



CHAPTER 12

Managing SSL VPNs

The SSL VPN feature enables users to access enterprise networks from any Internet-enabled location using only a web browser that natively supports Secure Socket Layer (SSL) encryption, without the need for a software or hardware client.

**Note**

SSL VPN is supported on ASA 5500 devices running software version 7.1 and 7.2, and on Cisco 870, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running software version 12.4(6)T and later. For ASA devices and routers running other software versions, a message is displayed stating that SSL VPN policies cannot be configured using Security Manager when you click SSL VPN in the Policy Selector.

**Note**

For security appliances running ASA 8.0 or 8.1, SSL VPN policies are not available for configuration from the Security Manager interface.

In Security Manager 3.1, if you configure SSL VPN policies on an ASA device running 7.0, activity validation fails with an error. In Security Manager 3.2, SSL VPN policies are not available for configuration itself in the Policy Selector for ASA 7.0 devices.

On IOS devices, remote access is provided through an SSL-enabled VPN gateway. Using an SSL-enabled web browser, the remote user establishes a connection to the SSL VPN gateway. After the remote user is authenticated to the secure

gateway via the web browser, an SSL VPN session is established and the user can access the internal corporate network. A portal page enables users to access all the resources available on the SSL VPN networks.

On ASA devices, remote users establish a secure, remote access VPN tunnel to the security appliance using the web browser. The SSL protocol provides the secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

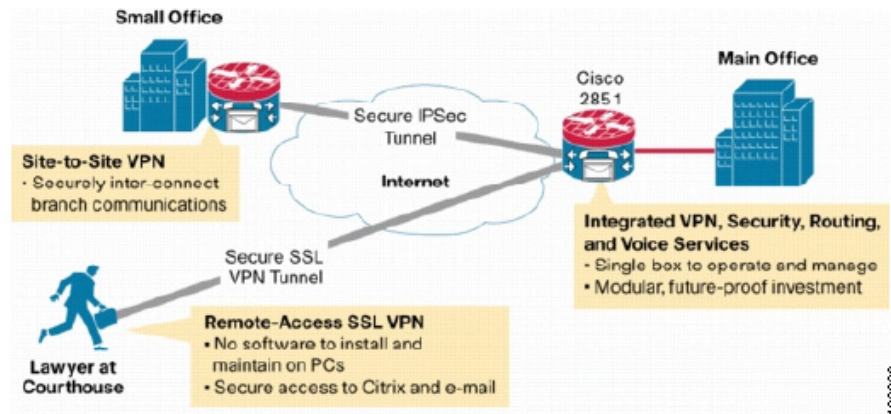


Note

Network administrators provide user access to SSL VPN resources on a group basis. Users have no direct access to resources on the internal network.

Figure 12-1 shows how a mobile worker 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 12-1 Secure SSL VPN Access Example



Prerequisites for Configuring SSL VPN

For a remote user to securely access resources on a private network behind an SSL VPN gateway, the following prerequisites must be met:

- A user account (login name and password).
- An SSL-enabled browser (such as, Internet Explorer, Netscape, Mozilla, or Firefox).
- An Email client (such as Eudora, Microsoft Outlook, or Netscape Mail).
- One of the following operating systems:
 - Microsoft Windows 2000 or Windows XP with either the Sun Microsystems Java Runtime Environment (JRE) for Windows version 1.4 or later, or a browser that supports ActiveX control.
 - Linux 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.

Related Topics

- [SSL VPN Access Modes, page 12-3](#)
- [Configuring SSL VPN on an IOS Device, page 12-6](#)
- [Configuring SSL VPN on an ASA Device, page 12-27](#)

SSL VPN Access Modes

SSL VPN provides three modes of remote access that are supported on IOS routers and ASA devices—Clientless, Thin Client, and Full Tunnel client.

Clientless Access Mode

In Clientless mode, the remote user accesses the internal or corporate network using a web browser on the client machine. No applet downloading is required.

Clientless mode is useful for accessing most content that you would expect in a web browser, such as Internet access, databases, and online tools that employ a web interface. It supports web browsing (using HTTP and HTTPS), file sharing using Common Internet File System (CIFS), and Outlook Web Access (OWA) email. For Clientless mode to work successfully, the PC of the remote user must run Windows 2000, Windows XP, or Linux operating systems.

Thin Client Access 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 this 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 configured on the SSL VPN gateway. The Java applet starts a new SSL connection for every client connection.

The Java applet initiates an HTTP request from the remote user client to the SSL VPN gateway. The name and port number of the internal email server is included in the HTTP request. The SSL VPN gateway creates a TCP connection to that internal email server and port.

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).



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 refuses to run if a compatible JRE version is not detected.

When using Thin Client mode, you should be aware of the following:

- The remote user must allow the Java applet to download and install.
- For TCP port-forwarding applications to work seamlessly, administrative privileges must be enabled for remote users.
- 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.

Full Tunnel Client Access Mode

Full Tunnel Client mode enables access to the corporate network completely over an SSL VPN tunnel, which is used to move data at the network (IP) layer. This mode supports most IP-based applications, such as, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet. Being part of the SSL VPN is completely transparent to the applications run on the client. A java applet is

downloaded to handle the tunneling between the client host and the SSL VPN gateway. The user can use any application as if the client host was in the internal network.

The tunnel connection is determined by the group policy configuration. The SSL VPN Client (SVC) is downloaded and installed to the remote client, and the tunnel connection is established when the remote user logs in to the SSL VPN gateway. By default, the SVC is removed from the remote client after the connection is closed, but you can keep it installed, if required.

**Note**

In Security Manager, the SVC is managed using a FlexConfig policy. For more information, see [Predefined FlexConfig Policy Objects, page 20-8](#).

**Note**

Full Tunnel SSL VPN access requires administrative privileges on the remote client.

Related Topics

- [Chapter 11, “Managing Remote Access VPNs”](#)
- [Configuring the Full Tunnel Access Mode, page 12-23](#)
- [Configuring the Clientless and Thin Client Access Modes, page 12-25](#)
- [Full Tunnel Access Mode Page, page I-10](#)
- [Clientless and Thin Client Access Modes Page, page I-13](#)

Working with SSL VPN Policies

SSL VPN policies define the configuration that is required for remote users to establish a secure remote access VPN tunnel between an Internet-enabled location and a private network behind an SSL VPN, using an SSL-enabled web browser.

**Note**

You can set up and configure SSL VPNs on Cisco IOS routers, and Adaptive Security Appliance (ASA) devices.

You cannot discover the configurations on a device that is already deployed in an

SSL VPN network. Security Manager leaves any existing SSL VPN configurations intact on the device until you deploy SSL VPN policies that were configured with Security Manager.

In Device view, you can view and configure SSL VPN policies for devices. To access Device view, select **View > Device View** or click the **Device View** button in the toolbar. You can right-click a policy in the Policy selector to display menu options that enable you to share the policy, assign the shared policy to, or unassign it from the selected device. For more information, see [Performing Basic Policy Management, page 7-18](#).

You can also view all shared policies for each policy type in an SSL VPN, edit policies, and modify their assignments to devices, in Policy view. See [Managing Shared Policies in Policy View, page 7-39](#).

**Note**

You must have read-write permissions to modify an SSL VPN policy. For more information, see [Modify Policies Permissions, page 2-13](#).

These topics provide information about configuring an SSL VPN from the Security Manager Device view:

- [Using the Wizard to Create an IOS SSL VPN Connection, page 12-7](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)
- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)
- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)

Configuring SSL VPN on an IOS Device

On Cisco IOS routers, remote access is provided through an SSL-enabled VPN gateway. Using an SSL-enabled web browser, the remote user establishes a connection to the SSL VPN gateway. After the remote user is authenticated to the secure gateway via the web browser, an SSL VPN session is established and the user can access the internal corporate network. A portal page enables users to access all the resources available on the SSL VPN networks.

SSL VPN configuration on Cisco IOS routers is usually deployed in small office/home office (SOHO) networks, remote branch offices, and main corporate sites.

Using Security Manager, you can create a basic connection with a limited set of features that enable an SSL VPN to function, and then configure additional policies and features for your SSL VPN.

These topics describe how to configure an SSL VPN connection and the policies required for it to function:

- [Using the Wizard to Create an IOS SSL VPN Connection, page 12-7](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

Using the Wizard to Create an IOS SSL VPN Connection

The SSL VPN wizard enables you to configure SSL VPN on your VPN gateway (server) device.

The wizard creates an SSL VPN connection with a limited set of features that enable a basic SSL VPN to function. After you complete the wizard, you can configure additional policies and features for the SSL VPN, or modify the existing ones. If required, you can return to the wizard to create additional SSL VPN configurations.

To access the SSL VPN wizard:

1. Click the **Device View** button in the toolbar.
2. From the Device Selector, select the IOS device you want to configure as your VPN gateway (server).
3. Select **SSL VPN > SSL VPN Wizard** from the Policy selector.
4. Click **SSL VPN Server Wizard**.

These topics describe the steps in the SSL VPN wizard:

- [Configuring an SSL VPN Gateway and Context, page 12-8](#)
- [Customizing the SSL VPN Portal Page, page 12-10](#)

Related Topics

- [Configuring SSL VPN on an IOS Device, page 12-6](#)

Configuring an SSL VPN Gateway and Context

The SSL VPN gateway acts as a proxy for connections to protected resources, which are accessed through an SSL-encrypted connection between the gateway and a web-enabled browser on a remote device.

