CHAPTER 26

Managing Remote Access VPNs

Cisco Security Manager lets you configure both remote access IPSec VPNs and remote access SSL VPNs. Security Manager provides flexible configuration and management of remote access VPNs:

- You can discover existing remote access VPN configuration policies from existing live devices or from configuration files. Then, you can change and deploy new or updated policies, as necessary.
- You can use the configuration wizard to help you quickly and easily set up these two types of remote access VPNs with basic functionality.
- If you know the functions and feature your network requires, you can configure remote access VPNs independently. You can also use the wizard to create a basic remote access VPN and then configure additional features that are not included in the wizard separately.

In addition, Cisco Security Manager provides flexibility in how remote access VPN configuration policies are assigned: Device view or Policy view.

For some policies, you can also assign either the factory default policy (a private policy), or a shared policy that you created using Security Manager.

Note As of version 3.2.1, Security Manager supports configuration of SSL VPN policies on ASA devices running software version 8.0 and later. Make sure that you upgrade your ASA devices to a supported version before configuring SSL VPNs.

This chapter contains the following topics:

Understanding Remote Access VPNs

Security Manager supports two types of remote access VPNs: IPSec and SSL.

This section contains the following topics:

Understanding Remote Access IPSec VPNs

Remote access IPSec VPNs permit secure, encrypted connections between a company's private network and remote users, by establishing an encrypted IPSec tunnel across the Internet using broadband cable, DSL, or dial-up connection.

A remote access IPSec VPN consists of a VPN client and a VPN headend device, or VPN gateway. The VPN client software resides on a user's workstation and initiates the VPN tunnel access to the corporate network. At the other end of the VPN tunnel is the VPN gateway at the edge of the corporate site.

When a VPN client initiates a connection to the VPN gateway device, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). Next the group profile is pushed to the VPN client using mode configuration, and an IPsec security association (SA) is created to complete the VPN connection.

For remote access IPSec VPNs, AAA (authentication, authorization, and accounting) is used for secure access. With user authentication, a valid user name and password must be entered before the connection is completed. User names and passwords can be stored on the VPN device itself, or on an external AAA server that can provide authentication to numerous other databases. For more information on using AAA servers, see Understanding AAA Server and Server Group Objects, page 6-20.

Note You can also use the Easy VPN technology to configure remote access IPSec VPN policies in site-to-site VPN topologies. Security policies are configured on hardware clients, such as routers, whereas in remote access IPSec VPNs, policies are configured on PCs running Cisco VPN client software. For more information, see Understanding Easy VPN, page 24-1.

Related Topics

- Working with IPSec VPN Policies, page 26-34
- Working with Policies Pertaining to Both IPSec and SSL VPNs, page 26-15
- Discovering Remote Access VPN Policies, page 26-8

Understanding Remote Access SSL VPNs

The SSL VPN feature lets users 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 8.0 and later, running in single-context and router modes, on Cisco 870, 880, 890, 1800, 2800, 3700, 3800, 7200, and 7301 Series routers running software version 12.4(6)T and later, and on Cisco 1900, 2900, and 3900 Series routers running software version 15.0(1)M and later. For the 880 Series routers, the minimum software version is 12.4(15)XZ, which is mapped to 12.4(20)T in Security Manager.

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 lets users 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.

User authentication can be done using usernames and passwords, certificates, or both.

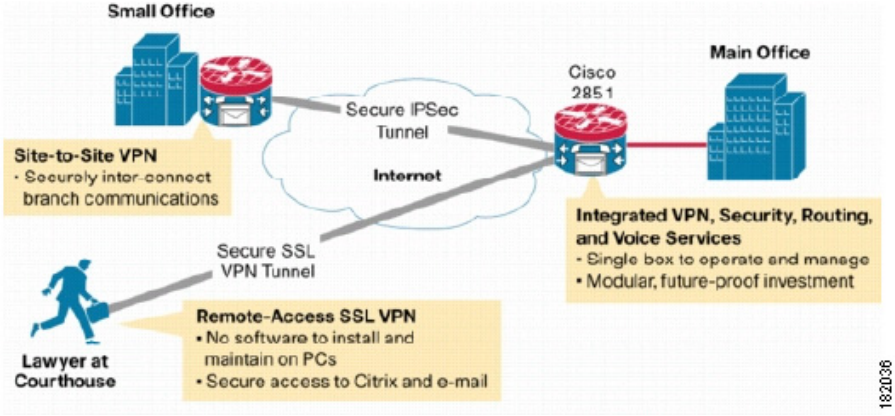
Note Network administrators provide user access to SSL VPN resources on a group basis instead of on an individual user basis.

