CHAPTER 19

Cisco IOS SSL VPN

Cisco IOS SSL VPN provides Secure Socket Layer (SSL) VPN remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. This enables companies to extend their secure enterprise networks to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS SSL VPN also enables access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hotspots, where an IT department cannot easily deploy and manage the VPN client software necessary for IPsec VPN connections.

There are three modes of SSL VPN access: clientless, thin-client and full-tunnel client. Cisco SDM supports all three. Each mode is described below:

- **Clientless SSL VPN**—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to use within a web browser, such as intranet access, and online tools that employ a web interface.
- **Thin Client SSL VPN** (port-forwarding Java applet)—Thin Client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as POP3, SMTP, IMAP, Telnet, and SSH.
- **Full Tunnel Client SSL VPN**—Full tunnel client mode offers extensive application support through its dynamically downloaded SSL VPN client software for Cisco IOS SSL VPN. With the Full tunnel Client for Cisco IOS SSL VPN, we delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that allows network layer connectivity access to virtually any application.

Cisco IOS SSL VPN Contexts, Gateways, and Policies describes how the components of a Cisco IOS SSL VPN configuration work together.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

Cisco IOS SSL VPN links on Cisco.com

This help topic lists the current links that provide the most useful information on Cisco IOS SSL VPN.

The following link provides access to documents that describe Cisco IOS SSL VPN. Return to this link from time to time for the latest information.

www.cisco.com/go/iosSSLVPN

The following link explains how to configure a AAA server using the RADIUS protocol for Cisco IOS SSL VPN.

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Create SSL VPN

You can use Cisco IOS SSL VPN wizards to create a new Cisco IOS SSL VPN or to add new policies or features to an existing Cisco IOS SSL VPN.

Click Cisco IOS SSL VPN to get an overview of the features that Cisco SDM supports. Cisco IOS SSL VPN Contexts, Gateways, and Policies describes how the components of a Cisco IOS SSL VPN configuration work together.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

Prerequisite Tasks

AAA and certificates must be configured on the router before you can begin a Cisco IOS SSL VPN configuration. If either or both of these configurations are missing, a notification appears in this area of the window, and a link is provided that enables you to complete the missing configuration. When all prerequisite configurations are complete, you can return to this window and start configuring Cisco IOS SSL VPN.

Cisco SDM enables AAA without user input. Cisco SDM can help you generate public and private keys for the router, and enroll them with a certification authority to obtain digital certificates. See Public Key Infrastructure for more information. Alternatively, you can configure a persistent self-signed certificate that does not require approval by a CA. For more information on the persistent self-signed certificate feature, see the information at this link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Make sure that the entire URL is present in the link field in your browser.

Create a new SSL VPN

Select this option to create a new Cisco IOS SSL VPN configuration. This wizard enables you to create a Cisco IOS SSL VPN with one user policy and a limited set of features. After you complete this wizard, you can use the other wizards to configure addition policies and features for the Cisco IOS SSL VPN. You can return to this wizard to create additional Cisco IOS SSL VPN configurations.

When you use Cisco SDM to create the first Cisco IOS SSL VPN configuration on a router, you create a Cisco IOS SSL VPN context, configure a gateway, and create a group policy. After you complete the wizard, click **Edit SSL VPN** to view the configuration and familiarize yourself with how Cisco IOS SSL VPN components work together. For information that will help you understand what you see, click Cisco IOS SSL VPN Contexts, Gateways, and Policies.

Add a new policy to an existing SSL VPN for a new group of users

Select this option to add a new policy to an existing Cisco IOS SSL VPN configuration for a new group of users. Multiple policies allow you to define separate sets of capabilities for different groups of users. For example, you might define a policy for engineering, and a separate policy for sales.

Configure advanced features for an existing SSL VPN

Select this option to configure additional features for an existing Cisco IOS SSL VPN policy. You must specify the context under which this policy is configured.

Launch the selected task button

Click to begin the configuration that you selected. You will receive a warning message if you cannot complete the task that you chose. If there is a prerequisite task that you need to complete, you will be told what it is and how to complete it.

Persistent Self-Signed Certificate

You can provide the information for a persistent self-signed certificate in this dialog. Using the information that you provide, the HTTPS server will generate a certificate that will be used in the SSL handshake. Persistent self-signed certificates remain in the configuration even if the router is reloaded, and are presented during the SSL handshake process. New users must manually accept these certificates, but users who have previously done so do not have to accept them again if the router was reloaded.

For more information on the persistent self-signed certificate feature, see the information at this link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Make sure that the entire URL is present in the link field in your browser.

Name

Cisco SDM places the name Router_Certificate in this field. You can change the name if you want to do so. This corresponds to the subject name that would be used in a certificate request.

Length of RSA Key

Cisco SDM places the value 512 in this field. You can specify a longer key, such as 1024, if you want to do so. The key length should be a multiple of 64.

Subject

Provide the information for the fields in the subject area. For more information on these fields, see the information in Other Subject Attributes.

Generate Button

After providing the information in this window, click **Generate** to have the router create the persistent self-signed certificate.

Welcome

The Welcome window for each wizard lists the tasks that the wizard enables you to complete. Use this information to ensure that you are using the correct wizard. If you are not, click **Cancel** to return to the Create SSL VPN window and choose the wizard that you want to use.

When you provide all the information asked for by the wizard, the Summary window displays the information that you provided. To see the Cisco IOS CLI commands that you are delivering to the router, click **Cancel** to leave the wizard, and go to **Edit** > **Preferences**, and check **Preview commands before delivering to router.** Then restart the wizard and provide the information that it asks for. When you deliver the configuration to the router, an additional window is displayed that allows you to view the Cisco IOS CLI commands you are delivering.

SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides the IP address and the digital certificate for the SSL VPN contexts that use it. You can provide the information for a gateway in this window, and the information that will allow users to access a portal.

IP Address and Name Fields

Use these fields to create the URL that users will enter to access the Cisco IOS SSL VPN portal. The IP address list contains the IP addresses of all configured router interfaces, and all existing Cisco IOS SSL VPN gateways. You can use the IP address of a router interface if it is a public address that the intended clients can reach, or you can use another public IP address that the clients can reach.

If you use an IP address that has not already been used for a gateway, you create a new gateway.

Allow Cisco SDM access through *IP Address* Checkbox

Check if you want to continue to access Cisco SDM from this IP address. This checkbox appears if you entered the IP address you are currently using to access Cisco SDM.

Note If you check this checkbox, the URL that you must use to access Cisco SDM changes after you deliver the configuration to the router. Review the information area at the bottom of the window to learn which URL to use. Cisco SDM places a shortcut to this URL on the desktop of your PC that you can use to access Cisco SDM in the future.

Digital certificate

If you are creating a new gateway, select the digital certificate that you want the router to present to clients when they log in to the gateway. If you chose the IP address of an existing gateway, the router will use the digital certificate configured for that gateway, and this field is disabled.