An SSL VPN gateway provides a reachable IP address and certificate for one or more SSL VPN contexts. Each gateway configured on a router must be configured with its own IP address—IP addresses cannot be shared among gateways. You can use the IP address of a router interface, or another reachable IP address if one is available. Either a digital certificate or a self-signed certificate must be configured for a gateway to establish a secure connection. All gateways on the router can use the same certificate.

An SSL VPN context defines the virtual configuration of the SSL VPN. It must be configured before an SSL VPN gateway can be used. An SSL VPN context can be associated with only one gateway. It supports one or more user group policies. Although one gateway can serve multiple SSL VPN contexts, resource constraints and IP address reachability must be taken into account.

The SSL VPN gateway and context configuration must be completed before a remote user can access resources on a private network behind the SSL VPN. In the first step of the SSL VPN wizard, you create an SSL VPN context, configure a gateway, and specify information that permits users to access a portal page, as described in the following procedure.

Before You Begin

- In Device view (**View > Device View**), select the required Cisco IOS router.

Related Topics

- [Using the Wizard to Create an IOS SSL VPN Connection, page 12-7](#)
- [Gateway and Context Page \(IOS\), page I-2](#)
- [Understanding User Groups in SSL VPN, page 12-17](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.

The wizard opens, displaying the Gateway and Context page. For a description of the elements on this page, see [Table I-1 on page I-3](#).

- Step 2** Select an option to specify the gateway to be used as a proxy for connections to the protected resources in your SSL VPN. You can select to use an existing gateway, or create a new gateway using the router's public static IP address or the public static IP address of the router interface.



Note The Portal Page URL field displays the URL that will appear on the Portal page to access the SSL VPN gateway.

- Step 3** If you selected to create a new gateway using the router's public static IP address or the public static IP address of the router interface, specify the number of the port that will carry the HTTPS traffic, and the trustpoint (self-signed certificate) required to establish the secure connection.

- Step 4** Enter a name for the context that defines the virtual configuration of the SSL VPN.



Note To simplify the management of multiple context configurations, you should use the domain or virtual hostname for the context name.

- Step 5** Specify the user group(s) that will be used in your SSL VPN connection. You can click **Edit** to open the User Groups selector from which you can select the user group(s), or open the User Group wizard in which you can create a user group. For more information, see [Configuring User Groups on an IOS Device, page 12-18](#).

- Step 6** Specify the name of the server group (LOCAL if the users are defined on the local device) to be used for user authentication.

- Step 7** Specify a list or method for SSL VPN remote user authentication.



Note If you do not specify a list or method, the gateway uses global AAA parameters for remote user authentication.

- Step 8** Specify the name of the accounting server group to be used for authentication.

- Step 9** Click **Next** to advance to the next step of the wizard.



Note When you click **Finish** in the wizard, the new gateway and context are displayed in the SSL VPN Policy page.

Customizing the SSL VPN Portal Page

The portal page enables the remote user access to all resources available on the SSL VPN 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. Only the websites that appear as links on the portal page are available to users.

This procedure describes how to define the appearance of the portal page. You can select among the predefined themes listed, and obtain a preview of the portal page as it would appear if that theme were used.

Before You Begin

In Device view (**View > Device View**), make sure the selected device is an Cisco IOS router.

Related Topics

- [Portal Page Customization Page, page I-5](#)
- [Using the Wizard to Create an IOS SSL VPN Connection, page 12-7](#)

-
- Step 1** Open the Portal Page Customization page by clicking **Next** on the Gateway and Context page, of the SSL VPN wizard. For a description of the elements on the Portal Page Customization page, see [Portal Page Customization Page, page I-5](#).
- Step 2** Customize the appearance of the portal page, by specifying:
- The title and logo to be displayed in the title bar of the login and portal page.
 - A message that will be displayed to the user upon login.
 - The colors of the primary and secondary title bars on the login and portal pages of the SSL VPN.
 - The colors of the text on the primary and secondary title bars of the login and portal pages.

A preview of the portal page is displayed.

- Step 3** When you have completed customizing the portal page, click **Finish** to close the wizard.

The SSL VPN connection you have defined in the wizard is displayed in the SSL VPN Policy page. If required, you can modify this connection from the SSL VPN folder. See [Configuring an SSL VPN Policy \(IOS\)](#), page 12-11.

Configuring an SSL VPN Policy (IOS)

After you create a basic SSL VPN connection on your server device using the SSL VPN wizard, you can modify the connection, if required, and configure additional policies and features from the SSL VPN folder in the Device view.

The SSL VPN Policy page displays a list of all the currently defined SSL VPN policies, including any policies that were created using the wizard. From this page, you can create, modify, or delete SSL VPN policies.

These topics enable you to configure SSL VPN policies on an IOS router:

- [Configuring General Settings for an IOS SSL VPN Policy](#), page 12-11
- [Configuring the Portal Page for an IOS SSL VPN Policy](#), page 12-13
- [Configuring the Secure Desktop Software for an IOS SSL VPN Policy](#), page 12-15
- [Configuring Advanced Settings for an IOS SSL VPN Policy](#), page 12-16

Related Topics

- [Configuring SSL VPN on an IOS Device](#), page 12-6
- [Using the Wizard to Create an IOS SSL VPN Connection](#), page 12-7
- [SSL VPN Policy Page \(IOS\)](#), page I-15

Configuring General Settings for an IOS SSL VPN Policy

This procedure describes how to create or edit the general settings required for an SSL VPN policy, such as, specifying the gateway, domain, AAA servers for accounting and authentication, and user groups.

Before You Begin

In Device view (**View > Device View**), select the required IOS router.

Related Topics

- [General Tab, page I-17](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Policy**.

The SSL VPN Policy page opens. For a description of the elements on the SSL VPN Policy page, see [Table I-7 on page I-15](#).

Step 2 Click **Create** on the SSL VPN Policy page, or select a row in the table on the page and click Edit.

The SSL VPN Context Editor dialog box opens, displaying the General tab. For a description of the elements on the General tab, see [Table I-8 on page I-17](#).

Step 3 If you are creating a policy, specify the name of the context that defines the virtual configuration of the SSL VPN.



Note To simplify the management of multiple context configurations, the context name is the same as the domain or virtual hostname.

Step 4 Enter or edit the gateway to be used in the SSL VPN policy. You can click **Select** to open a dialog box from which you can select the gateway from a list of SSL VPN gateway objects.



Note The Portal Page URL field displays the URL that will appear on the Portal page to access the SSL VPN gateway.

Step 5 Select or deselect **Enable SSL VPN** depending on whether you want this SSL VPN connection to be active.

Step 6 Enter or edit the name of the server group (LOCAL if the users are defined on the local device) to be used for user authentication. You can click **Select** to select an authentication server group from a list of AAA server group objects.

Step 7 Enter or edit a method for SSL VPN remote user authentication.



Note If you do not specify a method, the gateway uses global AAA parameters for remote user authentication.

Step 8 If the selected device is running IOS version 12.4(9)T or later, enter or edit the name of the accounting server group to be used for authentication. You can click **Select** to select an accounting server group from a list of AAA server group objects.

Step 9 Specify the user group(s) that will be used in your SSL VPN policy.

- To add a user group(s) to the User Groups table, click **Create**. The User Groups Selector opens, from which you can select the required user group(s).
If the required user group is not included in the Selector, click **Create** to open the Add User Group dialog box in which you can create a new user group object. For a description of the User Groups Selector, see [Table I-3 on page I-8](#).
- To modify the properties of a user group, select it and click **Edit**. The Edit User Group dialog box opens, enabling you to edit the user group object.

For more information about user group objects, see [Creating User Group Objects, page 9-199](#).

Step 10 Click **OK** to save your settings locally on the client and close the SSL VPN Context Editor, or click another tab in the dialog box.

Configuring the Portal Page for an IOS SSL VPN Policy

The portal page enables the remote user to access all resources available on the SSL VPN networks. Only the websites that appear as links on the portal page are available to users.

You can configure the appearance of the portal page when you create an SSL VPN connection, using the wizard (see [Customizing the SSL VPN Portal Page, page 12-10](#)). In the Portal Page tab of the SSL VPN Context Editor, you can redefine the themes for a selected SSL VPN policy, or customize the portal page for a new SSL VPN policy.

This procedure describes how to define the appearance of the portal page for an SSL VPN policy. You can select among the predefined themes listed, and obtain a preview of the portal page as it would appear if that theme were used.

Before You Begin

In Device view (**View > Device View**), select the required IOS router.