This section contains the following topics:

Remote Access SSL VPN Example

Figure 26-1 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 26-1 Secure SSL VPN Access Example



SSL VPN Access Modes

SSL VPN provides three modes of remote access on IOS routers: Clientless, Thin Client and Full Client. On ASA devices, there are two modes: Clientless (which includes Clientless and Thin Client port forwarding) and AnyConnect Client (which replaces Full Tunnel).

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 remote user's PC must be running Windows 2000, Windows XP, or Linux operating systems.

Browser-based SSL VPN users connecting from Windows operating systems can browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a Web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.

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 Sun's Java Runtime Environment (JRE) version 1.4 or later. 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. That is, 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 Full Tunnel SSL VPN access requires administrative privileges on the remote client.

Related Topics

- Chapter 26, "Managing Remote Access VPNs"

Understanding and Managing SSL VPN Support Files

SSL VPNs sometimes require supporting files that reside in the device's flash storage. This is especially true of SSL VPNs configured on ASA devices. Supporting files include Cisco Secure Desktop (CSD) packages, AnyConnect client images, and plug-in files. Security Manager includes many of these files for your use. However, some supporting files, such as graphic files used for portal pages, or client profiles used for AnyConnect clients are not provided by Security Manager.

Typically, you need to create a File Object to specify a supporting file, and you then select the File Object when you create a policy that refers to it. You can create the File Objects that you need when you create the policies, or you can create them before you start defining policies. For more information, see Add and Edit File Object Dialog Boxes, page 28-24.

When you deploy policies to the devices, any supporting files referenced in your policies are copied to the device and placed in flash memory in the \csm folder. For the most part, you do not have to do any manual work to make this happen. The following are some situations where you might need to do some manual work:

- If you are trying to discover existing SSL VPN policies, or rediscover them, file references from the SSL VPN policies must be correct. For detailed information on how supporting files are handled during policy discovery, see Discovering Remote Access VPN Policies, page 26-8.
- If you have configured the ASA device in an Active/Failover configuration, you must get the supporting files onto the failover device. The supporting files are not copied over to the failover device during a failover. You have these choices for getting the files onto the failover device:
  - Manually copy the files from the \csm folder on the active unit to the failover unit.
  - After deploying the policies to the active unit, force a failover and redeploy the policies to the now-active unit.
- If you are using a VPN cluster for load balancing, the same supporting files must be deployed to all devices in the cluster.

Cisco Secure Desktop (CSD) Packages

These packages are for ASA SSL VPNs. You select a package in the Dynamic Access policy. The package you select must be compatible with the ASA operating system version running on the device. When you create a Dynamic Access policy for an ASA device, the version number that is compatible with the device's operating system is displayed in the Version field.

You can find the CSD packages in Program Files\CSCOpx\objects\sslvpn\csd. The file names are in the form securedesktop-asa_k9-*version*.pkg or csd_*version*.pkg, where *version* is the CSD version number such as 3.3.0.118.

Following is the CSD compatibility with ASA versions for the CSD packages shipped with Security Manager:

- csd_3_5_841-3.5.841.pkg—ASA 8.0(4) or later.
- csd_3_4_2048-3.4.2048.pkg—ASA 8.0(4) or later.
- csd_3_4_1108-3.4.1108.pkg—ASA 8.0(4) or later.
- csd-3.4.0373.pkg—ASA 8.0(4) or later.
- securedesktop_asa_k9-3.3.0.151.pkg—ASA 8.0(3.1) or later.
- securedesktop_asa-k9-3.3.0.118.pkg—ASA 8.0(3.1) or later.
- securedesktop-asa-k9-3.2.1.126.pkg—ASA 8.0(3) or later.
- securedesktop-asa_k9-3.2.0.136.pkg—ASA 8.0(2) or later.

For more information on CSD version compatibility with ASA versions, see the CSD release notes at http://www.cisco.com/en/US/products/ps6742/prod_release_notes_list.html and Supported VPN Platforms on Cisco.com.

For more information on creating Dynamic Access policies to specify the CSD, see Configuring Cisco Secure Desktop Policies on ASA Devices, page 26-26.