Information area

When you provide the information in the IP Address and Name fields, this area contains the URL that users will enter. You must provide this URL to the users for whom you are creating this Cisco IOS SSL VPN.

If you checked **Allow Cisco SDM access through *IP address***, the URL that you must use in the future to access Cisco SDM is shown in this area. Cisco SDM places a shortcut to this URL on the desktop of your PC after you deliver the Cisco IOS SSL VPN configuration to the router.

User Authentication

Use this window to specify how the router is to perform user authentication. The router can authenticate Cisco IOS SSL VPN users locally, or it can send authentication requests to remote AAA servers.

External AAA server Button

Click if you want the router to use an AAA server to authenticate Cisco IOS SSL VPN users. The router will use the AAA servers that are listed in this window. If there are no AAA servers configured, you can configure them in this window. To use this option, there must be at least one AAA server configured on the router.

Locally on this router Button

Click if you want the router to authenticate users itself. The router will authenticate each user displayed in this window. If no users are configured on the router, you can add users in this window.

First on an external AAA server and then locally on this router Button

Click if you want the router to authenticate using a AAA server first, and if authentication fails, to attempt local authentication. If the user is not configured on either a configured AAA server or locally on the router, authentication for that user fails.

Use the AAA authentication method list Button

Click if you want the router to use a method list for authentication. A method list contains the authentication methods that should be used. The router attempts the first authentication method in the list. If authentication fails, the router tries the next method in the list and continues until the user is authenticated, or until it reaches the end of the list.

AAA servers configured for this router List

This list contains the AAA servers that the router uses to authenticate users. If you choose to authenticate users with AAA servers, this list must contain the name or IP address of at least one server. Use the **Add** button to add information for a new server. To manage AAA configurations on the router, leave the wizard, click **Additional Tasks**, and then click the AAA node in the Additional Tasks tree. This list does not appear if you have chosen **Locally on this router**.

Create user accounts locally on this router

Enter the users that you want the router to authenticate in this list. Use the **Add and Edit** buttons to manage the users on the router. This list does not appear if you chose **External AAA server**.

Configure Intranet Websites

Configure groups of intranet websites that you want users to have access to in this window. These links will appear in the portal that the users of this Cisco IOS SSL VPN see when they log in.

Action and URL List Columns

If you are adding a policy to an existing Cisco IOS SSL VPN context, there may be URL lists present in the table that is displayed. Check **Select** if you want to use a displayed URL list for the policy.

To create a new list, click **Add** and provide the required information in the dialog displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this table.

Add or Edit URL

Add or edit the information for a Cisco IOS SSL VPN link in this window.

Label

The label appears in the portal that is displayed when users log in to the Cisco IOS SSL VPN. For example, might use the label Payroll calendar if you are providing a link to the calendar showing paid holidays and paydays.

URL Link

Enter or edit the URL to the corporate intranet website that you want to allow users to visit.

Customize SSL VPN Portal

The settings that you make in this portal determine the appearance of the portal. You can select among the predefined themes listed, and obtain a preview of the portal as it would appear if that theme were used.

Theme

Select the name of a predefined theme.

Preview

This area shows what the portal looks like with the selected theme.You may want to preview several themes to determine which one you want to use.

SSL VPN Passthrough Configuration

In order for users to be able to connect to the intranet, access control entries (ACE) must be added to firewall and Network Access Control (NAC) configurations to permit SSL traffic to reach the intranet. Cisco SDM can configure these ACE for you, or you can configure them yourself by going to **Firewall and ACL** > **Edit Firewall Policy**/**ACL** and making the necessary edits.

If you are working in the Cisco IOS SSL VPN wizard, click **Allow SSL VPN to work with NAC and Firewall** if you want Cisco SDM to configure these ACEs. Click **View Details** to view the ACEs that Cisco SDM would create. An entry that Cisco SDM adds might look like this example:

```
permit tcp any host 172.16.5.5 eq 443
```

If you are editing a Cisco IOS SSL VPN context, Cisco SDM displays the affected interface and ACL that is applied to it. Click **Modify** to allow Cisco SDM to add entries to the ACL to allow SSL traffic to pass through the firewall. Click **Details** to view the entry that Cisco SDM adds. The entry will be one similar to the one already shown.

User Policy

This window allows you to choose an existing Cisco IOS SSL VPN and add a new policy to it. For example, you might have created a Cisco IOS SSL VPN named Corporate, and you want to define intranet access for a new group of users that you name Engineering.

Select existing SSL VPN

Choose the Cisco IOS SSL VPN for which you want to create a new group of users. The policies already configured for that Cisco IOS SSL VPN are displayed in a box under the list. You can click any of them to display the details of the policy. See Details of SSL VPN Group Policy: Policyname for more information.

Name of new policy

Enter the name that you want to give the new group of users. The area below this field lists the group policies that already exist for this Cisco IOS SSL VPN.

Details of SSL VPN Group Policy: Policyname

This window displays the details of an existing Cisco IOS SSL VPN policy.

Services

This area lists the services, such as URL mangling, and Cisco Secure Desktop, that this policy is configured for.

URLs exposed to users

This area lists the intranet URLs exposed to users who are governed by this policy.

Servers exposed to users

This area displays the IP addresses of the port forwarding servers that this policy is configured to use.

WINS servers

This area displays the IP addresses of the WINS servers that this policy is configured to use.

Select the SSL VPN User Group

Choose the Cisco IOS SSL VPN and associated user group for which you want to configure advanced services in this window.

SSL VPN

Choose the Cisco IOS SSL VPN that the user group is associated with from this list.

User Group

Choose the user group for which you will configure advanced features. The contents of this list is based on the Cisco IOS SSL VPN that you chose.

Select Advanced Features

Choose the features that you want to configure in this window. The wizard will display windows that allow you to configure the features that you choose.

For example, if you click Thin Client (Port Forwarding), Cisco Secure Desktop, and Common Internet File System (CIFS), the wizard will display configuration windows for these features.

You must choose at least one feature to configure.

Thin Client (Port Forwarding)

Remote workstations must sometimes run client applications to be able to communicate with intranet servers. For example Internet Mail Access Protocol (IMAP) or Simple Mail Transfer Protocol (SMTP) servers may require workstations to run client applications in order to send and receive e-mail. The

Thin-Client feature, also known as port forwarding, allows a small applet to be downloaded along with the portal so that a remote workstation can communicate with the intranet server.

This window contains a list of the servers and port numbers configured for the intranet. Use the **Add** button to add a server IP address and port number. Use the **Edit** and **Delete** buttons to make changes to the information in this list and to remove information for a server.

The list that you build appears in the portal that clients see when they log in.

Add or Edit a Server

Add or edit server information in this window.

Server IP Address

Enter the IP address or hostname of the server.

Server port on which service is listening

Enter the port the server is listening on for this service. This may be a standard port number for the service, such as port number 23 for Telnet, or it may be a nonstandard port number for which a Port-to-Application Map (PAM) has been created. For example if you changed the Telnet port number on the server to 2323, and you created a PAM entry for that port on that server, you would enter 2323 in this window.