Related Topics

- [Portal Page Tab, page I-19](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

-
- Step 1** Select **View > Device View > SSL VPN > SSL VPN Policy**.
- The SSL VPN Policy page opens. For a description of the elements on the SSL VPN Policy page, see [Table I-7 on page I-15](#).
- Step 2** Click **Create** on the SSL VPN Policy page, or select a row in the table on the page and click **Edit**. The SSL VPN Context Editor dialog box opens.
- Step 3** Click the **Portal Page** tab. For a description of the elements on the Portal Page tab, see [Table I-9 on page I-19](#).
- Step 4** Customize the appearance of the portal page for the SSL VPN policy, by specifying:
- The title and logo to be displayed in the title bar of the login and portal page.
 - A message that will be displayed to the user upon login.
 - The colors of the primary and secondary title bars on the login and portal pages of the SSL VPN.
 - The colors of the text on the primary and secondary title bars of the login and portal pages.
- A preview of the portal page is displayed.
- Step 5** When you have finished customizing the portal page, click **OK** to save your settings locally on the client and close the SSL VPN Context Editor, or click another tab in the dialog box.
-

Configuring the Secure Desktop Software for an IOS SSL VPN Policy

Cisco Secure Desktop (CSD) enables you to eliminate all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. CSD provides a session-based interface where sensitive data is shared only for the duration of a SSL VPN session. All session information is encrypted, and all traces of the session data are removed from the remote client when the session is terminated, even if the connection terminates abruptly.



Note

In Security Manager, the CSD is managed using a FlexConfig policy. For more information, see [Predefined FlexConfig Policy Objects, page 20-8](#).

This procedure describes how to configure CSD on an IOS router.

Before You Begin

- In Device view (**View > Device View**), select the required IOS router.
- Make sure the Secure Desktop Client software is installed and activated on the device. For more information, see [Configuring the Cisco Secure Desktop Software, page 12-44](#).

Related Topics

- [Configuring the Cisco Secure Desktop Software, page 12-44](#)
- [Secure Desktop Tab, page I-20](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

-
- Step 1** Select **View > Device View > SSL VPN > SSL VPN Policy**.
- The SSL VPN Policy page opens. For a description of the elements on the SSL VPN Policy page, see [Table I-7 on page I-15](#).
- Step 2** Click **Create** on the SSL VPN Policy page, or select a row in the table on the page and click **Edit**. The SSL VPN Context Editor dialog box opens.
- Step 3** Click the **Secure Desktop** tab. For a description of the elements on the Secure Desktop tab, see [Table I-10 on page I-21](#).
- Step 4** Select the **Enable** check box to enable CSD on the device.

Step 5 In the **Configuration** field, specify the filename of the CSD distribution package to install into the running configuration (the securedesktop_asa_<n>_<n>*.pkg file to be uploaded from your local computer to the flash device).

You can click **Select** to open the Secure Desktops Selector from which you can select a CSD distribution package file from a list of CSD distribution package objects. For more information, see [Understanding Secure Desktop Configuration Objects, page 9-171](#).

Step 6 Click **OK** to save your settings locally on the client, and close the SSL VPN Context Editor, or click another tab in the dialog box.

Configuring Advanced Settings for an IOS SSL VPN Policy

This procedure describes how to specify or edit the advanced settings required for an SSL VPN policy, including the maximum number of SSL VPN user sessions that can be configured, and Virtual Routing Forwarding (VRF) related information.

Before You Begin

In Device view (**View > Device View**), select the required IOS router.

Related Topics

- [Advanced Tab, page I-22](#)
- [Configuring an SSL VPN Policy \(IOS\), page 12-11](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Policy**.

The SSL VPN Policy page opens. For a description of the elements on the SSL VPN Policy page, see [Table I-7 on page I-15](#).

Step 2 Click **Create** on the SSL VPN Policy page, or select a row in the table on the page and click Edit. The SSL VPN Context Editor dialog box opens.

Step 3 Click the **Advanced** tab. For a description of the elements on the Advanced tab, see [Table I-11 on page I-22](#).

Step 4 Specify the maximum number of SSL VPN user sessions that can be configured (within the range of 1-1000).

- Step 5** If Virtual Routing Forwarding (VRF) is configured on the device, specify the name of the VRF instance that is associated with the SSL VPN context.
- Step 6** Click **OK** to save your settings locally on the client, and close the SSL VPN Context Editor, or click another tab in the dialog box.
-

Understanding User Groups in SSL VPN

SSL VPN user group policies allow you to accommodate the needs of different groups of users. For example, a group of engineers working remotely needs access to network resources different from the network resources to which sales personnel working in the field need access. Business partners and outside vendors must be able to access the information that they need to work with your organization, but you must ensure that they do not have access to confidential information or other resources they do not need. Creating a different policy for each group provides remote users with the resources they need, and prevents them from accessing other resources.

In Security Manager, user parameters are captured by user groups which define the resources accessible to the user when connecting to an SSL VPN gateway or ASA security appliance.

On an IOS router, a user group is defined within a context. Each context has a domain name. When a user types a URL to access the SSL VPN gateway, that domain name is used to associate the user with the user group defined in the context. You can have more than one user group in a context. Each SSL VPN context has its own user groups list.



Note

If more than one user group policy is configured on a device, you must configure the device to use an AAA server to authenticate users and to determine which user group a particular user belongs to.

An ASA security appliance has a built-in user group that is shared by all connections to the device. During SSL VPN user authentication, the AAA server returns a user group name that the user belongs to. The device first tries to match the name to the names in the User Groups list. If a match is found, the definition in the matching user group will be used. Otherwise, the default user group is used. If no default user group is defined, the device's built-in user group is used.

Related Topics

- [Configuring User Groups on an IOS Device, page 12-18](#)
- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)
- [Creating a New User Group, page 12-21](#)
- [Configuring an SSL VPN Gateway and Context, page 12-8](#)
- [Defining the ASA SSL VPN Connection Profile Parameters, page 12-29](#)

Configuring User Groups on an IOS Device

When you are configuring SSL VPN, you must specify the user group(s) that will be used in your SSL VPN connection. You can use predefined user group(s), edit them if required, and create user groups.

This procedure describes how to specify the user group(s) to use in your SSL VPN connection on an IOS router.

Before You Begin

In Device view (**View > Device View**), select the required IOS device.

Related Topics

- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Creating a New User Group, page 12-21](#)
- [Configuring an SSL VPN Gateway and Context, page 12-8](#)
- [User Groups Selector Page, page I-7](#)
- [Gateway and Context Page \(IOS\), page I-2](#)
- [Creating User Group Objects, page 9-199](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.

The Gateway and Context page of the SSL VPN wizard opens. For a description of the elements on the Gateway and Context page, see [Table I-1 on page I-3](#).

The User Groups table displays the currently defined user groups that will be used in your SSL VPN connection.

- Step 2** To select additional user group(s), or modify the properties of a selected user group in the table, click **Edit**.



Note You can select more than one user group for editing.

The User Groups Selector opens displaying a list of predefined user groups available for selection. For a description of the elements on the User Groups Selector page, see [Table I-3 on page I-8](#).

- Step 3** Select the required user group(s) and click >>.
- If the required user group is not included in the **Available User Groups** list, click **Create** below the list to create one. See [Creating a New User Group, page 12-21](#).
 - To specify a user group as the default, select it in the **Selected User Groups** list, and click **Set As Default**.
 - To modify the properties of a user group in the Selector, select it and click **Edit**. User groups are objects. The Edit User Group dialog box opens, enabling you to edit the user group object. See [User Group Dialog Box, page F-549](#).
- Step 4** Click **OK** to save your changes and close the User Groups Selector.

The newly defined, selected or edited user group(s) appears in the User Groups table on the Gateway and Context page.

Configuring User Groups on an ASA Device

When you are configuring SSL VPN on an ASA device, you must specify the user group(s) that will be used in your SSL VPN connection profile. You can select predefined user group(s), edit them if required, and create user groups.

This procedure describes how to specify the user group(s) to use in your SSL VPN connection profile on an ASA device.

Before You Begin

In Device view (**View > Device View**), select the required ASA device.

Related Topics

- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Creating a New User Group, page 12-21](#)
- [User Groups Selector Page, page I-7](#)
- [Connection Profile Page \(ASA\), page I-25](#)
- [Defining the ASA SSL VPN Connection Profile Parameters, page 12-29](#)
- [Creating ASA User Group Objects, page 9-44](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.

Step 2 Click **Next** in the Access page of the SSL VPN Configuration Wizard. The Connection Profile page of the SSL VPN wizard opens. For a description of the elements on the Connection Profile page, see [Table I-13 on page I-25](#).

The User Groups table on the Connection Profile page displays the currently defined ASA user groups that will be used in your SSL VPN connection profile.



Note ASA user groups are shared by all connection profiles on the selected device.

Step 3 To select additional user group(s), or modify the properties of a selected user group in the table, click **Edit**. You can select more than one user group for editing. The User Groups Selector opens displaying a list of predefined ASA user groups available for selection. For a description of the elements on the User Groups Selector page, see [Table I-3 on page I-8](#).

Step 4 Select the required ASA user group(s) and click **>>**.

- If the required user group is not included in the **Available User Groups** list, click **Create** below the list to create one. See [Creating a New User Group, page 12-21](#).
- To modify the properties of an ASA user group in the Selector, select it and click **Edit**. ASA user groups are objects. The Edit ASA User Group dialog box opens, enabling you to edit the user group object. See [ASA User Group Dialog Box, page F-56](#).

Step 5 Click **OK** to save your changes and close the User Groups Selector.

The newly defined, selected or edited ASA user group(s) appears in the User Groups table on the Connection Profile page.

Creating a New User Group

User groups define the resources accessible to the user when connecting to an IOS SSL VPN gateway, or an ASA security appliance. In Security Manager, you can create a new user group that will be used in your SSL VPN connection on an IOS router or ASA device, using the Policy Object Manager or from within the SSL VPN wizard.