AnyConnect Client Images

These images are for ASA SSL VPNs. The AnyConnect client is downloaded to the user's PC and manages the client's VPN connection. Security Manager includes these AnyConnect images, which you can find in Program Files\CSCOpx\objects\sslvpn\svc:

For more information on the AnyConnect client, its profiles, and how to configure policies to load the client onto the device, see the following topics:

- Understanding SSL VPN Client Settings, page 26-56
- Configuring SSL VPN Client Settings, page 26-57

Plug-in Files

These files are used as browser plug-ins. You can find plug-in files in Program Files\CSCOpx\objects\sslvpn\plugin. For complete information on the available files, see Understanding Plug-ins, page 26-53.

Prerequisites for Configuring SSL VPNs

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 JRE for Windows version 1.4 or later, or a browser that supports ActiveX controls.
  - Linux with JRE for Linux version 1.4 or later. To access Microsoft shared files from Linux in clientless remote access mode, Samba must also be installed.

Related Topics

- SSL VPN Access Modes, page 26-4
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices), page 26-12
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 26-10

SSL VPN Limitations

SSL VPN configurations in Security Manager are subject to the following limitations:

- SSL VPN license information cannot be imported into Security Manager. As a result, certain command parameters, such as **vpn sessiondb** and **max-webvpn-session-limit**, cannot be validated.
- You must configure DNS on each device in the topology in order to use clientless SSL VPN. Without DNS, the device cannot retrieve named URLs, but only URLs with IP addresses.
- If you share your Connection Profiles policy among multiple ASA devices, bear in mind that all devices share the same address pool unless you use device-level object overrides to replace the global definition with a unique address pool for each device. Unique address pools are required to avoid overlapping addresses in cases where the devices are not using NAT.

- If the device configuration contains an address pool for SSL VPN with a name that begins CSM_ (the naming convention used by Security Manager), Security Manager cannot detect whether the addresses in that pool overlap with the pool configured in your SSL VPN policy. (This can occur, for example, when the pool was configured by a user on a different installation of Security Manager.) This can lead to errors during deployment. Therefore, we recommend that you configure the same IP address pool as a network/host object in Security Manager and define it as part of the SSL VPN policy. This enables the proper validation to take place.
- The same IP address and port number cannot be shared by multiple SSL VPN gateways on the same IOS device. As a result, deployment errors can occur if a duplicate gateway exists in the device configuration but was not redefined using the Security Manager interface. If such an error occurs, you must choose a different IP address and port number and redeploy.
- If you define AAA authentication or accounting as part of an SSL VPN policy, the **aaa new-model** command is deployed to enable AAA services. Bear in mind that this command is not removed if you later delete the SSL VPN policy, as there might be other parts of the device configuration that require the **aaa new-model** command for AAA services.

Note In addition, we recommend that you define at least one local user on the device with a privilege level of 15. This ensures that you will not be locked out of the device if the **aaa new-model** command is configured without an associated AAA server.

Related Topics

- SSL VPN Access Modes, page 26-4
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices), page 26-12
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 26-10

Discovering Remote Access VPN Policies

Security Manager allows you to import the configurations of remote access IPSec, IPSec/GRE, DM VPN, and Easy VPN policies during policy discovery. You can also discover SSL VPN policies on ASA devices, but not on IOS devices. You can discover configurations on devices that are already deployed in your remote access VPN network, so that Security Manager can manage them. These configurations are imported into Security Manager as remote access VPN policies. Remote access VPN policy discovery can be performed by importing the configuration of a live device or by importing a configuration file. However, SSL VPN policies that refer to files in flash storage cannot be discovered from configuration files, therefore, we recommend that you do not discover SSL VPNs from configuration files.

When you initiate policy discovery on a device in a remote access VPN, the system analyzes the configuration on the device and then translates this configuration into Security Manager policies so that the device can be managed. Warnings are displayed if the imported configuration completes only a partial policy definition. If additional settings are required, you must go to the relevant page in the Security Manager interface to complete the policy definition. You can also rediscover the configurations of devices that are already managed with Security Manager.

When discovering SSL VPN policies, files residing in flash storage that are referenced in SSL VPN policies are copied to the Security Manager server to be stored in the /csm directory on the target device when policies are deployed from Security Manager. If the flash storage contains files that you want to

use, but they are not referenced by an SSL VPN policy, either configure commands that refer to them or manually copy them to the Security Manager server. Policy discovery fails if an SSL VPN policy on the device refers to a file that has been deleted from flash; in this case, either fix the configuration directly before discovering the device, or deselect the **RA VPN Policies** option when adding the device and create the desired SSL VPN configuration in Security Manager.

Note You should perform deployment immediately after you discover the policies on a device before you make any changes to policies or unassign policies from the device; otherwise, the changes that you configure in Security Manager might not be deployed to the device.

