
	Example:
	`Router(config-webvpn-group)# port-forward EMAIL`
		Attaches a port-forwarding list to a policy group configuration.

Step 9	**`timeout`** `{`**`idle`** *`seconds`* `|` **`session`** *`seconds`*`}`
	Example:
	`Router(config-webvpn-group)# timeout idle 1800`
	`Router(config-webvpn-group)# timeout session 36000`
		Configures the length of time that a remote user session can remain idle or the total length of time that the session can remain connected.
		• Upon expiration of either timer, the remote user connection is closed. The remote user must login (reauthenticate) to access the SSL VPN.

	Command or Action	Purpose
Step 10	**url-list** *name* **Example:** `Router(config-webvpn-group)# url-list ACCESS`	Attaches a URL list to policy group configuration.

Step 11	**end**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, configures a WebVPN policy group:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)# port-forward EMAIL
Router(config-webvpn-group)# timeout idle 1800
Router(config-webvpn-group)# timeout session 36000
Router(config-webvpn-group)# url-list ACCESS
Router(config-webvpn-group)# end
```

What to Do Next

At the completion of this task, the WebVPN gateway and context configurations are operational and enabled (in service), and the policy group has been defined. The WebVPN gateway is operational for clientless remote access (HTTPS only). Proceed to the next section to see information about configuring authentication, authorization, and accounting (AAA) for remote-user connections.

Configuring Local AAA Authentication for SSL VPN User Sessions

The steps in this task show how to configure a local AAA database for remote-user authentication. AAA is configured in global configuration mode. In this task, the **aaa authentication** command is not configured under the WebVPN context configuration. Omitting this command from the WebVPN context configuration causes the WebVPN gateway to use global authentication parameters by default.

Prerequisites

WebVPN gateway and context configurations are enabled and operational.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

4. **username** {*name* **secret** [**0** | **5**] *password*}
5. **aaa authentication login default local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.

Step 4	**username** {*name* **secret** [**0** | **5**] *password*}
	Example:
	`Router(config)# username USER1 secret 0 PsW2143`
		Establishes a username based authentication system.
		• Entering **0** configures the password as clear text. Entering **5** encrypts the password.

Step 5	**aaa authentication login default local** **Example:** `Router(config)# aaa authentication login default local`	Configures local AAA authentication.

Examples

The following example, starting in global configuration mode, configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a WebVPN context configuration.

```
Router(config)# aaa new-model
Router(config)# username USER1 secret 0 PsW2143
Router(config)# aaa authentication login default local
```

What to Do Next

The database that is configured for remote-user authentication on the WebVPN gateway can be a local database, as shown in this task, or the database can be accessed through any RADIUS or TACACS+ AAA server.

Cisco recommends that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions. Proceed to the next section to see more information.

Configuring AAA for SSL VPN Users Using a Secure Access Control Server

The steps in this task show how to configure AAA using a separate RADIUS or TACACS+ server. AAA is configured in global configuration mode. The authentication list/method is referenced in the WebVPN context configuration with the **aaa authentication** command. The steps in this task configure AAA using a RADIUS server.

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- A RADIUS or TACACS+ AAA server is operational and reachable from the WebVPN gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server** {**radius** *group-name* | **tacacs+** *group-name*}
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**
7. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
8. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]
9. **webvpn context** *name*
10. **aaa authentication** {**domain** *name* | **list** *name*}
11. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`aaa new-model`**
	Example:
	`Router(config)# aaa new-model`
		Enables the AAA access control model.

	Command or Action	Purpose

Step 4	**aaa group server** {**radius** *group-name* | **tacacs+** *group-name*}
	Example:
	`Router(config)# aaa group server radius myServer`
		Configures a RADIUS or TACACS+ server group and specifies the authentication list or method, and enters server-group configuration mode.

Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646`	Configures the IP address of the AAA group server.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server-group configuration mode.
Step 7	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login default local group myServer`	Sets AAA login parameters.
Step 8	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 10.1.1.20 auth-port 1645 acct-port 1646`	Specifies a host as the group server.
Step 9	**webvpn context** *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.

Step 10	**aaa authentication** {**domain** *name* | **list** *name*}
	Example:
	`Router(config-webvpn-context)# aaa authentication domain myServer`
		Configures AAA authentication for SSL VPN sessions.

Step 11	**exit** **Example:** `Router(config-webvpn-context)# exit`	Exits SSLVPN configuration mode, and enters global configuration mode.

Examples

The following example, starting in global configuration mode, configures a RADIUS server group and associates the AAA configuration under the WebVPN context configuration:

```
Router(config)# aaa new-model
Router(config)# aaa group server radius myServer
Router(config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router(config-sg-radius)# exit
Router(config)# aaa authentication login default local group myServer
Router(config)# radius-server host 10.1.1.20 auth-port 1645 acct-port 1646
Router(config)# webvpn context sslvpn
Router(config-webvpn-context)# aaa authentication list myServer
Router(config-webvpn-context)# exit
```

What to Do Next

Proceed to the section "Configuring RADIUS Attribute Support for WebVPN" to see RADIUS attribute-value pair information introduced to support this feature.

Configuring RADIUS Accounting for SSL VPN User Sessions

To configure RADIUS accounting for SSL VPN user sessions, perform the following steps.

Prerequisites

Before configuring RADIUS accounting for SSL VPN user sessions, you should first have configured AAA-related commands (in global configuration mode) and have set the accounting list. See the "Example" section after the section "DETAILED STEPS."

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **webvpn aaa accounting list** *aaa-list*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**webvpn aaa accounting-list** *aaa-list* **Example:** `Router(config)# webvpn aaa accounting-list sslvpnaaa`	Enables AAA accounting when you are using RADIUS for SSL VPN sessions.

Example

The following output example shows that RADIUS accounting has been configured for SSL VPN user sessions:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
aaa new-model
!
!
aaa accounting network sslvpnaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.16.2.133
ip name-server 172.16.11.48
!

line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
```

```
webvpn gateway GW1
 ip address 172.19.216.141 port 443
 inservice
 !
webvpn gateway SSLVPN
 no inservice
 !
webvpn install svc flash:/webvpn/svc.pkg
webvpn aaa accounting-list sslvpnaaa
 !
webvpn context Default_context
 ssl encryption
 ssl authenticate verify all
 !
 no inservice
!
!
```

Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session

To monitor and maintain your RADIUS accounting configuration, perform the following steps (the **debug** commands can be used together or individually).

SUMMARY STEPS

1. **enable**
2. **debug webvpn aaa**
3. **debug aaa accounting**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`debug webvpn aaa`**
	Example:
	`Router# debug webvpn aaa`
		Enables Web VPN session monitoring for AAA.

Step 3	**`debug aaa accounting`**
	Example:
	`Router# debug aaa accounting`
		Displays information on accountable events as they occur.

Configuring RADIUS Attribute Support for WebVPN

This section lists RADIUS attribute-value pair information introduced to support WebVPN. For information on using RADIUS attribute-value (AV) pairs with Cisco IOS software, see the “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 at the following URL:

http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_chapter09186a00804ec61e.html

Table 2 shows information about WebVPN RADIUS attribute-value pairs.

Note All WebVPN attributes (except for the standard IETF RADIUS attributes) start with **webvpn:** as follows:

```
webvpn:urllist-name=cisco
webvpn:nbnslist-name=cifs
webvpn:default-domain=cisco.com
```

Table 2 WebVPN RADIUS Attribute-Value Pairs

Attribute	Type of Value	Values	Default
addr (Framed-IP-Address[1])	ipaddr	*IP_address*	
addr-pool	string	*name*	
auto-applet-download	integer	0 (disable) 1 (enable)[2]	0
banner	string		
citrix-enabled	integer	0 (disable) 1 (enable)[3]	0
default-domain	string		
dns-servers	ipaddr	*IP_address*	
dpd-client-timeout	integer (seconds)	0 (disabled)–3600	300
dpd-gateway-timeout	integer (seconds)	0 (disabled)–3600	300
file-access	integer	0 (disable) 1 (enable)[3]	0
file-browse	integer	0 (disable) 1 (enable)[3]	0
file-entry	integer	0 (disable) 1 (enable)[3]	0
hide-urlbar	integer	0 (disable) 1 (enable)[3]	0
home-page	string		
idletime (Idle-Timeout[1])	integer (seconds)	0–3600	2100
ie-proxy-exception	string	*DNS_name*	
	ipaddr	*IP_address*	
ie-proxy-server	ipaddr	*IP_address*	
inacl	integer	1–199, 1300–2699	
	string	*name*	
keep-svc-installed	integer	0 (disable) 1 (enable)[3]	1

Table 2 WebVPN RADIUS Attribute-Value Pairs (continued)

Attribute	Type of Value	Values	Default
nbnslist-name	string	*name*	
netmask (Framed-IP-Netmask[1])	ipaddr	*IP_address_mask*	
port-forward-auto	integer	0 (disable) 1 (enable)	If this AV pair is not configured, the default is whatever was configured for the group policy. If this AV pair is configured with an integer of 1, the 1 will override a group policy value of 0.
port-forward-name	string	*name*	
primary-dns	ipaddr	*IP_address*	
rekey-interval	integer (seconds)	0–43200	21600
secondary-dns	ipaddr	*IP_address*	
split-dns	string		
split-exclude[4]	ipaddr ipaddr	*IP_address* *IP_address_mask*	
	word	local-lans	
split-include[4]	ipaddr ipaddr	*IP_address* *IP_address_mask*	
svc-enabled[5]	integer	0 (disable) 1 (enable)[3]	0
svc-ie-proxy-policy	word	none, auto, bypass-local	
svc-required[5]	integer	0 (disable) 1 (enable)[3]	0
timeout (Session-Timeout[1])	integer (seconds)	1–1209600	43200
urllist-name	string	*name*	
user-vpn-group	string	*name*	
wins-server-primary	ipaddr	*IP_address*	
wins-servers	ipaddr	*IP_address*	
wins-server-secondary	ipaddr	*IP_address*	

[1] Standard IETF RADIUS attributes.

[2] Any integer other than 0 enables this feature.

3. Any integer other than 0 enables this feature.
4. You can specify either split-include or split-exclude, but you cannot specify both options.
5. You can specify either svc-enable or svc-required, but you cannot specify both options.

What to Do Next

Proceed to the next section to see information about customizing the URL list configured in Step 10 of the of the WebVPN policy group configuration task.

Configuring a URL List for Clientless Remote Access

The steps in this configuration task show how to configure a URL list. The URL list, as the name implies, is a list of HTTP URLs that are displayed on the portal page after a successful login. The URL list is configured in SSLVPN configuration and SSLVPN Group Policy configuration modes.

Prerequisites

WebVPN gateway and context configurations are enabled and operational.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **url-list** *name*
5. **heading** *text-string*
6. **url-text** {*name* **url-value** *url*}
7. **exit**
8. **policy group** *name*
9. **url-list** *name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	**url-list** *name* **Example:** `Router(config-webvpn-context)# url-list ACCESS`	Enters enter SSLVPN URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSLVPN.
Step 5	**heading** *text-string* **Example:** `Router(config-webvpn-url)# heading “Quick Links”`	Configures the heading that is displayed above URLs listed on the portal page of a SSLVPN. • The URL list heading entered as a text string. The heading must be entered inside of quotation marks if it contains spaces.

Step 6	**url-text** {*name* **url-value** *url*}
	Example:
	`Router(config-webvpn-url)# url-text “Human Resources” url-value hr.mycompany.com`
		Adds an entry to a URL list.

Step 7	**exit** **Example:** `Router(config-webvpn-url)# exit`	Exits SSLVPN URL list configuration mode, and enters SSLVPN context configuration mode.
Step 8	**policy group** *name* **Example:** `Router(config-webvpn-context)# policy group ONE`	Enters SSLVPN Group Policy Configuration mode to configure a group policy.
Step 9	**url-list** *name* **Example:** `Router(config-webvpn-group)# url-list ACCESS`	Attaches the URL list to the policy group configuration.

Step 10	**end**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, creates a URL list and attaches it to policy group ONE:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading “Quick Links”
Router(config-webvpn-url)# url-text “Outlook Mail and Calendar” url-value
outlook.mycompany.com
Router(config-webvpn-url)# url-text “Human Resources” url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text “Sales and Marketing” url-value products.mycompany.com
Router(config-webvpn-url)# url-text Cisco url-value www.cisco.com
Router(config-webvpn-url)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# url-list ACCESS
Router(config-webvpn-group)# end
```

What to Do Next

Proceed to the next section to see information about configuring clientless remote access to file shares.

Configuring Microsoft Files Shares for Clientless Remote Access

In clientless remote access mode, files and directories created on Microsoft Windows servers can be accessed by the remote client through the HTTPS-enabled browser. When enabled, a list of file server and directory links are displayed on the portal page after login. The administrator can customize permissions on the WebVPN gateway to provide limited read-only access for a single file or full-write access and network browsing capabilities. The following access capabilities can be configured:

- Network browse (listing of domains)
- Domain browse (listing of servers)
- Server browse (listing of shares)
- Listing files in a share
- Downloading files
- Modifying files
- Creating new directories
- Creating new files
- Deleting files

Common Internet File System Support

CIFS is the protocol that provides access to Microsoft file shares and support for common operations that allow shared files to be accessed or modified.

NetBIOS Name Service Resolution

Windows Internet Name Service (WINS) uses NetBIOS name resolution to map and establish connections between Microsoft servers. A single server must be identified by its IP address in this configuration. Up to three servers can be added to the configuration. If multiple servers are added, one server should be configured as the master browser.

Samba Support

Microsoft file shares can be accessed through the browser on a Linux system that is configured to run Samba.

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- A Microsoft file server is operational and reachable from the WebVPN gateway over TCP/IP.

Restrictions

- Only file shares configured on Microsoft Windows 2000 or XP servers are supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **nbns-list** *name*
5. **nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]
6. **exit**
7. **policy group** *name*
8. **nbns-list** *name*
9. **functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	**nbns-list** *name* **Example:** `Router(config-webvpn-context)# nbns-list SERVER_LIST`	Enters SSLVPN NBNS List configuration mode to configure a NetBIOS Name Service (NBNS) server list for CIFS name resolution.

	Command or Action	Purpose

Step 5	**`nbns-server`** *`ip-address`* `[`**`master`**`] [`**`timeout`** *`seconds`*`] [`**`retries`** *`number`*`]`
	Example:
	`Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master`
	`Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5`
	`Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5`
		Adds a server to a NetBIOS Name Service (NBNS) server list.
		• The server specified with the ip-address argument can be a primary domain controller (PDC) in a Microsoft network.
		• When multiple NBNS servers are specified, a single server is configured as master browser.
		• Up to three NBNS server statements can be configured.

Step 6	**`exit`**
	Example:
	`Router(config-webvpn-nbnslist)# exit`
		Exits SSLVPN NBNS List configuration mode, and enters SSLVPN configuration mode.

Step 7	**`policy group`** *`name`*
	Example:
	`Router(config-webvpn-context)# policy group ONE`
		Enters SSLVPN Group Policy Configuration mode to configure a group policy.

Step 8	**`nbns-list`** *`name`*
	Example:
	`Router(config-webvpn-group)# nbns-list SERVER_LIST`
		Attaches a NBNS server list to a policy group configuration.

Step 9	**`functions`** `{`**`file-access`** `|` **`file-browse`** `|` **`file-entry`** `|` **`svc-enabled`** `|` **`svc-required`**`}`
	Example:
	`Router(config-webvpn-group)# functions file-access`
	`Router(config-webvpn-group)# functions file-browse`
	`Router(config-webvpn-group)# functions file-entry`
		Configures access for Microsoft file shares.
		• Entering the **file-access** keyword enables network file share access. File servers in the server list are listed on the SSL VPN home page when this keyword is enabled.
		• Entering the **file-browse** keyword enables browse permissions for server and file shares. The file-access function must be enabled in order to also use this function.
		• Entering the **file-entry** keyword enables “modify” permissions for files in the shares listed on the SSL VPN home page.

Step 10	**`end`**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

NBNS Server List Example

The following example, starting in global configuration mode, configures a server list for NBNS resolution:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
```

File Share Permissions Example

The following example attaches the server list to and enables full file and network access permissions for policy group ONE:

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)# functions file-access
Router(config-webvpn-group)# functions file-browse
Router(config-webvpn-group)# functions file-entry
Router(config-webvpn-group)# end
```

What to Do Next

Proceed to the next section to see information about configuring clientless remote access for Citrix-enabled applications.

Configuring Citrix Application Support for Clientless Remote Access

Clientless Citrix support allows the remote user to run Citrix-enabled applications through the SSL VPN as if the application was locally installed (similar to traditional thin-client computing). Citrix applications run on a MetaFrame XP server (or server farm). The WebVPN gateway provides access to the remote user. The applications run in real time over the SSL VPN. This task shows how to enable Citrix support for policy group remote users.

ICA Client

The Independent Computing Architecture (ICA) client carries keystrokes and mouse clicks from the remote user to the MetaFrame XP server. ICA traffic is carried over TCP port number 1494. This port is opened when a Citrix application is accessed. If multiple application are accessed, the traffic is carried over a single TCP session.

Prerequisites

- A Citrix Metaframe XP server is operational and reachable from the WebVPN gateway over TCP/IP.
- WebVPN gateway and context configurations are enabled and operational.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **citrix enabled**
6. **filter citrix** *extended-acl*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	**policy group** *name* **Example:** `Router(config-webvpn-context)# policy group ONE`	Enters SSLVPN Group Policy Configuration mode to configure a group policy.
Step 5	**citrix enabled** **Example:** `Router(config-webvpn-group)# citrix enabled`	Enables Citrix application support for remote users in a policy group.
Step 6	**filter citrix** *extended-acl* **Example:** `Router(config-webvpn-group)# filter citrix 100`	Configures a Citrix application access filter. • An extended access list is configured to define the application access filter. This filter is used to control remote user access to Citrix applications.

Step 7	**end**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, enables Citrix application support for remote users with a source IP address in the 192.168.1.0/24 network:

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)# filter citrix 100
```

What to Do Next

Support for standard applications that use well-known port numbers, such as e-mail and Telnet, can be configured using the port forwarding feature. Proceed to the next section to see more information.

Configuring Application Port Forwarding

Application port forwarding is configured for thin client mode WebVPN. Port forwarding extends the cryptographic functions of the SSL protected browser to provide remote access to TCP and UDP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the WebVPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the WebVPN session.

Administrative Privileges on the Remote Client

When enabling port forwarding, the WebVPN gateway will modify the hosts file on the PC of the remote user. Some software configurations and software security applications will detect this modification and prompt the remote user to select “Yes” to permit. To permit the modification, the remote user must have local administrative privileges.

Note There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, remove the line from the webvpn gateway subconfiguration.

Prerequisites

WebVPN gateway and context configurations are enabled and operational.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **port-forward** *name*
5. **local-port** {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}
6. **exit**
7. **policy group** *name*
8. **port-forward** *name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`webvpn context`** *`name`*
	Example:
	`Router(config)# webvpn context SSLVPN`
		Enters SSLVPN configuration mode to configure the WebVPN context.

Step 4	**`port-forward`** *`name`*
	Example:
	`Router(config-webvpn-context)# port-forward EMAIL`
		Enters SSLVPN port-forward list configuration mode to configure a port forwarding list.

Step 5	**`local-port`** {*`number`* **`remote-server`** *`name`* **`remote-port`** *`number`* **`description`** *`text-string`*}
	Example:
	`Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port 110 description POP3`
		Remaps (forwards) an application port number in a port forwarding list.
		• The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port forwarding list.

Step 6	**`exit`**
	Example:
	`Router(config-webvpn-port-fwd)# exit`
		Exits SSLVPN port-forward list configuration mode, and enters SSLVPN configuration mode.

Step 7	**`policy group`** *`name`*
	Example:
	`Router(config-webvpn-context)# policy group ONE`
		Enters SSLVPN Group Policy Configuration mode to configure a group policy.

Step 8	**`port-forward`** *`name`*
	Example:
	`Router(config-webvpn-group)# port-forward EMAIL`
		Attaches a port forwarding list to a policy group configuration.

Step 9	**`end`**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail1.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail2.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail3.company.com
remote-port 143 description IMAP
Router(config-webvpn-port-fwd)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# port-forward EMAIL
Router(config-webvpn-group)# end
```

Configuring the WebVPN Gateway to Distribute CSD and SVC Package Files

The WebVPN gateway is preconfigured to distribute Cisco Secure Desktop (CSD) and/or SSL VPN client (SVC) software package files to remote users. The files are distributed only when CSD or SVC support is needed. The administrator performs the following tasks to prepare the gateway:

- The current software package is downloaded from www.cisco.com
- The package file is copied to a local file system
- The package file is installed for distribution by configuring the **webvpn install** command

Remote Client Software Installation Requirements

The remote user must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client package can be installed.

For SVC software installation, the remote user must have either the Java Runtime Environment for Windows (version 1.4 or later), or the browser must support or be configured to permit Active X controls.

Software Package Download

The latest versions of the CSD and SVC software client packages should be installed for distribution on the WebVPN gateway.

The CSD software package can be downloaded at the following URL:

- http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

The SVC software package can be downloaded at the following URL:

- http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Note You will be prompted to enter your login name and password to download these files from Cisco.com.

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- Software installation packages are copied to a local files system, such as flash memory.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn install** [**csd** *location-name* | **svc** *location-name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`webvpn install`** [**`csd`** *`location-name`* | **`svc`** *`location-name`*] **Example:** `Router(config)# webvpn install svc flash:/webvpn/svc.pkg`	Installs a CSD or SVC package file to a WebVPN gateway for distribution to remote users. • The CSD and SVC software packages are pushed to remote users as access is needed.

Examples

The following example, starting in global configuration mode, installs the SVC package to a WebVPN gateway:

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example, starting in global configuration mode, installs the CSD package to a WebVPN gateway:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

What to Do Next

Support for CSD and SVC can be enabled for remote users after the gateway has been prepared to distribute CSD or SVC software.

Configuring Cisco Secure Desktop Support

Cisco Secure Desktop (CSD) provides a session-based interface where sensitive data can be shared for the duration of a WebVPN session. All session information is encrypted. All traces of the session data are removed from the remote client when the session is terminated, even if the connection is terminated abruptly. CSD support for remote clients is enabled in this task.

Java Runtime Environment

The remote user (PC or device) must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client packages can be installed.

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- The CSD software package is installed for distribution on the WebVPN gateway.

  See the Configuring the WebVPN Gateway to Distribute CSD and SVC Package Files section if you have not already prepared the WebVPN gateway to distribute CSD software.

Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **csd enable**
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`webvpn context` *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.

	Command or Action	Purpose
Step 4	**csd enable** **Example:** `Router(config-webvpn-context)# csd enable`	Enables Cisco Secure Desktop (CSD) support for SSL VPN sessions.

Step 5	**end**
	Example:
	`Router(config-webvpn-context)# end`
		Exits SSLVPN configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, enables CSD support:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# csd enable
```

What to Do Next

Upon competition of this task, the WebVPN gateway has been configured to provide clientless and thin client support for remote users. The WebVPN feature also has the capability to provide full VPN access (similar to IPsec). Proceed to the next section to see more information.

Configuring SSL VPN Client Full Tunnel Support

The SSL VPN client (SVC) is an application that allows a remote user to establish a full VPN connection similar to the type of connection that is established with an IPsec VPN. SVC client software is pushed (downloaded) and installed automatically on the PC of the remote user. The SVC client uses SSL to provide the security of an IPsec VPN without the complexity required to install IPsec in your network and on remote devices. The following configuration steps are completed in this task:

- An access list is applied to the tunnel to restrict VPN access
- SVC tunnel support is enabled
- An address pool is configured for assignment to remote clients
- The default domain is configured
- DNS is configured for SVC tunnel clients
- Dead peer timers are configured the WebVPN gateway and remote users.
- The login home page is configured
- The SVC client software package is configured to remain installed on the remote client
- Tunnel key refresh parameters are defined

Installing Remote Client Software from the WebVPN Gateway

The SVC client software package is pushed from the WebVPN gateway to remote clients when support is needed. The remote user (PC or device) must have either the Java Runtime Environment for Windows (version 1.4 later), or the browser must support or be configured to permit Active X controls. In either scenario, the remote user must have local administrative privileges.

Configuring an Address Pool

The address pool is first defined with the **ip local pool** command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Configuring Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in step 1.
3. Configure the **svc address-pool** command with name configured in Step 2.

See the examples in this section for a complete configuration example.

Manually Adding an Entry to the IP Forwarding Table

If the SVC software client is unable to update the IP forwarding table on the PC of the remote user, the following error message will be displayed in the router console or syslog:

```
Error : SSLVPN client was unable to Modify the IP forwarding table ......
```

This error can occur if the remote client does not have a default route. You can work around this error by performing the following steps:

1. Open a command prompt (DOS shell) on the remote client.
2. Enter the `route print` command.
3. If a default route is not displayed in the output, enter the `route` command followed by the `ADD` and `MASK` keywords. Include the default gateway IP address at the end of the route statement. See the following example: `C:\>route ADD 0.0.0.0 MASK 0.0.0.0 10.1.1.1`

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- The SVC software package is installed for distribution on the WebVPN gateway.
- The remote client has administrative privileges. Administrative privileges are required to download the SVC software client.

  See the Configuring the WebVPN Gateway to Distribute CSD and SVC Package Files section if you have not already prepared the WebVPN gateway to distribute SVC software.

Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **filter tunnel** *extended-acl*
6. **functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}
7. **svc address-pool** *name*
8. **svc default-domain** *name*
9. **svc dns-server** {**primary** | **secondary**} *ip-address*
10. **svc dpd-interval** {**client** | **gateway**} *seconds*
11. **svc homepage** *string*
12. **svc keep-client-installed**
13. **svc rekey** {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}
14. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`webvpn context` *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	`policy group` *name* **Example:** `Router(config-webvpn-context)# policy group ONE`	Enters SSLVPN Group Policy Configuration mode to configure a group policy.
Step 5	`filter tunnel` *extended-acl* **Example:** `Router(config-webvpn-group)# filter tunnel 101`	Configures a WebVPN tunnel access filter. • The tunnel access filter is used control network and application level access. The tunnel filter is also defined in an extended access list.

	Command or Action	Purpose

Step 6	**functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}
	Example:
	`Router(config-webvpn-group)# functions svc-enabled`
	`Router(config-webvpn-group)# functions svc-required`
		Configures SVC tunnel mode support.
		• Entering the **svc-enabled** keyword enables tunnel support for the remote user. If the SVC software package fails to install, the remote user can continue to use clientless mode or thin-client mode.
		• Entering the **svc-required** keyword enables only tunnel support for the remote user. If the SVC software package fails to install (on the PC of the remote user), the other access modes cannot be used.

Step 7	**svc address-pool** *name* **Example:** `Router(config-webvpn-group)# svc address-pool ADDRESSES`	Configures configure a pool of IP addresses to assign to remote users in a policy group. • The address pool is first defined with the **ip local pool** command in global configuration mode. • If you are configuring an address pool for a network that is not directly connected, an address from the pool must be configured on a locally loopback interface. See the third example at the end of this section.
Step 8	**svc default-domain** *name* **Example:** `Router(config-webvpn-group)# svc default-domain cisco.com`	Configures the default domain for a policy group.

Step 9	**svc dns-server** {**primary** | **secondary**} *ip-address*
	Example:
	`Router(config-webvpn-group)# svc dns-server primary 192.168.3.1`
	`Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1`
		Configures DNS servers for policy group remote users.