Port on Client PC

Cisco SDM enters a number in this field, beginning with the number 3000. Each time you add an entry, Cisco SDM increments the number by 1. Use the entries that Cisco SDM has placed in this field.

Description

Enter a description for the entry. For example, if you are adding an entry that enables users to telnet to a server at 10.10.11.2, you could enter “Telnet to 10.10.11.2.” The description you enter appears on the portal.

Learn More

Click this link for more information. You can view that information now by clicking Learn More about Port Forwarding Servers.

Learn More about Port Forwarding Servers

Port forwarding enables a remote Cisco IOS SSL VPN user to connect to static ports on servers with private IP addresses on the corporate intranet. For example, you can configure port forwarding on a router to give remote users Telnet access to a server on the corporate intranet. To configure port forwarding, you need the following information:

- The IP address of the server.
- The static port number on the server.
- The remote port number for the client PC. In the dialog, Cisco SDM supplies a port number that is safe to use.

To allow users to use Telnet to connect to a server with the IP address 10.0.0.100 (port 23) for example, you would create a port mapping entry with the following information:

Server IP address: 10.0.0.100

Server port on which user is connecting: 23

Port on client PC: Cisco SDM-supplied value. 3001 for this example.

Description: SSL VPN Telnet access to server-a. This description will be on the portal.

When the client's browser connects to the gateway router, a portal applet is downloaded to the client PC. This applet contains the server's IP address and static port number, and the port number that the client PC is to use. The applet does the following:

- Creates a mapping on the client PC that maps traffic for port 23 on 10.0.0.100 to the PC's loopback IP address 127.0.0.1, port 3001.
- Listens on port 3001, IP address 127.0.0.1

When the user runs an application that connects to port 23 on 10.0.0.100, the request is sent to 127.0.0.1 port 3001. The portal applet listening on that port and IP address gets this request and sends it over the Cisco IOS SSL VPN tunnel to the gateway. The gateway router forwards it to the server at 10.0.0.100, and sends return traffic back to the PC.

Full Tunnel

Full tunnel clients must download the full tunnel software and obtain an IP address from the router. Use this window to configure the IP address pool that full tunnel clients will draw from when they log in and to specify the location of the full tunnel install bundle.

Note If the software install bundle is not already installed, there must be sufficient memory in router flash for Cisco SDM to install it after you complete this wizard.

Enable Full Tunnel Checkbox

Check to allow the router to download the full tunnel client software to the user's PC, and to enable the other fields in this window.

IP Address Pool

Specify the IP address pool that full tunnel clients will draw from. You can enter the name of an existing pool in the field, or you can click the button to the right of the field and choose **Select an existing IP pool** to browse the list of pools, Choose **Create a new pool** and complete the dialog that is displayed to create a new pool. The address pool that you choose or create must contain addresses in the corporate intranet.

Keep the Full Tunnel Client software installed on client's PC Checkbox

Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this checkbox, clients download the software each time they establish communication with the gateway.

Install Full Tunnel Client Checkbox

Check if you want to install the full tunnel client software at this time. You can also install the client software when editing this Cisco IOS SSL VPN.

The full tunnel client software must be installed on the router so that clients can download it to establish full-tunnel connectivity. If the Full Tunnel software was installed along with Cisco SDM, the path to it automatically appears in the Location field, as shown in Example 19-1.

Example 19-1 Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```

In Example 19-1, the Full Tunnel install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with `disk`*n* or `slot`*n*.

If this field is empty, you must locate the install bundle so that Cisco SDM can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking on the Download latest... link at the bottom of the window. This link takes you to the following web page:

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

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle for Cisco SDM to learn how to locate the Full Tunnel software install bundle, and supply a path to it for Cisco SDM to use.

Advanced Button

Click to configure advanced options such as split tunneling, split DNS, and client Microsoft Internet Explorer settings.

Locating the Install Bundle for Cisco SDM

Use the following procedure to locate software install bundles for Cisco SDM so that it can use that location in the Cisco IOS SSL VPN configuration, or, if necessary, load the software onto the router.

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Step 1 Look at the **Location** field. If the path to the install bundle is in that field, no further action need be taken. Cisco SDM configures the router to download the software from that location. Example 19-2 shows a path to a software install bundle.

Example 19-2 Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```

Step 2 If the Location field is empty, click the **...** button to the right of the field to specify the location of the software.

Step 3 If the software is installed on the router, choose **Router File System** and then browse for the file.

If the software is on your PC, choose **My Computer** and browse for the file.

Cisco SDM places the router file system or PC path you specified in the Location field.

Step 4 If the software is not on the router or on your PC, you must download it to your PC, and then provide the path to the file in this field.

a. Click the Download latest... link in the window. You are connected to the download page for the software you want.

b. There may be software packages available for Cisco IOS platforms and other platforms on the web page that appears. Double-click the latest version of the software that you want to download for Cisco IOS platforms, and provide your CCO username and password when prompted to do so.

c. Download the package to the PC.

d. In the Cisco IOS SSL VPN wizard, click the **...** button to the right of the Location field, choose **My Computer** in the Select Location window that is displayed, and navigate to the directory in which you placed the file.

e. Select the install bundle file then click **OK** in the Select Location window. Cisco SDM places that path in the Location field. examples shows an install bundle located on the PC's desktop.