To perform discovery of all remote access VPN policies that are configured on a selected device in a remote access VPN, select the **RA VPN Policies** check box in the Discover Policies on Device dialog box. For more information, see Create Discovery Task and Bulk Rediscovery Dialog Boxes, page 5-18.

Related Topics

- Discovering Policies, page 5-12
- Discovering Policies on Devices Already in Security Manager, page 5-15
- VPN Discovery Rules, page 21-21

Using the Remote Access VPN Configuration Wizard

The Remote Access VPN Configuration wizard lets you quickly and easily configure a device as a remote access IPSec VPN server. After the policies are configured, specific security parameters defined in these policies are pushed to the client by the server, minimizing configuration on the client.

Depending on the device type and VPN type (IPSec or SSL), the wizard takes you through the steps to configure a basic remote access VPN.

To access the Remote Access Configuration wizard:

1. In Device view, select the device to configure as your remote access server from the Device selector.
2. Select **Remote Access VPN > Configuration Wizard** from the Policy selector.
3. Select the radio button corresponding to the type of remote access VPN you want to create: **Remote Access SSL VPN** or **Remote Access IPSec VPN**.
4. Click **Remote Access Configuration Wizard**.

The appropriate wizard opens.

This section contains the following topics:

- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 26-10
- Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 26-11
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices), page 26-12
- Creating IPSec VPNs Using the Remote Access VPN Configuration wizard (ASA Devices), page 26-14

Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices)

This procedure describes how to create or edit SSL VPNs on IOS devices using the Remote Access VPN Configuration Wizard.

Related Topics

- Understanding Remote Access SSL VPNs, page 26-3

Step 1 In Device view, select the desired IOS device.

Step 2 From the Policy selector, select **Remote Access VPN > Configuration Wizard**.

Step 3 Select the **Remote Access SSL VPN** radio button.

Step 4 Click **Remote Access Configuration Wizard**. The Gateway and Context page opens. For a description of the elements on this page, see Gateway and Context Page (IOS), page 27-10.

Step 5 Select the gateway to be used as a proxy for connections to the protected resources in your SSL VPN. Options are:

- **Use Existing Gateway**—Lets you use an existing gateway for your SSL VPN. If you select this option, specify the name of the gateway.
- **Create Using IP Address**—Lets you configure a new gateway using a reachable (public, static) IP address on the router.
- **Create Using Interface**—Lets you configure a new gateway using the public, static IP address of the router interface.

If you elected to create a new gateway using an IP address or an interface:

- Specify the number of the port that will carry the HTTPS traffic (between 1024 and 65535). The default is 443, unless HTTP port redirection is enabled, in which case the default HTTP port number is 80.
- Enter the digital certificate required to establish a secure connection. If you need to configure a specific CA certificate, a self-signed certificate is generated when an SSL VPN gateway is activated. All gateways on the router can use the same certificate.

Step 6 Enter the name of the context that identifies the resources needed to support the SSL VPN tunnel between remote clients and the corporate or private intranet.

Step 7 Enter the URL that will be displayed on the Portal page to access the SSL VPN gateway.

Step 8 Enter the names of the group policies that will be used in your SSL VPN connection, and whether Full Tunnel access mode is enabled or disabled for them (see Configuring User Group Policies, page 26-43).

Step 9 Enter the name of the authentication server group (LOCAL if the users are defined on the local device).

Step 10 Enter a list or method for SSL VPN remote user authentication.

Step 11 Enter the name of the accounting server group.

Step 12 Click **Next**. The Portal Page Customization page opens. For a description of the elements on this page, see Portal Page Customization Page, page 27-11.

Step 13 Enter the title to be displayed in the title bar of the portal page. The default title is “SSL VPN Service”.

Step 14 Enter the logo to be displayed on the title bar of the SSL VPN login and portal page. Options are:

- **None**—No logo is displayed.
- **Default**—Use the default logo.
- **Custom**—When selected, you can specify your own logo. Specify the source image file for the logo in the **Logo File** field, or click **Select** to select an image file.

The source image file for the logo can be a GIF, JPG, or PNG file, with a file name of up to 255 characters, and up to 100 kilobytes in size.

Step 15 Enter a message that will be displayed to the user upon login.

Step 16 Enter the color of the primary and secondary title bars on the login and portal pages of the SSL VPN.

Step 17 Enter the color of the text on the primary and secondary title bars of the login and portal pages. Options are white or black (the default).

Note The color of the text must be aligned with the color of the text on the title bar.

Step 18 If you want to preview how the portal page will appear, click **Preview**.