Step 10	**svc dpd-interval** {**client** | **gateway**} *seconds*
	Example:
	`Router(config-webvpn-group)# svc dpd-interval gateway 30`
	`Router(config-webvpn-group)# svc dpd-interval client 300`
		Configures the dead peer detection (DPD) timer value for the gateway or client.
		• The DPD timer is reset every time a packet is received over the SSL VPN tunnel from the gateway or remote user.

Step 11	**svc homepage** *string* **Example:** `Router(config-webvpn-group)# svc homepage www.cisco.com`	Configures configure the URL of the web page that is displayed upon successful user login. • The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length.
Step 12	**svc keep-client-installed** **Example:** `Router(config-webvpn-group)# svc keep-client-installed`	Configures the remote user to keep SSL VPN Client (SVC) software installed when the SSL VPN connection is not enabled.

	Command or Action	Purpose

Step 13	**svc rekey** {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}
	Example:
	`Router(config-webvpn-group)# svc rekey method new-tunnel`
	`Router(config-webvpn-group)# svc rekey time 3600`
		Configures the time and method that a tunnel key is refreshed for policy group remote users.
		• The tunnel key is refreshed by renegotiating the SSL connection or initiating a new tunnel connection.
		• The time interval between tunnel refresh cycles is configured in seconds.

Step 14	**end**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

Tunnel Filter Configuration

The following example, starting in global configuration mode, configures a deny access filter for any host from the 172.16.2/24 network:

```
Router(config)# access-list 101 deny ip 172.16.2.0 0.0.0.255 any
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# filter tunnel 101
Router(config-webvpn-group)# end
```

Address Pool (Directly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context SSLVPM
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

Address Pool (Nondirectly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback interface is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.126 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context SSLVPM
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

Full Tunnel Configuration

The following example, starting in global configuration mode, configures full SVC tunnel support on a WebVPN gateway:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# functions svc-required
Router(config-webvpn-group)# svc default-domain cisco.com
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)# svc homepage www.cisco.com
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
Router(config-webvpn-group)# end
```

What to Do Next

Proceed to the next section to see advanced SVC tunnel configuration information.

Configuring Advanced SSL VPN Tunnel Features

This section describes advanced SVC tunnel configurations. The following configuration steps are completed in this task:

- Split tunnel support and split DNS resolution is enabled on the WebVPN gateway
- WebVPN gateway support for Microsoft Internet Explorer proxy settings is configured
- WINS resolution is configured for SVC tunnel clients

Microsoft Internet Explorer Proxy Configuration

The WebVPN gateway can be configured to pass or bypass Microsoft Internet Explorer (MSIE) proxy settings. Only HTTP proxy settings are supported by the WebVPN gateway. MSIE proxy settings have no effect on any other supported browser.

Split Tunneling

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside of the SVC tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the ISP or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the sametime. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as network printer.

Prerequisites

- WebVPN gateway and context configurations are enabled and operational.
- The SVC software package is installed for distribution on the WebVPN gateway.

Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **svc split exclude** {{*ip-address mask* | **local-lans**} | **include** *ip-address mask*}
6. **svc split dns** *name*
7. **svc msie-proxy** {**exception** *host* | **option** {**auto** | **bypass-local** | **none**}}
8. **svc msie-proxy server** *host*
9. **svc wins-server** {**primary** | **secondary**} *ip-address*
10. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`webvpn context`** *`name`*
	Example:
	`Router(config)# webvpn context SSLVPN`
		Enters SSLVPN configuration mode to configure the WebVPN context.

Step 4	**`policy group`** *`name`*
	Example:
	`Router(config-webvpn-context)# policy group ONE`
		Enters SSLVPN Group Policy Configuration mode to configure a group policy.

Step 5	**`svc split exclude`** {{*`ip-address mask`* | **`local-lans`**} | **`include`** *`ip-address mask`*}
	Example:
	`Router(config-webvpn-group)# svc split exclude 192.168.1.1 0.0.0.255`
	`Router(config-webvpn-group)# svc split include 171.16.1.1 0.0.0.255`
		Configures split tunneling for policy group remote users.
		• Split tunneling is configured to include or exclude traffic in the SVC tunnel. Traffic that is included is sent over the SSL VPN tunnel. Traffic is excluded is resolved outside of the tunnel.
		• Exclude and include statements are configured with IP address/wildcard mask pairs.

	Command or Action	Purpose

Step 6	**svc split dns** *name*
	Example:
	`Router(config-webvpn-group)# svc split dns www.cisco.com`
	`Router(config-webvpn-group)# svc split dns my.company.com`
		Configures the WebVPN gateway to resolve the specified fully qualified DNS names through the SVC tunnel.
		• A default domain was configured in the previous task with the **svc default-domain** command. DNS names configured with the **svc split dns** command are configured in addition.
		• Up to 10 split DNS statements can be configured.

Step 7	**svc msie-proxy** {**exception** *host* | **option** {**auto** | **bypass-local** | **none**}}
	Example:
	`Router(config-webvpn-group)# svc msie-proxy option auto`
	`Router(config-webvpn-group)# svc msie-proxy exception www.cisco.com`
	`Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1`
		Configures configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group remote users.
		• Entering the **option auto** keywords configures the browser of the remote user to auto-detect proxy settings.
		• Entering the **option bypass-local** keywords configures local addresses to bypass the proxy.
		• Entering the **option none** keywords configures the browser on the remote client to not use a proxy.

Step 8	**svc msie-proxy server** *host* **Example:** `Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80`	Specifies a Microsoft Internet Explorer (MSIE) proxy server for policy group remote users. • The proxy server is specified by entering an IP address or a fully qualified domain name.

Step 9	**svc wins-server** {**primary** | **secondary**} *ip-address*
	Example:
	`Router(config-webvpn-group)# svc wins-server primary 172.31.1.1`
	`Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1`
		Configures Windows Internet Name Service (WINS) servers for policy group remote users.

Step 10	**end**
	Example:
	`Router(config-webvpn-group)# end`
		Exits SSLVPN Group Policy Configuration mode, and enters privileged EXEC mode.

Examples

Split DNS Configuration

The following example, starting in global configuration mode, configures the following DNS names to be resolved in the SVC tunnel:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns www.cisco.com
Router(config-webvpn-group)# svc split dns my.company.com
```

Including and Excluding IP Prefixes

The following example configures a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.1 0.0.0.255
Router(config-webvpn-group)# svc split include 171.16.1.1 0.0.0.255
```

MSIE Proxy Configuration

The following example configures MSIE proxy settings:

```
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.cisco.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

WINS Server Configuration

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.3.1
Router(config-webvpn-group)# end
```

Configuring VRF Virtualization

VRF Virtualization allows you to associate a traditional VRF with a WebVPN context configuration. This feature allows you to apply different configurations and reuse address space for different groups of users in your organization.

Prerequisites

- A VRF has been configured in global configuration mode.
- WebVPN gateway and context configurations are enabled and operational.
- A policy group has been configured and associated with the WebVPN context.

Restrictions

- Only a single VRF can be configured for each WebVPN context configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **vrf-name** *name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**webvpn context** *name* **Example:** `Router(config)# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	**vrf-name** *name* **Example:** `Router(config-webvpn-context)# vrf-name BLUE`	Associates a VRF with a WebVPN context.

Step 5	**end**
	Example:
	`Router(config-webvpn-context)# end`
		Exits SSLVPN configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, associates the VRF under the WebVPN context configuration:

```
Router(config)# ip vrf BLUE
Router(config-vrf)# rd 10.100.100.1
Router(config-vrf)# exit
Router(config)# webvpn context BLUE
Router(config-webvpn-context)# policy group BLUE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy BLUE
Router(config-webvpn-context)# vrf-name BLUE
Router(config-webvpn-context)# end
```

Disabling NTLM Authentication

To disable NTLM authentication, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*

4. **policy group** *name*
5. **functions httpauth-disabled**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**webvpn context** *name* **Example:** `Router# webvpn context SSLVPN`	Enters SSLVPN configuration mode to configure the WebVPN context.
Step 4	**policy group** *name* **Example:** `Router (config-webvpn-context)# policy group ONE`	Enters SSLVPN group policy configuration mode to configure a group policy.
Step 5	**functions httpauth-disabled** **Example:** `Router (config-webvpn-group)#` **`functions httpauth-disabled`**	Disables NTLM authentication.

Using WebVPN Clear Commands

This section describes **clear** commands that are used to perform the following tasks:

- Clear NBNS cache information
- Clear remote user sessions
- Clear (or reset) WebVPN application and access counters

SUMMARY STEPS

1. **enable**
2. **clear webvpn nbns** [**context** {*name* | **all**}]
3. **clear webvpn session** {[**user** *name*] **context** {*name* | **all**}}
4. **clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **tunnel**] [**context** {*name* | **all**}]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear webvpn nbns** [**context** {*name* | **all**}] **Example:** `Router# clear webvpn nbns context all`	Clears clear the NBNS cache on a WebVPN gateway.

Step 3	**clear webvpn session** {[**user** *name*] **context** {*name* | **all**}}
	Example:
	`Router# clear webvpn session context all`
		Clears WebVPN remote user sessions.

Step 4	**clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **tunnel**] [**context** {*name* | **all**}]] **Example:** `Router# clear webvpn stats`	Clears WebVPN application and access counters.

Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

The following example clears all session information:

```
Router# clear webvpn session context all
```

The following example all statistics counters for all WebVPN processes:

```
Router# clear webvpn stats
```

Verifying WebVPN Configuration

This section describes show commands that are used to verify the following:

- WebVPN gateway configuration
- WebVPN context configuration
- CSD and SVC installation status
- NetBIOS name services information
- WebVPN group policy configuration
- WebVPN user session information
- WebVPN application statistics

SUMMARY STEPS

1. **enable**
2. **show webvpn context** [*name*]
3. **show webvpn gateway** [*name*]
4. **show webvpn install** {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | **svc**}}
5. **show webvpn nbns** {**context** {**all** | *name*}}
6. **show webvpn policy** {**group** *name* **context** {**all** | *name*}}
7. **show webvpn session** {[**user** *name*] **context** {**all** | *name*}}
8. **show webvpn stats** {**cifs** | **citrix** | **mangle** | **port-forward** | **tunnel**} [**detail**] [**context** {**all** | *name*}]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**show webvpn context** [*name*] **Example:** `Router# show webvpn context`	Displays the operational status and configuration parameters for WebVPN context configurations.
Step 3	**show webvpn gateway** [*name*] **Example:** `Router# show webvpn gateway`	Displays the status of the WebVPN gateway.

Step 4	**show webvpn install** {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | svc}}
	Example:
	`Router# show webvpn install status csd`
		Displays the installation status of SVC or CSD client software packages.

Step 5	**show webvpn nbns** {**context** {**all** | *name*}}
	Example:
	`Router# show webvpn nbns context all`
		Displays information in the NetBIOS Name Service (NBNS) cache.

Step 6	**show webvpn policy** {**group** *name* **context** {**all** | *name*}}
	Example:
	`Router# show webvpn policy group ONE context all`
		Displays the context configuration associated with a policy group.

	Command or Action	Purpose

Step 7	**show webvpn session** {[**user** *name*] **context** {**all** | *name*}}
	Example:
	`Router# show webvpn session context all`
		Displays WebVPN user session information.

Step 8	**show webvpn stats** {**cifs** | **citrix** | **mangle** | **port-forward** | **tunnel**} [**detail**] [**context** {**all** | *name*}] **Example:** `Router# show webvpn stats tunnel detail context all`	Displays WebVPN application and network statistics.

Examples

show webvpn context Example

The following is sample output from the **show webvpn context** command:

```
Router# show webvpn context

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host

Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

show webvpn context name Example

The following is sample output from the **show webvpn context** command, entered with the name of a specific WebVPN context:

```
Router# show webvpn context SSLVPN

Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: PG_1
Associated WebVPN Gateway: GW_ONE
Domain Name: DOMAIN_ONE
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

show webvpn gateway Example

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                       Admin  Operation
------------                       -----  ---------
GW_1                               up     up
GW_2                               down   down
```

show webvpn gateway name Example

The following is sample output from the **show webvpn gateway** command, entered with a specific WebVPN gateway name:

```
Router# show webvpn gateway GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

show webvpn install file Example

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt

SSLVPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

show webvpn install package svc Example

The following is sample output from the **show webvpn install** command, entered with the **package svc** keywords:

```
Router# show webvpn install package svc

SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

show webvpn install status svc Example

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

show webvpn nbns context all Example

The following sample output from the **show webvpn nbns** command, entered with the **context all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

show webvpn policy Example

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group ONE context all

WEBVPN: group policy = ONE ; context = SSLVPN
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
WEBVPN: group policy = ONE ; context = SSLVPN_TWO
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

show webvpn policy Example (with NTLM disabled)

The following is sample output from the **show webvpn policy** command. NTLM authentication has been disabled.

```
Router# show webvpn policy group ntlm context ntlm

WEBVPN: group policy = ntlm; context = ntlm
      url list name = "ntlm-server"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      functions =
                httpauth-disabled
                file-access
                svc-enabled

      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

show webvpn session Example

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context SSLVPN

WebVPN context name: SSLVPN
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.2.1.220                 2         04:47:16  00:01:26
user2              10.2.1.221                 2         04:48:36  00:01:56
```

show webvpn session user Example

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

WebVPN user name = user1 ; IP address = 10.2.1.220; context = SSLVPN
    No of connections: 0
    Created 00:00:19, Last-used 00:00:18
    CSD enabled
    CSD Session Policy
       CSD Web Browsing Allowed
       CSD Port Forwarding Allowed
       CSD Full Tunneling Disabled
       CSD FILE Access Allowed
    User Policy Parameters
      Group name = ONE
    Group Policy Parameters
      url list name = "Cisco"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "EMAIL"
      tunnel mode = disabled
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep stc installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 3600 sec
```

show webvpn stats Example

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context SSLVPN

WebVPN context name : SSLVPN
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
    CEF switched packets - client: 0         , server: 0
    CEF punted packets - client: 0         , server: 0

Mangling statistics:
    Relative urls            : 0          Absolute urls            : 0
    Non-http(s) absolute urls: 0          Non-standard path urls   : 0
    Interesting tags         : 0          Uninteresting tags       : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles            : 0
    HTML comments            : 0          HTTP/1.0 requests        : 0
    HTTP/1.1 requests        : 0          Unknown HTTP version     : 0
    GET requests             : 0          POST requests            : 0
    CONNECT requests         : 0          Other request methods    : 0
    Through requests         : 0          Gateway requests         : 0
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 0          Processed req body bytes : 0
    HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
    HTML responses           : 0          CSS responses            : 0
    XML responses            : 0          JS responses             : 0
    Other content type resp  : 0          Chunked encoding resp    : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0

CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies             : 0
    NB DGM Requests          : 0          NB DGM Replies           : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  HTTP related Per Context:
    Requests                 : 0          Request Bytes RX         : 0
    Request Packets RX       : 0          Response Bytes TX        : 0
    Response Packets TX      : 0          Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0

Socket statistics:
    Sockets in use           : 0          Sock Usr Blocks in use   : 0
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 0          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 0          Sock Tx Unblocked        : 0
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 0
    Sock Select Timeout Errs : 0

Port Forward statistics:
    Connections serviced     : 0          Server Aborts (idle)     : 0
  Client                                Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0

WEBVPN Citrix statistics:
Connections serviced : 0

               Server                   Client
  Packets in  : 0                        0
  Packets out : 0                        0
  Bytes in    : 0                        0
  Bytes out   : 0                        0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
    SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
    SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
    DPD timeout              : 0
  Client                                Server
    in  CSTP frames          : 0          out IP pkts              : 0
    in  CSTP data            : 0          out stitched pkts        : 0
    in  CSTP control         : 0          out copied pkts          : 0
    in  CSTP Addr Reqs       : 0          out bad pkts             : 0
    in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
    in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
    in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
    in  CSTP bytes           : 0          out IP bytes             : 0
    out CSTP frames          : 0          in  IP pkts              : 0
    out CSTP data            : 0          in  invalid pkts         : 0
    out CSTP control         : 0          in  congested pkts       : 0
    out CSTP Addr Resps      : 0          in  bad pkts             : 0
    out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
    out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
    out CSTP Msg Reqs        : 0
    out CSTP bytes           : 0          in  IP bytes             : 0
```

Using WebVPN Debug Commands

This section describes troubleshooting WebVPN applications and network activity with the **debug webvpn** command.

SUMMARY STEPS

1. **enable**
2. **debug webvpn** [**aaa** | **cifs** | **citrix** | **cookie** | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | *http* | **package** | **port-forward** | **sdps** [**level** *number*] | **sock** [**flow**] | **timer** | **trie** | **tunnel** [**detail** | **traffic** *acl-number*] | **url_disp** | **webservice**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug webvpn** [**aaa** | **cifs** | **citrix** | **cookie** | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | *http* | **package** | **port-forward** | **sdps** [**level** *number*] | **sock** [**flow**] | **timer** | **trie** | **tunnel** [**detail** | **traffic** *acl-number*] | **url_disp** | **webservice**] **Example:** `Router# debug webvpn`	Enables the display of debug information for WebVPN applications and network activity.

How to Set Up WebVPN for the Remote User

This section describes the tasks required to set up WebVPN for remote users. It summarizes configuration tasks and system requirements to provide WebVPN access to a remote user. It also specifies information to communicate to remote users to help them use WebVPN.

This section contains the following tasks:

- WebVPN Prerequisites for the Remote User, page 59
- Usernames and Passwords, page 60
- End User Interface, page 61
- Using Other WebVPN Features, page 72
- Security Tips, page 73
- Application Access—Recovering from Hosts File Errors, page 74
- Eudora 5.2 on Windows 2000, page 85
- Netscape Mail 7 on Windows 2000, page 91

WebVPN Prerequisites for the Remote User

The following are required to start WebVPN on a PC or device for a remote user:

- 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—The following browsers have been verified for WebVPN. Other browsers might not fully support WebVPN features.

On Microsoft Windows:

  - Internet Explorer 6.0 SP1 (SP2 required for Windows XP)
  - Netscape 7.2

On Linux:

  - Netscape version 7.2

- Cookies enabled—Cookies must be enabled on the browser in order to access applications through port forwarding.
- Pop-ups enabled—Pop-ups should be enabled on the browser to allow the browser to display the floating WebVPN toolbar and timeout warnings. If pop-ups are blocked, change the browser setting and click the WebVPN floating toolbar icon on the in-page toolbar to display the floating toolbar.

  If pop-ups are disabled on the browser, WebVPN will not warn the remote user before disconnecting due to an idle timeout or a maximum connect time.
- 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 WebVPN gateway, for example https://10.89.192.163 or https://vpn.company.com.
- WebVPN username and password
- (Optional) Local printer—WebVPN does not support printing from a web browser to a network printer. However, printing to a local printer is supported.

Usernames and Passwords

Table 3 lists the type of usernames and passwords that WebVPN users might have to know.

Table 3 Usernames and Passwords for WebVPN Users

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

End User Interface

A remote user whose enterprise network has configured WebVPN can access the network by launching a browser and connecting to the WebVPN gateway. The remote user presents his or her credentials, authenticates, and a portal page (home page) of the enterprise site is displayed. The portal page displays WebVPN features (for example, e-mail and web browsing) to which the remote user has access on the basis of his or her credentials. If the remote user has access to all features enabled on the WebVPN gateway, the home page will provide access links.

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

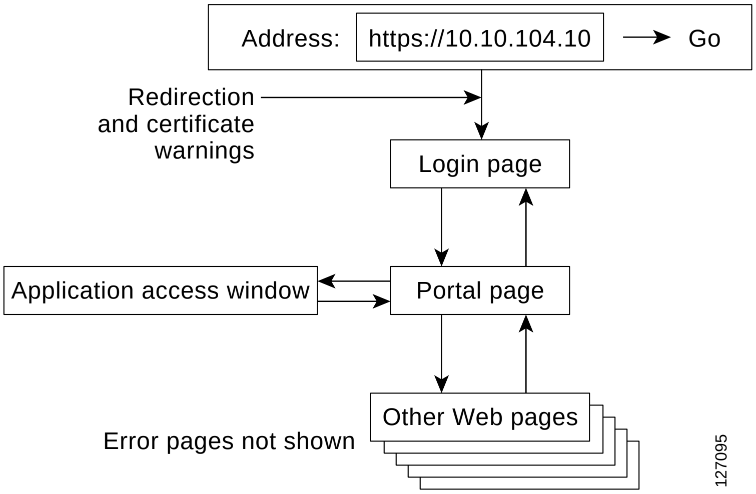
- Page Flow, page 61
- Initial Connection, page 62
- Login Page, page 63
- Certificate Authentication, page 64
- Logout Page, page 64
- Portal Page, page 65
- Remote Servers, page 66
- DNS and Connection Errors, page 68
- Session Timeout, page 69
- TCP Port Forwarding and Application Access, page 69

Page Flow

This section describes the page flow process (see Figure 4) for a WebVPN session. When the remote user enters the Hypertext Transfer Protocol Secure (HTTPS) URL (https://*address*) into his or her browser, the remote user is then redirected to https://*address*/index.html, where the login page is located.

Note Depending on the configuration of the browser, this redirection may cause a warning in the browser of the remote user indicating that he or she is being redirected to a secure connection.

Figure 4 Page Flow



Initial Connection

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

- 503 Service Unavailable Message, page 62
- Out of Service Page, page 62
- SSL/TLS Certificate, page 63

503 Service Unavailable Message

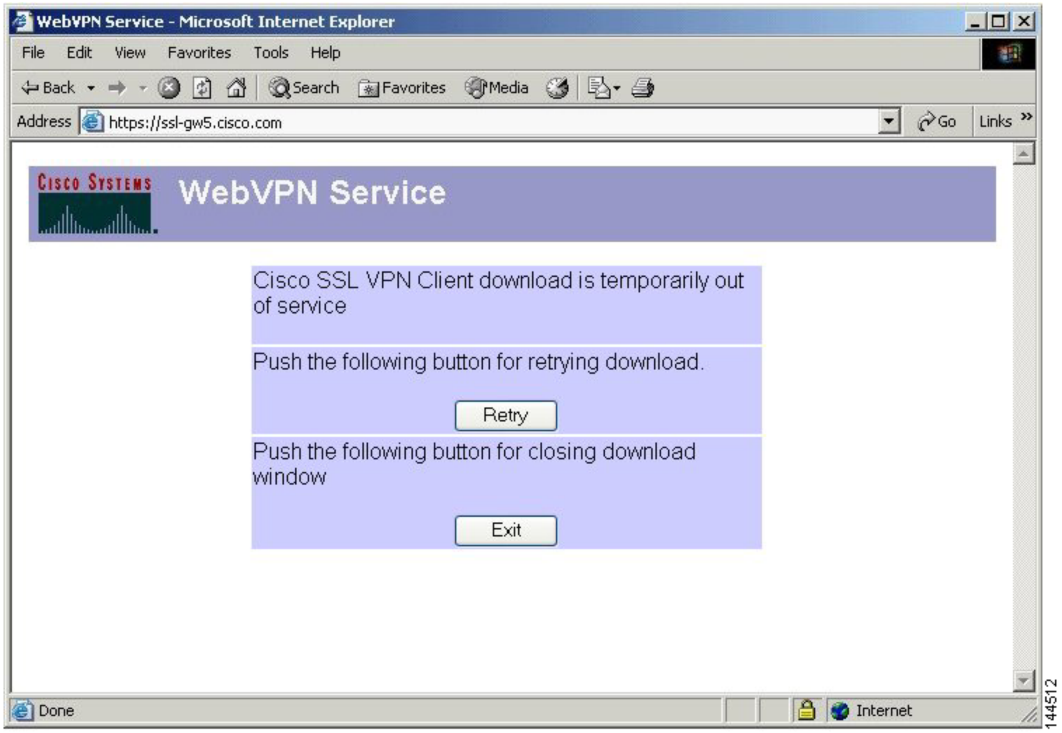
Remote users might see a "503 Service Unavailable" message if the gateway is experiencing high traffic loads. Remote users who receive this message should try to connect again later.

Out of Service Page

When remote users attempt to download the SSL VPN client (SVC), the file system that stores the SVC binary might be out of service temporarily. When this event occurs, an Out of Service page (see Figure 5) displays on the browser of the remote user. The Out Of Service page will prompt the remote user to retry the download or to exit from the process.

In most cases, when remote users click the Retry button, they will successfully download the SVC. However, if the gateway continues to respond with the Out Of Service page, the remote user should exit the process and report the error to the gateway administrator.

Figure 5 Out of Service Page


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ssl-gw5.cisco.com
Go Links
Cisco Systems
WebVPN Service
Retry
Exit
Done
Internet
144512

Cisco SSL VPN Client download is temporarily out of service

Push the following button for retrying download.

Push the following button for closing download window

SSL/TLS Certificate

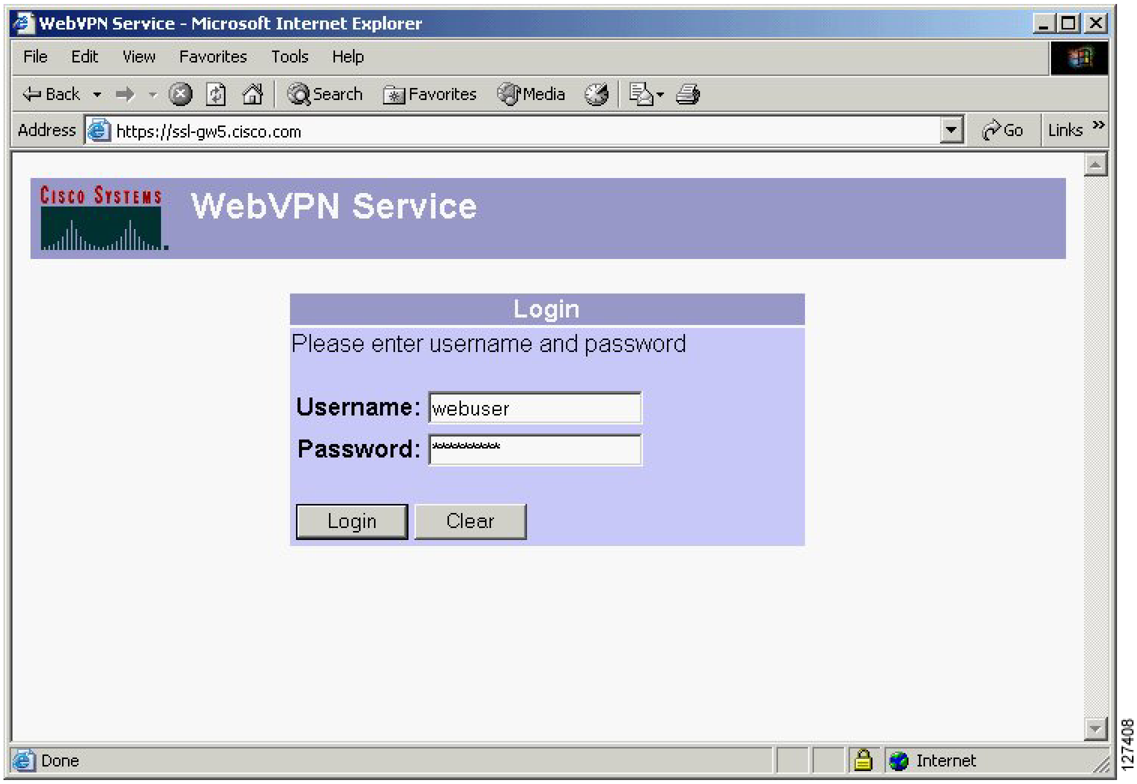
When the HTTPS connection is established, a warning about the SSL/TLS certificate may display. If the warning displays, the remote user should install this certificate. If the warning does not display, then the system already has a certificate that the browser trusts.