These topics describe the steps you may configure to create a user group from within the SSL VPN wizard:

- [Defining the User Group Name and Access Methods, page 12-21](#)
- [Configuring the Full Tunnel Access Mode, page 12-23](#)
- [Configuring the Clientless and Thin Client Access Modes, page 12-25](#)

For information about creating user groups from the Policy Object Manager, see:

- [Creating ASA User Group Objects, page 9-44](#)
- [Creating User Group Objects, page 9-199](#)

Related Topics

- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Configuring User Groups on an IOS Device, page 12-18](#)
- [Configuring User Groups on an ASA Device, page 12-19](#)
- [Create User Group Wizard, page I-8](#)

Defining the User Group Name and Access Methods

This procedure describes how to define a name for your user group, and optionally, select and configure the remote access method(s) that will be used to access the SSL-enabled gateway (IOS router) or ASA security appliance.

Before You Begin

- In Device view (**View > Device View**), select the required device (Cisco IOS router or ASA device).

Related Topics

- [Name and Access Method Page](#), page I-9
- [Creating a New User Group](#), page 12-21
- [Configuring the Full Tunnel Access Mode](#), page 12-23
- [Configuring the Clientless and Thin Client Access Modes](#), page 12-25

-
- Step 1** Select **View > Device View > SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.
- Step 2** Open the User Groups Selector page as follows:
- If you selected an IOS router, click **Edit** alongside the User Groups table in the [Gateway and Context Page \(IOS\)](#), page I-2.
 - If you selected an ASA device, click **Next** in the [Access Page \(ASA\)](#), page I-23, then click **Edit** alongside the User Groups table in the [Connection Profile Page \(ASA\)](#), page I-25.
- Step 3** Click **Create** in the User Groups Selector page. The Create User Group wizard opens, displaying the Name and Access Method page opens. For a description of the elements on this page, see [Table I-4 on page I-10](#).
- Step 4** Specify a name for the user group.
- Step 5** Select the access mode(s) you want to configure for the user group:
- **Full Tunnel**—Select to enable access to the corporate network completely over the SSL VPN tunnel. The SSL VPN Client (SVC) is downloaded and installed to the remote client, and the tunnel connection is established when the remote user logs in to the SSL VPN gateway. For more information, see [SSL VPN Access Modes](#), page 12-3..
 - **Clientless**—Select to enable remote user access to the internal or corporate network using a web browser on the client machine.
 - **Thin Client**—Select to enable the client application to use TCP to connect to a well-known server and port. The remote user downloads a Java applet that acts as a TCP proxy on the client machine for the services that you configure on the SSL VPN gateway.

- Step 6** Click **Next** to configure the Full Tunnel, Clientless and/or Thin Client access modes, or click **Finish** to complete the user group configuration.
-

Configuring the Full Tunnel Access Mode

Full Tunnel Client mode enables access to the corporate network completely over an SSL VPN tunnel. In Full Tunnel Client access mode, the tunnel connection is determined by the group policy configuration. The full tunnel client software, SSL VPN Client (SVC), is downloaded to the remote client, so that a tunnel connection is established when the remote user logs in to the SSL VPN gateway, or connects to the ASA security appliance.

For more information, see [SSL VPN Access Modes, page 12-3](#).

This procedure describes how to configure the Full Tunnel access mode to be used in your user group configuration.



Note

You can configure the Full Tunnel client access mode only if you selected the **Full Tunnel** option in Step 1 of the Create User Group wizard. See [Defining the User Group Name and Access Methods, page 12-21](#).

Before You Begin

- In Device view (**View > Device View**), select the required device (Cisco IOS router or ASA device).

Related Topics

- [Full Tunnel Access Mode Page, page I-10](#)
- [Creating a New User Group, page 12-21](#)
- [Configuring the Clientless and Thin Client Access Modes, page 12-25](#)

- Step 1** Open the Full Tunnel page by clicking **Next** on the [Name and Access Method Page, page I-9](#) of the Create User Group wizard. For a description of the elements on the Full Tunnel page, see [Table I-5 on page I-11](#).



Note This page is only available if you selected to configure the Full Tunnel access mode, in step 1 of the wizard.

- Step 2** Select **Use Other Access Modes if SSL VPN Client Download Fails** if you want to enable the remote client to use clientless or thin client access modes if the SSL VPN Client (SVC) software download fails.
- Step 3** Select **Full Tunnel Only** to enable the configuration of the Full Tunnel access mode.
- Step 4** If the device is an IOS router, specify the IP address ranges of the address pool that full tunnel clients will draw from, when they log on. You can click **Select** to open the Networks/Hosts Selector from which you can make your selection(s).
- Step 5** Specify the IP addresses of the primary and secondary (optional) DNS servers to be used for the Full Tunnel SSL VPN connection. You can click **Select** to open the Networks/Hosts Selector from which you can make your selections.
- Step 6** Specify the domain name of the DNS server to be used for the Full Tunnel SSL VPN connection.
- Step 7** Specify the IP addresses of the primary and secondary (optional) WINS servers to be used for the Full Tunnel SSL VPN connection. You can click **Select** to open the Networks/Hosts Selector from which you can make your selections.
- Step 8** Specify the traffic that will be secured or transmitted unencrypted across the public network, from these options:
- **Disable**—Split tunneling is disabled and no traffic will be secured.
 - **Exclude Specified Networks**—Split tunneling is enabled. You can specify the networks to which traffic is transmitted in the clear (unencrypted).
 - **Tunnel Specified Networks**—Split tunneling is enabled. All traffic from or to the specified networks will be secured.
- Step 9** If the device is an IOS router, specify the networks to which traffic will be transmitted secured or unencrypted, depending on the selected Split Tunneling option.
- Step 10** If the device is an IOS router, and if you selected the **Exclude Tunneling Specified Traffic** option, you can select **Exclude Local LAN** if you want to disallow a non split-tunneling connection to access the local subnetwork at the same time as the client.

- Step 11** If the device is an ASA security appliance, specify the access control lists (ACLs) to be used for split tunneling. You can click **Select** to open the Access Control Lists selector, from which you can select the required access control list.
- Step 12** Specify a list of domain names that must be tunneled or resolved to the private network. All other names will be resolved via the public DNS server.
- Step 13** Click **Next** to configure the Clientless and/or Thin Client access modes, or click **Finish** to complete the user group configuration.
-

Configuring the Clientless and Thin Client Access Modes

In Clientless access mode, the remote user accesses the internal or corporate network using a web browser on the client machine. No applet downloading is required. In Thin Client access mode, the client application to use TCP to connect to a well-known server and port. The remote user downloads a Java applet that acts as a TCP proxy on the client machine for the services that you configure on the SSL VPN gateway.

This procedure describes how to configure the Clientless and/or Thin Client access modes to be used in your SSL VPN user group configuration.



Note

You can configure these access modes only if you selected the **Clientless** and/or **Thin Client** options in Step 1 of the wizard. See [Defining the User Group Name and Access Methods](#), page 12-21.

Before You Begin

- In Device view (**View > Device View**), select the required device (Cisco IOS router or ASA device).

Related Topics

- [Clientless and Thin Client Access Modes Page](#), page I-13
- [Creating a New User Group](#), page 12-21
- [Defining the User Group Name and Access Methods](#), page 12-21
- [Configuring the Full Tunnel Access Mode](#), page 12-23
- [SSL VPN Access Modes](#), page 12-3

-
- Step 1** Open the Clientless and Thin Client page by clicking **Next** on the [Full Tunnel Access Mode Page, page I-10](#) of the Create User Group wizard. For a description of the elements on the Clientless and Thin Client page, see [Table I-6 on page I-14](#).



Note The elements displayed on this page depend on whether you selected to configure both Clientless and Thin Client access modes, or either one of them, in Step 1 of the wizard.

- Step 2** If you are configuring Clientless access mode, specify a list of websites that will be displayed on the portal page as a bookmark to enable users to access the resources available on the SSL VPN websites.
- You can click **Select** to open the URL List Selector from which you can make your selection from a list of URL List objects. For more information, see [Understanding URL List Objects, page 9-196](#).
- Step 3** If you are configuring Thin Client access mode, specify a Port Forwarding List, that defines the mapping of the port number on the client machine to the application's IP address and port behind the SSL VPN gateway.
- You can click **Select** to open the Port Forwarding List Selector from which you can make your selection from a list of Port Forwarding List objects. For more information, see [Understanding Port Forwarding List Objects, page 9-165](#).
- Step 4** If the device is an ASA security appliance, specify the Java applet that will be used as a TCP proxy on the client machine, and if required, select to download it.
- Step 5** If required, select the check box to enable a port-forwarding Java applet to be automatically downloaded when the remote client logs in.
- Step 6** Click **Finish** to complete the user group configuration and close the wizard.
- The new user group is displayed in the User Groups Selector page, from where you can select it for use in your SSL VPN. See [Creating a New User Group, page 12-21](#).
-

Configuring SSL VPN on an ASA Device

SSL VPN configuration is supported on Cisco ASA 5500 Series Security Appliances, software version 7.1 and 7.2.

**Note**

For security appliances running ASA 8.0 or 8.1, SSL VPN policies are not available for configuration from the Security Manager interface.

In an SSL VPN connection, the security appliance acts as a proxy between the end user web browser and target web servers. When an SSL VPN user connects to an SSL-enabled web server, the security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. The security appliance establishes a secure connection and validates the server SSL certificate.