Step 19 Click **Finish** to save your definitions locally on the Security Manager client and close the dialog box.

Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices)

This procedure describes how to create or edit IPSec VPNs on IOS devices using the Remote Access VPN Configuration Wizard.

Related Topics

- Understanding Remote Access IPSec VPNs, page 26-2

Step 1 In Device view, select the desired IOS device.

Step 2 From the Policy selector, select **Remote Access VPN > Configuration Wizard**.

Step 3 Select the **Remote Access IPSec VPN** radio button.

Step 4 Click **Remote Access Configuration Wizard**. The User Group Policy page opens. For a description of the elements on this page, see User Group Policy Page (IOS), page 27-15.

Step 5 Select the required user groups from the Available User Groups list and click **>>**.

If the required user group is not in the list, click **Create** to open the User Groups Editor dialog box, which enables you to create or edit a user group object. See Add or Edit User Group Dialog Box, page 28-68.

Step 6 Click **Next**. The Defaults page opens. For a description of the elements on this page, see Defaults Page, page 27-16.

Step 7 Enter the defaults to be used for this IPSec VPN.

Step 8 Click **Finish** to save your definitions locally on the Security Manager client and close the dialog box.

Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (ASA Devices)

This procedure describes how to create or edit SSL VPNs on ASA devices using the Remote Access VPN Configuration Wizard.

Related Topics

- Understanding Remote Access SSL VPNs, page 26-3

Step 1 In Device view, select the desired ASA device.

Step 2 From the Policy selector, select **Remote Access VPN > Configuration Wizard**.

Step 3 Select the **Remote Access SSL VPN** radio button.

Step 4 Click **Remote Access Configuration Wizard**. The Access page opens. For a description of the elements on this page, see Access Page (ASA), page 27-2.

Step 5 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 6 Specify the port number you want to use for the SSL VPN sessions.

The default port is 443, for HTTPS traffic. The port number can be 443, or within the range of 1-65535. If you change the port number, all current SSL VPN connections terminate, and current users must reconnect.

Note If HTTP port redirection is enabled, the default HTTP port number is 80.

You can click **Select** to open the Port List Selector dialog box from which you can make your selection, or create a new port list.

Step 7 To allow users to select a tunnel group from a list of tunnel group connection profiles configured on the device at login, select the **Allow Users to Select Connection Profile in Portal Page** check box.

Step 8 To enable the AnyConnect functionality on the ASA device, select the **Enable AnyConnect Access** checkbox.

Step 9 Click **Next**. The Connection Profile page opens. For a description of the elements on this page, see Connection Profile Page (ASA), page 27-3.

Step 10 Enter a name for this Connection Profile.

Step 11 Enter or Select the name of the tunnel group that contains the policies for this SSL VPN connection profile.

Step 12 Specify the default Group Policy associated with the device. You can click **Edit** to open the Group Policy Selector. If the required Group Policy is not included in the list, click the Create button to open the Create User Group Wizard in which you can create a Group Policy. See Create User Group Wizard, page 27-6.

If you want to modify the properties of a Group Policy in the list, select it and click **Edit**. The Edit User Groups dialog box opens, enabling you to edit the Group Policy object.

Step 13 Specify the customization profile that defines the appearance of the portal page that allows the remote user access to all the resources available on the SSL VPN networks.

You can click **Select** to open the SSL VPN Customization Selector dialog box that lists all available customization objects, from which you can make your selection.

Note You can set up different login windows for different groups by using a combination of customization profiles and tunnel groups. For example, assuming that you had created a customization profile called salesgui, you can create an SSL VPN tunnel group called sales that uses that customization profile.

Step 14 Select a protocol (**http** or **https**) from the list, and specify the URL including the name of the connection profile, in the field provided.

Specify the URL that is associated with the connection profile. This URL provides users with direct access to the portal page of the connection profile. The URL is made up of the host name or IP address of the ASA device and port number, and the alias used to identify the SSL VPN connection profile.

Note If you do not specify a URL, you can access the portal page by entering the portal page URL, and then selecting the connection profile alias from a list of configured connection profile aliases configured on the device. See Access Page (ASA), page 27-2.

Step 15 Specify the address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to six pools.

If you want to use a different address pool, or select additional address pools, click **Select** to open the Network/Hosts selector from which you can make your selection(s).

Step 16 Enter the name of the authentication server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 17 If an external AAA server group is selected, you can enable fallback to the local database for authentication if the selected authentication server group fails.

Step 18 Enter the name of the authorization server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 19 Enter the name of the accounting server group. You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 20 Click **Finish** to save your definitions locally on the Security Manager client and close the dialog box.