The remote user is then connected to the login page.

Login Page

The login page (see Figure 6) prompts the remote user to enter his or her username and password, which are entered into an HTML form. If an authentication failure occurs, the login page displays an error message.

Figure 6 Default Login Page



WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ssl-gw5.cisco.com
Go Links
Cisco Systems
Login
Clear
Done
Internet
127408

WebVPN Service

Login

Please enter username and password

Username: webuser

Password: *********

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

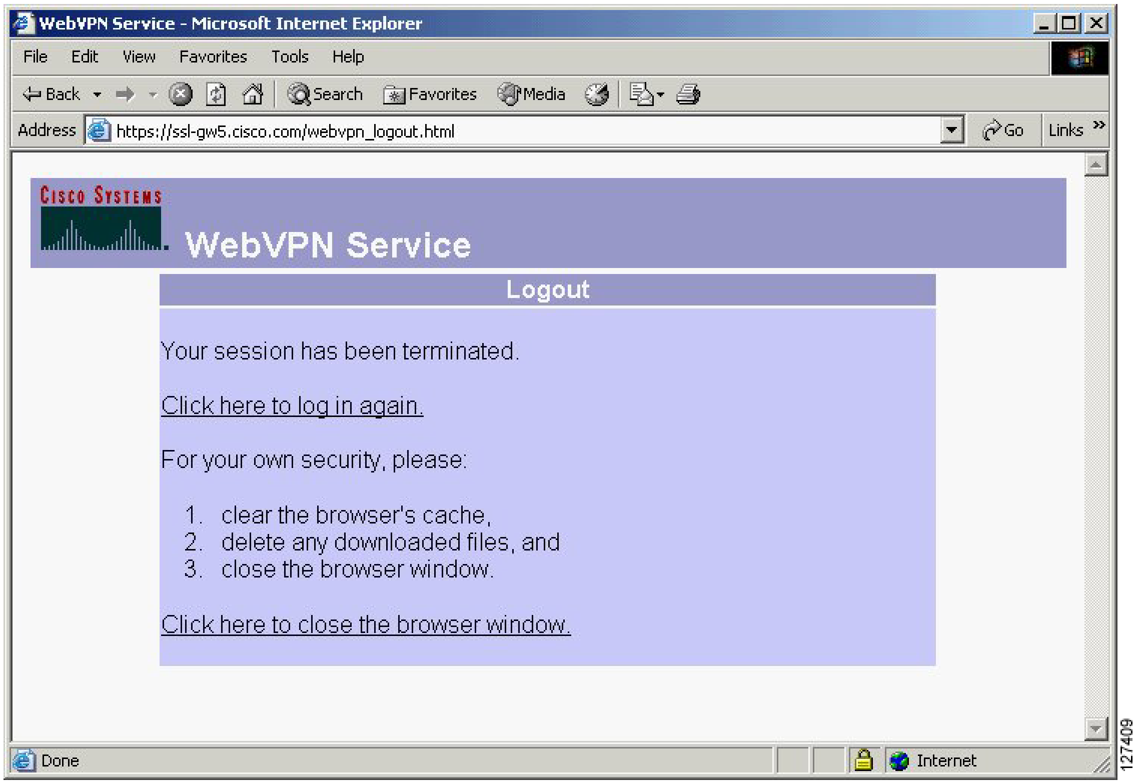
Certificate Authentication

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

Logout Page

The logout page (see Figure 7) displays if the remote user clicks the logout link, or if the session terminates because of an idle timeout or a maximum connection time.

Figure 7 Logout Page


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ssl-gw5.cisco.com/webvpn_logout.html
Go Links
Cisco Systems
WebVPN Service
Logout
Done
Internet
127409

Your session has been terminated.

Click here to log in again.

For your own security, please:

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

Click here to close the browser window.

Portal Page

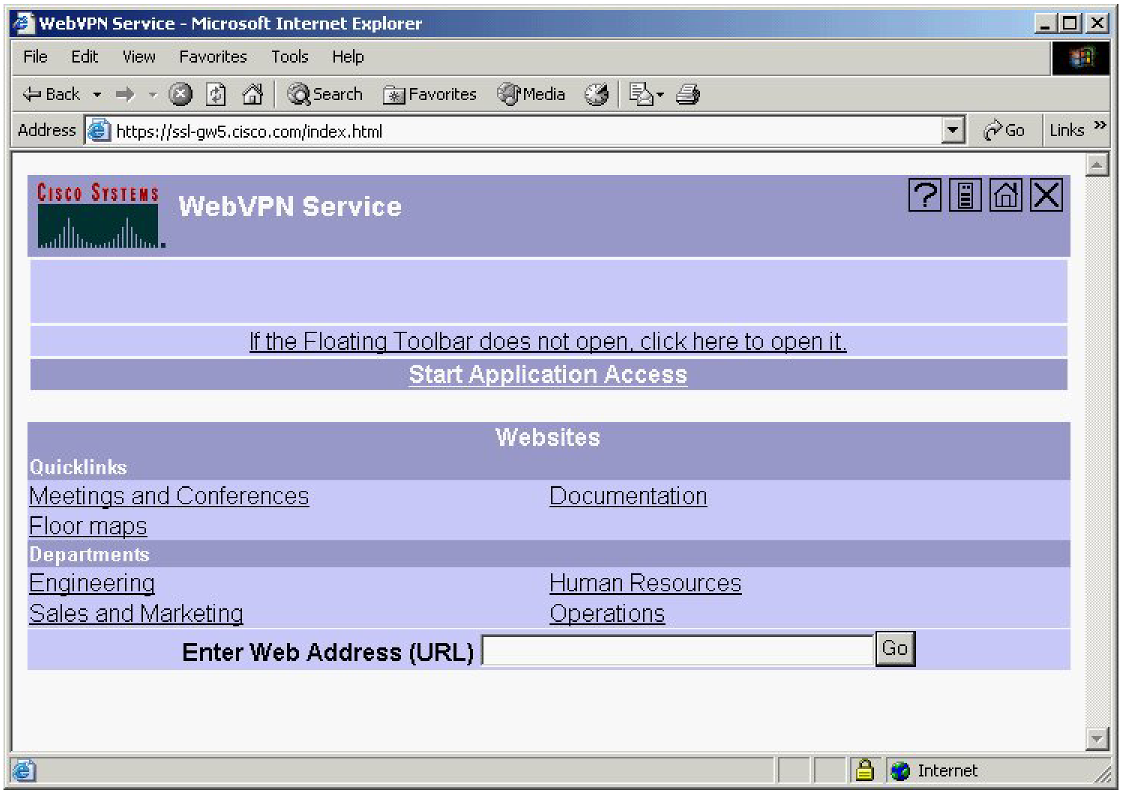
The portal page (see Figure 8) is the main page for the WebVPN functionality. You can customize this page to contain the following:

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

Items that you have not configured are not displayed on the portal page.

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

Figure 8 Portal Page



https://ssl-gw5.cisco.com/index.html

WebVPN Service

If the Floating Toolbar does not open, click here to open it.

Start Application Access

Websites

Quicklinks

Meetings and Conferences	Documentation
Floor maps	

Departments

Engineering	Human Resources
Sales and Marketing	Operations

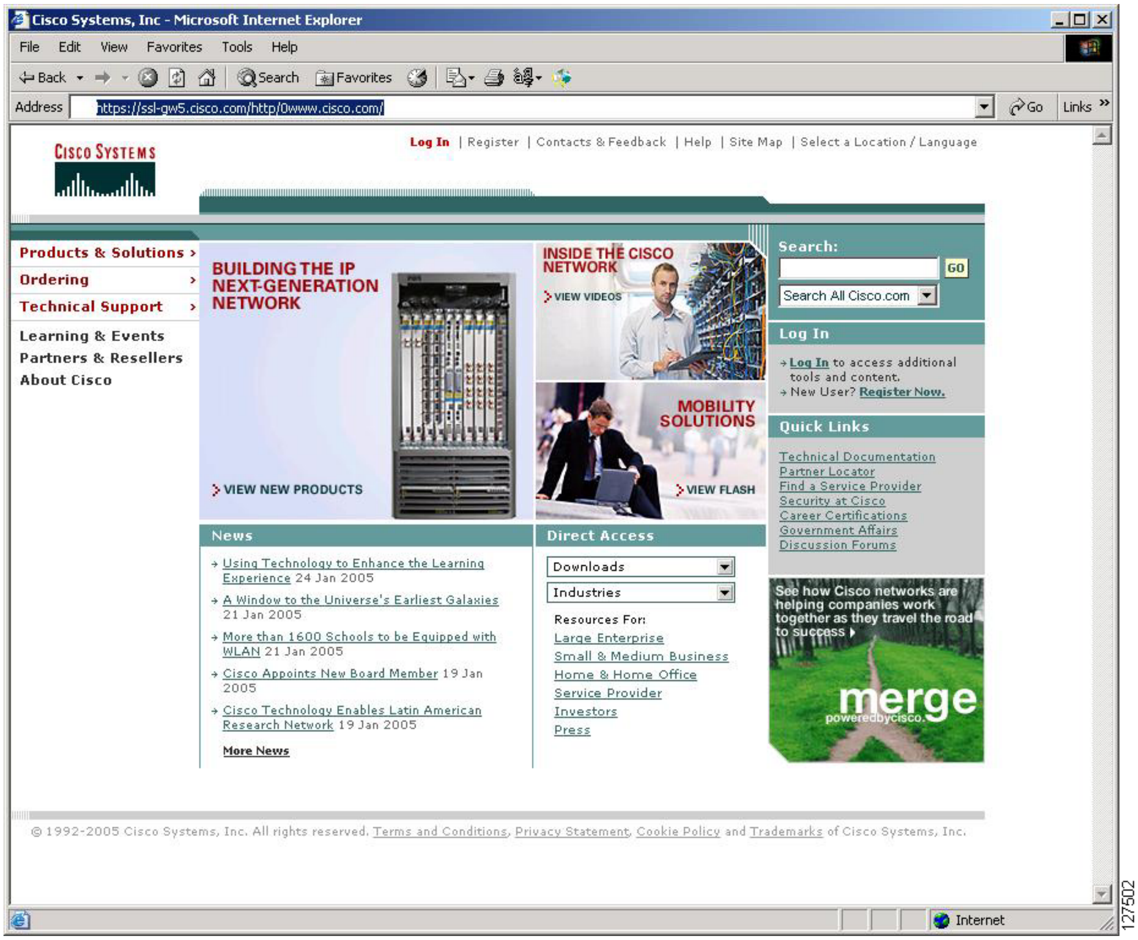
Enter Web Address (URL) Go

Remote Servers

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

Figure 9 illustrates the portal page of a typical website. By clicking the home icon button on the floating toolbar (see Figure 10), the remote user can go back to the portal page.

Figure 9 Website with a Toolbar



Address: https://ssl-gw5.cisco.com/http/0www.cisco.com/

Log In to access additional tools and content.
New User? Register Now.

- Using Technology to Enhance the Learning Experience 24 Jan 2005
- A Window to the Universe's Earliest Galaxies 21 Jan 2005
- More than 1600 Schools to be Equipped with WLAN 21 Jan 2005
- Cisco Appoints New Board Member 19 Jan 2005
- Cisco Technology Enables Latin American Research Network 19 Jan 2005

See how Cisco networks are helping companies work together as they travel the road to success

© 1992-2005 Cisco Systems, Inc. All rights reserved. Terms and Conditions, Privacy Statement, Cookie Policy and Trademarks of Cisco Systems, Inc.

WebVPN Floating Toolbar

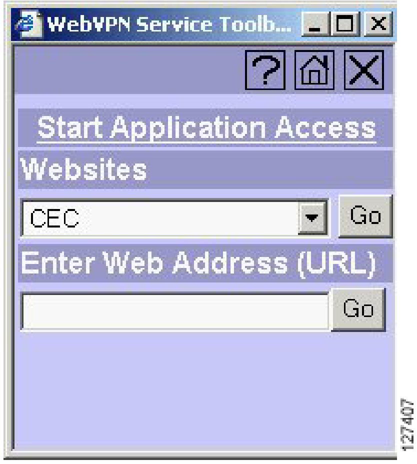
A floating toolbar (see Figure 10) allows the remote user to enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.

The floating toolbar represents the WebVPN session. If the remote user clicks the window Close button, the WebVPN gateway prompts the remote user to confirm that he or she wants to close the session.

Note Clicking the Home icon when viewing certain web pages, such as Hotmail.com and CNN.com, opens a new browser window because these sites rename the WebVPN browser window as part of how they function.

Tip To paste text into a text field, press Ctrl-V. Right-clicking is disabled in the WebVPN toolbar.

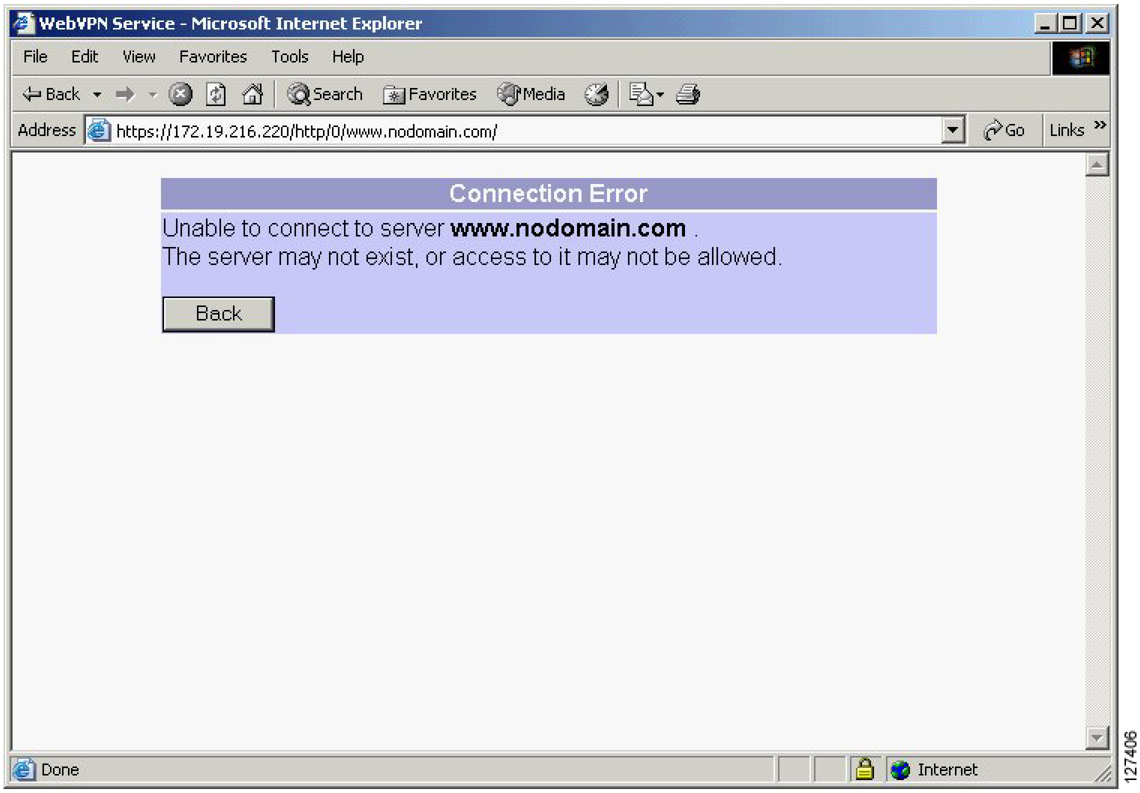
Figure 10 Floating Toolbar



DNS and Connection Errors

If a remote user specifies a remote server to which he or she cannot connect because of domain naming system (DNS) or other connection errors, an error displays (see Figure 11). Because of TCP timeouts, it may take a while for connection errors to be returned to the remote user.

Figure 11 DNS Errors


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.19.216.220/http/0/www.nodomain.com/
Go Links
Done
Internet
127406

Connection Error

Unable to connect to server **www.nodomain.com** .
The server may not exist, or access to it may not be allowed.

Back

Session Timeout

End users receive a warning approximately 1 minute before the session expires due to inactivity, and they receive another warning when the session expires (see Figure 12). The local time on the workstation is also displayed to indicate when the message was displayed.

The first message will be similar to the following:

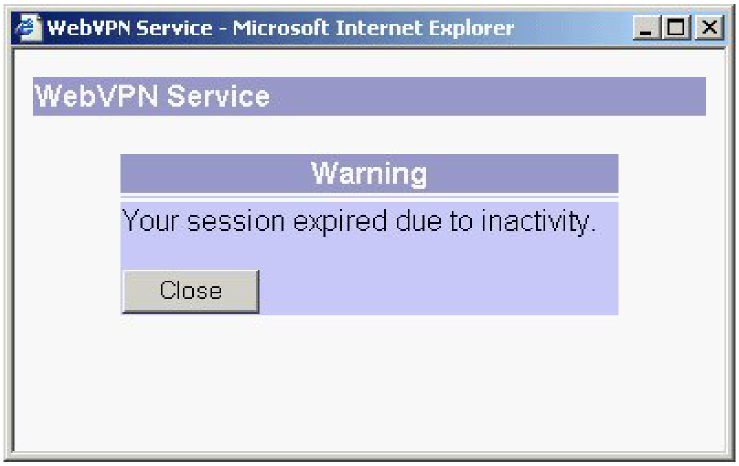
- "Your session will expire in *x* seconds due to inactivity. Click [Close] to reset the inactivity timer. (browser time and date)"

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

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

- "Your session has expired due to inactivity."

Figure 12 Session Inactivity or Timeout Window



WebVPN Service - Microsoft Internet Explorer

WebVPN Service

Warning

Your session expired due to inactivity.

TCP Port Forwarding and Application Access

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

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

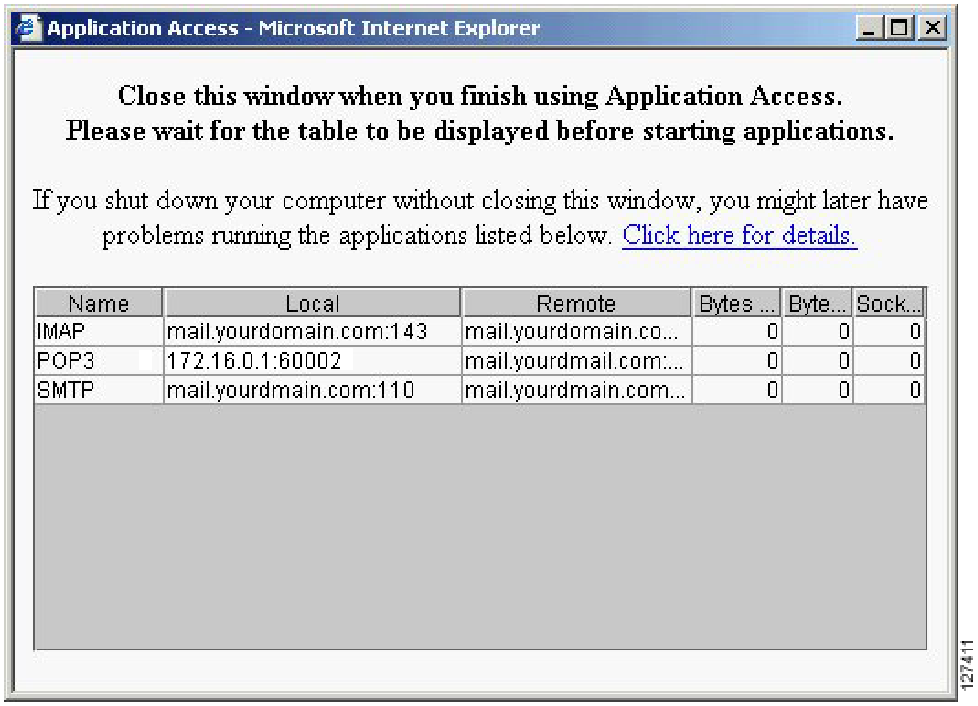
When the remote user clicks the Application Access link, a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks the remote user to verify the certificate with which this applet is signed. When the remote user accepts the certificate, the applet starts running, and port-forwarding entries are displayed (see Figure 13). The number of active connections and bytes that are sent and received is also listed on this window.

Note When remote users launch Application Access, their system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If the remote user connection hangs, tell the remote user to minimize the browser windows to check for this dialog box.

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

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

Figure 13 TCP Port Forwarding Page



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

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

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

Caution You should tell users to 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 to be disabled. See the "Application Access—Recovering from Hosts File Errors" section on page 74 for details.

Table 4 lists the requirements for Application Access (Port Forwarding) on the PC or device of a remote user.

Table 4 WebVPN Remote System Application Access Requirements

Remote User System Requirements	Specifications or Use Suggestions
Client applications installed.	—

Table 4 WebVPN Remote System Application Access Requirements (continued)

Remote User System Requirements	Specifications or Use Suggestions
Cookies enabled on browser.	—
Administrator priviliges.	Remote user must be local administrator on his or her PC.
Sun Microsystems JRE version 1.4 or later installed.	WebVPN automatically checks for JRE whenever the remote user starts Application Access. If it is necessary to install JRE, a pop-up window displays directing remote users to a site where it is available.
Client applications configured, if necessary. **Note** The Microsoft Outlook client does not require this configuration step.	To configure the client application, use the locally mapped IP address and port number of the server. To find this information, do the following: • Start WebVPN on the remote system and click the Application Access link on the WebVPN home page. The Application Access window is displayed. • In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column). • Use this IP address and port number to configure the client application. The configuration steps vary for each client application.
Windows XP SP2 patch.	End users running Windows XP SP2 must install a patch from Microsoft that is available at the following address: http://support.microsoft.com/?kbid=884020 This problem is a known Microsoft issue.

Using Other WebVPN Features

Table 5 lists the requirements for various WebVPN features.

Table 5 WebVPN Remote User System Requirements

Task	Remote User System Requirements	Specifications or Use Suggestions
Web Browsing	Usernames and passwords for protected websites	Using WebVPN does not ensure that communication with every site is secure. See the "Security Tips" section on page 73.
		The look and feel of web browsing with WebVPN might be different from what remote users are accustomed to. For example, when using WebVPN, note the following: • The WebVPN title bar appears above each web page • You can access websites as follows: – 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 by one of the previous two methods Also, depending on how you configured a particular account, the following might have occurred: • Some websites are blocked. • Only the websites that appear as links on the WebVPN home page are available.
Network Browsing and File Management	File permissions configured for shared remote access	Only shared folders and files are accessible through 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 the network of your organization.
	Note 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 5 WebVPN Remote User System Requirements (continued)

Task	Remote User System Requirements	Specifications or Use Suggestions
Using e-mail: Application Access	Fulfill requirements for Application Access (see the "TCP Port Forwarding and Application Access" section on page 69)	To use e-mail, start Application Access from the WebVPN home page. The e-mail client is then available for use.
	Note If the remote users are using an IMAP client and they lose their e-mail server connection or are unable to make a new connection, remote users should close the IMAP application and restart WebVPN.	
	Other Mail Clients	Cisco has tested Microsoft Outlook Express versions 5.5 and 6.0. WebVPN should support other SMTPS, POP3S, or IMAP4S e-mail programs, such as Netscape Mail, Lotus Notes, and Eudora, but Cisco has not verified them.
Using e-mail: Web Access	Web-based e-mail product installed	Supported products are as follows: • Outlook Web Access (OWA) 5.5, 2000, and 2003 Netscape, Mozilla, and Internet Explorer are supported with OWA 5.5 and 2000. Internet Explorer 6.0 or higher is required with OWA 2003. Netscape and Mozilla are not supported with OWA 2003. • Lotus Notes Other web-based e-mail products should also work, but Cisco has not verified them.
Using the WebVPN floating toolbar	Most platforms except for PocketPC	To paste text into a text field, press Ctrl-V. Right-clicking is disabled in the floating toolbar.
Using the Cisco SSL VPN Client (SVC)		To retrieve SVC log messages using the Windows Event Viewer, go to Program Files > Administrative Tools > Event Viewer in Windows.
Using Secure Desktop Manager	A Secure Desktop Manager-supported browser	On Microsoft Windows: • Internet Explorer version 6.0 • Netscape version 7.2 On Linux: • Netscape version 7.2
Using Cache Cleaner or Secure Desktop	A Cisco Secure Desktop-supported browser	Any browser supported for Secure Desktop Manager.

Security Tips

Advise remote users always to log out from the WebVPN session when they are finished. (To log out of WebVPN, click the logout icon on the WebVPN toolbar or quit the browser.)

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

Browser Caching and Security Implications

If remote users access WebVPN through a public or shared Internet system, such as at an Internet cafe or kiosk, to ensure the security of their information after terminating or logging out of the WebVPN session, remote users must delete all files that they saved on the PC during the WebVPN session. These files are not removed automatically upon disconnect.

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

Application Access—Recovering from Hosts File Errors

It is very important to tell remote users to close the Application Access window properly by clicking the close icon. If they do not close the window properly, the following could occur:

- The next time remote users try to start Application Access, it might be disabled; they will receive a “Backup HOSTS File Found” error message
- The applications might be disabled or might malfunction even when the remote user is running them locally

These errors can result from remote users terminating the Application Access window in any improper way:

- The browser crashes while using Application Access
- A power outage or system shutdown occurs while using Application Access
- End users minimize the Application Access window and then shut down the computer with the window active (but minimized)

How WebVPN Uses the Hosts File

The hosts file on the remote user system maps IP addresses to hostnames. When the remote user starts Application Access, WebVPN modifies the hosts file by adding WebVPN-specific entries. When the remote user stops Application Access by properly closing the Application Access window, WebVPN returns the hosts file to its original state. The hosts file goes through the following states:

- Before invoking Application Access, the hosts file is in its original state.
- When Application Access starts, WebVPN does the following:
  1. Copies the hosts file to hosts.webvpn and creates a backup.
  2. Edits the hosts file, inserting WebVPN-specific information.
- When Application Access stops, WebVPN does the following:
  1. Copies the backup file to the hosts file, which restores the hosts file to its original state.

2. Deletes hosts.webvpn.

- After finishing Application Access, the hosts file is in its original state.

What Happens When the Remote User Stops Application Access Improperly

If the remote user improperly terminates Application Access, the hosts file is left in a WebVPN-customized state. WebVPN checks for this possibility the next time that the remote user starts Application Access by searching for a hosts.webvpn file. If WebVPN finds the file, the remote user receives a “Backup HOSTS File Found” error message, and Application Access is temporarily disabled.

When remote users shut down Application Access improperly, they leave the remote access client/server applications in a suspended state. If remote users try to start these applications without using WebVPN, the applications might malfunction. Remote users might find that hosts that they normally connect to are unavailable. This situation could commonly occur if remote users run applications remotely from home, fail to quit the Application Access window before shutting down the computer, and then try to run the applications later from the office.

What to Do

To reenable Application Access or malfunctioning applications, remote users should do the following:

- If they can connect to their remote access server, they should follow the steps in the “Reconfiguring the Hosts File Automatically Using WebVPN” section on page 75.
- If they cannot connect to their remote access server from their current location or if they have made custom edits to the hosts file, they should follow the steps in the “Reconfiguring the Hosts File Manually” section on page 76.