Digital certificates are used for authentication. The security appliance creates a self-signed SSL server certificate when it boots, or you can install in the security appliance, an SSL certificate that has been issued in a PKI context (see [Public Key Infrastructure Policies in Remote Access VPNs, page 11-25](#)). For HTTPS, this certificate must then be installed on the client. You only need to install the certificate from a given security appliance once.

Using Security Manager, you can create a basic connection profile with a limited set of features that enable an SSL VPN to function, and then configure additional policies and features for your SSL VPN.

These topics describe how to configure an SSL VPN connection profile on an ASA device, and the policies required for it to function:

- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)
- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)

Using the Wizard to Create an ASA SSL VPN Connection Profile

The SSL VPN wizard provides a quick and convenient way to configure and enable SSL VPN on your ASA security appliance.

The wizard creates an SSL VPN connection profile with a limited set of features that enable a basic SSL VPN to function. After you complete the wizard, you can configure additional policies and features for the SSL VPN, or modify the existing ones. If required, you can return to the wizard to create additional SSL VPN configurations.

To access the ASA SSL VPN wizard:

1. Click the **Device View** button in the toolbar.
2. From the Device Selector, select the ASA device on which you want to configure SSL VPN.
3. Select **SSL VPN > SSL VPN Wizard** from the Policy selector.
4. Click **SSL VPN Server Wizard**.

These topics describe the steps you configure to define a basic SSL VPN connection profile using the ASA SSL VPN wizard:

- [Defining the ASA SSL VPN Access Parameters, page 12-28](#)
- [Defining the ASA SSL VPN Connection Profile Parameters, page 12-29](#)

Related Topics

- [Configuring SSL VPN on an ASA Device, page 12-27](#)

Defining the ASA SSL VPN Access Parameters

The Access page of the SSL VPN Configuration Wizard enables you to configure the security appliance interfaces for SSL VPN sessions and select a port for your SSL VPN connection profiles.

This procedure describes how to configure the access parameters on an ASA device.

Before You Begin

- In Device view (**View > Device View**), make sure the selected device is an ASA device.

Related Topics

- [Access Page \(ASA\), page I-23](#)
- [Configuring SSL VPN on an ASA Device, page 12-27](#)

- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)

Step 1 Select **View > Device View > SSL VPN > SSL VPN Wizard**, then click **SSL VPN Server Wizard**.

The wizard opens, displaying the Access page. For a description of the elements on this page, see [Table I-12 on page I-24](#).

Step 2 Specify the interfaces on which you want to enable the SSL VPN connection profiles. You can click **Select** to open a dialog box from which you can select an interface from a list of interface or interface role objects.

Step 3 Specify the port number that you want to use for SSL VPN sessions. You can click **Select** to open the Port List Selector dialog box from which you can make your selection.



Note The Portal Page URL field displays the URL that will appear on the Portal page to access the security appliance.

Step 4 Select **Allow Users to Select Connection Profile in Portal Page** to include a list of configured tunnel groups on the SSL VPN end-user interface from which the user can select a tunnel group at login.

Step 5 Select **Enable SSL VPN Access** to enable the SSL VPN functionality on the device.

Step 6 Click **Next** to advance to the next step of the wizard.



Note When you click **Finish** in the wizard, these parameters are displayed in the Access Policy page.

Defining the ASA SSL VPN Connection Profile Parameters

An SSL VPN connection profile comprises a set of records that contain VPN tunnel connection profile policies, including the attributes that pertain to creating the tunnel itself. When you define the parameters for your ASA SSL VPN connection profile, you configure a tunnel group policy. Tunnel groups identify the group policy for a specific connection profile, which includes user-oriented

attributes. In Security Manager, user parameters are captured by user groups which define the resources accessible to the user when connecting to the ASA security appliance.

For more information, see [Understanding SSL VPN Connection Profile Policies, page 12-33](#).

In the Connection Profile page of the SSL VPN wizard you configure the tunnel group policies on your security appliance.

This procedure describes how to configure a tunnel group policy, which includes specifying the associated user groups, address pools, and authentication server group settings.

Before You Begin

- In Device view (**View > Device View**), make sure the selected device is an ASA device.

Related Topics

- [Connection Profile Page \(ASA\), page I-25](#)
- [Understanding User Groups in SSL VPN, page 12-17](#)
- [Configuring User Groups on an ASA Device, page 12-19](#)
- [Configuring SSL VPN on an ASA Device, page 12-27](#)
- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)

Step 1 Open the Connection Profile page by clicking **Next** on the Access page of the SSL VPN wizard. For a description of the elements on the Connection Profile page, see [Table I-13 on page I-25](#).

Step 2 In the **Connection Profile** field, specify the name of the tunnel group that contains the policies for this SSL VPN connection profile.

Step 3 In the **Default User Group** field, specify the default user group policy associated with the device. The **Full Tunnel** field indicates whether full tunnel access mode was configured for the user group.

The default user group is used if no match is found when the AAA server tries to match the user group name to the names in the User Groups list on the ASA device. You can click **Select** to open a dialog box that lists all available ASA user groups, and from which you can create an ASA user group object. For more information, see [Understanding ASA User Group Objects, page 9-42](#).



Note If no default user group is defined, the device's built-in user group is used.

Step 4 Specify the user group(s) that will be used in your SSL VPN connection profile.



Note All SSL VPN connection profiles on an ASA device share one built-in user group. Each time you create a connection profile using the wizard, the User Groups list may be populated with data from the previous connection profile defined on the device.

You can click **Edit** to open the User Groups Selector, in which you can select the required ASA user groups, and from which you can create and edit ASA user groups. See [Configuring User Groups on an ASA Device, page 12-19](#).

- Step 5** In the **Portal Page Customization** field, specify the customization profile that defines the appearance of the portal page. You can click **Select** to make your selection from a list of SSL VPN customization objects. See [Understanding SSL VPN Customization Objects, page 9-203](#).
- Step 6** Specify the group URL that is associated with the tunnel group connection profile.
- Step 7** Specify up to 6 address pools from which IP addresses will be assigned. The server uses these pools in the order listed.
- Step 8** From the **Authentication Method** list, select the type of authentication to perform—**AAA** (the default), **Certificate** or **Both** (AAA and Certificate authentication).
- Step 9** Specify the name of the server group to be used for user authentication (LOCAL if the tunnel group is configured on the local device). You can click **Select** to make your selection from a list of AAA Server Group objects.
- Step 10** If you selected LOCAL for the authentication server group, select the check box to enable fallback to the local database for authentication if the selected authentication server group fails.
- Step 11** Specify the name of the authorization server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to make your selection from a list of AAA Server Group objects.
- Step 12** Specify the name of the accounting server group. You can click **Select** to make your selection from a list of AAA Server Group objects.

- Step 13** When you have completed configuring the connection profile policy, click **Finish** to close the SSL VPN Configuration wizard.

The SSL VPN connection profile you have defined in the wizard is displayed in the SSL VPN Connection Profile Policy page. You can modify this connection profile, if required. See [Configuring SSL VPN Policies on an ASA Device, page 12-32](#).

Configuring SSL VPN Policies on an ASA Device

After you create a basic SSL VPN connection profile on your server device using the SSL VPN wizard, you can modify the connection profile, if required, and configure additional policies and features.

These topics describe the SSL VPN policies you can configure on an ASA device:

- [Configuring an Access Policy, page 12-32](#)
- [Configuring an SSL VPN Connection Profile Policy, page 12-35](#)
- [Configuring ASA User Groups Policy in Your SSL VPN, page 12-42](#)
- [Configuring the Cisco Secure Desktop Software, page 12-44](#)
- [Configuring Global Settings, page 12-45](#)

Related Topics

- [Using the Wizard to Create an ASA SSL VPN Connection Profile, page 12-27](#)

Configuring an Access Policy

An Access policy specifies the security appliance interfaces on which an SSL VPN connection profile can be enabled, the port to be used for the connection profile, the SSL VPN session timeout and maximum number of sessions.

This procedure describes how to configure an Access policy on an ASA device.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device).

Related Topics

- [SSL VPN Access Policy Page, page I-29](#)
- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)

-
- Step 1** Select **View > Device View > SSL VPN > Access** from the Policy selector. The Access page appears. For a description of the elements on this page, see [Table I-14 on page I-29](#).
- Step 2** Specify the interfaces on which you want to enable SSL VPN connection profiles. You can click **Select** to open a dialog box from which you can select an interface from a list of interface or interface role objects.
- Step 3** Specify the port number that you want to use for SSL VPN sessions. You can click **Select** to open the Port List Selector dialog box from which you can make your selection.
- Step 4** Specify the amount of time, in seconds, that an SSL VPN session can be idle before the security appliance terminates the session.
- Step 5** Specify the maximum number of SSL VPN sessions you want to allow.
- Step 6** Select the **Allow Users to Select Connection Profile in Portal Page** check box to include a list of the configured tunnel groups on the SSL VPN end-user interface, from which users can select a tunnel group when they log on.
- Step 7** Select the **Enable SSL VPN Access** check box to enable the SSL VPN functionality on the device.
- Step 8** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Understanding SSL VPN Connection Profile Policies



Note For a description of the procedure to configure an SSL VPN Connection Profiles policy, see [Configuring SSL VPN on an ASA Device, page 12-27](#).