Creating IPSec VPNs Using the Remote Access VPN Configuration wizard (ASA Devices)

This procedure describes how to create or edit IPSec VPNs on ASA devices using the Remote Access VPN Configuration Wizard.

Related Topics

- Understanding Remote Access IPSec VPNs, page 26-2

Step 1 In Device view, select the desired ASA device.

Step 2 From the Policy selector, select **Remote Access VPN > Configuration Wizard**.

Step 3 Select the **Remote Access IPSec VPN** radio button.

Step 4 Click **Remote Access Configuration Wizard**. The Connection Profile page opens. For a description of the elements on this page, see IPSec VPN Connection Profile Page (ASA), page 27-13.

Step 5 Enter a name for this IPSec VPN connection profile.

Step 6 Specify the default group policy associated with the device. You can click **Select** to open the ASA User Groups Selector from which you can select a user group from a list of objects.

If the required default user group is not included in the list, click **Create** to open the Create User Group Wizard. See Create User Group Wizard, page 27-6.

If you want to modify the properties of a user group in the list, select it and click **Edit**. The Edit User Groups dialog box opens.

Step 7 Enter the address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.

If you want to use a different address pool, or select additional address pools, click **Select** to open the Network/Hosts selector from which you can make your selection(s).

Step 8 Enter the name of the authentication server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 9 If you selected LOCAL for the authentication server group, you can enable fallback to the local database for authentication if the selected authentication server group fails.

Step 10 Enter the name of the authorization server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 11 Enter the name of the accounting server group. You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects.

Step 12 Click Next. The IPSec Settings page opens. For a description of the elements on this page, see IPSec Settings Page (ASA), page 27-14.

Step 13 Enter the value of the preshared key for the tunnel group. The maximum length of a preshared key is 127 characters.

Note You must retype this value in the Confirm field.

Step 14 Enter the trustpoint name if any trustpoints are configured. A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

Step 15 Select whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate. During IKE negotiations, peers must identify themselves to one another.

Step 16 To enable the sending of the certificate chain for authorization, select the **Enable Sending Certificate Chain** check box. A certificate chain includes the root CA certificate, identity certificate, and key pair.

Step 17 To enable passwords to be updated with the RADIUS authentication protocol, select the **Enable Password Update with RADIUS Authentication** check box. For more information, see Supported AAA Server Types, page 6-21.

Step 18 Specify the following ISAKMP Keepalive settings:

- To configure IKE keepalive as the default failover and routing mechanism, select the **Monitor Keepalive** check box. For more information, see Understanding ISAKMP/IPsec Settings, page 22-13.
- Enter the number of seconds that a device waits between sending IKE keepalive packets.
- Enter the number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.

Step 19 Configure the specific revision level and image URL of the VPN clients.

Step 20 Click **Next**. The Defaults page opens. For a description of the elements on this page, see Defaults Page, page 27-16.

Step 21 Enter the defaults to be used for this IPSec VPN.

Step 22 Click **Finish** to save your definitions locally on the Security Manager client and close the dialog box.

Working with Policies Pertaining to Both IPSec and SSL VPNs

Certain policies can be configured and applied to both IPSec and SSL VPNs.

This section contains the following topics:

Understanding Cluster Load Balancing (ASA)

In a remote client configuration in which you are using two or more devices connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. Load balancing is effective only on remote sessions initiated with an ASA device.

To implement load balancing, you must group two or more devices on the same private LAN-to-LAN network into a virtual cluster. All devices in the virtual cluster carry session loads. One device in the virtual cluster, called the virtual cluster master, directs incoming calls to the other devices, called secondary devices. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly.

The virtual cluster appears to outside clients as a single virtual cluster IP address. This IP address is not tied to a specific physical device—it belongs to the current virtual cluster master. A VPN client trying to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available host in the cluster. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

The role of virtual cluster master is not tied to a physical device—it can shift among devices. If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to another active device in the cluster. Should the virtual cluster master itself fail, a secondary device in the cluster immediately takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is available.

Understanding Redirection Using a Fully Qualified Domain Name (FQDN)

By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a secondary device. As a VPN cluster master, this security appliance can send a fully qualified domain name (FQDN) of a cluster device (another security appliance in the cluster) when redirecting VPN client connections to that cluster device. The security appliance uses reverse DNS lookup to resolve the FQDN of the device to its outside IP address to redirect connections and perform VPN load balancing. All outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

After you enable load balancing using FQDNs, add an entry for each of your ASA outside interfaces into your DNS server, if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup. Enable DNS lookups on your ASA and define your DNS server IP address on the ASA.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 26-5
- Configuring Cluster Load Balance Policies (ASA), page 26-17
- ASA Cluster Load Balance Page, page 27-17

Configuring Cluster Load Balance Policies (ASA)

The Cluster Load Balance page enables you to configure load balancing on your VPN device. You must explicitly enable load balancing, as it is disabled by default. All devices that participate in a cluster must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.