Reconfiguring the Hosts File Automatically Using WebVPN

If remote users are able to connect to their remote access server, they should follow these steps to reconfigure the hosts file and reenable both Application Access and the applications:

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

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

Step 3 Choose one of the following options:

- Restore from backup—WebVPN forces a proper shutdown. WebVPN copies the hosts.webvpn backup file to the hosts file, restoring it to its original state, and then deletes hosts.webvpn. You then have to restart Application Access.
- Do nothing—Application Access does not start. You return to your remote access home page.
- Delete backup—WebVPN deletes the hosts.webvpn file, leaving the hosts file in its WebVPN-customized state. The original hosts file settings are lost. Then Application Access starts, using the WebVPN-customized hosts file as the new original. Choose this option only if you are unconcerned about losing hosts file settings. If you 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 the Hosts File Manually” section on page 76.)

Reconfiguring the Hosts File Manually

If remote users are not able to connect to their remote access server from their current location, or if remote users have customized the hosts file and do not want to lose their edits, they should follow these steps to reconfigure the hosts file and reenable both Application Access and the applications:

Step 1 Locate and edit your hosts file.

Step 2 Check if any lines contain the “added by WebVpnPortForward” string.

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

```
10.23.0.3 server1 # added by WebVpnPortForward
10.23.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
10.23.0.4 server2 # added by WebVpnPortForward
10.23.0.4 server2.example.com.vpn3000.com # added by WebVpnPortForward
10.23.0.5 server3 # added by WebVpnPortForward
10.23.0.5 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 hostnames. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding hostname.
# The IP address and the hostname should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      172.16.102.97     rhino.acme.com          # source server
#      192.168.63.10     x.acme.com              # x client host

10.23.0.1       localhost
```

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

Step 4 Save and close the file.

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

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

E-mail Proxy

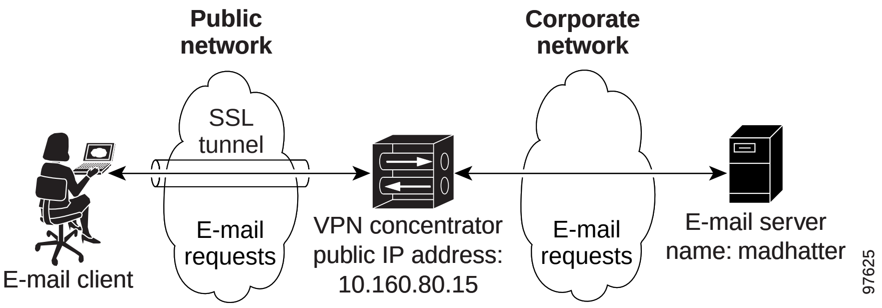
WebVPN lets you set up native mail applications on remote systems for automatic access to office e-mail. This feature, called E-mail Proxy, uses the WebVPN gateway as a proxy to the mail server. You need to configure E-mail Proxy on both the WebVPN gateway and the user mail application.

The following instructions explain how to configure the most commonly used e-mail applications: Outlook Express, Netscape, and Eudora.

Example Configuration

Figure 14 shows the network environment used in the example.

Figure 14 A Typical E-mail Proxy Network Scenario



To configure the mail application on the remote system to participate in e-mail proxy, you need to know certain information about the user, the WebVPN gateway, and the e-mail server. Table 6 shows the information needed, as well as sample values used in the example configurations.

Table 6 Sample Values Used in the Example E-mail Proxy Configuration

User	WebVPN Gateway	E-mail Server
Name: Smith E-mail address: me@mycompany.com Outgoing Mail Port (SMTPS): 988 Incoming Mail Port (POP3S): 995	Username: AliceSmith Password: 12345 Public IP Address: 10.160.80.15 Outgoing Mail Port (SMTPS): 988 Incoming Mail Port (POP3S): 995 Incoming Mail Port (IMAP4S): 993	Username: alice Password: abcde Server Name: Email

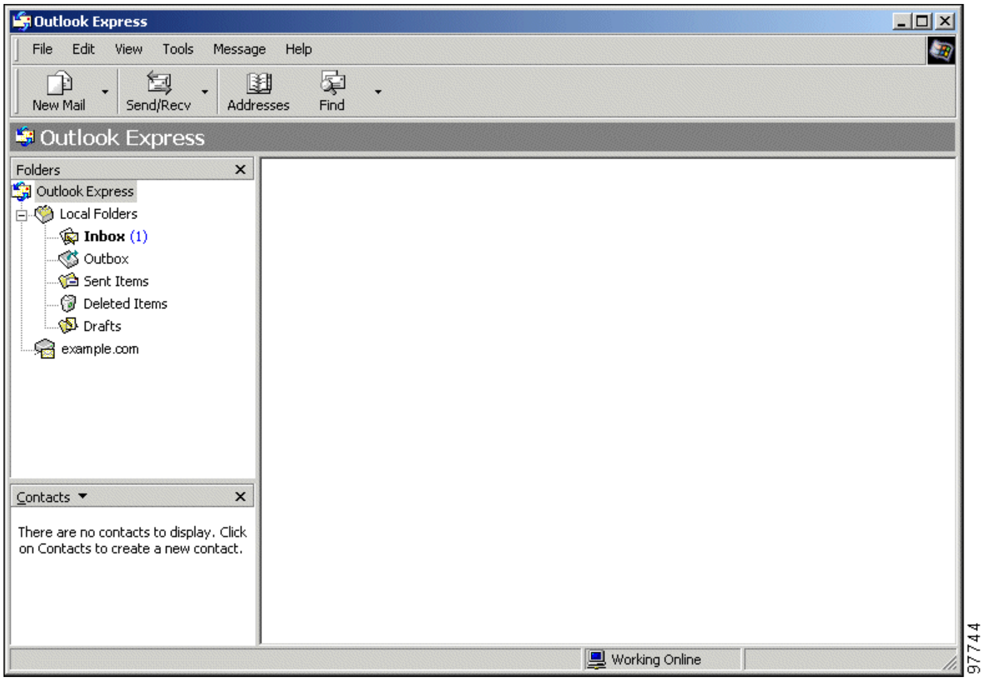
Outlook Express on Windows 2000

These instructions explain how to configure an Outlook Express client running on Windows 2000 to participate in E-mail Proxy.

Configuring Outlook Express

Step 1 Click Start -> Programs -> Outlook Express on the Windows 2000 desktop toolbar. The Outlook Express main window appears. (See Figure 15.)

Figure 15 Outlook Express Main Window

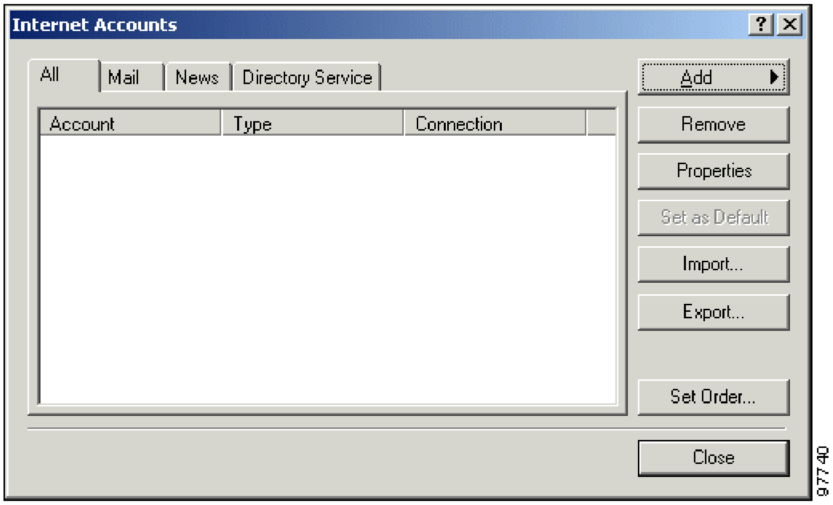


There are no contacts to display. Click on Contacts to create a new contact.

Step 2 Choose **Accounts** from the Tools drop-down menu. The Internet Accounts window is displayed. (See Figure 16.)

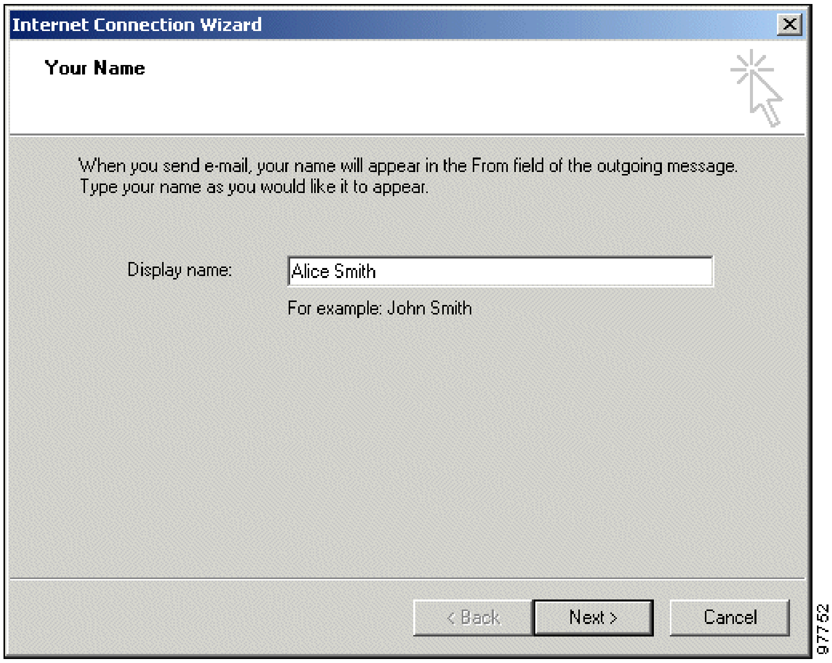
Figure 16 Internet Accounts Window

]



Step 3 Click the **Add** button and choose **Mail** from the menu. The Internet Connection Wizard Your Name window is displayed. (See Figure 17.)

Figure 17 Internet Connection Wizard: Your Name Window



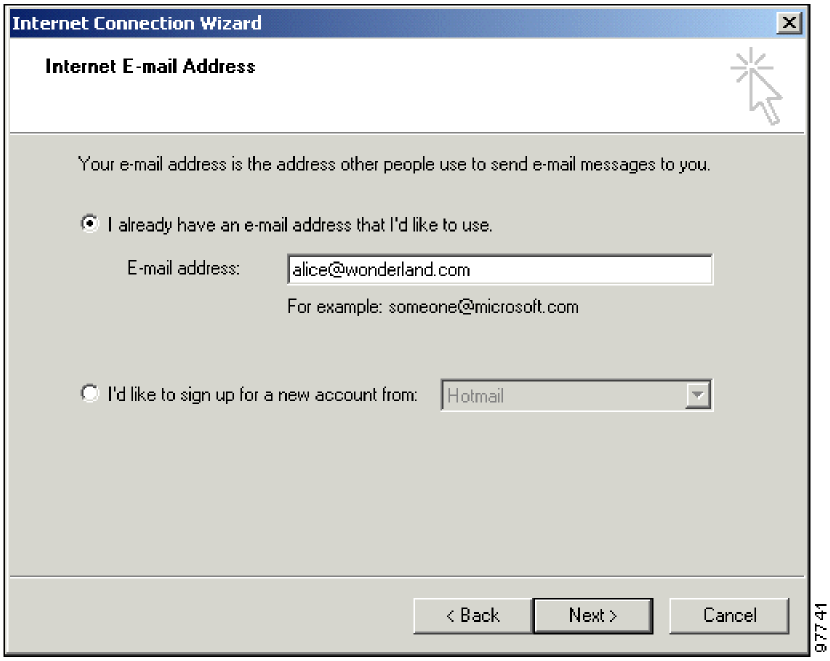
When you send e-mail, your name will appear in the From field of the outgoing message. Type your name as you would like it to appear.

Display name: Alice Smith

For example: John Smith

Step 4 Enter a **Display name** for the user. This name will appear in the From header of e-mails the user sends. Click Next. The Internet E-mail Address window appears. (See Figure 18.)

Figure 18 Internet E-mail Address Window



Your e-mail address is the address other people use to send e-mail messages to you.

● I already have an e-mail address that I'd like to use.

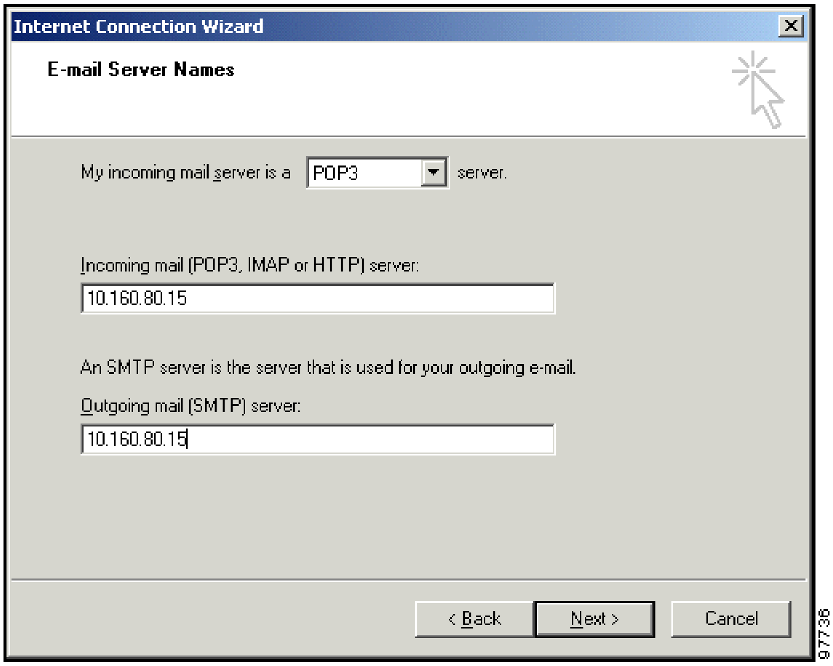
E-mail address: alice@wonderland.com

For example: someone@microsoft.com

○ I'd like to sign up for a new account from: Hotmail

Step 5 Select the option **I already have an e-mail address that I'd like to use**. Enter the user e-mail address at the prompt. Click **Next**. The E-mail Server Names window appears. (See Figure 19.)

Figure 19 E-mail Server Names Window



Internet Connection Wizard

E-mail Server Names

My incoming mail server is a POP3 server.

Incoming mail (POP3, IMAP or HTTP) server:
10.160.80.15

An SMTP server is the server that is used for your outgoing e-mail.

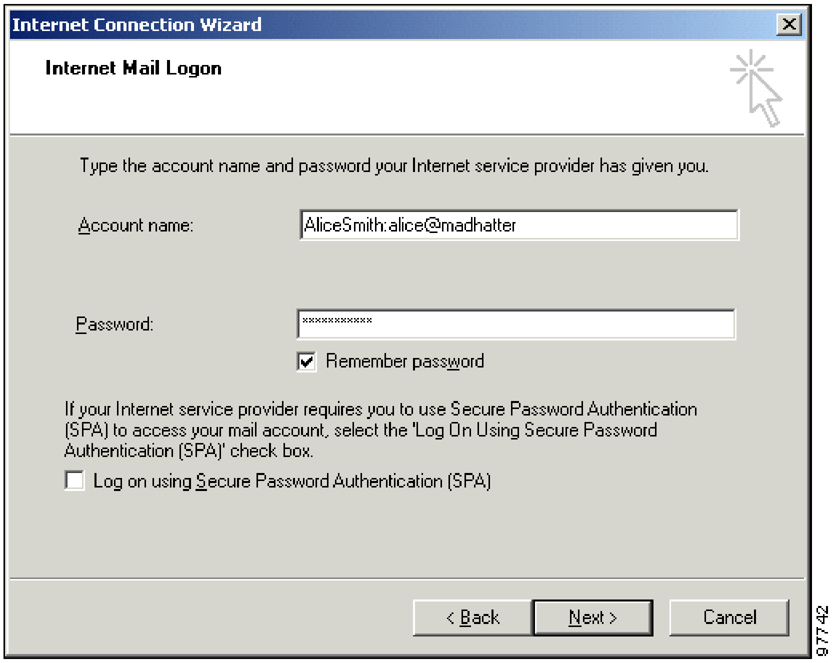
Outgoing mail (SMTP) server:
10.160.80.15

Step 6 Choose the e-mail protocol you configured for E-mail Proxy on the WebVPN gateway.

Step 7 Enter in both the Incoming and the Outgoing Mail fields the IP address of the interface of the WebVPN gateway on which you enabled E-mail Proxy protocols. (The example uses the Public interface.)

Step 8 Click **Next**. The Internet Mail Logon window appears. (See Figure 20.)

Figure 20 Internet Mail Logon Window



Internet Connection Wizard

Internet Mail Logon

Type the account name and password your Internet service provider has given you.

Account name: AliceSmith:alice@madhatter

Password: ************

☑ Remember password

If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box.

☐ Log on using Secure Password Authentication (SPA)

Step 9 If the WebVPN gateway username and mail server username are the same, enter this name at the prompt, in the form:

(*E-Mail Username*) [*E-mail Server Delimiter*] [*E-mail Server Name*]

Where:

- *E-mail Username* = The e-mail login name of the remote user.
- *E-mail Server Delimiter* = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.
- *E-mail Server Name* = The name of the user e-mail server. You can omit this field if using the default mail server.

For example: me@mycompany.com

If the user WebVPN gateway username and mail server username are different, enter both usernames in the following form:

(*WebVPN gateway Username*) (*VPN Name Delimiter*) (*E-mail Username*) [*E-mail Server Delimiter*] [*E-mail Server Name***]**

Where:

- *WebVPN gateway Username* = The user WebVPN gateway login name.
- *VPN Name Delimiter* = The delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen that separates the VPN username from the e-mail username. (The default VPN Name Delimiter is a colon.)
- *E-mail Username* = The name of the user e-mail account.

- *E-mail Server Delimiter* = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.
- *E-mail Server Name* = The name of the user e-mail server. You can omit this field if using the default mail server.

Step 10 Enter the user e-mail password, in the form:

[*WebVPN gateway Password*] [*VPN Name Delimiter*] [*E-mail Password*]

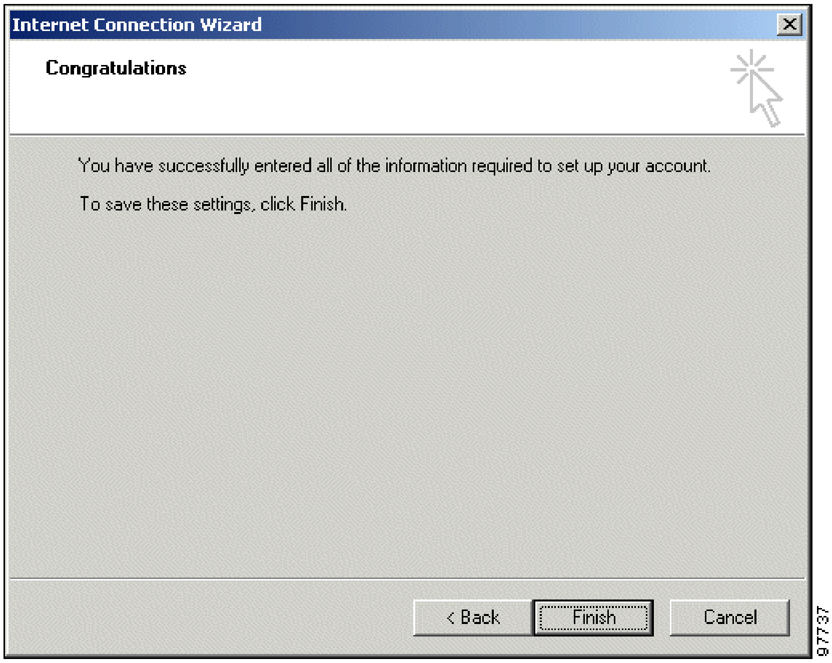
Where:

- *WebVPN gateway Password* = The user WebVPN gateway login password. If the WebVPN gateway password and the mail password are the same, you can omit this field.
- *VPN Name Delimiter* = The delimiter you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail that separates the VPN username from the e-mail username. (The default VPN NAme Delimiter is a colon.) This delimiter is necessary only if the WebVPN gateway password is present.
- *E-mail Password* = The password for the user e-mail account.

  For example, 12345:abcde.

Step 11 Click **Next**. A final window appears. Click **Finish**. (See Figure 21.)

Figure 21 Final Wizard Window



Internet Connection Wizard

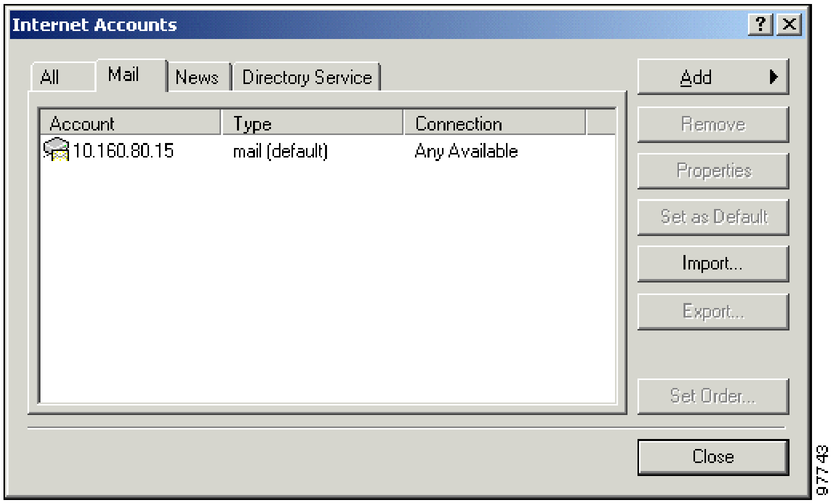
Congratulations

You have successfully entered all of the information required to set up your account.

To save these settings, click Finish.

Step 12 In the Internet Accounts window, click the **Mail** tab. (See Figure 22.)

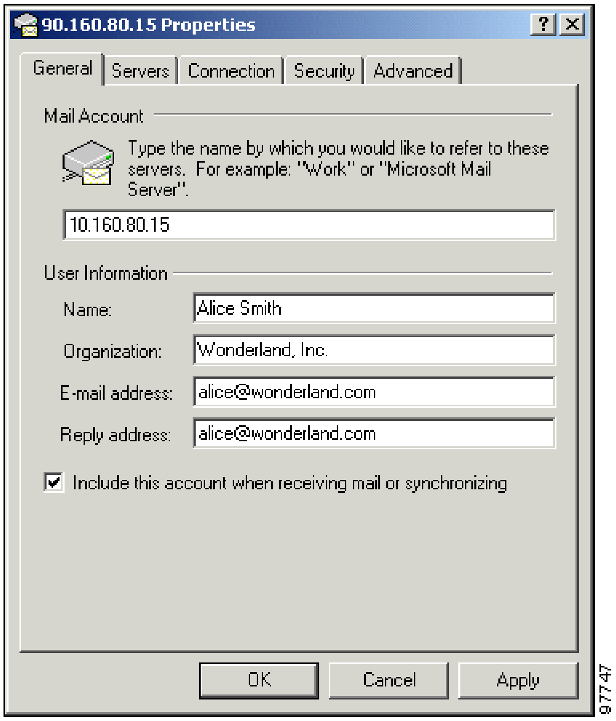
Figure 22 Internet Accounts Window: Mail Tab



Account	Type	Connection
10.160.80.15	mail (default)	Any Available

Step 13 Select the new mail account, and then click the **Add** button. The Properties window appears. (See Figure 23.)

Figure 23 Properties Window: General Tab



Mail Account

Type the name by which you would like to refer to these servers. For example: "Work" or "Microsoft Mail Server".

10.160.80.15

User Information

Name: Alice Smith

Organization: Wonderland, Inc.

E-mail address: alice@wonderland.com

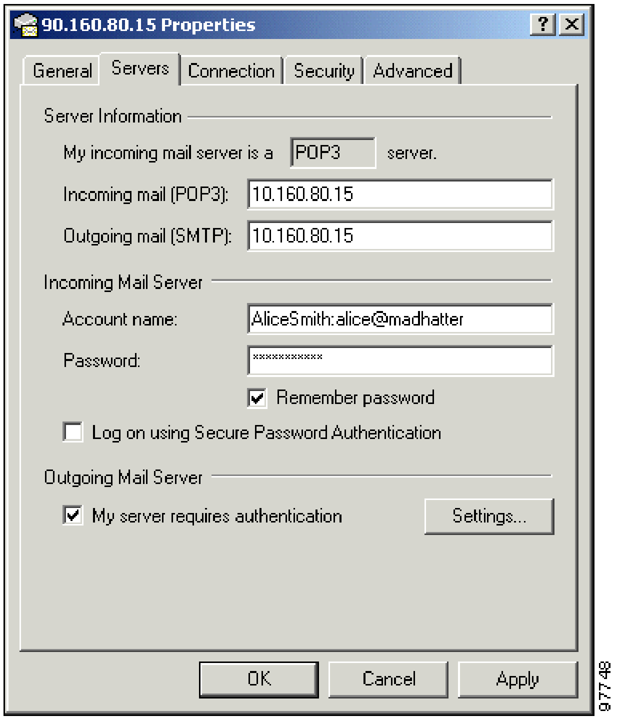
Reply address: alice@wonderland.com

☑ Include this account when receiving mail or synchronizing

Step 14 (Optional) Fill in a server name and add additional user information.

Step 15 Click the **Servers** tab. (See Figure 24.)

Figure 24 Properties Window: Server Tab



90.160.80.15 Properties

General | Servers | Connection | Security | Advanced

Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): 10.160.80.15

Outgoing mail (SMTP): 10.160.80.15

Incoming Mail Server

Account name: AliceSmith:alice@madhatter

Password: ***********

☑ Remember password

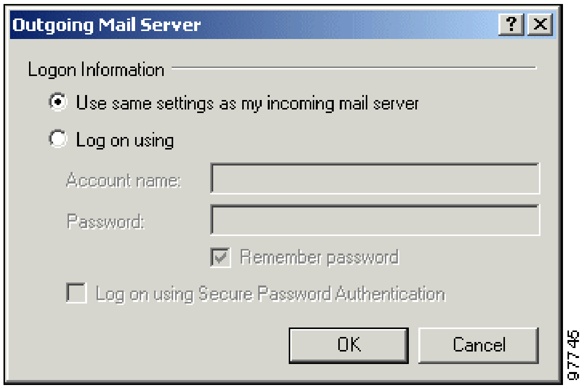
☐ Log on using Secure Password Authentication

Outgoing Mail Server

☑ My server requires authentication

Step 16 Under Outgoing Mail Server, click the **My server requires authentication** check box. Click the **Settings** button. The Outgoing Mail Server window appears. (See Figure 25.)