An SSL VPN connection profile comprises a set of records that contain VPN tunnel connection profile policies, including the attributes that pertain to creating the tunnel itself. When you define the parameters for your ASA SSL VPN connection profile, you configure a tunnel group policy. Tunnel groups identify the group policy for a specific connection profile, which includes user-oriented attributes. User parameters are captured by user groups which define the resources accessible to the user when connecting to the ASA security appliance.

You can create one or more tunnel groups specific to your environment. Tunnel groups may be configured on the local remote access VPN server or on external AAA servers. Configuring a tunnel group policy includes specifying the associated user groups, address pools, servers, and authentication server group settings.

About Group Aliases

When configuring an SSL VPN Connection Profile policy, you may specify group aliases for your tunnel group. Specifying a group alias creates one or more alternate names by which a user can refer to a tunnel group. This feature is useful when the same group is known by several common names (such as “Devtest” and “QA”). The group alias appears on the login page. If you want the actual name of the tunnel group to appear on the list, you must specify it as an alias. Each tunnel group can have multiple aliases or no alias.

About Group URLs

Specifying a group URL eliminates the need for the user to select a tunnel group at login. When a user logs in, the security appliance looks for the user’s incoming URL in the tunnel group policy table. If it finds the URL and if this feature is enabled, the security appliance selects the appropriate server and presents the user with only the username and password fields in the login window. This simplifies the user interface and has the added advantage of never exposing the list of groups to the user. The login window that the user sees uses the customizations configured for that tunnel group. You can configure multiple URLs (or no URLs) for a tunnel group. Each URL can be enabled or disabled individually. You must use a separate specification for each URL, specifying the entire URL using either the HTTP or HTTPS protocol.

Related Topics

- [Configuring an SSL VPN Connection Profile Policy, page 12-35](#)
- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)

- [SSL VPN Connection Profiles Policy Page, page I-31](#)

Configuring an SSL VPN Connection Profile Policy

The SSL VPN Connection Profiles Policy page displays a list of all the SSL VPN Connection Profile policies currently defined on the security appliance, including any policies that were created using the wizard. From this page, you can create, edit, or delete the policies.

These topics enable you to configure SSL VPN Connection Profile policies on an ASA device:

- [Defining Basic Parameters, page 12-35](#)
- [Defining AAA Parameters, page 12-37](#)
- [Defining Servers and Address Pools, page 12-40](#)

Related Topics

- [SSL VPN Connection Profiles Policy Page, page I-31](#)
- [Understanding SSL VPN Connection Profile Policies, page 12-33](#)

Defining Basic Parameters

The Basic settings you must define for an SSL VPN Connection Profile policy include specifying a name for the tunnel group, the user group policy, address pools for available for assignment throughout the policy, the DNS server to be used for the tunnel group, group aliases, and incoming group URLs.

For more information about these settings, see [Understanding SSL VPN Connection Profile Policies, page 12-33](#).

This procedure describes how to create or edit the basic settings required for an SSL VPN Connection Profile policy.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.

Related Topics

- [Understanding SSL VPN Connection Profile Policies, page 12-33](#)
- [Configuring an SSL VPN Connection Profile Policy, page 12-35](#)

- [Basic Tab \(ASA\), page I-33](#)

-
- Step 1** Select **View > Device View > SSL VPN > Connection Profiles**.
- The SSL VPN Connection Profiles policy page opens. For a description of the elements on this page, see [Table I-15 on page I-31](#).
- Step 2** Click **Create** on the SSL VPN Connection Profiles policy page, or select the row of a policy in the table on the page, and click **Edit**.
- The Add/Edit SSL VPN Connection Profile dialog box opens, displaying the **Basic** tab. For a description of the elements on the **Basic** tab, see [Table I-16 on page I-33](#).
- Step 3** In the **Connection Profile Name** field, specify the name or IP address of the tunnel group that contains the policies for this SSL VPN connection profile.
- Step 4** If required, specify the default user group to be associated with the device.
- You can click **Select** to open a dialog box from which you can select a user group from a list of ASA user group objects. For more information, see [Understanding ASA User Group Objects, page 9-42](#).
- Step 5** If required, specify an alternate user group to be applied to the tunnel group.
- You can click **Select** to open a dialog box from which you can select a user group from a list of ASA user group objects. For more information, see [Understanding ASA User Group Objects, page 9-42](#).
- Step 6** Specify the DNS group to use for the tunnel group. The DNS group resolves the hostname to the appropriate DNS server for the tunnel group.
- Step 7** Specify up to 6 address pools from which the client IP addresses will be assigned.
- Address pools are predefined network objects. You can click **Select** to open the Network/Hosts selector from which you can make your selection(s). For more information, see [Understanding Network/Host Objects, page 9-144](#).
- Step 8** From the Group Aliases table, you can create a new group alias or edit an existing one, as follows:
- Click **Create** below the table, or select a group alias in the table and click **Edit**. The Add/Edit Group Alias dialog box opens. For a description of the elements on this dialog box, see [Table I-17 on page I-36](#).
 - Select the **Enabled** check box (by default it is selected).
 - In the **Group Alias** field, specify an alternative name for the tunnel group.

- Click **OK** to save the changes, or **Cancel** to cancel the operation.

Step 9 From the Group URLs table, you can create a new group URL or edit an existing one, as follows:

- Click **Create** below the table, or select a group URL in the table and click **Edit**. The Add/Edit Group URL dialog box opens. For a description of the elements on this dialog box, see [Table I-18 on page I-37](#).
- Select the **Enabled** check box (by default it is selected).
- In the **Group URL** field, select a protocol (http or https) from the list, and specify the incoming URL for the group.
- Click **OK** to save the changes, or **Cancel** to cancel the operation.



Note If you want to delete a group alias or group URL from a table, select it and click **Delete**.

Step 10 When you have finished configuring the basic settings of your SSL VPN Connection Profile policy, click **OK** to save your changes locally on the client and close the Add/Edit SSL VPN Connection Profile dialog box. Alternatively, you can click the **AAA** or **Settings** tabs to continue the Connection Profile policy configuration.

Defining AAA Parameters

When you define the AAA authentication parameters for your SSL VPN Connection Profile policy, you must specify the type of authentication, the authorization, authentication, and accounting server groups, parameters relevant to password management, values for usernames that the security appliance recognizes for authorization, and configure interface-specific server groups for authentication.

This procedure describes how to create or edit the AAA authentication parameters required for an SSL VPN Connection Profile policy.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.

Related Topics

- [Understanding SSL VPN Connection Profile Policies, page 12-33](#)
- [Configuring an SSL VPN Connection Profile Policy, page 12-35](#)
- [AAA Tab \(ASA\), page I-37](#)

-
- Step 1** Select **View > Device View > SSL VPN > Connection Profiles**.
- The SSL VPN Connection Profiles policy page opens. For a description of the elements on this page, see [Table I-15 on page I-31](#).
- Step 2** Click **Create** on the SSL VPN Connection Profiles policy page, or select the row of a policy in the table on the page, and click **Edit**.
- The Add/Edit SSL VPN Connection Profile dialog box opens.
- Step 3** Click the **AAA** tab. For a description of the elements on the AAA tab of the Add/Edit SSL VPN Connection Profile dialog box, see [Table I-19 on page I-38](#).
- Step 4** From the **Authentication** list, select the type of authentication to perform—**AAA** (the default), **Certificate** or **Both** (AAA and Certificate authentication).
- Step 5** Specify the name of the server group to be used for user authentication (LOCAL if the tunnel group is configured on the local device). You can click **Select** to make your selection from a list of AAA Server Group objects.
- Step 6** If you selected LOCAL for the authentication server group, select the check box to enable fallback to the local database for authentication if the selected authentication server group fails.
- Step 7** Specify the name of the authorization server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to make your selection from a list of AAA Server Group objects.
- Step 8** To enable authorization on the local device, select the **LOCAL Authorization** check box.
- Step 9** Select the **Users Must Exist in the Authorization Database to Connect** check box, if you want the security appliance to allow only users in the authorization database to connect.
- Step 10** Specify the name of the accounting server group. You can click **Select** to make your selection from a list of AAA Server Group objects.
- Step 11** For users that authenticate with digital certificates and require LDAP or RADIUS authorization, you can set values for the usernames that the security appliance recognizes for authorization, as follows:

- **Use the Entire DN as the Username**—Select to allow the use of the entire Distinguished Name (DN) as the identifier for the username.
- **Specify Individual DN Fields as the Username**—Select to enable the use of individual DN fields as the username when matching users to the tunnel group.

Then select one of the following options:

- **Primary DN Field**—Select the primary DN field identifier to be used for identification.
- **Secondary DN Field**—Select the secondary DN field identifier to be used for identification.



Note Select **None** if no secondary field identifier is required.

- Step 12** Select the **Override Account-Disabled Indication from AAA Server** check box to override the “account-disabled” indicator from a AAA server. This configuration is valid for servers, such as RADIUS with NT LDAP, and Kerberos, that return an “account-disabled” indication.



Note Allowing override account-disabled is a potential security risk.