Related Topics

- Understanding Cluster Load Balancing (ASA), page 26-16

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > ASA Cluster Load Balance** from the Policy selector.
- (Policy view) Select **Remote Access VPN > ASA Cluster Load Balance** from the Policy Type selector. Select an existing policy or create a new one.

The ASA Cluster Load Balance page opens. For a description of the elements on this page, see ASA Cluster Load Balance Page, page 27-17.

Step 2 Select the **Participating in Load Balancing Cluster** check box to specify the device belongs to the load-balancing cluster.

Step 3 Specify the single IP address that represents the entire virtual cluster. Choose an IP address that is in the same subnet as the external interface.

Step 4 Specify the UDP port for the virtual cluster to which the device belongs. If another application is using this port, enter the UDP destination port number to use for load balancing. The default is 9023.

Step 5 If required, select **Enable IPsec Encryption** to ensure that all load-balancing information communicated between the devices is encrypted.

Step 6 If you selected the **Enable IPsec Encryption** check box, you must specify an **IPsec Shared Secret** password. The security appliances in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec. This password must match the passwords passed on by the client.

Step 7 In the **Priority** area, select one of the following options:

- **Accept default device value**—To accept the default priority value assigned to the device.
- **Configure same priority on all devices in the cluster**—To configure the same priority value to all the devices in the cluster. Then enter the priority number (1-10) to indicate the likelihood of the device becoming the virtual cluster master, either at startup or when the existing master fails.

Step 8 Specify the public and private interfaces to be used on the server.

Note Interfaces are objects. You can click **Select** to open a dialog box that lists all available interface roles and interfaces and in which you can create interface role objects. For more information, see Understanding Interface Role Objects, page 6-55.

Step 9 If required, select the **Send FQDN to client instead of an IP address when redirecting** check box to enable redirection using FQDNs. This check box is available only for ASA devices running 8.0.2 or later. For more information, see Understanding Cluster Load Balancing (ASA), page 26-16.

Note To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Understanding Connection Profiles (ASA)

A connection profile is a set of records which contain VPN tunnel connection policies, including the attributes that pertain to creating the tunnel itself. Connection profiles identify the group policies for a specific connection, which includes user-oriented attributes. If you do not assign a group policy to a user, the default connection profile for the connection applies. You can create one or more connection profiles specific to your environment. You can configure connection profiles on the local remote access VPN server or on external AAA servers.

If you are configuring a connection profile on an ASA device, you have the option of configuring double authentication. The double authentication feature implements two-factor authentication for remote access to the network, in accordance with the Payment Card Industry Standards Council Data Security Standard. This feature requires that the user enter two separate sets of login credentials at the login page. For example, the primary authentication might be a one-time password, and the secondary authentication might be a domain (Active Directory) credential. If the primary credential authentication fails, the security appliance does not attempt to validate the secondary credentials. If either authentication fails, the connection is denied. Both the AnyConnect VPN client and Clientless WebVPN support double authentication. The AnyConnect client supports double authentication on Windows computers (including supported Windows Mobile devices and Start Before Login), Mac computers, and Linux computers.

Related Topics

- Configuring Connection Profiles (ASA), page 26-18
- Connection Profiles Page, page 27-18

Configuring Connection Profiles (ASA)

This procedure describes how to create or edit connection profiles on your remote access VPN server using the Connection Profile option on the Policy selector.

Note You can also create or edit connection profiles from the Remote Access VPN Configuration wizard. For more information, see Using the Remote Access VPN Configuration Wizard, page 26-9.

Related Topics

- Understanding Connection Profiles (ASA), page 26-18
- Remote Access VPN Configuration Wizard, page 27-1

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Connection Profiles** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Connection Profiles (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Connection Profiles page opens. For a description of the elements on this page, see Connection Profiles Page, page 27-18.

Step 2 Click **Create** in the Connection Profiles page, or select a device from the table on the Connection Profiles page and click **Edit**. The Connection Profiles dialog box opens with the General tab open by default.

Step 3 On the General tab, specify the connection profile name and group policies and select which method (or methods) of address assignment to use. For a description of the elements on the tab, see Table 27-15 on page 27-20.