Example 19-3 Full Tunnel Package Installed on Router

```
C:\Documents and Settings\username\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco SDM installs the software onto the router from the PC directory that you specified when you deliver the configuration to the router by clicking **Finish**.

Enable Cisco Secure Desktop

The router can install Cisco Secure Desktop on the user PC when the user logs in to the Cisco IOS SSL VPN. Web transactions can leave cookies, browser history files, e-mail attachments, and other files on the PC after the user logs out. Cisco Secure Desktop create a secure partition on the desktop and uses a Department of Defense algorithm to remove the files after the session terminates.

Install Cisco Secure Desktop

Clients must download the Cisco Secure Desktop software install bundle from the router. If this software was installed along with Cisco SDM, the path to it automatically appears in the **Location** field as shown in Example 19-4.

Example 19-4 Cisco Secure Desktop Package Installed on Router

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

In Example 19-4, the Cisco Secure Desktop install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with `disk`*`n`* or `slot`*`n`*.

If this field is empty, you must locate the install bundle so that Cisco SDM can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking the **Download latest...** link at the bottom of the window. This link takes you to the following web page:

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

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle for Cisco SDM to learn how to locate the Cisco Secure Desktop software install bundle, and supply a path to it for Cisco Cisco SDM to use.

Common Internet File System

Common Internet File System (CIFS) allows clients to remotely browse, access, and create files on Microsoft Windows-based file servers using a web browser interface.

WINS Servers

Microsoft Windows Internet Naming Service (WINS) servers maintain the database that maps client IP addresses to their corresponding NetBIOS names. Enter the IP addresses of the WINS servers in your network in this box. Use semicolons (;) to separate addresses.

For example, to enter the IP addresses 10.0.0.18 and 10.10.10.2, you enter 10.0.0.18;10.10.10.2 in this box.

Permissions

Specify the permissions to grant to users.

Enable Clientless Citrix

Clientless Citrix allows users to run applications such as Microsoft Word or Excel on remote servers in the same way that they would run them locally, without the need for client software on the PC. The Citrix software must be installed on one or more servers on a network that the router can reach.

Citrix Server

To create a new list, click **Add** and provide the required information in the dialog displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this table.

Summary

This window displays a summary of the Cisco IOS SSL VPN configuration that you have created. Click **Finish** to deliver the configuration to the router, or click **Back** to return to a wizard window to make changes.

To see the CLI commands that you are delivering to the router, go to **Edit** > **Preferences**, and check **Preview commands before delivering to router.**

Edit SSL VPN

The Edit SSL VPN window allows you modify or create Cisco IOS SSL VPN configurations. The top portion of the tab lists the configured Cisco IOS SSL VPN contexts. The bottom portion displays details for that context.

Click Cisco IOS SSL VPN to get an overview of the Cisco IOS SSL VPN features that Cisco SDM supports.

Click Cisco IOS SSL VPN links on Cisco.com for links to Cisco IOS SSL VPN documents.

Click Cisco IOS SSL VPN Contexts, Gateways, and Policies for a description of how the components of a Cisco IOS SSL VPN configuration work together.

SSL VPN Contexts

This area displays the Cisco IOS SSL VPN contexts configured on the router. Click a context in this area to display the detailed information for it in the lower part of the window. Add a new context by clicking **Add** and entering information in the dialog displayed. Edit a context by selecting it and clicking **Edit**. Remove a context and its associated group policies by selecting it and clicking **Delete**.

You can enable a context that is not in service by choosing it and clicking **Enable**. Take a context out of service by choosing it and clicking **Disable**.

The following information is displayed for each context.

Name

The name of the Cisco IOS SSL VPN context. If you created the context in the Cisco IOS SSL VPN wizard, the name is the string that you entered in the IP Address and Name window.

Gateway

The gateway that the context uses contains the IP address, and digital certificate that the Cisco IOS SSL VPN context will use.

Domain

If a domain has been configured for the context, it is displayed in this column. If a domain is configured, users must enter that domain in the web browser to access the portal.

Status

Contains icons for quick status identification.

Administrative Status

Textual description of status.

- In Service—Context is in service. Users specified in policies configured under the context can access their Cisco IOS SSL VPN portal.
- Not in Service—Context is not in service. Users specified in policies configured under the context cannot access their Cisco IOS SSL VPN portal.

Sample Display

The following table shows a sample Cisco IOS SSL VPN contexts display.

Name	Gateway	Domain	Status	Administrative Status
WorldTravel	Gateway1	wtravel.net	🟢	In Service
A+Insurance	Gateway2	aplus.com	🔴	Not in Service

Details about SSL VPN Context: *Name*

This area displays details about the context with the name *name* that you selected in the upper part of the window. You can modify the settings that you see by clicking **Edit** in the top part of the window.

SSL VPN Context

Use this window to add or edit a Cisco IOS SSL VPN context.

Name

Enter the name of a new context, or choose the name of an existing context to edit it.

Associated Gateway

Select an existing gateway, or click **Create gateway** to configure a new gateway for the context. The gateway contains the IP address and digital certificate is used for this context. Each gateway requires a unique public IP address.

Domain

If you have a domain for this context, enter it in this field. Cisco IOS SSL VPN users will be able to use this domain name when accessing the portal, instead of an IP address. An example is mycompany.com.

Authentication List

Choose the AAA method list to be used to authenticate users to this context.

Authentication Domain

Enter the domain name that is to be appended to the username before it is sent for authentication. This domain must match the domain used on the AAA server for the users that will be authenticated for this context.

Enable Context Checkbox

Check if you want the context to be enabled when you finish configuring it. You do not have to return to this window to disable it if you enable it here. You can enable and disable individual contexts in the Edit SSL VPN tab.

Maximum Number of Users

Enter the maximum number of users that should be allowed to use this context at one time.

VRF Name

Enter the VPN Routing and Forwarding (VRF) name for this context. This VRF name must have already been configured on the router.

Default Group Policy

Select the policy that you want to use as the default group policy. The default group policy will be used for users who have not been included in any policy configured on the AAA server.

Designate Inside and Outside Interfaces

An ACL that is applied to an interface on which a Cisco IOS SSL VPN connection is configured may block the SSL traffic. Cisco SDM can automatically modify the ACL to allow this traffic to pass through the firewall. However, you must indicate which interface is the inside (trusted) interface, and which is the outside (untrusted) interface for Cisco SDM to create the Access Control Entry (ACE) that will allow the appropriate traffic to pass through the firewall.

Check **Inside** if the listed interface is a trusted interface, and check **Outside** if it is an untrusted interface.

Select a Gateway

Select an existing gateway from this window. This window provides you with the information you need to determine which gateway to select. It displays the names and IP addresses of all gateways, the number of contexts each is associated with, and whether the gateway is enabled or not.

Context: Group Policies

This window displays the group policies configured for the chosen Cisco IOS SSL VPN context. Use the **Add**, **Edit**, and **Delete** buttons to manage these group policies.

For each policy, this window shows the name of the policy and whether the policy is the default group policy. The default group policy is the policy assigned to a user who has not been included in another policy. You can change the group policy by returning to the Context window and selecting a different policy as the default.

Click a policy in the list to view details about the policy in the lower part of the window. For a description of these details, click the following links

Group Policy: General Tab

Group Policy: Clientless Tab

Group Policy: Thin Client Tab

Group Policy: SSL VPN Client (Full Tunnel) Tab

Click here to learn more

Click the link in the window for important information. To get to that information from this help page, click Learn More About Group Policies.

Learn More About Group Policies

Cisco IOS SSL VPN group policies define the portal and links for the users included in those policies. When a remote user enters the Cisco IOS SSL VPN URL they have been given, the router must determine which policy the user is a member of so that it can display the portal configured for that policy. If only one Cisco IOS SSL VPN policy is configured on the router, it can authenticate users locally or using a AAA server, and then display the portal.

However, if more than one policy is configured, the router must rely on a AAA server to determine which policy to use each time a remote user attempts to log in. If you have configured more than one Cisco IOS SSL VPN group policy, you must configure at least one AAA server for the router, and you must configure a policy on that server for each group of users for which you created a Cisco IOS SSL VPN policy. The policy names on the AAA server must be the same as the names of the group policies configured on the router, and they must be configured with the credentials of the users who are members of the group.

For example, if a router has been configured with local authentication for Bob Smith, and only the group policy Sales has been configured, there is only one portal available to display when Bob Smith attempts to log in. However, if there are threeCisco IOS SSL VPN group policies configured, Sales, Field, and Manufacturing, the router cannot, by itself, determine which policy group Bob Smith is a member of. If a AAA server is configured with the proper information for those policies, the router can contact that server, and receive the information that Bob Smith is a member of the group Sales. The router can then display the correct portal for the Sales group.

For information on how to configure the AAA server, see the “Configuring RADIUS Attribute Support for SSL VPN” section in the *SSL VPN Enhancements* document at the following link:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Group Policy: General Tab