- Step 13** Select the **Enable Notification Upon Password Expiration to Allow User to Change Password** check box, to enable the security appliance to notify the remote user at login that the current password is about to expire or has expired.
- Step 14** Select the **Enable Notification Prior to Expiration** check box, to warn the user about the pending expiration, and specify the number of days (1-180) before the current password expires in the **Notify Prior to Expiration** field.
- Step 15** From the **Interface-Specific Authentication Server Groups** table, you can configure interface-specific authentication for your SSL VPN connection profile policy, as follows:
- Click **Create** below the table, or select a row in the table and click **Edit**. The Add/Edit SSL VPN Interface Specific Authentication Server Groups dialog box opens. For a description of the elements on this dialog box, see [Table I-20 on page I-42](#).
 - Specify the interface to be associated with the authentication server group.

- Specify the server group to be associated with the selected interface.
- Select **Use LOCAL if Server Group Fails** to enable fallback to the LOCAL database if the selected server group fails.
- Click **OK** to save the changes, or **Cancel** to cancel the operation.

**Note**

If you want to delete an interface-specific authentication server group from the table, select it and click **Delete**.

- Step 16** When you have finished configuring the AAA parameters for your SSL VPN Connection Profile policy, click **OK** to save your changes locally on the client and close the Add/Edit SSL VPN Connection Profile dialog box. Alternatively, you can click the **Basic** or **Settings** tabs to continue the Connection Profile policy configuration.
-

Defining Servers and Address Pools

The Settings tab lets you configure the WINS servers for the connection profile policy, select a customized look and feel for the SSL VPN end-user logon web page, DHCP servers to be used for client address assignment, and establish an association between an interface and client IP address pools.

This procedure describes how to create or edit these settings for an SSL VPN Connection Profile policy.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.

Related Topics

- [Understanding SSL VPN Connection Profile Policies](#), page 12-33
- [Configuring an SSL VPN Connection Profile Policy](#), page 12-35
- [Settings Tab \(ASA\)](#), page I-42

-
- Step 1** Select **View > Device View > SSL VPN > Connection Profiles**.

The SSL VPN Connection Profiles policy page opens. For a description of the elements on this page, see [Table I-15 on page I-31](#).

Step 2 Click **Create** on the SSL VPN Connection Profiles policy page, or select the row of a policy in the table on the page, and click **Edit**.

The Add/Edit SSL VPN Connection Profile dialog box opens.

Step 3 Click the **Settings** tab. For a description of the elements on the Settings tab of the Add/Edit SSL VPN Connection Profile dialog box, see [Table I-21 on page I-43](#).

Step 4 Specify the name of the WINS servers list to use for CIFS name resolution.

Step 5 Specify the SSL VPN customization profile that defines the appearance of the portal page.

Step 6 Specify the IP addresses of up to 10 DHCP servers to be used for client address assignments.

Step 7 From the **Client IP Address Pool** table, you can specify client IP address pools on an interface-specific basis, which override the global IP address pools (configured on the Basic tab), as follows:

- Click **Create** below the table, or select a row in the table and click **Edit**. The Add/Edit SSL VPN Interface Specific Client Address Pools dialog box opens. For a description of the elements on this dialog box, see [Table I-22 on page I-45](#).
- Specify the address pool to be used to assign a client address to the selected interface.
- Specify the IP address pool to be used to assign server group to be associated with the selected interface.
- Click **OK** to save the changes, or **Cancel** to cancel the operation.



Note If you want to delete a client IP address pool from the table, select it and click **Delete**.

Step 8 When you have finished configuring these settings for your SSL VPN Connection Profile policy, click **OK** to save your changes locally on the client and close the Add/Edit SSL VPN Connection Profile dialog box. Alternatively, you can click the **Basic** or **AAA** tabs to continue the Connection Profile policy configuration.

Configuring ASA User Groups Policy in Your SSL VPN

When you configure an SSL VPN connection profile, you must create user groups to which remote clients will belong. A user group policy specifies the attributes that determine user access to, and use of the SSL VPN. User groups simplify system management, enabling you to quickly configure SSL VPN access for large numbers of users.

A user group policy is a set of user-oriented attribute/value pairs for SSL VPN connection profiles that are stored either internally (locally) on the device or externally on an AAA server. The tunnel group uses a user group policy that sets terms for user connection profiles after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.



Note

If more than one user group policy is configured on a device, you must configure the device to use an AAA server to authenticate users and to determine which user group a particular user belongs to.

An ASA security appliance has a built-in user group. During SSL VPN user authentication, the AAA server returns a user group name that the user belongs to. The device first tries to match the name to the names in the User Groups list. If a match is found, the definition in the matching user group is used. Otherwise, the default user group is used. If no default user group is defined, the device's built-in user group is used.

The ASA User Groups Policy page displays the ASA user groups currently defined for your SSL VPN connection profile. From this page you can create new user group policies and edit existing ones. In Security Manager, ASA user groups are predefined objects. When creating an ASA User Groups policy, you may need to select one or more objects to include in the policy definition.

This procedure describes how to specify the user groups you want to assign to your SSL VPN connection profile on an ASA device.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.

Related Topics

- [ASA User Groups Policy Page, page I-46](#)

- [Configuring SSL VPN Policies on an ASA Device, page 12-32](#)
- [Understanding ASA User Group Objects, page 9-42](#)

Step 1 Select **View > Device View > SSL VPN > User Groups** from the Policy selector. The ASA User Groups Policy page opens, displaying a table listing the ASA user groups defined for your SSL VPN. For a description of the elements on this page, see [Table I-23 on page I-46](#).

Step 2 To add an ASA user group to the list:

- a. Click **Create** below the table.

ASA user groups are predefined objects. The Add User Group Selector opens, displaying a list of available ASA user group objects. For a description of the elements in this selector, see [Creating and Editing Deployment Jobs, page 19-36](#).

- b. Select the required ASA user group in the list. The selected user group is displayed in the **Selected** field.
- c. If the required user group is not included in the Add User Group Selector list, click **Create** to open a dialog box that enables you to create or edit an ASA user group object.



Note You can also edit the properties of an ASA user group from the Add User Group Selector, by selecting it and clicking the **Edit** button.

For information on how to create or edit an ASA user group object, see [Creating ASA User Group Objects, page 9-44](#).

- d. Click **OK** to close the Add User Group Selector. The newly selected ASA user group is displayed in the table on the ASA User Groups Policy page.

Step 3 To modify the properties of an ASA user group displayed in the ASA User Groups Policy page, select the ASA user group in the table, and click **Edit**.

The Edit ASA User Group dialog box opens, enabling you to edit the selected ASA user group object. For more information, see [Creating ASA User Group Objects, page 9-44](#).

Step 4 When you have finished configuring the ASA user groups for your SSL VPN connection profile, click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Configuring the Cisco Secure Desktop Software

Cisco Secure Desktop (CSD) enables you to eliminate all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. This ensures that cookies, browser history, temporary files, and downloaded content do not remain on a system after a remote user logs out or an SSL VPN session times out. CSD increases protection against data theft and client system malware (malicious software) by encrypting all data and files associated with or downloaded during the SSL VPN session.

CSD encrypts all information in the session. This protection is valuable in case of an abrupt session termination, or if a session times out due to inactivity. Furthermore, CSD stores all session information in the secure vault desktop partition. When the session closes, CSD overwrites and removes all data using a U.S. Department of Defense (DoD) sanitation algorithm to provide endpoint security protection.

This procedure describes how to configure the CSD on an ASA device. For the procedure to configure CSD on an IOS router, see [Configuring the Secure Desktop Software for an IOS SSL VPN Policy, page 12-15](#).

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure the Secure Desktop Client software is installed and activated on the device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Understanding Secure Desktop Configuration Objects, page 9-171](#).
- [Configuring the Secure Desktop Software for an IOS SSL VPN Policy, page 12-15](#)
- [Cisco Secure Desktop Page \(ASA\), page I-48](#)

-
- Step 1** In Device view, select **SSL VPN > Cisco Secure Desktop** from the Policy selector. The Cisco Secure Desktop policy page opens.
- Step 2** Select the **Enable** check box to enable CSD on the ASA device.
- Step 3** In the **Configuration** field, specify the filename of the CSD distribution package to install into the running configuration (the `securedesktop_asa_<n>_<n>*.pkg` file to be uploaded from your local computer to the flash device).
- You can click **Select** to open the Secure Desktops Selector from which you can select a CSD distribution package file from a list of available CSD distribution package objects. See [Understanding Secure Desktop Configuration Objects, page 9-171](#).
- Step 4** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Configuring Global Settings

In Security Manager, you can define SSL VPN global settings that apply to all devices in your SSL VPN topology. These settings include caching, content rewriting, character encoding, proxy, and proxy bypass definitions.

These topics describe how to configure these global VPN settings:

- [Defining Performance Settings, page 12-46](#)
- [Defining Content Rewrite Rules, page 12-47](#)
- [Defining Encoding Rules, page 12-49](#)
- [Defining Proxies and Proxy Bypass Rules, page 12-51](#)
- [Defining Advanced Settings, page 12-53](#)

Defining Performance Settings

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

This procedure describes how to enable caching on your ASA security appliance.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Configuring Global Settings, page 12-45](#)
- [Performance Tab, page I-50](#)

Step 1 Select **View > Device View > SSL VPN > Global Settings** from the Policy selector.

The Global Settings page opens, displaying the Performance tab. For a description of the elements on this tab, see [Table I-26 on page I-50](#).