Figure 25 Outgoing Mail Server Window



Outgoing Mail Server

Logon Information

● Use same settings as my incoming mail server

○ Log on using

Account name:

Password:

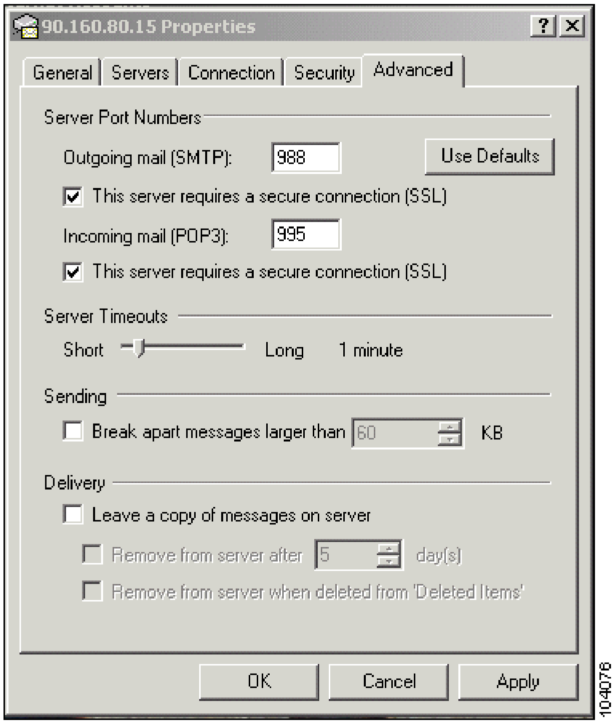
☑ Remember password

☐ Log on using Secure Password Authentication

Step 17 Click **Use same settings as my incoming mail server**. Click OK.

Step 18 Click the **Advanced** tab in the Properties window (See Figure 26).

Figure 26 Properties Window: Advanced Tab



90.160.80.15 Properties

Server Port Numbers

Outgoing mail (SMTP): 988

☑ This server requires a secure connection (SSL)

Incoming mail (POP3): 995

☑ This server requires a secure connection (SSL)

Server Timeouts

Short — Long 1 minute

Sending

☐ Break apart messages larger than 60 KB

Delivery

☐ Leave a copy of messages on server

☐ Remove from server after 5 day(s)

☐ Remove from server when deleted from 'Deleted Items'

Step 19 Under Server Port Numbers:

a. For the Outgoing Mail field:

– Enter the SMTPS port number you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen.

– Click the **This server requires a secure connection (SSL)** check box.

b. For the Incoming Mail field:

– Enter the POP3S or IMAP4S port numbers you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen.

– Click **This server requires a secure connection (SSL)** check box.

Step 20 Click **Apply**.

Step 21 Click **OK**.

The configuration is complete.

To test the configuration, send or receive e-mail. If the test fails, see the Outlook Express error messages and check EMAILPROXY events in the WebVPN gateway error log.

Eudora 5.2 on Windows 2000

These instructions explain how to configure an Eudora 5.2 client running on Windows 2000 to participate in E-mail Proxy.

Configuring Eudora

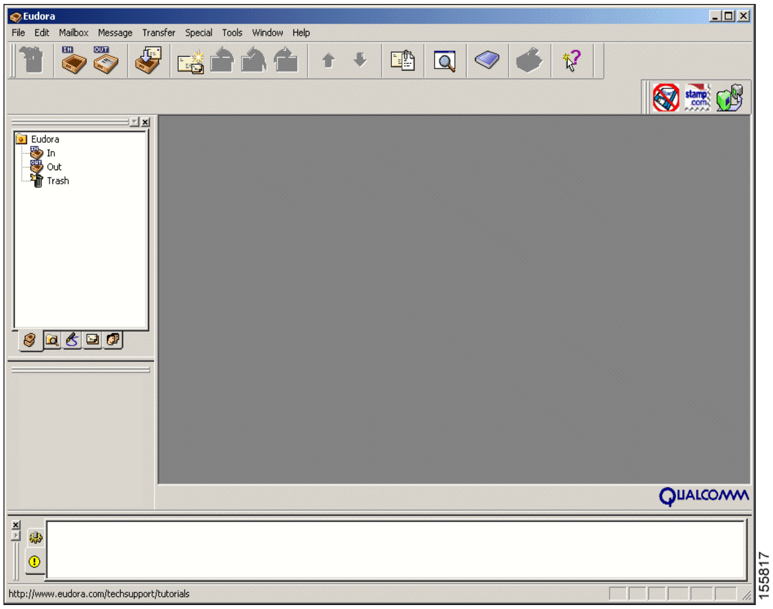
Configuring Eudora to participate in E-Mail Proxy has two steps:

- Configure the client application
- Edit the eudora.ini file

Configuring the Client Application

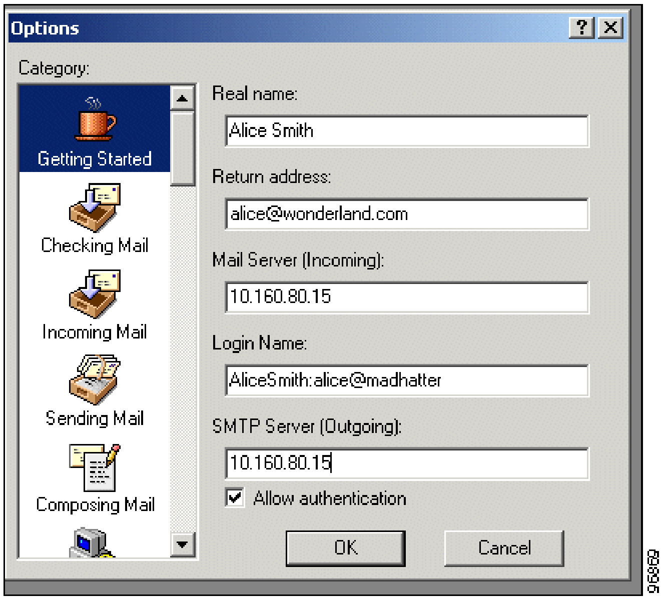
Step 1 Start Eudora. The Eudora Main Window is displayed. (See Figure 27.)

Figure 27 Eudora Main Window


Eudora
File Edit Mailbox Message Transfer Special Tools Window Help
IN
OUT
stamps.com
Eudora
In
Out
Trash
QUALCOMM
http://www.eudora.com/techsupport/tutorials
155817

Step 2 Choose **Options** from the Tools drop-down menu. The Options window is displayed. Click the **Getting Started** icon. (See Figure 28.)

Figure 28 Eudora Options Window, Getting Started



Real name: Alice Smith

Return address: alice@wonderland.com

Mail Server (Incoming): 10.160.80.15

Login Name: AliceSmith:alice@madhatter

SMTP Server (Outgoing): 10.160.80.15

☑ Allow authentication

a. In the Real Name field, enter the name of the user.

b. In the Return Address field, enter a return e-mail address for the user; for example, me@mycompany.com. Replies to mail sent by this user go to this address.

c. In the Mail Server (Incoming) field, enter the hostname or IP address of the WebVPN gateway interface on which you enabled (POP3 or IMAP) E-mail Proxy protocols.

d. If the user WebVPN gateway username and mail server username are the same, enter this name in the Login Name field in the form:

(*E-Mail Username*) [*E-mail Server Delimiter*] [*E-mail Server Name*]

Where:

– *E-mail Username* = The user e-mail login name.

– *E-mail Server Delimiter* = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.

– *E-mail Server Name* = The name of the user e-mail server. You can omit this field if using the default mail server.

For example: me@mycompany.com

If the user WebVPN gateway username and mail server username are different, enter both usernames in the following form:

(*WebVPN gateway Username*) (*VPN Name Delimiter*) (*E-mail Username*) [*E-mail Server Delimiter*] [*E-mail Server Name*]

Where:

– *WebVPN gateway Username* = The user WebVPN gateway login name.

– *VPN Name Delimiter* = The delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen that separates the VPN username from the e-mail username. (The default VPN Name Delimiter is a colon.)

– *E-mail Username* = The name of the user e-mail account.

– *E-mail Server Delimiter* = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.

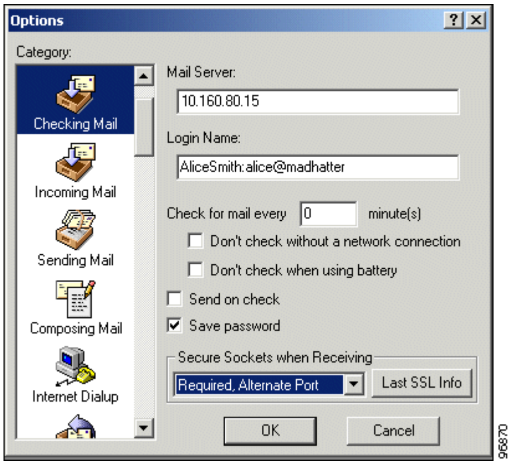
– *E-mail Server Name* = The name of the user e-mail server. You can omit this field if using the default mail server.

e. In the SMTP Server (Outgoing) field, enter the hostname or IP of the WebVPN gateway interface on which you enabled the SMTP E-mail Proxy protocol.

f. Click the **Allow Authentication** check box.

Step 3 Click the **Checking Mail** icon. (See Figure 29.) Under Secure Sockets when Receiving, choose **Required, Alternate Port** from the drop-down menu.

Figure 29 Eudora Options WIndow, Checking Mail



Mail Server: 10.160.80.15

Login Name: AliceSmith:alice@madhatter

Check for mail every 0 minute(s)

□ Don't check without a network connection

□ Don't check when using battery

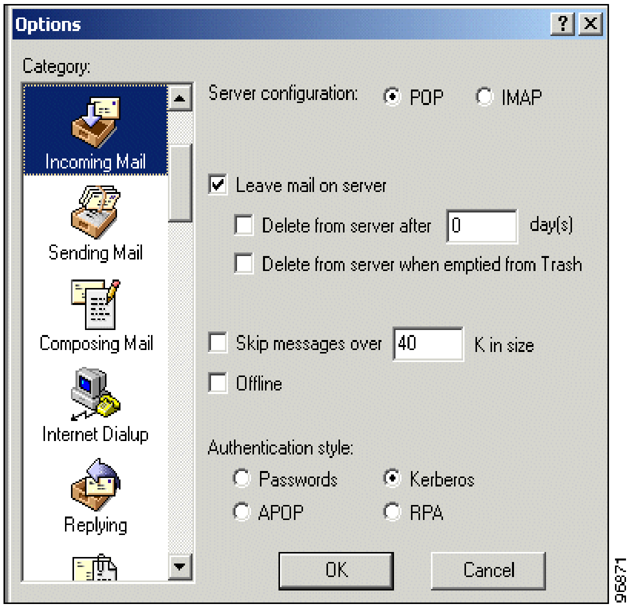
□ Send on check

☑ Save password

Secure Sockets when Receiving: Required, Alternate Port

Step 4 Click the **Incoming Mail** icon. (See Figure 30.) Click **POP** or **IMAP** to choose your server configuration type.

Figure 30 Eudora Options Window, Incoming Mail



Server configuration: ● POP ○ IMAP

☑ Leave mail on server

□ Delete from server after 0 day(s)

□ Delete from server when emptied from Trash

□ Skip messages over 40 K in size

□ Offline

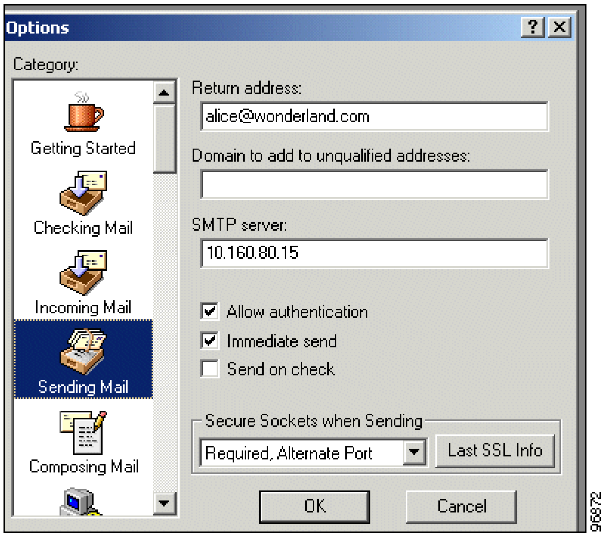
Authentication style:

○ Passwords ● Kerberos

○ APOP ○ RPA

Step 5 Click the **Sending Mail** icon. (See Figure 31.) Under Secure Sockets when sending, choose **Required, Alternate Port** from the drop-down menu.

Figure 31 Eudora Options Window, Sending Mail



Return address: alice@wonderland.com

Domain to add to unqualified addresses:

SMTP server: 10.160.80.15

☑ Allow authentication

☑ Immediate send

□ Send on check

Secure Sockets when Sending: Required, Alternate Port

Step 6 Click the **OK** button. The Options window closes.

Step 7 Choose **Exit** from the File menu to quit Eudora.

Editing the eudora.ini File

Step 1 Locate the eudora.ini file in the Eudora default installation directory.

Note If you do not have an eudora.ini file on your system, copy the deudora.ini file and rename it eudora.ini.

Step 2 Open eudora.ini in any text editor.

Step 3 Find the following line of text:

[Settings]

Step 4 Beneath this line, add the following three lines:

SSLPOPAlternatePort=[POP Port]

SSLIMAPAlternatePort=[IMAP Port]

SSLSMTPAlternatePort=[SMTP Port]

Where:

- *POP Port* = The POP3S port configured on the Configuration | Tunneling and Security | WebVPN | E-mail screen of the WebVPN gateway. The default is 995.
- *IMAP Port* = The IMAP4S port configured on the Configuration | Tunneling and Security | WebVPN | E-mail screen of the WebVPN gateway. The default is 993.
- *SMTP Port* = The SMTPS port configured on the Configuration | Tunneling and Security | WebVPN | E-mail screen of the WebVPN gateway. The default is 988.

  For example:

  [Settings]

  SSLPOPAlternatePort=995

  SSLIMAPAlternatePort=993

  SSLSMTPAlternatePort=988

The configuration is complete.

Using Eudora with E-Mail Proxy

When the user sends or receives mail, Eudora prompts for a password.

- If the user WebVPN gateway password and e-mail password are the same, enter that password.
- If the WebVPN gateway password and e-mail password are different, enter them both in the form:

  [*WebVPN gateway Password*] [*VPN Name Delimiter*] [*E-mail Password*]

  Where:

  – WebVPN gateway Password = The user WebVPN gateway login password.

  – VPN Name Delimiter = The delimiter you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail that separates the VPN username from the e-mail username. (The default VPN NAme Delimiter is a colon.)

  – E-mail Password = The password for the user e-mail account.

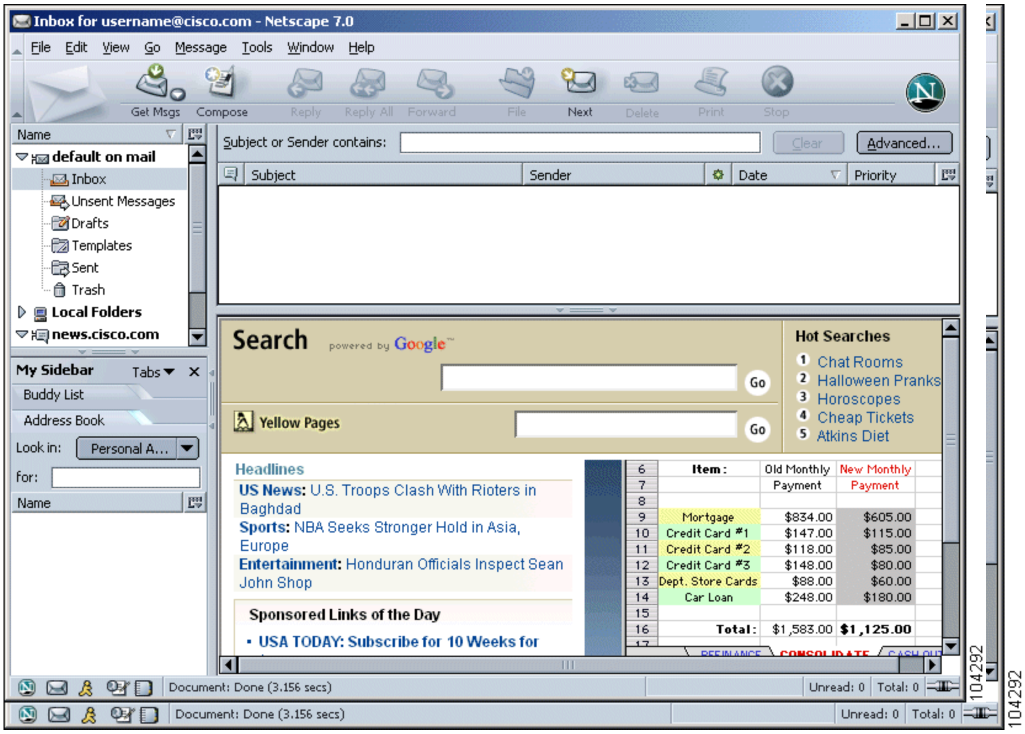
For example, 12345:abcde.

Netscape Mail 7 on Windows 2000

These instructions explain how to configure a Netscape client running on Windows 2000 to participate in E-mail Proxy.

Step 1 Start the Netscape Mail and Newsgroups program. The Netscape Mail window appears. (See Figure 32.)

Figure 32 Netscape Mail Window



US News: U.S. Troops Clash With Rioters in Baghdad
Sports: NBA Seeks Stronger Hold in Asia, Europe
Entertainment: Honduran Officials Inspect Sean John Shop

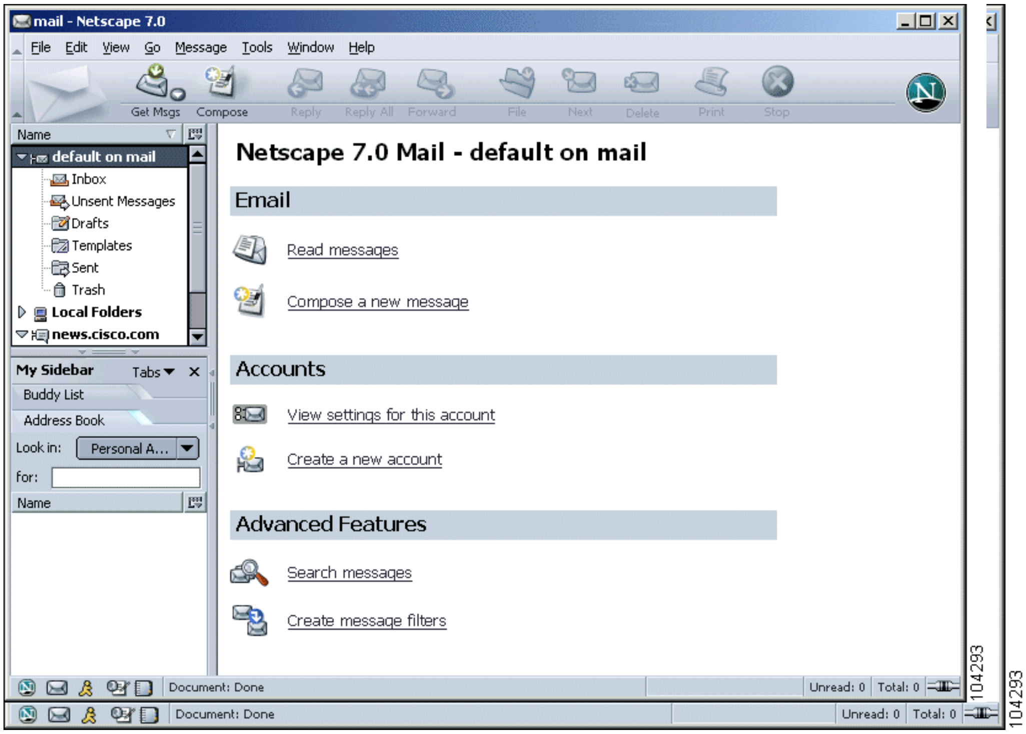
Sponsored Links of the Day

- USA TODAY: Subscribe for 10 Weeks for

	Item:	Old Monthly Payment	New Monthly Payment
6			
7			
8			
9	Mortgage	$834.00	$605.00
10	Credit Card #1	$147.00	$115.00
11	Credit Card #2	$118.00	$85.00
12	Credit Card #3	$148.00	$80.00
13	Dept. Store Cards	$88.00	$60.00
14	Car Loan	$248.00	$180.00
15			
16	Total:	$1,583.00	$1,125.00

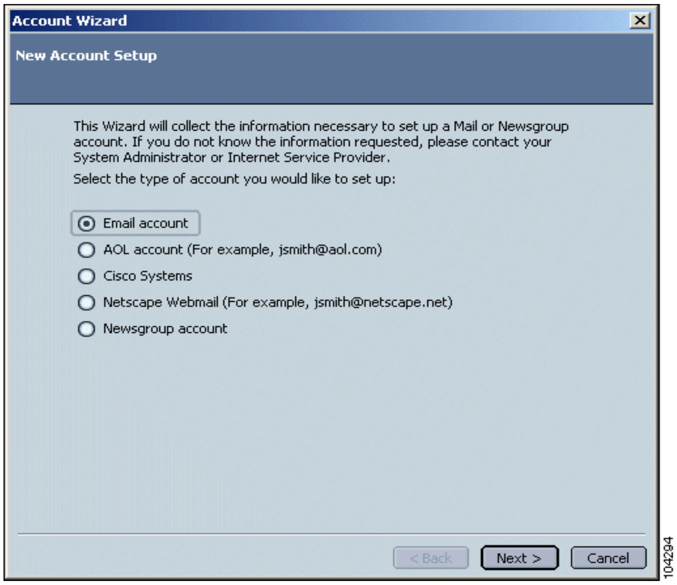
Step 2 Choose **default on mail** from the Name list at the left. The Default on Mail window appears. (See Figure 33.)

Figure 33 Default on Mail Window



Step 3 Under Accounts, click the **Create a New Account** link. The Account Wizard New Account Setup window appears. (See Figure 34.)

Figure 34 Account Wizard: New Account Setup Window



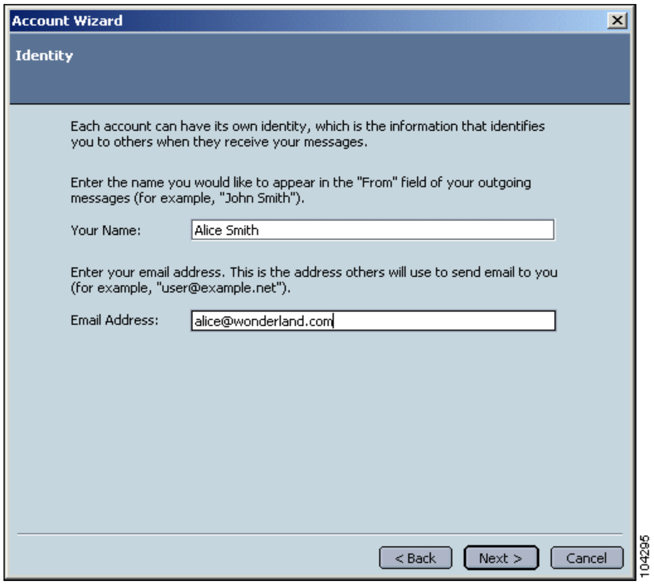
This Wizard will collect the information necessary to set up a Mail or Newsgroup account. If you do not know the information requested, please contact your System Administrator or Internet Service Provider.

Select the type of account you would like to set up:

● Email account
○ AOL account (For example, jsmith@aol.com)
○ Cisco Systems
○ Netscape Webmail (For example, jsmith@netscape.net)
○ Newsgroup account

Step 4 Choose the **Email account** option. Click **Next**. The Identity window appears. (See Figure 35.)

Figure 35 Account Wizard: Identity Window



Each account can have its own identity, which is the information that identifies you to others when they receive your messages.

Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").

Your Name: Alice Smith

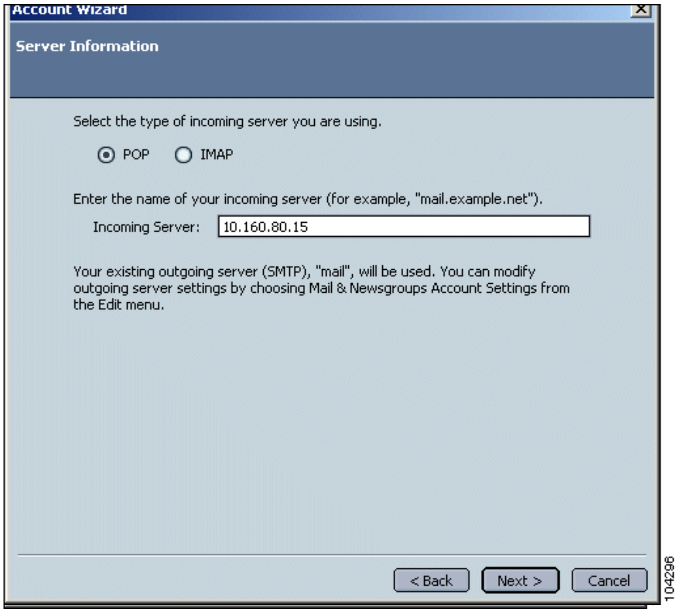
Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").

Email Address: alice@wonderland.com

Step 5 In the Your Name field, enter the username. This name will appear in the From header of e-mails the user sends.

Step 6 In the Email Address field, enter the user e-mail address. Click **Next**. The Server Information window appears. (See Figure 36.)

Figure 36 Account Wizard: Server Information Window



Select the type of incoming server you are using.

◉ POP ○ IMAP

Enter the name of your incoming server (for example, "mail.example.net").

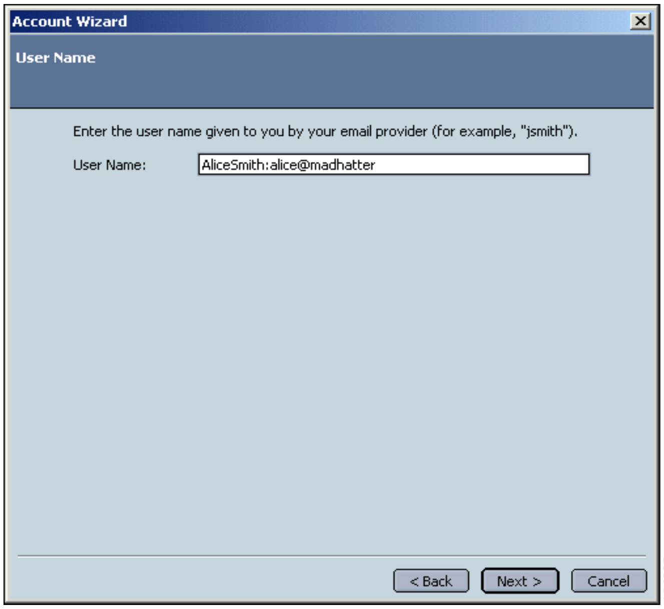
Incoming Server: 10.160.80.15

Your existing outgoing server (SMTP), "mail", will be used. You can modify outgoing server settings by choosing Mail & Newsgroups Account Settings from the Edit menu.

Step 7 Click **Mail** (**POP** or **IMAP**) to choose the mail protocol you are using for incoming mail.

Step 8 Enter the IP address of the interface of the WebVPN gateway on which you enabled the POP or IMAP E-mail Proxy protocol. Click **Next**. The User Name window appears. (See Figure 37.)

Figure 37 Account Wizard: User Name Window



Enter the user name given to you by your email provider (for example, "jsmith").

User Name: AliceSmith:alice@madhatter

Step 9 Enter the user mail server username at the prompt. If the user WebVPN gateway username and mail server username are the same, enter this name in the form:

(E-Mail Username) (E-mail Server Delimiter) [E-mail Server Name]

Where:

- E-mail Username = The user e-mail login name.
- E-mail Server Delimiter = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.
- E-mail Server Name = The name of the user e-mail server. You can omit this field if using the default mail server.