When creating a new group policy, you must enter information in each field of the General tab.

Name

Enter a name for the group policy, for example Engineering, Human Resources, or Marketing.

Timeouts

For Idle Timeout, enter the number of seconds that the client can remain idle before the session is terminated.

For Session Timeout, enter the maximum number of seconds for a session, regardless of the activity on the session.

Make this the default group policy for context Checkbox

Check if you want to make this the default group policy. The default group policy is the policy assigned to a user who is not included in another policy. If you check this checkbox, this policy will be shown as the default policy in the Group Policy window.

Group Policy: Clientless Tab

Clientless Citrix allows users to run applications on remote servers in the same way that they would run them locally, without client software needing to be installed on the remote systems using these applications. The Citrix software must be installed on one or more servers on a network that the router can reach.

Enter information if you want Cisco IOS SSL VPN clients to be able to use Clientless Citrix.

Clientless Web Browsing

Select one or more URL lists that you want to display in the portal that the users in this group will see. If you want to examine a URL list, choose a name from the list and click **View**. URLs in the list that you specify will be displayed in the portal.

If you want to restrict users to URLs in the list, and prevent them from entering additional URLs, click **Hide URL bar in the portal page**.

Enable CIFS

Choose this option if you want to allow group members to browse files on MS Windows servers in the corporate network. You must specify the WINS server list that will enable the appropriate files to be displayed to these users. To verify the contents of a WINS server list, choose the list and click **View**.

Click **Read** to allow group members to read files. Click **Write** to allow group members to make changes to files.

To make this feature available, configure at least one WINS server list for this Cisco IOS SSL VPN context.

Group Policy: Thin Client Tab

Make settings in this tab if you want to configure Thin Client, also known as port forwarding, for members of this group.

Click **Enable Thin Client** (**Port Forwarding**) and specify a port forward list to enable this feature. At least one port forward list must be configured for the Cisco IOS SSL VPN context under which this group policy is configured. Click **View** to examine the port forwarding list you have chosen.

Group Policy: SSL VPN Client (Full Tunnel) Tab

Make setting in this tab if you want to enable the group members to download and use full-tunnel client software.

Note You must specify the location of the Full Tunnel client software by clicking **Packages** in the SSL VPN tree, specifying the location of the install bundle, and then clicking **Install**.

Enable Full Tunnel connections by choosing **Enable** from the list. If you want to require Full Tunnel connections, choose **Required**. If you choose **Required**, Clientless and Thin Client communication will work only if the Cisco IOS SSL VPN client software is successfully installed on the client PC.

IP address pool from which clients will be assigned an IP address

Clients who establish Full Tunnel communication are assigned IP addresses by the router. Specify the name of the pool, or click the **...** button to create a new pool from which the router can assign addresses.

Keep full-tunnel client software installed on client's PC Checkbox

Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this checkbox, clients download the software each time they establish communication with the gateway.

Renegotiate Key field

Enter the number of seconds after which the tunnel should be brought down so that a new SSL key can be negotiated and the tunnel can be reestablished.

ACL to restrict access for users in this group to corporate resources

You can choose or create an access list (ACL) that specifies the resources on the corporate network that group members will be restricted to.

Home page client should see when a web browser is opened with full tunnel software installed

Enter the URL to the home page that is to be displayed to full-tunnel clients in this group.

Dead Peer Detection Timeouts

Dead Peer Detection (DPD) allows a system to detect a peer that is no longer responding. You can set separate timeouts that the router can use to detect clients that are no longer responding, and servers that are no longer responding. The range for both is from 0 to 3600 seconds.

Configure DNS and WINS servers Button

Click to display the DNS and WINS Servers dialog, which allows you to provide the IP addresses of the DNS and WINS servers on the corporate intranet that clients should use when accessing intranet hosts and services.

Configure Advanced Tunnel Options Button

Click to display the Advanced Tunnel Options dialog, which allows you to configure tunnel settings for split tunneling, split DNS, and proxy server settings for clients using Microsoft Internet Explorer.

Advanced Tunnel Options

The settings that you make in this dialog allow you to control the traffic that is encrypted, specify the DNS servers on the corporate intranet, and specify the proxy server settings that are to be sent to client browsers.

Split Tunneling

Encrypting all tunnel traffic may take excessive system resources. Split tunneling allows you to specify the networks whose traffic should be encrypted, and exempt traffic destined for other networks from encryption. You can either specify which tunnel traffic is to be encrypted or you can specify the traffic that is *not* to be encrypted and allow the router to encrypt all other tunnel traffic. You can only build one list; included and excluded traffic are mutually exclusive.

Click **Include traffic** and use the **Add**, **Edit**, and **Delete** keys to build a list of destination networks whose traffic is to be encrypted. Or, click **Exclude traffic** and build a list of the destination networks whose traffic is *not* to be encrypted.

Click **Exclude Local LANs** to explicitly exclude from encryption client traffic destined for LANs that the router is connected to. If there are networked printers on these LANs, you must use this option.

Learn More About Split Tunneling.

Split DNS

If you want Cisco IOS SSL VPN clients to use the DNS server in the corporate network only to resolve specific domains, you can enter those domains in this area. They should be domains within the corporate intranet. Separate each entry with a semicolon and do not use carriage returns. Here is a sample list of entries:

yourcompany.com;dev-lab.net;extranet.net

Clients must use the DNS servers provided by their ISPs to resolve all other domains.

Browser Proxy Settings

The settings in this area are sent to client Microsoft Internet Explorer browsers with full tunnel connections. These settings have no effect if clients use a different browser.

Do not use proxy server

Click to instruct Cisco IOS SSL VPN client browsers not to use a proxy server.

Auto-detect proxy settings

Click if you want the Cisco IOS SSL VPN client browsers to auto detect proxy server settings.

Bypass proxy settings for local addresses

Click if you want clients connecting to local addresses to be able to bypass normal proxy settings.

Proxy Server

Enter the IP address of the proxy server and the port number for the service that it provides in these fields. For example, if the proxy server supports FTP requests, enter the IP address of the proxy server and port number 21.

Do not use proxy server for addresses beginning with

If you do not want clients to use proxy servers when sending traffic to specific IP addresses or networks, you can enter them here. Use a semicolon to separate each entry. For example, if you do not want clients to use a proxy server when connecting to any server in the 10.10.0.0 or 10.11.0.0 networks, enter 10.10;10.11. You can enter as many networks as you want.

DNS and WINS Servers

Enter the IP addresses for the corporate DNS and WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet.

Provide addresses for primary and for secondary DNS servers and WINS servers.

Learn More About Split Tunneling

When a Cisco IOS SSL VPN connection is set up with a remote client, all traffic that the client sends and receives may travel through the Cisco IOS SSL VPN tunnel, including traffic that is not on the corporate intranet. This can degrade network performance. Split tunneling allows you to specify the traffic that you want to send through the Cisco IOS SSL VPN tunnel and allow other traffic to remain unprotected and be handled by other routers.

In the Split Tunneling area, you can specify the traffic to *include* in the Cisco IOS SSL VPN and exclude all other traffic by default, or you can specify the traffic to *exclude* from the CCisco IOS SSL VPN and include all other traffic by default.

For example, suppose that your organization uses the 10.11.55.0 and the 10.12.55.0 network addresses. Add these network addresses to the Destination Network list, then click the **Include traffic** radio button. All other Internet traffic, such as traffic to Google or Yahoo, would go direct to the Internet.

Or suppose it is more practical to exclude traffic to certain networks from the Cisco IOS SSL VPN tunnel. In that case, enter the addresses for those networks in the Destination Networks list, then click the **Exclude traffic** radio button. All traffic destined for the networks in the Destination Networks list is sent over nonsecure routes, and all other traffic is sent over the Cisco IOS SSL VPN tunnel.

If users have printers on local LANs that they want to use while connected to the Cisco IOS SSL VPN, you must click **Exclude local LAN** in the Split Tunneling area.

Note The Destination Network list in the Split Tunneling area may already contain network addresses. The traffic settings you make in the Split Tunneling area override any settings previously made for the listed networks.

DNS and WINS Servers

Enter the IP addresses for the corporate DNS and WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet.

Provide addresses for primary and for secondary DNS servers and WINS servers.

Context: HTML Settings

The settings that you make in this window control the appearance of the portal for the selected Cisco IOS SSL VPN context.

Select theme

You can specify the appearance of the portal by selecting a predefined theme instead of by selecting each color yourself. When you select a theme, the settings for that theme are displayed in the fields associated with the **Customize** button.

Customize Button

Click if you want to select each color used in the portal and specify a login message and title. If you selected a predefined theme, the values for that theme are displayed in the fields in this section. You can change these values, and the values you enter are used in the portal for the selected context. Changes that you make in this window only affect the portal you are creating. They do not change the default values for the theme.

Login Message

Enter the login message that you want clients to see when their browsers display the portal. For example:

```
Welcome to the company-name network. Log off if you are not an
authorized user.
```

Title

Enter the title that you want to give the portal. For example:

```
Company-name network login page
```

Background Color for Title

The default value for the background color that appears behind the title is #9999CC. Change this value by clicking the **...** button and selecting a different color.

Background Color for Secondary Titles

The default value for the background color that appears behind the title is #9729CC. Change this value by clicking the **...** button and selecting a different color, or by entering the hexadecimal value for a different color.

Text Color

The default value for the text color is white. Change this value by clicking the down arrow and selecting a different color.

Secondary Text Color

The default value for the secondary text color is black. Change this value by clicking the down arrow and selecting a different color.

Logo File

If you have a logo that you want to display on the portal, click the **...** button to browse for it on your PC. It is saved to router flash after you click **OK**, and will appear in the upper-left corner of the portal.

Preview Button

Click to see a preview of the portal as it will look with the predefined theme or custom values you have specified.

Select Color

Click **Basic** to select a predefined color, or click **RGB** to create a custom color.

Basic

Select the color that you want to use from the palette on the left. The color you select appears in the large square in the right side of the dialog.

RGB

Use the Red, Green, and Blue sliders in combination to create a custom color. The color you create appears in the large square in the right side of the dialog.

Context: NetBIOS Name Server Lists

View all the NetBIOS name server lists that are configured for the selected Cisco IOS SSL VPN context in this window. CIFS uses NetBIOS servers to display the corporate Microsoft Windows file system to Cisco IOS SSL VPN users.

Each name server list configured for the context is shown in the **NetBIOS Name Server Lists** area. Use the **Add**, **Edit**, and **Delete** buttons to manage these lists. Click a list name to view the contents of the list in the **Details of NetBIOS Name Server** area.

Add or Edit a NetBIOS Name Server List

Create or maintain a NetBIOS name server list in this window. You must enter a name for each list that you create, and provide the IP address, timeout and number of retries to attempt for each server in the list. One server in each list must be designated as the master server.

Each server in the list is displayed in this dialog, along with its master status, timeout, and retries values.

Add or Edit an NBNS Server

You must enter the IP address of each server, along with the number of seconds that the router is to wait before attempting to connect to the server again, and the number of times the router is to attempt to contact the server.

Check **Make this server the master server** if you want this server to be the first server that the router contacts on the list.

Context: Port Forward Lists

Configure the port forwarding lists for the selected context in this window. The lists can be associated to any group policy configured under the selected context. Port forward lists reveal TCP application services to Cisco IOS SSL VPN clients.

The upper part of the window displays the port forward lists configured for the selected context. Click a list name to display the details for the list in the lower part of the window.

The window displays the IP address, port number used, corresponding port number on the client, and a description if one was entered.

Add or Edit a Port Forward List

Create and maintain port forward lists in this window. Each list must be given a name, and contain at least one server entry. Use the **Add**, **Edit**, and **Delete** buttons to create, modify, and remove entries from the list.

Context: URL Lists

URL lists specify which links can appear on the portal for users in a particular group. Configure one or more URL lists for each context, then use the group policy windows to associate these lists with specific group policies.

The upper part of the window displays all the URL lists configured for the context. The lower part of the window displays the contents of the selected list. For each list, it displays the heading that is displayed at the top of the URL list, and each URL that is in the list.

Use the **Add**, **Edit**, and **Delete** buttons to create and manage URL lists.

Add or Edit a URL List

You must enter a name for each URL list, and heading text that will appear at the top of the URL list.

Heading text should describe the overall contents of the links in the list. For example, if a URL list provides access to the health plan web pages and insurance web pages, you might use the heading text `Benefits`.

Use the **Add** button to create a new entry for the list, and the **Edit** and **Delete** buttons to maintain the list. Each entry that you add appears in the list area.

Context: Cisco Secure Desktop

Cisco Secure Desktop encrypts cookies, browser history files, temporary files, and e-mail attachments that could create security problems if left unencrypted. After a Cisco IOS SSL VPN session is terminated, Cisco Secure Desktop removes the data using a Department of Defense sanitation algorithm.

Click **Enable Cisco Secure Desktop** to allow all users of this context to download and use **Cisco Secure Desktop**. This window displays a message if the install bundle for this software is not found on the router.

To load the install bundle for Cisco Secure Desktop on the router, click Packages in the Cisco IOS SSL VPN tree and follow the instructions in the window.

SSL VPN Gateways

This window displays the Cisco IOS SSL VPN gateways configured on the router and enables you to modify existing gateways and configure new ones. A Cisco IOS SSL VPN gateway is the user portal to the secure network.

SSL VPN Gateways

This area of the window lists the Cisco IOS SSL VPN gateways that are configured on the router. It shows the name and IP address of the gateway, the number of contexts configured to use the gateway, and the status of the gateway.

▲	The gateway is enabled and in service.
▼	The gateway is disabled and out of service.

Click a gateway to view details about it in the lower part of the window. Enable a gateway that is **Disabled** by choosing it and clicking **Enable**. Take an enabled gateway out of service by choosing it and clicking **Disable**. To edit a gateway, select the gateway and click the **Edit** button. To remove a gateway, choose the gateway and click the **Delete** button.

Details of SSL VPN Gateway

This area of the window displays configuration details about the gateway selected in the upper part of the window, and the names of the Cisco IOS SSL VPN contexts that are configured to use this gateway.

For more information on gateway configuration details, click Add or Edit a SSL VPN Gateway. For more information on contexts, click SSL VPN Context.

Add or Edit a SSL VPN Gateway

Create or edit a Cisco IOS SSL VPN gateway in this window.

Gateway Name

The gateway name uniquely identifies this gateway on the router, and is the name used to refer to the gateway when configuring Cisco IOS SSL VPN contexts.

IP Address

Choose or enter the IP address that the gateway is to use. This must be a public IP address, and cannot be an address used by another gateway on the router.

Digital Certificate