Step 2 Select the **Enable** check box to enable caching on the security appliance.

Step 3 Specify the minimum size document that the security appliance can cache. The range is 0-10000 Kb. The default is 0 Kb.



Note The maximum object size must be greater than the minimum object size.

Step 4 Specify the maximum size document that the security appliance can cache. The range is 0 to 10000 Kb. The default is 1000 Kb.

Step 5 Specify an integer to set a revalidation policy for caching objects that have only the last-modified timestamp, and no other server-set expiration values. The range is 1-100. The default is 20.

Step 6 Enter an integer to set the number of minutes to cache objects without revalidating them. Valid values range from 0 to 900. The default is one minute.

- Step 7** Select the **Cache Compressed Content** check box to cache compressed content.
- Step 8** Select the **Cache Static Content** check box to cache static content.
- Step 9** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Defining Content Rewrite Rules

SSL VPN processes application traffic through a content transformation/rewriting engine that includes advanced elements (such as, JavaScript, VBScript, Java, and multi-byte characters) to proxy HTTP traffic depending on whether the user is using an application within or independently of an SSL VPN device.

If you do not want some applications and web resources, such as public websites, to go through the security appliance, you can create rewrite rules that permits users to browse certain sites and applications without going through the security appliance itself. This is similar to split tunneling in an IPsec VPN connection.

In the Content Rewrite tab of the SSL VPN Global Settings page, you can configure multiple content rewrite rules. The Content Rewrite tab lists all applications for which content rewrite is enabled or disabled.



Note The security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

From this tab, you can create or edit content rewrite rules, as described in the following procedure.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Configuring Global Settings, page 12-45](#)

- [Content Rewrite Tab, page I-52](#)
- [Add/Edit Content Rewrite Dialog Box, page I-53](#)

-
- Step 1** Select **View > Device View > SSL VPN > Global Settings** from the Policy selector.
- Step 2** On the Global Settings page, click the **Content Rewrite** tab. The Content Rewrite tab opens, displaying all applications for which content rewrite is enabled or disabled. For a description of the elements on this tab, see [Table I-27 on page I-52](#).
- Step 3** On the Content Rewrite tab, click **Create**, or select a rewrite rule in the table and click **Edit**.
- The Add/Edit Content Rewrite dialog box opens. For a description of the elements in this dialog box, see [Table I-28 on page I-54](#).
- Step 4** Select the **Enable** check box to enable content rewrite for this rewrite rule.
- Step 5** Enter a number for this rule. This number specifies the position of the rule in the list. Rules without a number are at the end of the list. The range is 1 to 65534.
- Step 6** Enter an alphanumeric string that describes the rule, maximum 128 characters.
- Step 7** Enter the name of the application or resource to which the rule applies (up to 300 characters).
- Step 8** Click **OK**. The Add Content Rewrite Rule dialog box closes, and the content rewrite rule is added to the table.



Note If you want to delete a content rewrite rule from a table, select it and click **Delete**.

- Step 9** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Defining Encoding Rules

Character encoding is the pairing of raw data (such as 0's and 1's) with characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the remote user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly.

The encoding attribute lets you specify the value of the character encoding method in the SSL VPN portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, or any changes made to the browser.

The character encoding attribute is a global setting that, by default, all SSL VPN portal pages inherit. However, you can override the file-encoding attribute for Common Internet File System (CIFS) servers that use character encoding that differs from the value of the character-encoding attribute. You can use different file-encoding values for CIFS servers that require different character encodings.

The SSL VPN portal pages downloaded from the CIFS server to the SSL VPN user encode the value of the SSL VPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the proper character set to use. The SSL VPN portal pages do not specify a value if SSL VPN configuration does not specify a file encoding entry for the CIFS server and the character encoding attribute is not set. The remote browser uses its own default encoding if the SSL VPN portal page does not specify the character encoding, or if it specifies a character encoding value that the browser does not support.

In the Encoding tab of the SSL VPN Global Settings page, you can view the currently configured character sets associated with the CIFS server to be encoded in the portal pages. From this tab, you can create or edit the character sets, as described in the following procedure.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Configuring Global Settings, page 12-45](#)
- [Encoding Tab, page I-55](#)
- [Add/Edit File Encoding Dialog Box, page I-57](#)

-
- Step 1** Select **View > Device View > SSL VPN > Global Settings** from the Policy selector.
- Step 2** On the Global Settings page, click the **Encoding** Tab. For a description of the elements on this tab, see [Table I-29 on page I-55](#).
- Step 3** From the **Global SSL VPN Encoding Type** list, select the attribute that determines the character encoding that all SSL VPN portal pages inherit, except for those from the CIFS servers listed in the table.



Note If you choose **none** or specify a value that the browser on the SSL VPN client does not support, it uses its own default encoding.

- Step 4** Click **Create**, or select a character set in the table and click **Edit**.
The Add/Edit File Encoding dialog box opens. For a description of the elements in this dialog box, see [Table I-30 on page I-58](#).
- Step 5** In the **CIFS Server** field, enter the name or IP address of each CIFS server for which the encoding requirement differs from the **Global SSL VPN Encoding Type** attribute setting.
CIFS servers are predefined network objects. You can click **Select** to open the Network/Hosts Selector dialog box that lists all available network hosts, and in which you can create network host objects.
- Step 6** From the **Encoding Type** list, select the character encoding that the CIFS server should provide for SSL VPN portal pages.
- Step 7** Click **OK**. The Add/Edit File Encoding dialog box closes, and the newly created or edited character set is added to the table.



Note If you want to delete a character set from a table, select it and click **Delete**.

- Step 8** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Defining Proxies and Proxy Bypass Rules

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



Note The HTTP/HTTPS proxy does not support connections to personal digital assistants.

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

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

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

In the Proxy tab of the SSL VPN Global Settings page, you can view the currently configured proxy bypass rules, create new rules or edit the existing ones, as described in the following procedure.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Configuring Global Settings, page 12-45](#)
- [Defining Content Rewrite Rules, page 12-47](#)
- [Proxy Tab, page I-58](#)
- [Add/Edit Proxy Bypass Dialog Box, page I-60](#)

-
- Step 1** Select **View > Device View > SSL VPN > Global Settings** from the Device Policies selector.
- Step 2** On the Global Settings page, click the **Proxy** Tab. For a description of the elements on this tab, see [Table I-31 on page I-59](#).
- Step 3** Specify the IP address of the external HTTP proxy server to which the security appliance forwards HTTP connections. You can click **Select** to make your selection from a list of network host objects.
- Step 4** Specify the port that listens for HTTP requests. The default port is 80. You can click **Select** to make your selection from the Port List Selector dialog box.
- Step 5** Specify the IP address of the external HTTPS proxy server to which the security appliance forwards HTTP connections. You can click **Select** to make your selection from a list of network host objects.
- Step 6** Specify the port that listens for HTTPS requests. The default port is 443. You can click **Select** to make your selection from the Port List Selector dialog box.
- Step 7** Under the Proxy Bypass table, click **Create**, or select a rule in the table and click **Edit**.
- The Add/Edit Proxy Bypass dialog box opens. For a description of the elements in this dialog box, see [Table I-32 on page I-61](#).
- Step 8** Specify the name of the interface on the security appliance for proxy bypass. You can click **Select** to make your selection from a list of interface and interface role objects.
- Step 9** Select the required **Bypass Traffic** option, as follows:
- **On Port**—To specify a port number to be used for proxy bypass. Valid port numbers are 20000-21000. You can click **Select** to open the Port List Selector dialog box from which you can make your selection.
 - **Match Specifying Pattern**—To specify a URL path to match for proxy bypass.

- Step 10** In the **URL** field, select the **http** or **https** protocol, and enter the URL to which you want to apply proxy bypass.
- Step 11** Select the **Rewrite XML** check box to rewrite XML sites and applications to be bypassed by the security appliance.
- Step 12** Select the **RewriteHostname** check box to rewrite absolute external links.



Note You can configure the security appliance to perform no content rewriting, or rewrite XML links, or a combination of XML and links.

- Step 13** Click **OK**. The Add Proxy Bypass Rule dialog box closes, and the proxy bypass rule is added to the table.



Note If you want to delete a proxy bypass rule from the table, select it and click **Delete**.

- Step 14** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.

Defining Advanced Settings

The Advanced tab lets you configure the amount of security appliance memory that SSL VPN can use for its sessions.

Before You Begin

- In Device view (**View > Device View**), select the required ASA device.
- Make sure a connection profile policy has been configured on the device. See [Configuring an SSL VPN Connection Profile Policy, page 12-35](#).

Related Topics

- [Configuring Global Settings, page 12-45](#)
- [Advanced Tab, page I-62](#)

-
- Step 1** Select **View > Device View > SSL VPN > Global Settings** from the Device Policies selector.
- Step 2** On the Global Settings page, click the **Advanced** Tab. For a description of the elements on this tab, see [Table I-33 on page I-63](#).
- Step 3** Specify the amount of memory that you want to allocate to the SSL VPN processes, either as a percentage of total memory or in kilobytes. The default percentage is 50%. Different ASA models have different total amounts of memory.



Note When you change the memory size, the new setting takes effect only after the system reboots.

- Step 4** Click **Save** to save your changes to the server.



Note To publish your changes, click the **Submit** button on the toolbar.