  For example: me@mycompany.com

If the user WebVPN gateway username and mail server username are different, enter both usernames in the following form:

(*WebVPN gateway Username*) (*VPN Name Delimiter*) (*E-mail Username*) (*E-mail Server Delimiter*) (*E-mail Server Name*)

Where:

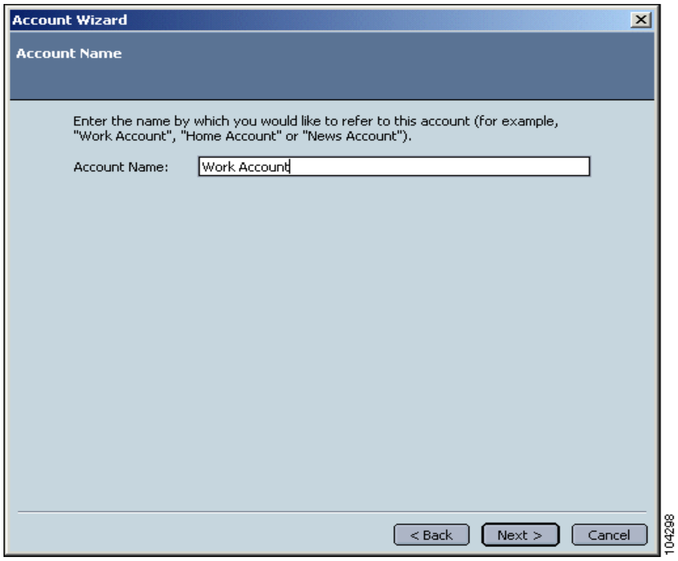
- WebVPN gateway Username = The user WebVPN gateway login name.
- VPN Name Delimiter = The delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen that separates the VPN username from the e-mail username. (The default VPN Name Delimiter is a colon.)
- E-mail Username = The name of the user e-mail account.

- E-mail Server Delimiter = The server delimiter you set on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen to separate the mail username from the server name. (The default e-mail server delimiter is the @ sign.) The delimiter is necessary only if a server name is present.
- E-mail Server Name = The name of the user e-mail server. You can omit this field if using the default mail server.

For example: myself:me@mycompany

Step 10 Click **Next**. The Account Name window appears. (See Figure 38.)

Figure 38 Account Wizard: Account Name



Account Wizard

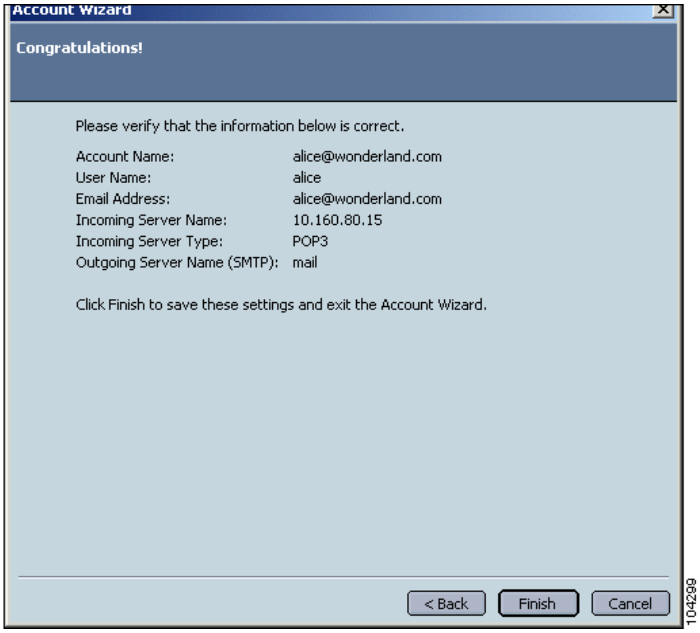
Account Name

Enter the name by which you would like to refer to this account (for example, "Work Account", "Home Account" or "News Account").

Account Name: Work Account

Step 11 Enter a name for this account. Click **Next**. The Account Wizard displays a final window. (See Figure 39.)

Figure 39 Account Wizard: Final Window



Account Wizard

Congratulations!

Please verify that the information below is correct.

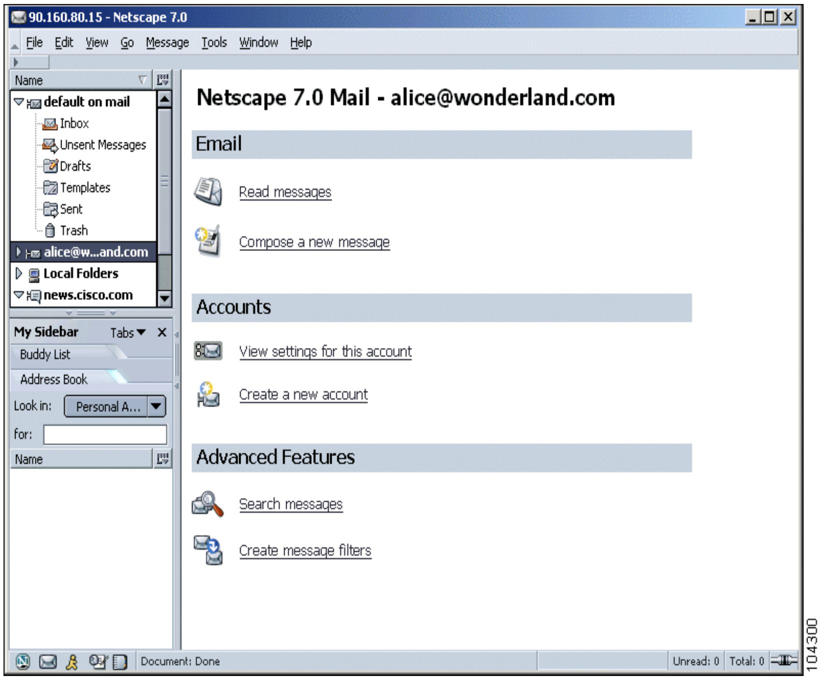
Account Name: alice@wonderland.com
User Name: alice
Email Address: alice@wonderland.com
Incoming Server Name: 10.160.80.15
Incoming Server Type: POP3
Outgoing Server Name (SMTP): mail

Click Finish to save these settings and exit the Account Wizard.

Step 12 Click **Finish**. The Account Wizard window closes.

Step 13 Click the name of the account you just created from the Name list at the left of the Netscape Mail window. (See Figure 40.) The Netscape Mail window appears. (See Figure 41.)

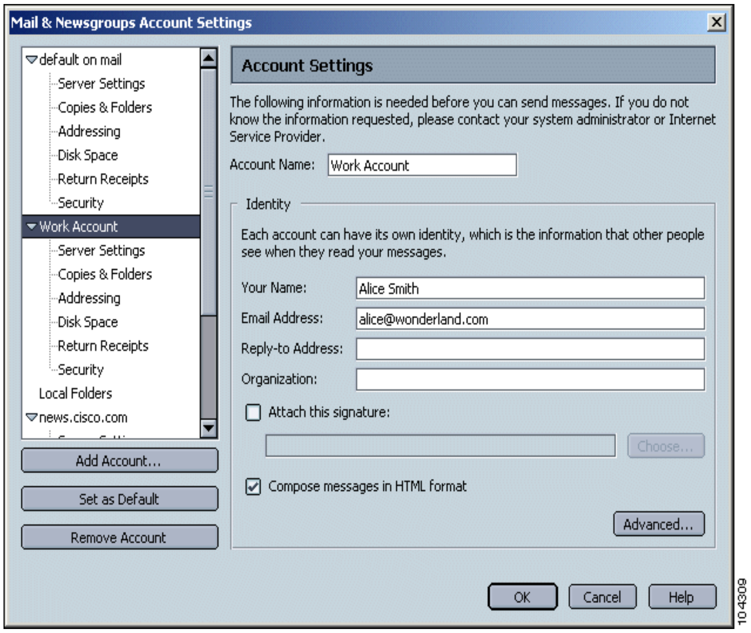
Figure 40 Netscape Mail Window



Netscape 7.0 Mail - alice@wonderland.com

Step 14 Click the **View settings for this account** link. The Account Settings window appears. (See Figure 41.)

Figure 41 Account Settings



Account Settings

The following information is needed before you can send messages. If you do not know the information requested, please contact your system administrator or Internet Service Provider.

Account Name: Work Account

Identity

Each account can have its own identity, which is the information that other people see when they read your messages.

Your Name: Alice Smith

Email Address: alice@wonderland.com

Reply-to Address:

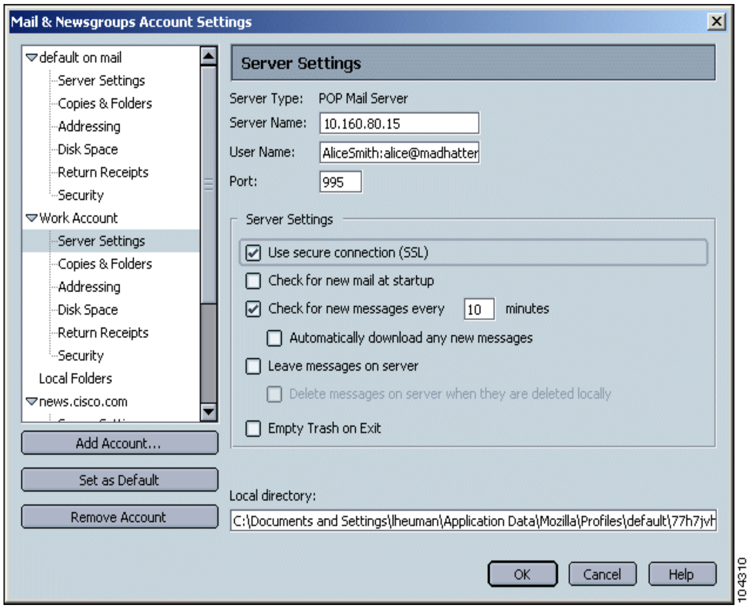
Organization:

☐ Attach this signature:

☑ Compose messages in HTML format

Step 15 Choose **Server Settings** from the list at the left of the window. The Server Settings window appears. (See Figure 42.)

Figure 42 Server Settings Window



Server Settings

Server Type: POP Mail Server

Server Name: 10.160.80.15

User Name: AliceSmith:alice@madhatter

Port: 995

Server Settings

☑ Use secure connection (SSL)

☐ Check for new mail at startup

☑ Check for new messages every 10 minutes

☐ Automatically download any new messages

☐ Leave messages on server

☐ Delete messages on server when they are deleted locally

☐ Empty Trash on Exit

Local directory:

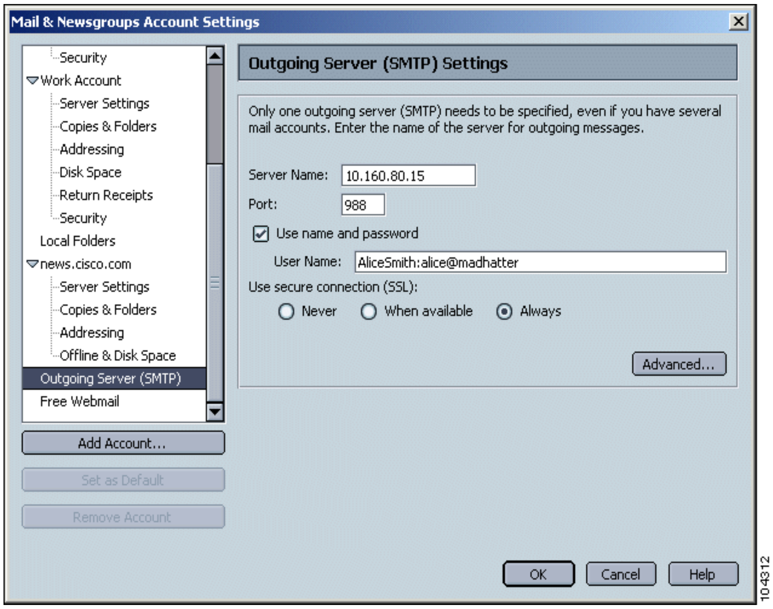
C:\Documents and Settings\heuman\Application Data\Mozilla\Profiles\default\77h7jvh

Step 16 In the Port field, enter the POP3S or IMAP4S port number you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen.

Step 17 Check the **Use Secure Connection (SSL)** check box.

Step 18 At the left side of the window, choose **Outgoing Server (SMTP)**. The Outgoing Server Settings window appears. (See Figure 43.)

Figure 43 Outgoing Server Settings Window



Outgoing Server (SMTP) Settings

Only one outgoing server (SMTP) needs to be specified, even if you have several mail accounts. Enter the name of the server for outgoing messages.

Server Name: 10.160.80.15

Port: 988

☑ Use name and password

User Name: AliceSmith:alice@madhatter

Use secure connection (SSL):

○ Never ○ When available ● Always

Step 19 In the **Server Name field**, enter the IP address of the interface of the WebVPN gateway on which you enabled the SMTP E-mail Proxy protocol.

Step 20 In the **Port field**, enter the SMTP port number you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail screen.

Step 21 Check the **Use Name and password** check box, and enter the user e-mail account name, in the same format you used in Step 9.)

Step 22 Choose **Use secure Connection (SSL): Always**.

Step 23 Click **OK**.

The configuration is complete.

Sending and Receiving E-mail

When users send or receive e-mail, Netscape prompts for a password. Enter the password, in the form:

[*WebVPN gateway Password*] [*VPN Name Delimiter*] [*E-mail Password*]

Where:

- *WebVPN gateway Password* = The user WebVPN gateway login password. If the WebVPN gateway password and the mail password are the same, you can omit this field.
- *VPN Name Delimiter* = The delimiter you configured on the WebVPN gateway Configuration | Tunneling and Security | WebVPN | E-mail that separates the VPN username from the e-mail username. (The default VPN Name Delimiter is a colon.) This delimiter is necessary only if the WebVPN gateway password is present.

- *E-mail Password* = The password for the user e-mail account.

For example, 12345:abcde.

Additional References

The following sections provide references related to WebVPN.

Related Documents

Related Topic	Document Title
Security configurations	*Cisco IOS Security Configuration Guide*, Release 12.4 http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html
Security commands	*Cisco IOS Security Command Reference*, Release 12.4T http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html
Cisco Secure Desktop	Cisco Secure Desktop Home Page http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html
Cisco SSL VPN Client	Cisco SSL VPN Client Home Page http://www.cisco.com/en/US/partner/products/ps6496/tsd_products_support_series_home.html
IANA Application Port Numbers	*Port Numbers* http://www.iana.org/assignments/port-numbers
RADIUS accounting	"Configuring RADIUS" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.4

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **aaa authentication (WebVPN)**
- **banner (WebVPN)**
- **citrix enabled**
- **clear webvpn nbns**
- **clear webvpn session**
- **clear webvpn stats**
- **csd enable**
- **debug webvpn**
- **default-group-policy**
- **filter citrix**
- **filter tunnel**
- **functions**
- **gateway (WebVPN)**
- **heading**
- **hide-url-bar**
- **hostname (WebVPN)**
- **http-redirect**
- **inservice (WebVPN)**
- **ip address (WebVPN)**
- **local-port (WebVPN)**
- **login-message**
- **logo**
- **max-users (WebVPN)**
- **nbns-list**
- **nbns-list (policy group)**
- **nbns-server**
- **policy group**
- **port-forward**
- **port-forward (policy group)**
- **secondary-color**
- **secondary-text-color**
- **show webvpn gateway**
- **show webvpn gateway**
- **show webvpn nbns**
- **show webvpn session**

- show webvpn session
- ssl encryption
- ssl encryption
- ssl truspoint
- svc address-pool
- svc default-domain
- svc dns-server
- svc dpd-interval
- svc homepage
- svc keep-client-installed
- svc msie-proxy
- svc rekey
- svc split
- svc split dns
- svc wins-server
- timeout (policy group)
- title
- title-color
- url-list
- url-list (policy group)
- url-text
- vrf-name
- webvpn aaa accounting-list
- webvpn context
- webvpn gateway
- webvpn install

aaa authentication (WebVPN)

To configure AAA authentication for SSL VPN sessions, use the **aaa authentication** command in SSLVPN configuration mode. To remove the AAA configuration from the WebVPN context configuration, use the **no** form of this command.

aaa authentication {**domain** *name* | **list** *name*}

no aaa authentication {**domain** | **list**}

Syntax Description

domain *name*	Configures authentication using the specified domain name.
list *name*	Configures authentication using the specified list name.

Command Default

If this command is not configured or if the **no** form of this command is entered, the WebVPN gateway will use global AAA parameters (if configured).

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **aaa authentication** command is entered to specify an authentication list or server group under a WebVPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the WebVPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

Examples

Local AAA Example (Default to Global Configuration)

The following example configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a context configuration.

```
Router (config)# aaa new-model
Router (config)# username USER1 secret 0 PsW2143
Router (config)# aaa authentication login default local
```

AAA Access Control Server Example

The following example configures a RADIUS server group and associates the AAA configuration under the WebVPN context configuration.

```
Router (config)# aaa new-model
Router (config)# aaa group server radius myServer
Router (config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router (config-sg-radius)# exit
Router (config)# aaa authentication login default local group myServer
Router (config)# radius-server host 10.1.1.0 auth-port 1645 acct-port 1646
Router (config)# webvpn context sslvpn
Router (config-webvpn-context)# aaa authentication list myServer
Router (config-webvpn-context)# exit
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

banner (WebVPN)

To configure a banner to be displayed after a successful login, use the **banner** command in SSLVPN group policy configuration mode. To remove the banner from the policy group configuration, use the **no** form of this command.

banner *string*

no banner

Syntax Description

string	Text string that contains 7-bit ASCII values and HTML tags and escape sequences. The text banner must be in quotation marks if it contains spaces.

Command Default

A banner is not displayed after a successful login.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures “Login Successful” to be displayed after login:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

citrix enabled

To enable Citrix application support for end users in a policy group, use the **citrix enabled** command in SSLVPN group policy configuration mode. To remove Citrix support from the policy group configuration, use the **no** form of this command.

citrix enabled

no citrix enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Citrix application support is not enabled.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Citrix support allows a citrix client to use applications running on a remote server as if they were running locally. Entering the **citrix-enabled** command configures Citrix support for the policy group.

Examples

The following example configures Citrix support under the policy group:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)#
```

Related Commands

Command	Description
filter citrix	Configures a Citrix application access filter.
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a WebVPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

clear webvpn nbns [**context** {*name* | **all**}]

Syntax Description

context	(Optional) Clears NBNS statistics for a specific context or all contexts.
name	Clears NBNS statistics for a specific context.
all	Clears NBNS statistics for all contexts.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without any keywords or arguments clears all NBNS counters on the network device.

Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

RelatedCommands

Command	Description
clear webvpn session	Clears remote users sessions on a WebVPN gateway.
clear webvpn stats	Clears application and access counters on a WebVPN gateway.

clear webvpn session

To clear WebVPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

clear webvpn session {[**user** *name*] **context** {*name* | **all**}}

Syntax Description

user *name*	(Optional) Clears session information for a specific user.
context {*name* | **all**}	Clears session information for a specific context or all contexts.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a WebVPN gateway.
clear webvpn stats	Clears application and access counters on a WebVPN gateway.

clear webvpn stats

To clear (or reset) WebVPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

clear webvpn stats [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

Syntax Description

cifs	(Optional) Clears Windows file share (CIFS) statistics.
citrix	(Optional) Clears Citrix application statistics.
mangle	(Optional) Clears URL mangling statistics.
port-forward	(Optional) Clears port forwarding statistics.
sso	(Optional) Clears statistics for Single SignOn (SSO) activities.
tunnel	(Optional) Clears SVC tunnel statistics.
context {*name* | **all**}	(Optional) Clears information for either a specific context or all contexts.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(5th)T	The **sso** keyword was added.

Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, and SVC tunnels. The counter are cleared for either the specified context or all contexts on the WebVPN gateway.

Examples

The following example clears all statistics counters for all WebVPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

Related Commands

Command	Description
clear webvpn nbns	Clears the NBNS cache on a WebVPN gateway.
clear webvpn session	Clears remote users sessions on a WebVPN gateway.

csd enable

To enable Cisco Secure Desktop (CSD) support for SSL VPN sessions, use the **csd enable** command in SSLVPN configuration mode. To remove CSD support from the WebVPN context configuration, use the **no** form of this command.

csd enable

no csd enable

Syntax Description

This command has no keywords or arguments.

Command Default

CSD support is not enabled.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The CSD software installation package must be present in a local file system, such as flash memory, and it must be cached for distribution to end users (remote PC or networking device). The **webvpn install** command is used to install the software installation package to the distribution cache.

Examples

The following example enables CSD support for SSL VPN sessions:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# csd enable
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.
webvpn install	Installs a CSD or SSL VPN client package file to a WebVPN gateway for distribution to end users.

debug webvpn

To enable the display of debug information for WebVPN applications and network activity, use the **debug webvpn** command in privileged EXEC mode. To stop debugging messages from being process and displayed, use the **no** form of this command.

debug webvpn [**aaa** | **cifs** | **citrix** | **cookie** | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | **http** | **package** | **port-forward** | **sdps** [**level** *number*] | **sock** [**flow**] | **timer** | **trie** | **tunnel** [**detail** | **traffic** *acl-number*] | **url_disp** | **webservice**]

no debug webvpn

Syntax Description

aaa	(Optional) Displays authentication, authorization, and accounting (AAA) event and error messages.
cifs	(Optional) Displays Microsoft Windows file share access event and error messages.
citrix	(Optional) Displays Citrix application event and error messages.
cookie	(Optional) Displays event and error messages that relate to the cookie that is pushed to the browser of the end user.
count	(Optional) Displays count debug messages.
csd	(Optional) Displays Cisco Secure Desktop (CSD) event and error messages.
data	(Optional) Displays data debug messages.
dns	(Optional) Displays domain name system (DNS) event and error messages.
emweb [**state**]	(Optional) Displays emweb state debug messages.
http	(Optional) Displays HTTP debug messages.
package	(Optional) Deploys event and error messages for the software packages that are pushed to the end user.
port-forward	(Optional) Displays port-forwarding event and error messages.
sdps [**level** *number*]	(Optional) Displays SDPS debug messages. The level is entered as a number from 1 to 5.
sock [**flow**]	(Optional) Displays socket debug messages.
timer	(Optional) Displays timer debug messages.
trie	(Optional) Displays trie debug messages.
tunnel [**detail** | **traffic** *acl-number*]	(Optional) Displays tunnel debug messages.
url_disp	(Optional) Displays URL debug messages.
webservice	(Optional) Displays web service event and error messages.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	Support for the WebVPN enhancements feature was added.

Usage Guidelines

This command should be used with caution on a production router or networking device. We recommend that debugging is enabled for only individual components as necessary. This restriction is intended to prevent the console session from be overwhelmed by large numbers of messages.

Examples

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

```
Router# debug webvpn

*Jan 19 03:05:22.796: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
          Data buffer(buffer: 0x0D2EF888, data: 0x1A7E756C, len: 335, offset: 0, domain:
0)
*Jan 19 03:05:22.796: SSLVPN: http request: / with domain cookie
*Jan 19 03:05:22.796: SSLVPN: [Q]Client side Chunk data written..
 buffer=0x0D2EF748 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.796: SSLVPN: Client side Chunk data written..
 buffer=0x0D2EF8A8 total_len=1167 bytes=1167 tcb=0x0C5920C8
*Jan 19 03:05:22.836: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
          Data buffer(buffer: 0x0D2EF888, data: 0x1A7E836C, len: 383, offset: 0, domain:
0)
*Jan 19 03:05:22.836: SSLVPN: http request: /paramdef.js with domain cookie
*Jan 19 03:05:22.836: SSLVPN: Created 323 byte content data to send to external client
*Jan 19 03:05:22.836: SSLVPN: Client side Chunk data written..
 buffer=0x0D2EF8A8 total_len=440 bytes=440 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
          Data buffer(buffer: 0x0D2EF888, data: 0x1A7E916C, len: 381, offset: 0, domain:
0)
*Jan 19 03:05:22.860: SSLVPN: http request: /shared.js with domain cookie
*Jan 19 03:05:22.860: SSLVPN: [Q]Client side Chunk data written..
 buffer=0x0D2EF8A8 total_len=1600 bytes=1600 tcb=0x0C5920C8
*Jan 19 03:05:22.860: SSLVPN: Client side Chunk data written..
 buffer=0x0D2EF748 total_len=986 bytes=986 tcb=0x0C5920C8
*Jan 19 03:05:22.896: SSLVPN: Entering APPL with Context: 0x0D2B1EB0,
          Data buffer(buffer: 0x0D2EF888, data: 0x1A7E9F6C, len: 384, offset: 0, domain:
0)
*Jan 19 03:05:22.896: SSLVPN: http request: /img/logo.gif with domain cookie
*Jan 19 03:05:22.896: SSLVPN: Created 552 byte content data to send to external client
*Jan 19 03:05:22.896: SSLVPN: Client side Chunk data written..
 buffer=0x0D2EF748 total_len=669 bytes=669 tcb=0x0C5920C8
```

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

```
Router# debug webvpn

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

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

The following sample output displays WebVPN cookie output during login:

```
Router# debug webvpn cookie
```

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

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

```
Router# debug webvpn cookie

*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
          buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
          cookie: 0x1A8BBFB5, length: 152
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Set-Cookie
*Jan 19 03:12:10.480: SSLVPN: Enter Cookie mangler with Context: 0x0D2B1FA0,
          buffer: 0x0D2EF728, buffer->data: 0x1A8BBF6C, buffer->len: 510,
          cookie: 0x1A8BBFC1, length: 140
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.480: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: expires
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: Sun, 17-Jan-2038
19:14:07 GMT
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: path
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: /
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: domain
*Jan 19 03:12:10.480: SSLVPN: Limited cookie parser element display: .cisco.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .cisco.com
*Jan 19 03:12:10.480: SSLVPN: Saved cookie name: PREF
*Jan 19 03:12:10.480: SSLVPN: Created internal cookie: 11@73@3315093130@3318152330
*Jan 19 03:12:10.480: SSLVPN: Saved cookie domain: .cisco.com
*Jan 19 03:12:10.484: SSLVPN: Enter Cookie unmangler with Context: 0x0D2B1EB0,
          buffer: 0x0D2EF728, buffer->data: 0x1A8BCD6C, buffer->len: 589,
          cookie: 0x1A8BCEA3, length: 276
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: Cookie
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display: PREF
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
11@73@3315093130@3318152330
*Jan 19 03:12:10.484: SSLVPN: Received internal cookie 11@73@3315093130@3318152330 is
converted to gw-index: 11, int-index: 73, time: 3315093130, rand: 3318152330
*Jan 19 03:12:10.484: SSLVPN: Limited cookie parser element display: .cisco.com
*Jan 19 03:12:10.484: SSLVPN: Cookie domain- unmangled request matched
*Jan 19 03:12:10.484: SSLVPN: Unlimited cookie parser element display:
ID=1554661243d89be2:TM=1106105034:LM=1106105034:S=CqAJHwx2xudAY1YM
*Jan 19 03:12:10.488: SSLVPN: Unlimited cookie parser element display:
CP_GUTC=128.107.163.142.1100045930344008
*Jan 19 03:12:10.488: SSLVPN: Not a mangled internal cookie - ignore
*Jan 19 03:12:10.488: SSLVPN: Limited cookie parser element display:
2154537870@11@3315093038@210936245@ssl-vpn
*Jan 19 03:12:10.488: SSLVPN: Gateway cookie 2154537870@11@3315093038@210936245@ssl-vpn is
converted to ip: 128.107.163.142, gw_index: 11, time: 3315093038, rand: 210936245,
context_name: ssl-vpn
```

The following sample output displays WebVPN HTTP during browsing:

```
Router# debug webvpn http
```

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

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

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

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

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

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

The following sample output displays WebVPN web service information:

```
Router# debug webvpn webservice

*Jan 19 03:18:39.060: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.060: SSLVPN: Created 2608 byte content data to send to external client
for requested file: /webvpn.html
*Jan 19 03:18:39.100: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:39.120: SSLVPN: Created 2459 byte content data to send to external client
for requested file: /shared.js
*Jan 19 03:18:39.152: SSLVPN: Date: Wed, 19 Jan 2005 03:18:39 GMT, Expires: Wed, 19 Jan
2005 02:18:39 GMT
*Jan 19 03:18:47.496: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:47.496: SSLVPN: Created 1375 byte content data to send to external client
for requested file: /logon.html
*Jan 19 03:18:47.516: SSLVPN: HTTP request: 0, path: /paramdef.js
*Jan 19 03:18:47.516: SSLVPN: Date: Wed, 19 Jan 2005 03:18:47 GMT, Expires: Wed, 19 Jan
2005 02:18:47 GMT
*Jan 19 03:18:48.036: SSLVPN: HTTP request: 0, path: /index.html
```

```
*Jan 19 03:18:48.036: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.036: SSLVPN: Created 8269 byte content data to send to external client
for requested file: /index.html
*Jan 19 03:18:48.220: SSLVPN: HTTP request: 0, path: /toolbarframe.html
*Jan 19 03:18:48.220: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.220: SSLVPN: Created 1312 byte content data to send to external client
for requested file: /toolbarframe.html
*Jan 19 03:18:48.256: SSLVPN: HTTP request: 0, path: /img/logo.gif
*Jan 19 03:18:48.256: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: HTTP request: 0, path: /test.html
*Jan 19 03:18:48.268: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.268: SSLVPN: Created 684 byte content data to send to external client for
requested file: /test.html
*Jan 19 03:18:48.316: SSLVPN: HTTP request: 0, path: /toolbar.html
*Jan 19 03:18:48.316: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.316: SSLVPN: Created 2618 byte content data to send to external client
for requested file: /toolbar.html
*Jan 19 03:18:48.364: SSLVPN: HTTP request: 0, path: /tools.html
*Jan 19 03:18:48.364: SSLVPN: Date: Wed, 19 Jan 2005 03:18:48 GMT, Expires: Wed, 19 Jan
2005 02:18:48 GMT
*Jan 19 03:18:48.364: SSLVPN: Created 2284 byte content data to send to external client
for requested file: /tools.html
```

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

default-group-policy

To associate a group policy with a WebVPN context configuration, use the **default-group-policy** command in SSLVPN configuration mode. To remove the group policy from the WebVPN context configuration, use the **no** form of this command.

default-group-policy *name*

no default-group-policy

Syntax Description

name	Name of the policy configured with the **policy group** command.

Command Default

A group policy is not associated with a WebVPN context configuration.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **policy group** command is first configured to define policy group configuration parameters. This command is configured to attach the policy group to the WebVPN context when multiple group policies are defined under the context. This policy will be used as default unless an authentication, authorization, and accounting (AAA) server pushes an attribute that specifically requests another group policy.

Examples

The following example configures policy group ONE as the default group policy:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy-group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# policy-group TWO
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
Router(config-webvpn-context)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

filter citrix

To configure a Citrix application access filter, use the **filter citrix** command in SSLVPN group policy configuration mode. To remove the access filter from the policy group configuration, use the **no** form of this command.

filter citrix *extended-acl*

no filter citrix *extended-acl*

Syntax Description

extended-acl	Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered.

Command Default

A Citrix application access filter is not configured.

Command Modes

SSLVPN Group Policy Configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Citrix application support is enabled under the policy group by configuring the **citrix enabled** command. User access to Citrix applications is configured with the **filter citrix** command. An extended access list is configured to define the filter.

Examples

The following example configures Citrix support for end users that have a source address in the 192.168.1.0/24 network:

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)# filter citrix 100
Router(config-webvpn-group)#
```

Related Commands

Command	Description
citrix enabled	Enables Citrix support under a policy group.
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

filter tunnel

To configure a WebVPN tunnel access filter, use the **filter tunnel** command in SSLVPN group policy configuration mode. To remove the tunnel access filter, use the **no** form of this command.

filter tunnel *extended-acl*

no filter tunnel *extended-acl*

Syntax Description

extended-acl	Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered.

Command Default

A WebVPN tunnel access filter is not configured.

Command Modes

SSLVPN Group Policy Configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The tunnel access filter is used to control network- and application-level access.

Examples

The following example configures a deny access filter for any host from the 172.16.2/24 network:

```
Router(config)# access-list 101 deny ip 172.16.2.0 0.0.0.255 any
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# filter tunnel 101
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

functions

To enable a file access function or tunnel mode support in a group policy configuration, use the **functions** command in SSLVPN group policy configuration mode. To remove file access or tunnel support from the group policy configuration, use the **no** form of this command.

functions {**file-access** | **file-browse** | **file-entry** | **httpauth-disabled** | **svc-enabled** | **svc-required**}

no functions {**file-access** | **file-browse** | **file-entry** | **httpauth-disabled** | **svc-enabled** | **svc-required**}

Syntax Description

file-access	Enables network file-share access. File servers in the server list are listed on the SSL VPN home page if this keyword is enabled.
file-browse	Enables browse permissions for server and file shares. The file-access function must be enabled to also use this function.
file-entry	Enables “modify” permissions for files in the shares listed on the SSL VPN home page.
httpauth-disabled	Disables NT LAN Manager (NTLM) authentication. To reinstate NTLM authentication, use the **no** form of the **functions** command with the **httpauth-disabled** keyword.
svc-enabled	Enables tunnel support for the user. Allows the user of the group to use tunnel mode. If the SVC software package fails to install on the PC of the end user, the end user can continue to use clientless mode or thin-client mode.
svc-required	Enables only tunnel support for the user. If the SVC software package fails to install on the PC of the end user, the other access modes cannot be used.

Command Default

File access function or tunnel mode support is not enabled.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **httpauth-disabled** keyword was added.

Usage Guidelines

The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or later must be installed before Cisco Secure Desktop (CSD) or SVC client packages can be installed.

Examples

The following example enables file share access with server-browse and file-modify permission:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions file-access
Router(config-webvpn-group)# functions file-browse
Router(config-webvpn-group)# functions file-entry
```

The following example disables NTLM authentication:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions httpauth-disabled
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

gateway (WebVPN)

To associate a WebVPN gateway with a WebVPN context, use the **gateway** command in SSLVPN configuration mode. To remove the gateway from the WebVPN context configuration, use the **no** form of this command.

gateway *name* [**domain** *name* | **virtual-host** *name*]

no gateway *name*

Syntax Description

domain *name*	(Optional) Maps SSL VPN sessions to the specified domain name (for example, “https://gw-address/domain”).
virtual-host *name*	(Optional) Maps SSL VPN sessions to the specified virtual host.

Command Default

A WebVPN gateway is not associated with a WebVPN context.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to attach a WebVPN gateway to a WebVPN context configuration.

A virtual host name is specified when multiple virtual hosts are mapped to the same IP address on the WebVPN gateway (similar to a canonical domain name). The virtual host name differentiates the host request on the gateway. The host header in the HTTP message is modified to direct traffic to the virtual host.

Examples

The following example configures the gateway and then attaches the WebVPN context:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# ip address 10.1.1.1
Router(config-webvpn-gateway)# inservice
Router(config-webvpn-gateway)# exit
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# gateway GW_1 domain cisco.com
Router(config-webvpn-context)# inservice
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.
webvpn gateway	Enters SSL VPN gateway configuration mode to configure a WebVPN gateway.

heading

To configure the heading that is displayed above URLs listed on the portal page of an SSL VPN, use the **heading** command in SSLVPN URL list configuration mode. To remove the heading, use the **no** form of this command.

heading *text-string*

no heading

Syntax Description

text-string	The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces.

Command Default

A heading is not configured.

Command Modes

SSLVPN URL list configuration

Command History

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

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading “Quick Links”
Router(config-webvpn-url)#
```

Related Commands

Command	Description
url-list	Enters SSLVPN URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSLVPN.

hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the **hide-url-bar** command in SSLVPN group policy configuration mode. To display the URL bar on the portal page, use the **no** form of this command.

hide-url-bar

no hide-url-bar

Syntax Description

This command has no arguments or keywords.

Command Default

The URL bar is displayed on the SSL VPN portal page.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies only to clientless mode access.

Examples

The following example hides the URL bar on the SSL VPN portal page:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

hostname (WebVPN)

To configure the hostname for a WebVPN gateway, use the **hostname** command in SSLVPN gateway configuration mode. To remove the hostname from the WebVPN gateway configuration, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Specifies the hostname.

Command Default

The hostname is not configured.

Command Modes

SSLVPN Gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple WebVPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

Examples

The following example configures a hostname for a WebVPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the **http-redirect** command in SSLVPN Gateway configuration mode. To remove the HTTPS configuration from the WebVPN gateway, use the **no** form of this command.

http-redirect [**port** *number*]

no http-redirect

Syntax Description

port *number*	(Optional) Specifies a port number. The value for this argument is a number from 1 to 65535.

Command Default

The following default value is used if this command is configured without entering the **port** keyword:

port *number* : 80

Command Modes

SSLVPN Gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When this command is enabled, the HTTP port is opened and the WebVPN gateway listens for HTTP connections. HTTP connections are redirected to use secure HTTP (HTTPS). Entering the **port** keyword and *number* argument configures the gateway to listen for HTTP traffic on the specified port. Entering the **no** form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

Examples

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# http-redirect
```

Related Commands

Command	Description
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

inservice (WebVPN)

To enable a WebVPN gateway or context process, use the **inservice** command in SSLVPN gateway configuration or SSLVPN configuration mode. To disable a WebVPN gateway or context process without removing the configuration from the router configuration file, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Command Default

A WebVPN gateway or context process is not enabled.

Command Modes

SSLVPN gateway configuration
SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the WebVPN gateway or context process. The gateway and context processes must both be “inservice” to enable WebVPN.

Examples

The following example enables the WebVPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# inservice
router(config-webvpn-gateway)#
```

The following example configures and activates the WebVPN context configuration:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# inservice
router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

ip address (WebVPN)

To configure a proxy IP address on a WebVPN gateway, use the **ip address** command in SSLVPN Gateway configuration mode. To remove the proxy IP address from the WebVPN gateway, use the **no** form of this command.

ip address *number* [**port** *number*] [**secondary**]

no ip address

Syntax Description

number	IPv4 address.
port *number*	(Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument.
secondary	(Optional) Configures the gateway using a secondary IP address.

Command Default

The following default value is used if this command is configured without entering the **port** keyword:

port *number* : 443

Command Modes

SSLVPN Gateway configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **ip address** command is used to configure a proxy IP address for a WebVPN gateway. The IP address is the termination point for all WebVPN client connections. This IP address can be any routable IP address assigned to a valid interface.

A secondary IP address is configured if an external device performs load-balancing functions.

A secondary address must be configured if the proxy IP address is not on a directly connected network.

Note A secondary IP address will not respond to Area Response Protocol (ARP) or Internet Control Message Protocol (ICMP) requests.

Examples

The following example configures 192.168.1.1 as a proxy address on a WebVPN gateway. Proxy traffic is directed over port 443.

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 192.168.1.1 port 443
```

Related Commands

Command	Description
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the **local-port** command in SSLVPN port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the **no** form of this command.

local-port {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}

no local-port {*number*}

Syntax Description

number	Configures the port number to which the local application is mapped. A number from 1 through 65535 is entered.
remote-server *name*	Identifies the remote server. An IPv4 address or fully qualified domain name is entered.
remote-port *number*	Specifies the well-known port number of the application, for which port-forwarding is to be configured. A number from 1 through 65535 is entered.
description *text-string*	Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered.

Command Default

An application port number is not remapped.

Command Modes

SSLVPN port-forward list configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **local-port** command is configured to add an entry to the port-forwarding list. The forward list is created with the **port-forward** command in SSLVPN configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

Related Commands

Command	Description
port-forward	Enters SSLVPN port-forward list configuration mode to configure a port forwarding list.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

login-message

To configure a login message for the text box on the user login page, use the **login-message** command in SSLVPN configuration mode. To reconfigure the WebVPN context configuration to display the default message, use the **no** form of this command.

login-message [*message-string*]

no login-message [*message-string*]

Syntax Description

message-string	(Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences.

Defaults

The following message is displayed if this command is not configured or if the **no** form is entered:

"Please enter your username and password"

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The **no** form of this command is entered to configure the default message to be displayed. When the **login-message** command is entered without the optional text string, no login message is displayed.

Examples

The following example changes the default login message to "Please enter your login credentials":

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

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

logo

To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the **logo** command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the **no** form of this command.

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

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

Syntax Description

file *filename*	(Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length.
none	(Optional) No logo is displayed.

Defaults

The Cisco logo is displayed if the **no** form of this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

Examples

The following example references mylogo.gif (from flash memory) to use as the SSL VPN logo:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo file flash:/mylogo.gif
Router(config-webvpn-context)#
```

In the following example, no logo is to be displayed on the login or portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

max-users (WebVPN)

To limit the number of connections to an SSL VPN that will be permitted, use the **max-users** command in SSLVPN configuration mode. To remove the connection limit from the WebVPN context configuration, use the **no** form of this command.

max-users *number*

no max-users

Syntax Description

number	Maximum number of SSL VPN user connections. A number from 1 to 1000 can be entered for this argument.

Command Default

The following is the default if this command is not configured or if the **no** form is entered:

number : 1000

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a limit of 500 user connections that will be accepted by the SSL VPN:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# max-users 500
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

nbns-list

To enter the SSLVPN NBNS list configuration mode to configure a NetBIOS Name Service (NBNS) server list for Common Internet File System (CIFS) name resolution, use the **nbns-list** command in SSLVPN configuration mode. To remove the NBNS server list from the WebVPN context configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list *name*

Syntax Description

name	Name of the NBNS list. The name can be up to 64 characters in length. This argument is case sensitive.

Command Default

SSLVPN NBNS list configuration mode is not entered, and a NBNS server list cannot be configured.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The NBNS server list is used to configure a list of Windows Internet Name Service (WINS) to resolve Microsoft file-directory shares. Entering the **nbns-list** command places the router in SSLVPN NBNS list configuration mode. You can specify up to three NetBIOS name servers. A single server is configured as the master browser if multiple servers are specified in the server list.

Note NBNS and CIFS resolution is supported only on Microsoft Windows 2000 or Linux Samba servers.

Examples

The following example configures an NBNS server list:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)#
```

Related Commands

Command	Description
nbns-server	Adds a server to an NBNS server list.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

nbns-list (policy group)

To attach a NetBIOS name service (NBNS) server list to a policy group configuration, use the **nbns-list** command in SSLVPN group policy configuration mode. To remove the NBNS server list from the policy group configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list

Syntax Description

name	Name of the NBNS server list configured in SSLVPN configuration mode.

Command Default

An NBNS server list is not attached to a policy group configuration.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

Examples

The following example applies the NBNS server list to the policy group configuration:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)#
```

Related Commands

Command	Description
nbns-list	Enters SSLVPN NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
nbns-server	Adds a server to an NBNS server list.
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

nbns-server

To add a server to a NetBIOS name service (NBNS) server list, use the **nbns-server** command in SSLVPN NBNS list configuration mode. To remove the server entry from the NBNS server list, use the **no** form of this command.

nbns-server *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

no nbns-server *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

Syntax Description

ip-address	The IPv4 address of the NetBIOS server.
master	(Optional) Configures a single NetBIOS server as the master browser.
timeout *seconds*	(Optional) Configures the length of time, in seconds, that the networking device will wait for a query reply before sending a query to another NetBIOS server. A number from 1 through 30 can be configured for this argument.
retries *number*	(Optional) Number of times that the specified NetBIOS server will be queried. A number from 0 through 10 can be configured for this argument. Entering the number 0 configures the networking device not to resend a query.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

timeout 2
retries 2

Command Modes

SSLVPN NBNS list configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The server specified with the *ip-address* argument can be a primary domain controller (PDC) in a Microsoft network. A Windows Internet Naming Service (WINS) server cannot and should not be specified. When multiple NBNS servers are specified, a single server is configured as master browser.

Examples

The following example adds three servers to an NBNS server list:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)#
```

Related Commands

Command	Description
nbns-list	Enters SSLVPN NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

policy group

To enter SSLVPN group policy configuration mode to configure a group policy, use the **policy group** command in SSLVPN configuration mode. To remove the group policy from the router configuration file, use the **no** form of this command.

policy group *name*

no policy group *name*

Syntax Description

name	Name of the group policy.

Command Default

SSLVPN group policy configuration mode is not entered, and a group policy is not configured.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of end users. Entering the **policy group** command places the router in SSLVPN group policy configuration mode. After the group policy is configured, the group policy is attached to the WebVPN context configuration by configuring the **default-group-policy** command.

Examples

The following example configures a policy group named ONE:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
Router(config-webvpn-context)#
```

Related Commands

Command	Description
banner	Configures a banner to be displayed after a successful login.
citrix enabled	Enables Citrix application support for end users in a policy group.
default-group-policy	Configures a default group policy for SSL VPN sessions.
filter citrix	Configures a Citrix application access filter.
filter tunnel	Configures a WebVPN tunnel access filter.

Command	Description
functions	Enables a file access function or tunnel mode support in a group policy configuration.
hide-url-bar	Prevents the URL bar from being displayed on the SSL VPN portal page.
nbns-list (policy group)	Attaches a NBNS server list to a policy group configuration.
port-forward (policy group)	Attaches a port-forwarding list to a policy group configuration.
svc address-pool	Configures a pool of IP addresses to assign to end users in a policy group.
svc default-domain	Configures the domain for a policy group.
svc dns-server	Configures DNS servers for policy group end users.
svc dpd-interval	Configures the DPD timer value for the gateway or client.
svc homepage	Configures the URL of the web page that is displayed upon successful user login.
svc keep-client-installed	Configures the end user to keep SVC software installed when the SSL VPN connection is not enabled.
svc msie-proxy	Configures MSIE browser proxy settings for policy group end users.
svc msie-proxy server	Specifies a Microsoft Internet Explorer proxy server for policy group end users.
svc rekey	Configures the time and method that a tunnel key is refreshed for policy group end users.
svc split	Configures split tunneling for policy group end users.
svc wins-server	Configures configure WINS servers for policy group end users.
timeout	Configures the length of time that an end user session can remain idle or the total length of time that the session can remain connected.
url-list (policy group)	Attaches a URL list to policy group configuration.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

port-forward

To enter SSLVPN port-forward list configuration mode to configure a port forwarding list, use the **port-forward** command in SSLVPN configuration mode. To remove the port-forwarding list from the WebVPN context configuration, use the **no** form of this command.

port-forward *name*

no port-forward *name*

Syntax Description

name	Name of the port-forwarding list.

Command Default

SSLVPN port-forward list configuration mode is not entered, and a port forwarding list is not configured.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

The **port-forward** command is used to create the port-forwarding list. Application port number mapping (port forwarding) is configured with the local-port command in SSLVPN port-forward configuration mode.

A port-forwarding list is configured for thin client mode WebVPN. Port forwarding extends the cryptographic functions of the SSL protected browser to provide remote access to TCP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the WebVPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the WebVPN session.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

port-forward (policy group)

To attach a port-forwarding list to a policy group configuration, use the **port-forward** command in SSLVPN group policy configuration mode. To remove the port-forwarding list from the policy group configuration, use the **no** form of this command.

port-forward *name* [**auto-download**]

no port-forward *name* [**auto-download**]

Syntax Description

name	Name of the port-forwarding list configured in SSLVPN configuration mode.
auto-download	(Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website.

Command Default

A port-forwarding list is not attached to a policy group configuration.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	The **auto-download** keyword was added.

Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

Examples

The following example applies the port-forwarding list to the policy group configuration:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
Router(config-webvpn-port-fwd)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# port-forward EMAIL auto-download
Router(config-webvpn-group)#
```

Related Commands

Command	Description
local-port (WebVPN)	Remaps an application port number in a port-forwarding list.
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
port-forward	Enters SSLVPN port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

secondary-color

To configure the color of the secondary title bars on the login and portal pages of a SSLVPN, use the **secondary-color** command in SSLVPN configuration mode. To remove the color from the WebVPN context configuration, use the **no** form of this command.

secondary-color *color*

no secondary-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default color is purple.

Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

Configuring a new color overrides the color of the preexisting color.

Examples

The following examples show the three forms in which the secondary color is configured:

```
Router(config-webvpn-context)# secondary-color darkseagreen
Router(config-webvpn-context)# secondary-color #8FBC8F
Router(config-webvpn-context)# secondary-color 143,188,143
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

secondary-text-color

To configure the color of the text on the secondary bars of an SSL VPN, use the **secondary-text-color** command in SSLVPN configuration mode. To revert to the default color, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

The color of the text on secondary bars is black if this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

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

Examples

The following example sets the secondary text color to white:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# secondary-text-color white
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

show webvpn context

To display the operational status and configuration parameters for SSL VPN context configurations, use the **show webvpn context** command in privileged EXEC mode.

show webvpn context [*name*]

Syntax Description

name	(Optional) Filters the output to display more detailed information about the named context.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without specifying a context name displays general information about the operational status of all SSL VPN contexts. Entering a context name displays more detailed information, such as the operational status and specific configuration information for the named context.

Examples

The following is sample output from the **show webvpn context** command:

```
Router# show webvpn context SSLVPN

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host

Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

Table 1 describes the significant fields shown in the display.

Table 7 show webvpn context Field Descriptions

Field	Description
Context Name	Displays the name of the context.
Gateway	Displays the name of the associated gateway. n/a is displayed if no gateway is associated.
Domain/VHost	Displays the SSL VPN domain or virtual host name.

Table 7 show webvpn context Field Descriptions (continued)

Field	Description
VRF	Displays the Virtual Private Network (VPN) routing and forwarding (VRF) —if configured—that is associated with the context configuration.
AS	Displays the administrative status of the SSL VPN context. The status is displayed as “up” or “down.”
OS	Displays the operational status of the SSL VPN context. The status is displayed as “up” or “down.”

The following is sample output from the **show webvpn context** command, entered with the name of a specific SSL VPN context:

```
Router# show webvpn context SSLVPN

Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: PG_1
Associated WebVPN Gateway: GW_1
Domain Name: DOMAIN_ONE
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

Table 2 describes the significant fields shown in the display.

Table 8 show webvpn context (Specific WebVPN Context) Field Descriptions

Field	Description
Admin Status	Administrative status of the context. The status is displayed as “up” or “down.” The **inservice** command is used to configure this configuration parameter.
Operation Status	Displays the operational status of the SSL VPN. The status is displayed as “up” or “down.” The context and the associated gateway must both be in an enabled state for the operational status to be “up.”
CSD Status	Displays the status of Cisco Secure Desktop (CSD). The status is displayed as “Enabled” or “Disabled.”
Certificate authentication type	Displays the CA type.
AAA Authentication List...	Displays the authentication list if configured.
AAA Authentication Domain...	Displays the AAA domain if configured.
Default Group Policy	Name of the group policy configured under the named context.
Domain Name	Domain name or virtual host name configured under the named context.

Table 8 show webvpn context (Specific WebVPN Context) Field Descriptions (continued)

Field	Description
Maximum Users Allowed	Displays the maximum number of user sessions that can be configured
NAT Address...	Displays the Network Address Translation (NAT) address if configured.
VRF	Displays the Virtual Private Network (VPN) routing and forwarding (VRF)—if configured—that is associated with the context configuration.

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

show webvpn gateway

To display the status of a WebVPN gateway, use the **show webvpn gateway** command in EXEC mode.

show webvpn gateway [*name*]

Syntax Description

name	(Optional) Filters the output to display more detailed information about the named gateway.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without specifying a gateway name, displays general the operational status of all WebVPN gateways. Entering a gateway name displays the IP address and CA trustpoint.

Examples

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                      Admin  Operation
------------                      -----  ---------
GW_1                              up     up
GW_2                              down   down
```

Table 1 describes the significant fields shown in the display.

Table 9 show webvpn gateway Field Descriptions

Field	Description
Gateway Name	Name of the gateway.
Admin	The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command.
Operation	The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state.

The following is sample output from the **show webvpn gateway** command, entered with a specific WebVPN gateway name:

```
Router# show webvpn gateway GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

Table 2 describes the significant fields shown in the display.

Table 10 show webvpn gateway name Field Descriptions

Field	Description
Admin Status	The administrative status of the gateway, displayed as "up" or "down." Administrative status is configured with the **inservice** command.
Operation Status	The operational status of the gateway, displayed as "up" or "down." The gateway must be "inservice" and configured with a valid IP address to be in an "up" state.
IP: ... port: ...	The configured IP address and port number of the WebVPN gateway. The default port number 443.
SSL Trustpoint:	Configures the CA certificate trust point.

Related Commands

Command	Description
webvpn gateway	Enters SSL VPN gateway configuration mode to configure a WebVPN gateway.

show webvpn nbns

To display information in the NetBIOS Name Service (NBNS) cache, use the **show webvpn nbns** command.

show webvpn nbns {**context** {**all** | *name*}}

Syntax Description

context *name*	Filters the output to display NBNS information for the named context.
context all	Displays NBNS information for all contexts.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about NBNS cache entries. The NetBIOS name, IP address of the Windows Internet Name Service (WINS) server, and associated time stamps.

Examples

The following is sample output from the **show webvpn nbns** command, entered with the **context** and **all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

Table 11 describes the significant fields shown in the display.

Table 11 show webvpn nbns context all Field Descriptions

Field	Description
NetBIOS name	NetBIOS name.
IP Address	The IP address of the WINs server.

Table 11 show webvpn nbns context all Field Descriptions (continued)

Field	Description
Timestamp	Time stamp for the last entry.
... total entries	Total number of NetBIOS cache entries.

Related Commands

Command	Description
nbns-list	Enters SSLVPN NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn install	Installs a CSD or SVC package file to a WebVPN gateway for distribution to end users.

show webvpn policy

To display the context configuration associated with a policy group, use the **show webvpn policy** command in privileged EXEC mode.

show webvpn policy {**group** *name* **context** {**all** | *name*}}

Syntax Description

group *name*	Displays information for the named policy group.
context all	Displays information for all context configurations with which the policy group is associated.
context *name*	Displays information for the named context configuration.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display configuration settings that apply only to the policy group. This command can also be used to display all contexts for which the policy group is configured.

Examples

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group ONE context all

WEBVPN: group policy = ONE ; context = SSLVPN
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
WEBVPN: group policy = ONE ; context = SSLVPN_TWO
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

The following output example displays information about a SSO server configured for a policy group of the SSL VPN context:

```
Router# show webvpn policy group ONE context all

WV: group policy = sso ; context = test_sso
  idle timeout = 2100 sec
  session timeout = 43200 sec
  citrix disabled
  dpd client timeout = 300 sec
  dpd gateway timeout = 300 sec
  keep sslvpn client installed = disabled
  rekey interval = 3600 sec
  rekey method =
  lease duration = 43200 sec
```

Table 1 describes the significant fields shown in the display.

Table 12 show webvpn policy Field Descriptions

Field	Description
group policy	Name of the policy group.
context	Name of the SSL VPN context.
idle timeout	Length of time that an remote-user session can remain idle.
session timeout	Length of time that a remote-user session can remain active.
citrix	Support for Citrix applications, shown as “disabled” or “enabled.”
dpd client timeout	Length of time that a session will be maintained with a nonresponsive end user (remote client).
dpd gateway timeout	Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway.
keep sslvpn client installed	SVC software installation policy on the end user (remote PC). “enabled” indicates that SVC client software remains installed after the SSL VPN session is terminated. “disabled” indicates that SVC software is pushed to the end user each time a connection is established.
rekey interval	Length of time between tunnel key refresh cycles.
rekey method	Tunnel key authentication method.
lease duration	Tunnel key lifetime.

Related Commands

Command	Description
policy group	Enters SSL VPN group policy configuration mode to configure a group policy.

show webvpn session

To display WebVPN user session information, use the **show webvpn session** command in EXEC mode.

show webvpn session {[**user** *name*] **context** {**all** | *name*}}

Syntax Description

user *name*	(Optional) Displays detailed information about the named user session.
context all	Displays a list of active users sessions for all locally configured contexts.
context *name*	Displays a list of active users for only the named context.

Command Default

Session information is not displayed.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to list active Secure Sockets Layer (SSL) Virtual Private Network (VPN) connections or to display context configuration policies that apply to the specified end user.

Examples

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context SSLVPN

WebVPN context name: SSLVPN
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.2.1.220                 2         04:47:16  00:01:26
user2              10.2.1.221                 2         04:48:36  00:01:56
```

Table 1 describes the significant fields shown in the display.