Choose the certificate that is to be sent to Cisco IOS SSL VPN clients for SSL authentication.

HTTP Redirect Checkbox

Uncheck if you do not want HTTP redirect to be used. HTTP redirect automatically redirects HTTP requests to port 443, the port used for secure Cisco IOS SSL VPN communication.

Enable Gateway Checkbox

Uncheck if you do not want to enable the gateway. You can also enable and disable the gateway from the SSL VPN Gateways window.

Packages

This window enables you to obtain software install bundles that must be downloaded to Cisco IOS SSL VPN clients to support Cisco IOS SSL VPN features, and to load them on the router. You can also use this window to remove install bundles that have been installed.

Follow the steps described in the window to download the install bundles from Cisco.com to your PC, and then copy them from your PC to the router. If you need to obtain any of the install bundles, start with Step 1 by clicking on the link to the download site.

Note Access to these download sites requires a CCO username and password. If you don't have a CCO username and password, you can obtain one by clicking Register at the top of any Cisco.com webpage, and completing the form that is displayed. Your username and password will be mailed to you.

If you have already loaded install bundles onto your PC or the router, complete steps 2 and 3 to specify the current location of the install bundles and copy them to router flash.

Click the **...** button in each section to specify the current location of the install bundle.

After you specify the current location, and where you want to copy it to in router flash, click **Install**.

After the bundles have been loaded onto the router, the window displays name, version, and build date information about the package. If an administration tool is available with the package, the window displays a button enabling you to run this tool.

The Cisco IOS SSL VPN client install bundle is available from the following link:

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

The Cisco Secure Desktop install bundle is available from the following link:

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

Install Package

Specify the current location of an install bundle by browsing for it in this window. If the install bundle is already located on the router, click **Router** and browse for it. If it is located on the PC, click **My Computer** and browse for it. When you have specified the current location of the install bundle, click **OK**.

The location will be visible in the Packages window.

Cisco IOS SSL VPN Contexts, Gateways, and Policies

Cisco SDM provides an easy way to configure Cisco IOS SSL VPN connections for remote users. However, the terminology used in this technology can be confusing. This help topic discusses the Cisco IOS SSL VPN terms used in Cisco SDM configuration windows and describes how Cisco IOS SSL VPN components work together. An example of using the Cisco IOS SSL VPN wizard and edit windows in Cisco SDM is also provided.

Before discussing each component individually, it is helpful to note the following:

- One Cisco IOS SSL VPN context can support multiple group policies.
- Each context must have one associated gateway.
- One gateway can support multiple contexts.
- If there is more than one group policy on the router, a AAA server must be used for authentication.

Cisco IOS SSL VPN Contexts

A Cisco IOS SSL VPN context identifies resources needed to support SSL VPN tunnels between remote clients and a corporate or private intranet, and supports one or more group policies. A Cisco IOS SSL VPN context provides the following resources:

- An associated Cisco IOS SSL VPN gateway, which provides an IP address that clients can reach and a certificate used to establish a secure connection.
- Means for authentication. You can authenticate users locally, or by using AAA servers.
- The HTML display settings for the portal that provides links to network resources.
- Port forwarding lists that enable the use of Thin Client applets on remote clients. Each list should be configured for use in a specific group policy.
- URL lists that contain links to resources in the corporate intranet. Each list should be configured for use in a specific group policy.
- NetBIOS Name Server lists. Each list should be configured for use in a specific group policy.

These resources are available when configuring Cisco IOS SSL VPN group policies.

A Cisco IOS SSL VPN context can support multiple group policies. A Cisco IOS SSL VPN context can be associated with only one gateway.

Cisco IOS SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides a reachable IP address and certificate for one or more Cisco IOS SSL VPN contexts. Each gateway configured on a router must be configured with its own IP address; IP addresses cannot be shared among gateways. It is possible to 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 gateways to use. All gateways on the router can use the same certificate.

Although one gateway can serve multiple Cisco IOS SSL VPN contexts, resource constraints and IP address reachability must be taken into account.

Cisco IOS SSL VPN Policies

Cisco IOS SSL VPN group policies allow you to accommodate the needs of different groups of users. A group of engineers working remotely needs access to different network resources than sales personnel working in the field. Business partners and outside vendors must access the information 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 of these groups allows you provide remote users with the resources they need, and prevent them from accessing other resources.

When you configure a group policy, resources such as URL lists, Port Forwarding lists, and NetBIOS name server lists configured for the policy's associated context are available for selection.

If there is more than one group policy configured on the router, you must configure the router to use a AAA server to authenticate users and to determine which policy group a particular user belongs to. Click Learn More About Group Policies for more information.

Example

In this example, a user clicks **Create a new SSL VPN** and uses the wizard to create the first Cisco IOS SSL VPN configuration on the router. Completing this wizard creates a new context, gateway, and group policy. The following table contains the information the user enters in each wizard window, and the configuration that Cisco SDM creates with that information.

Cisco IOS SSL VPN Wizard Window	Configuration
Create SSL VPN Window	
Prerequisite Tasks area indicates that digital certificates are not configured on the router. User clicks **self signed certificate** and configures a certificate in the Persistent Self Signed Certificate dialog. The user does not change the Cisco SDM-supplied name Router_Certificate. User clicks **Create new SSL VPN**.	Cisco SDM configures a self-signed certificate named "Router_Certificate" that will be available for use in all Cisco IOS SSL VPN configurations.
IP Address and Name Window	
User enters the following information: IP Address: 172.16.5.5 Name: Asia Check **Enable secure SDM access through 192.168.1.1**. Certificate: **Router_Certificate**	Cisco SDM creates a context named "Asia." Cisco SDM creates a gateway named "gateway_1" that uses the IP address 172.16.5.5 and Router_Certificate. This gateway can be associated with other Cisco IOS SSL VPN contexts. Users will access the Cisco IOS SSL VPN portal by entering http://172.16.5.5/Asia. If this gateway is associated with additional contexts, the same IP address will be used in the URL for those contexts. For example if the context Europe is also configured to use gateway_1, users enter https://172.16.5.5/Europe to access the portal. After the configuration is delivered to the router, users must enter http://172.16.5.5:4443 to launch Cisco SDM using this IP address. Cisco SDM also begins to configure the first group policy, named policy_1.