Table 13 show webvpn session Field Descriptions

Field	Description
WebVPN context name	Name of the context.
Client_Login_Name	Login name for the end user (remote PC or device).
Client_IP_Address	IP address of the remote user.
No_of_Connections	Number of times the remote user has connected.

Table 13 show webvpn session Field Descriptions (continued)

Field	Description
Created	Time, in hh:mm:ss, when the remote connection was established.
Last_Used	Time, in hh:mm:ss, that the user connection last generated network activity.

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

WebVPN user name = user1 ; IP address = 10.2.1.220; context = SSLVPN
    No of connections: 0
    Created 00:00:19, Last-used 00:00:18
    CSD enabled
    CSD Session Policy
       CSD Web Browsing Allowed
       CSD Port Forwarding Allowed
       CSD Full Tunneling Disabled
       CSD FILE Access Allowed
    User Policy Parameters
      Group name = ONE
    Group Policy Parameters
      url list name = "Cisco"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "EMAIL"
      tunnel mode = disabled
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep stc installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 3600 sec
```

Table 2 describes the significant fields shown in the display.

Table 14 show webvpn session Field Descriptions

Field	Description
WebVPN user name	Name of the end user.
IP address	IP address of the end user.
context	Name of the context to which user policies apply.
No of connections	Number of times the remote user has connected.
Created	Time, in hh:mm:ss, when the remote connection was established.
Last-used	Time, in hh:mm:ss, that the user connection last generated network activity.
CSD enabled	Status of Cisco Secure Desktop (CSD).

Table 14 show webvpn session Field Descriptions (continued)

Field	Description
CSD Session Policy	CSD policy configuration parameters. The parameters are each displayed as “Allowed” or “Disabled.”
CSD Web Browsing	Status of Web Internet access through the SSL VPN.
CSD Port Forwarding	Status of application port forwarding.
CSD Full Tunneling	Status of CSD full-tunnel support.
CSD FILE Access	Status of CSD network share and file access.
User Policy Parameters	User policy configuration parameters.
Group name	Name of the policy group to which the user belongs.
Group Policy Parameters	Policy group configuration parameters. The parameters are displayed as default and administrator-defined values.
url list name	Name of the URL list configured with the **url-list** command.
idle timeout	Length of time that a remote-user session can remain idle.
session timeout	Length of time that a remote-user session can remain active.
port forward name	Name of the port-forwarding list configured with the **port-forward (policy group)** command.
tunnel mode	Tunnel mode of the remote-user session.
citrix...	Citrix support for the remote user.
dpd client timeout	Length of time that a session will be maintained with a nonresponsive end user (remote client).
dpd gateway timeout	Length of the time that a session will be maintained with a nonresponsive WebVPN gateway.
keep stc installed	SSL VPN Client (SVC) software installation policy on the end user (remote PC). “enabled” indicates that SVC client software remains installed after the SSL VPN session is terminated. “disabled” indicates that SVC software is pushed to the end user each time a connection is established.
rekey interval	Length of time between tunnel key refresh cycles.
rekey method	Tunnel key authentication method.
lease duration	Tunnel key lifetime.

show webvpn stats

To display SSL VPN application and network statistics, use the **show webvpn stats** command in privileged EXEC mode.

show webvpn stats [**cifs** | **citrix** | **mangle** | **port-forward** | **tunnel**] [**detail**] [**context** {**all** | *name*}]

Syntax Description

cifs	(Optional) Displays Windows file share (CIFS) statistics.
citrix	(Optional) Displays Citrix application statistics.
mangle	(Optional) Displays URL mangling statistics.
port-forward	(Optional) Displays port forwarding statistics.
tunnel	(Optional) Displays VPN tunnel statistics.
detail	(Optional) Displays detailed information.
context {**all** | *name*}	(Optional) Displays information for a specific context or all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display SSL VPN application, authentication, and network statistics and counters.

Examples

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context SSLVPN

WebVPN context name : SSLVPN
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
    CEF switched packets - client: 0         , server: 0
    CEF punted packets - client: 0         , server: 0

Mangling statistics:
    Relative urls            : 0          Absolute urls            : 0
    Non-http(s) absolute urls: 0          Non-standard path urls   : 0
    Interesting tags         : 0          Uninteresting tags       : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles            : 0
    HTML comments            : 0          HTTP/1.0 requests        : 0
    HTTP/1.1 requests        : 0          Unknown HTTP version     : 0
    GET requests             : 0          POST requests            : 0
    CONNECT requests         : 0          Other request methods    : 0
    Through requests         : 0          Gateway requests         : 0
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 0          Processed req body bytes : 0
    HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
    HTML responses           : 0          CSS responses            : 0
    XML responses            : 0          JS responses             : 0
    Other content type resp  : 0          Chunked encoding resp    : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0

CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies             : 0
    NB DGM Requests          : 0          NB DGM Replies           : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  HTTP related Per Context:
    Requests                 : 0          Request Bytes RX         : 0
    Request Packets RX       : 0          Response Bytes TX        : 0
    Response Packets TX      : 0          Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0

Socket statistics:
    Sockets in use           : 0          Sock Usr Blocks in use   : 0
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 0          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 0          Sock Tx Unblocked        : 0
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 0
    Sock Select Timeout Errs : 0

Port Forward statistics:
    Connections serviced     : 0          Server Aborts (idle)     : 0
  Client                                Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0

WEBVPN Citrix statistics:
Connections serviced : 0

               Server                   Client
  Packets in  : 0                        0
  Packets out : 0                        0
  Bytes in    : 0                        0
  Bytes out   : 0                        0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
    SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
    SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
    DPD timeout              : 0
  Client                                Server
    in  CSTP frames          : 0          out IP pkts              : 0
    in  CSTP data            : 0          out stitched pkts        : 0
    in  CSTP control         : 0          out copied pkts          : 0
    in  CSTP Addr Reqs       : 0          out bad pkts             : 0
    in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
    in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
    in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
    in  CSTP bytes           : 0          out IP bytes             : 0
    out CSTP frames          : 0          in  IP pkts              : 0
    out CSTP data            : 0          in  invalid pkts         : 0
    out CSTP control         : 0          in  congested pkts       : 0
    out CSTP Addr Resps      : 0          in  bad pkts             : 0
    out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
    out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
    out CSTP Msg Reqs        : 0
    out CSTP bytes           : 0          in  IP bytes             : 0
```

The descriptions in the displays are self-explanatory.

Related Commands

Command	Description
clear webvpn stats	Clears application and access counters on a SSL VPN gateway.

ssl encryption

To specify the encryption algorithm that the Secure Sockets Layer (SSL) protocol uses for SSL Virtual Private Network (SSL VPN) connections, use the **ssl encryption** command in SSLVPN gateway configuration mode. To remove an algorithm from the WebVPN gateway, use the **no** form of this command.

ssl encryption [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]

no ssl encryption

Syntax Description

3des-sha1	(Optional) Configures the 3 DES-SHA1 encryption algorithm.
aes-sha1	(Optional) Configures the AES-SHA1 encryption algorithm.
rc4-md5	(Optional) Configures the RC4-MD5 encryption algorithm.

Defaults

All algorithms are available in the order shown above.

Command Modes

SSLVPN Gateway configuration

Command History

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

Usage Guidelines

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Configuring this command allows you to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

Examples

The following example configures the gateway to use, in order, the 3DES-SHA1, AES-SHA1, or RC4-MD5 encryption algorithms for SSL connections:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl encryption rc4-md5
Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

ssl truspoint

To configure the certificate trustpoint on a WebVPN gateway, use the **ssl trustpoint** command in SSLVPN gateway configuration mode. To remove the trustpoint association, use the **no** form of this command.

ssl trustpoint *name*

no ssl trustpoint

Syntax Description

name	Name of the trust point.

Defaults

This command has no default behavior or values.

Command Modes

SSLVPN gateway configuration

Command History

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

Usage Guidelines

You can configure a persistent self-signed certificate or an external CA server to generate a valid trustpoint.

Examples

The following example configures a trustpoint named CA_CERT:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl trustpoint CA_CERT
Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a WebVPN gateway and enters SSLVPN gateway configuration mode.

svc address-pool

To configure a pool of IP addresses to assign to end users in a policy group, use the **svc address-pool** command in SSLVPN group policy configuration mode. To remove the address pool from the policy group configuration, use the **no** form of this command.

svc address-pool *name*

no svc address-pool

Syntax Description

name	Name of the address pool that is configured using the **ip local pool** command.

Command Default

A pool of IP addresses are not assigned to end users.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The address pool is first defined with the **ip local pool** command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Configuring Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Configure the **svc address-pool** command with name configured in Step 2.

See the second example on this command reference page for a complete configuration example.

Examples

Directly Connected Network Example

The following example configures the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context SSLVPM
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

Nondirectly Connected Network Example

The following example configures the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.128 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context SSLVPM
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc default-domain

To configure the Secure Sockets Layer (SSL) VPN Client (SVC) domain for a policy group, use the **svc default-domain** command in SSLVPN group policy configuration mode. To remove the domain from the policy group configuration, use the **no** form of this command.

svc default-domain *name*

no svc default-domain

Syntax Description

name	Name of the domain.

Command Default

SVC domain is not configured.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures cisco.com as the default domain:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc default-domain cisco.com
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc dns-server

To configure Domain Name System (DNS) servers for policy group end users, use the **svc dns-server** command in SSLVPN group policy configuration mode. To remove a DNS server from the policy group configuration, use the **no** form of this command.

svc dns-server {**primary** | **secondary**} *ip-address*

no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary DNS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

DNS servers are not configured.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc dpd-interval

To configure the dead peer detection (DPD) timer value for the gateway or client, use the **svc dpd-interval** command in SSLVPN group policy configuration mode. To remove a DPD timer value from the policy group configuration, use the **no** form of this command.

svc dpd-interval {**client** | **gateway**} *seconds*

no svc dpd-interval {**client** | **gateway**}

Syntax Description

client | **gateway**	Specifies the client or gateway.
seconds	Sets the time interval, in seconds, for the DPD timer. A number from 0 through 3600 is entered.

Command Default

The DPD timer is reset every time a packet is received over the Secure Sockets Layer (SSL) Virtual Private Network (VPN) tunnel from the gateway or end user.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example sets the DPD timer to 30 seconds for a WebVPN gateway and to 5 minutes for end users (remote PC or device):

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc homepage

To configure the URL of the web page that is displayed upon successful user login, use the **svc homepage** command in SSLVPN group policy configuration mode. To remove the URL from the policy group configuration, use the **no** form of this command.

svc homepage *string*

no svc homepage

Syntax Description

string	The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length.

Command Default

URL of the home page is not configured.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures www.cisco.com as the Secure Sockets Layer (SSL) VPN Client (SVC) home page:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc homepage www.cisco.com
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc keep-client-installed

To configure the end user to keep Secure Sockets Layer (SSL) VPN client (SVC) software installed when the SSL VPN connection is not enabled, use the **svc keep-client-installed** command in SSLVPN group policy configuration mode. To remove the software installation requirement from the policy group configuration, use the **no** form of this command.

svc keep-client-installed

no svc keep-client-installed

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command removes the overhead of pushing the SVC software client to the end user on each connection attempt.

Examples

The following example configures end users to keep SVC software installed:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc msie-proxy

To configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group end users, use the **svc msie-proxy** command in SSLVPN group policy configuration mode. To remove a MSIE proxy setting from the policy group configuration, use the **no** form of this command.

svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

no svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

Syntax Description

server *host*	Specifies a MSIE proxy server for policy group end users. The *host* argument specifies the location of the MSIE server. The *host* argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.
exception *host*	Configures the browser not to send traffic for a single Domain Name System (DNS) hostname or IP address through the proxy.
option auto	Configures the browser to automatically detect proxy settings.
option bypass-local	Configures the browser to bypass proxy settings that are configured on the remote user.
option none	Configures the browser to use no proxy settings.

Command Default

MSIE browser proxy settings are not configured for policy group end users.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command is applied to end users that use a MSIE browser. The configuration of this command has no effect on any other browser type.

Examples

The following example configures automatic detection of MSIE proxy settings and configures proxy exceptions for traffic from www.example.com and the 10.20.20.1 host:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
Router(config-webvpn-group)#
```

The following example configures a connection to an MSIE proxy server through a fully qualified domain name (FQDN) and a port number:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.example.com:80
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc rekey

To configure the time and method that a tunnel key is refreshed for policy group end users, use the **svc rekey** command in SSLVPN group policy configuration mode. To remove the tunnel key configuration from the policy group configuration, use the **no** form of this command.

svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

no svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

Syntax Description

method new-tunnel	Refreshes the tunnel key by creating a new tunnel connection to the end user.
method ssl	Refreshes the tunnel key by renegotiating the SSL session.
time *seconds*	Configures the time interval, in seconds, at which the tunnel key is refreshed. A number from 0 through 43200 seconds is entered.

Command Default

Time and method are not configured.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures the tunnel key to be refreshed by initiating a new tunnel connection once an hour:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc split

To enable split tunneling for Secure Sockets Layer (SSL) VPN Client (SVC) tunnel clients, use the **svc split** command in SSLVPN group policy configuration mode. To remove the split tunneling configuration from the policy group configuration, use the **no** form of this command.

svc split {**exclude** {*ip-address mask* | **local-lans**} | **include** *ip-address mask*}

no svc split {**exclude** {*ip-address mask* | **local-lans**} | **include** *ip-address mask*}

Syntax Description

exclude *ip-address mask*	The arguments are entered as a destination prefix. Traffic from the specified IP address and mask is not resolved through the SVC tunnel.
exclude local-lans	Permits remote users to access their local LANs.
include *ip-address mask*	The arguments are entered as a destination prefix. Traffic from the specified IP address and mask is resolved through the SVC tunnel.

Command Default

Split tunneling is not enabled for SVC tunnel clients.

Command Modes

SSLVPN Group Policy Configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside the SVC tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet service provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the sametime. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as network printer.

Examples

The following example configures a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.1 0.0.0.255
Router(config-webvpn-group)# svc split include 171.16.1.1 0.0.0.255
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc split dns

To configure the WebVPN gateway to resolve the specified fully qualified Domain Name System (DNS) names through the Secure Sockets Layers (SSL) VPN Client (SVC) tunnel, use the **svc split dns** command in SSLVPN group policy configuration mode. To remove the split DNS statement from the policy group configuration, use the **no** form of this command.

svc split dns *name*

no svc split dns *name*

Syntax Description

dns *name*	The *name* argument is entered as a fully qualified DNS name.

Command Default

The WebVPN gateway is not configured to resolve the specified fully qualified DNS names through the SVC tunnel.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command configures the WebVPN gateway to resolve the specified DNS suffixes (domains) through the tunnel. The gateway automatically incudes the default domain into the list of domains that are resolved through the tunnel. Up to 10 DNS statements can be configured.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns cisco.com
Router(config-webvpn-group)# svc split dns my.company.net
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc wins-server

To configure Windows Internet Name Service (WINS) servers for policy group end users, use the **svc wins-server** command in SSLVPN group policy configuration mode. To remove a WINS server from the policy group configuration, use the **no** form of this command.

svc wins-server {**primary** | **secondary**} *ip-address*

no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary WINS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

WINS servers are not configured for policy group end users.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

timeout (policy group)

To configure the length of time that an end user session can remain idle or the total length of time that the session can remain connected, use the **timeout** command in SSLVPN group policy configuration mode. To configure timeout timers to default values, use the **no** form of this command.

timeout {**idle** *seconds* | **session** *seconds*}

no timeout {**idle** | **session**}

Syntax Description

idle *seconds*	Configures the length time that an end user connection can remain idle.
session *seconds*	Configures the total length of time that an end user can maintain a single connection.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

idle 2100
session 43200

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to configure the idle or session timer value. The idle timer sets the length of time that a session will remain connected when the end user generates no activity. The session timer sets the total length of time that a session will remain connected, with or without activity. Upon expiration of either timer, the end user connection is closed. The user must login or reauthenticate to access the SSL VPN.

Note The idle timer is not the same as the dead peer timer. The dead peer timer is reset when any packet type is received over the Secure Sockets Layer (SSL) VPN Client (SVC) tunnel. The idle timer is reset only when the end user generates activity.

Examples

The following example sets the idle timer to 30 minutes and session timer to 10 hours:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# timeout idle 1800
Router(config-webvpn-group)# timeout session 36000
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

title

To configure the HTML title string that is shown in the browser title and on the title bar of a Secure Sockets Layer (SSL) Virtual Private Network (VPN), use the **title** command in SSLVPN configuration mode. To revert to the default text string, use the **no** form of this command.

title [*title-string*]

no title [*title-string*]

Syntax Description

title-string	(Optional) Title string, up to 255 characters in length, that is displayed in the browser of the user. The string value may contain 7-bit ASCII characters, HTML tags, and escape sequences.

Defaults

If this command is not configured or if the **no** form is entered, the following text is displayed:

“WebVPN Service”

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string “WebVPN Service” is displayed.

Examples

The following example configures “Secure Access: Unauthorized users prohibited” as the title string:

```
Router(config)# webvpn context
Router(config-webvpn-context)# title “Secure Access: Unauthorized users prohibited”
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

title-color

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

title-color *color*

no title-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a“#”), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default is purple.

Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	Support for the WebVPN enhancements feature was added.

Usage Guidelines

Configuring a new color overrides the color the preexisting color.

Examples

The following examples show the three command forms that can be used to configure the title color:

```
Router(config-webvpn-context)# title-color darkseagreen
Router(config-webvpn-context)# title-color #8FBC8F
Router(config-webvpn-context)# title-color 143,188,143
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

url-list

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

url-list *name*

no url-list *name*

Syntax Description

name	Name of the URL list. The list name can up to 64 characters in length.

Command Default

SSLVPN URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of a SSL VPN is not configured.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

Entering this command places the router in SSLVPN URL list configuration mode. In this mode, the list of URLs is configured. A URL list can be configured under the WebVPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

Examples

The following example creates a URL list:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading “Quick Links”
Router(config-webvpn-url)# url-text “Human Resources” url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text “Sales and Marketing” products.mycompany.com
Router(config-webvpn-url)#
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSLVPN.
url-list (policy group)	Attaches a URL list to policy group configuration.

Command	Description
url-text	Adds an entry to a URL list.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

url-list (policy group)

To attach a URL list to a policy group configuration, use the **url-list** command in SSLVPN group policy configuration mode. To remove the URL list from the policy group configuration, use the **no** form of this command.

url-list *name*

no url-list *name*

Syntax Description

name	Name of the URL list configured in SSLVPN configuration mode.

Command Default

A URL list is not attached to a policy group configuration.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The URL list is first defined in SSLVPN configuration mode and then attached to the group policy.

Examples

The following example attaches a URL list to the policy group configuration:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading “Quick Links”
Router(config-webvpn-url)# url-text “Human Resources” url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text “Sales and Marketing” products.mycompany.com
Router(config-webvpn-url)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# url-list ACCESS
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
url-list	Enters SSLVPN URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSLVPN.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

url-text

To add an entry to a URL list, use the **url-text** command in SSLVPN URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

url-text {*name* **url-value** *url*}

no url-text {*name* **url-value** *url*}

Syntax Description

name	Text label for the URL. The label must be inside quotation marks if it contains spaces.
url-value *url*	An HTTP URL.

Command Default

An entry is not added to a URL list.

Command Modes

SSLVPN URL list configuration

Command History

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

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading “Quick Links”
Router(config-webvpn-url)# url-text “Human Resources” url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text “Sales and Marketing” products.mycompany.com
Router(config-webvpn-url)#
```

Related Commands

Command	Description
url-list	Enters SSLVPN URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSLVPN.

vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a WebVPN context, use the **vrf-name** command in SSLVPN configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

vrf-name *name*

no vrf-name

Syntax Description

name	Name of the VRF.

Command Default

A VPN VRF is not associated with a WebVPN context.

Command Modes

SSLVPN configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each WebVPN context configuration.

Examples

The following example associates a VRF with a WebVPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context SSLVPN
Router (config-webvpn-context)# vrf-name BLUE
Router (config-vrf)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

webvpn aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer (SSL) Virtual Private Network (VPN) sessions, use the **webvpn aaa accounting-list** command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

webvpn aaa accounting-list *aaa-list*

no webvpn aaa accounting-list *aaa-list*

Syntax Description

aaa-list	Name of the AAA accounting list that has been configured under global configuration.

Defaults

AAA accounting is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# webvpn aaa accounting-list sslvpnaaa
```

Related Commands

Command	Description
aaa accounting network SSLVPN start-stop group radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

webvpn context

To enter SSLVPN configuration mode to configure the WebVPN context, use the **webvpn context** command in global configuration mode. To remove the WebVPN configuration from the router configuration file, use the **no** form of this command.

webvpn context *name*

no webvpn context *name*

Syntax Description

name	Name of the WebVPN context configuration.

Command Default

SSLVPN configuration mode is not entered, and a WebVPN context is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The WebVPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in SSLVPN configuration mode.

Note The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a WebVPN gateway is in an enabled state (in service).

Examples

The following example configures and activates the Secure Sockets Layer (SSL) Virtual Private Network (VPN) WebVPN context configuration:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# inservice
Router(config-webvpn-context)#
```

Related Commands

Command	Description
aaa authentication (WebVPN)	Configures AAA authentication for SSL VPN sessions.
csd enable	Enables CSD support for SSL VPN sessions.
default-group-policy	Specifies a default group policy for SSL VPN sessions.
gateway (WebVPN)	Specifies the gateway for SSL VPN sessions.
inservice	Enables a WebVPN gateway or context process.
login-message	Configures a message for a user login text box on the login page.

Command	Description
logo	Configures a custom logo to be displayed on the login and portal pages of a SSL VPN.
max-users (WebVPN)	Limits the number of connections to a SSL VPN that will be permitted
nbns-list	Enters SSLVPN NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
policy group	Enters a SSLVPN group policy configuration mode to configure a group policy.
port-forward	Enters SSLVPN port-forward list configuration mode to configure a port forwarding list.
secondary-color	Configures the color of the secondary title bars on the login and portal pages of a SSLVPN.
secondary-text-color	Configures the color of the text on the secondary bars of a SSLVPN.
title	Configures the HTML title string that is shown in the browser title and on the title bar of a SSLVPN.
title-color	Configures the color of the title bars on the login and portal pages of a SSLVPN.
url-list	Enters SSLVPN URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSLVPN.
vrf-name	Associates a VRF with a WebVPN context.

webvpn gateway

To enter SSLVPN gateway configuration mode to configure a WebVPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the WebVPN gateway from the router configuration file, use the **no** form of this command.

webvpn gateway *name*

no webvpn gateway *name*

Syntax Description

name	Name of the virtual gateway service.

Command Default

SSLVPN gateway configuration mode is not entered, and a WebVPN gateway is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering the **webvpn gateway** command places the router in SSLVPN gateway configuration mode. Configuration settings specific to the WebVPN gateway are entered in this configuration mode.

The WebVPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a Web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which WebVPN remote-user sessions terminate. The gateway is not active until the inservice command has been entered in SSLVPN gateway configuration mode. Only one gateway can be configured in a WebVPN-enabled network.

Examples

The following example creates and enables a WebVPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN
Router(config-webvpn-gateway)# http-redirect 80
Router(config-webvpn-gateway)# inservice
```

Related Commands

Command	Description
hostname (WebVPN)	Configures a WebVPN hostname.
http-redirect	Configures HTTP traffic to be carried over HTTPS.
inservice	Enables a WebVPN gateway or context process.

Command	Description
ip address (WebVPN)	Configures a proxy IP address on a WebVPN gateway.
ssl encryption	Configures the specify the encryption algorithms that the SSL protocol will use for an SSLVPN.
ssl trustpoint	Configures the certificate trust point on a WebVPN gateway.

webvpn install

To install a Cisco Secure Desktop (CSD) or Secure Sockets Layer (SSL) Virtual Private Network (VPN) Client (SVC) package file to a WebVPN gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the WebVPN gateway, use the **no** form of this command.

webvpn install [**csd** *location-name* | **svc** *location-name*]

no webvpn install [**csd** *location-name* | **svc** *location-name*]

Syntax Description

csd *location-name*	(Optional) Installs the CSD client software package. The filename and path are entered.
svc *location-name*	(Optional) Installs the SVC client software package. The filename and path are entered.

Command Default

A CSD or SSL VPN Client package file is not installed to a WebVPN gateway.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The installation packages must first be copied to a local files system, such as flash memory. The CSD and SVC software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or later must be installed before a CSD or SVC client package can be installed.

Examples

The following example installs the SVC package to a WebVPN gateway:

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example installs the CSD package to a WebVPN gateway:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

Feature Information for SSL VPN–WebVPN

Table 15 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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

Note Table 15 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 15 Feature Information for SSL VPN–WebVPN

Feature Name	Release	Feature Information
SSL VPN–WebVPN	12.4(6)T	This feature enhances SSL VPN support in Cisco IOS software. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN–WebVPN introduced three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.
WebVPN Auto Applet Download	12.4(9)T	This feature provides administrators with the option of automatically downloading the port-forwarding applet under the policy group. The following section provides information about this feature: • “Automatic Applet Download” section The following command was modified by this feature: **port-forward (policy group)**
WebVPN NTLM Authentication	12.4(9)T	This feature provides NT LAN Manager (NTLM) authentication support. The following section provides information about this feature: • “WebVPN NTLM Authentication” section The following command was modified by this feature: **functions**

WebVPN RADIUS Accounting	12.4(9)T	This feature provides for RADIUS accounting for SSL VPN sessions. The following section provides information about this feature: • "WebVPN RADIUS Accounting" section The following command was added by this feature: **webvpn aaa accounting-list**

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