Cisco IOS SSL VPN Wizard Window	Configuration
User Authentication Window	
User chooses **Locally on this router**. User adds one user account to the existing list.	Cisco SDM creates the authentication list "sdm_vpn_xauth_ml_1." This list will be displayed in the Cisco IOS SSL VPN Contexts window when the user completes the wizard. Those users listed in the User Authentication window are the members of this authentication list, and will be governed by policy_1.
Configure Intranet Websites Window	
User configures the URL list Ulist_1. The heading is "Taiwan."	The URL list with the heading Taiwan will be visible in the portal that users in "sdm_vpn_xauth_ml_1" see when they log in. The URL list will be available for configuration in other group policies configured under the context "Asia."
Enable Full Tunnel Window	
User clicks **Enable Full Tunnel**, and selects a predefined address pool. No advanced options are configured.	Client PCs will download Full Tunnel client software when they log in for the first time, and a full tunnel is established between the PC and the router when the user logs in to the portal.
Customize SSL VPN Portal Window	
User chooses **Ocean Breeze**.	Cisco SDM configures the HTTP display settings with this color scheme. The portal displayed when policy_1 users log in uses these settings. These portal settings also apply to all policies configured under the context "Asia." The user can customize the HTTP display settings in the Edit SSL VPN windows after completing the wizard.
SSL VPN Passthrough Configuration Window	
User checks **Allow SSL VPN to work with NAC and Firewall**	Cisco SDM adds an ACL with the following entry. `permit tcp any host 172.16.5.5 eq 443`

Cisco IOS SSL VPN Wizard Window	Configuration
Summary Window	

The Summary window displays the information shown at the right. Additional details can be viewed in the Edit SSL VPN windows.	`SSL VPN Policy Name: policy_1`
	`SSL VPN Gateway Name: gateway_1`
	
	`User Authentication Method List:  Local`
	
	`Full Tunnel Configuration`
	`    SVC Status: Yes`
	`    IP Address Pool: Pool_1`
	`    Split Tunneling: Disabled`
	`    Split DNS: Disabled`
	`    Install Full Tunnel Client: Enabled`

When this configuration is delivered, the router has one Cisco IOS SSL VPN context named Asia, one gateway named gateway_1, and one group policy named policy_1. This is displayed in the Edit SSL VPN window as shown in the following table:

Name	Gateway	Domain	Status	Administrative Status
Asia	gateway_1	Asia	▲	In Service
Details about SSL VPN context Asia:				
Item Name		**Item Value**		
Group Policies				
policy_1				
Services		URL Mangling, Full Tunnel		
URLs exposed to Users		http://172.16.5.5/pricelist		
		http://172.16.5.5/catalog		
Servers Exposed to users		<None>		
WINS servers		<None>		

policy_1 provides the basic Cisco IOS SSL VPN service of URL mangling, and specifies that a full tunnel be established between clients and the router. No other features are configured. You can add features to policy_1, such as Thin Client and Common Internet File System by choosing **Configure advanced features for an existing SSL VPN**, choosing **Asia** and **policy_1** in the Select the Cisco IOS SSL VPN user group window, then choosing the features in the Advanced Features window. Additional URL lists can also be configured in this wizard.

You can create a new group policy under context “Asia” by choosing **Add a new policy to an existing SSL VPN for a new group of users**.

You can customize settings and the policies configured for context Asia by choosing Asia in the context list and clicking **Edit**. The Edit SSL VPN Context Asia window displays a tree that allows you to configure more resources for the context, and to edit and configure additional policies. You can edit the settings for gateway_1 by clicking **SSL VPN Gateways** under the SSL VPN node, selecting gateway_1, then clicking **Edit**.

How Do I...

“How do I” topics explain common configuration tasks associated with this feature.

How do I verify that my Cisco IOS SSL VPN is working?

The best way to determine that a Cisco IOS SSL VPN context will provide the access that you configured for users is to configure yourself as a user, then attempt to access all the websites and services that the context is configured to provide for them. Use the following procedure as a guide in setting up this test.

Step 1 Ensure that credentials you can use are included in all appropriate policies on the AAA server.

Step 2 If you can do so, open a Cisco SDM session to the router so that you can monitor the Cisco IOS SSL VPN traffic that you will create. This must be done on a separate PC if the PC you use to test the Cisco IOS SSL VPN context is not in a network from which you can access Cisco SDM. Go to **Monitor** > **VPN Status** > **SSL VPN**.

Step 3 Enter the URL to each of the web portals that are configured for this Cisco IOS SSL VPN context. Determine that each page has the appearance that you configured for it, and that all links specified in the URL lists for the policy appear on the page.

Step 4 Test all links and services that should be available to users included in this policy. If any of the policies that you are testing provide for downloading Cisco Secure Desktop or the Full Tunnel client software, enter the URLs to the web portals for those policies and click the links that will require the download of this software. Determine that the software downloads properly and that you are able to access the services that a user should be able to access from these links.

Step 5 If you were able to establish a Cisco SDM session before you began testing, click the branch for the context that you are testing and observe the Cisco IOS SSL VPN traffic statistics in the Cisco IOS SSL VPN window.

Step 6 Based on the results of your tests, go back to Cisco SDM if necessary and fix any configuration problems you discovered.

How do I configure a Cisco IOS SSL VPN after I have configured a firewall?

If you have already configured a firewall, you can still use the Cisco IOS SSL VPN wizards in Cisco SDM to create Cisco IOS SSL VPN contexts and policies. Cisco SDM validates the Cisco IOS SSL VPN CLI commands that it generates against the existing configuration on the router. If it detects an existing firewall configuration that would have to be modified to allow Cisco IOS SSL VPN traffic to pass through, you are informed. You can allow Cisco SDM to make the necessary modifications to the firewall, or you can leave the firewall intact and make the changes manually by going to **Configure** > **Firewall and ACL** > **Edit Firewall ACL** and entering the permit statements that allow Cisco IOS SSL VPN traffic to pass through the firewall.

How do I associate a VRF instance with a Cisco IOS SSL VPN context?

VPN Routing and Forwarding (VFR) instances maintain a routing table and a forwarding table for a VPN. You can associate a VRF instance or name with a Cisco IOS SSL VPN context by going to **Configure > VPN > SSL VPN > Edit SSL VPN**. Select the context that you want to associate a VRF instance to and click **Edit**. Select the name of the VRF instance in the dialog displayed.

Note The VRF instance must already be configured on the router.