Step 4 Click the **AAA** tab to specify the AAA authentication parameters for an SSL VPN connection profile policy. For a description of the elements on the tab, see Table 27-17 on page 27-22.

Step 5 If you are setting up a connection profile on an ASA device, you can configure secondary authentication. To do so, click the **Secondary AAA** tab. For a description of the elements on the tab, see Secondary AAA Tab (Connection Profiles), page 27-25.

Step 6 Click the **IPsec** tab to specify IPsec and IKE parameters for the connection profile. For a description of the elements on the tab, see Table 27-20 on page 27-28.

Step 7 Click the **SSL** tab to specify the WINS servers for the connection profile policy, select a customized look and feel for the SSL VPN end-user logon web page, specify DHCP servers to be used for client address assignment, and establish an association between an interface and client IP address pools. For a description of the elements on the tab, see Table 27-22 on page 27-30.

Step 8 Click **OK**.

Understanding Dynamic Access Policies

Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

Dynamic access policies (DAP) on a security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session. The DAP system includes the following components that require your attention:

- DAP Selection Configuration File—A text file containing criteria that the security appliance uses for selecting and applying DAP records during session establishment. It is stored on the security appliance. You can use Security Manager to modify it and upload it to the security appliance in XML

data format. DAP selection configuration files include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding, and URL lists.

- DfltAccess Policy—Always the last entry in the DAP summary table, always with a priority of 0. You can configure Access Policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes. You cannot delete the DfltAccessPolicy, and it must be the last entry in the summary table.

Tip Dynamic Access policies take precedence over Group policies. If a setting is not specified in a Dynamic Access policy, an ASA device checks for Group policies that specify the setting.

Integration of Cisco Secure Desktop with DAP

The security appliance integrates the Cisco Secure Desktop (CSD) features into dynamic access policies (DAPs). Depending on the configuration, the security appliance uses one or more endpoint attribute values in combination with optional, AAA attribute values as conditions for assigning a DAP. The Cisco Secure Desktop features supported by the endpoint attributes of DAPs include OS detection, prelogin policies, Basic Host Scan results, and Endpoint Assessment.

As an administrator, you can specify a single attribute or combine attributes that together form the conditions required to assign a DAP to a session. The DAP provides network access at the level that is appropriate for the endpoint AAA attribute value. The security appliance applies a DAP when all of its configured endpoint criteria are satisfied.

Related Topics

- Configuring Dynamic Access Policies, page 26-20
- Configuring DAP Attributes, page 26-25

Configuring Dynamic Access Policies

This procedure describes how to create or edit a dynamic access policy.

Related Topics

- Understanding Dynamic Access Policies, page 26-19
- Understanding DAP Attributes, page 26-22
- Configuring Cisco Secure Desktop Policies on ASA Devices, page 26-26

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 27-33.

Step 2 Click **Create** or select a policy in the table and click **Edit**.

The Add/Edit Dynamic Access Policy dialog box opens, with the Main tab open by default. For a description of the elements in this dialog box, see Table 27-26 on page 27-35.

Step 3 Enter the name of the DAP record (up to 128 characters).

Step 4 Specify a priority for the DAP record. The security appliance applies access policies in the order you set here, highest number having the highest priority.

Step 5 Enter a description for the DAP record.

Step 6 In the **Main** tab, configure the DAP attributes and the type of remote access method supported by the DAP system on your security appliance. For a detailed description of the elements on this tab, see Table 27-27 on page 27-36.

a. Click **Create** below the table, or select a DAP entry in the table and click **Edit**. The Add/Edit DAP Entry dialog box opens. For a description of the elements on this dialog box, see Table 27-28 on page 27-41.

   For a full description of the procedure to define the DAP attributes, see Configuring DAP Attributes, page 26-25.

b. Select the type of remote access permitted by the DAP system.

c. Select the **Network ACL** tab to select and configure network ACLs to apply to this DAP record.

   This tab is available only if you selected an access method other than Web Portal.

d. Select the **WebType ACL** tab to select and configure Web-type ACLs to apply to this DAP record.

   This tab is available only if you selected an access method other than AnyConnect Client.

e. Select the **Functions** tab to configure file server entry and browsing, HTTP proxy, and URL entry for the DAP record.

   This tab is available only if you selected an access method other than AnyConnect Client.

f. Select the **Port Forwarding** tab to select and configure port forwarding lists for user sessions.

   This tab is available only if you selected an access method other than AnyConnect Client.

g. Select the **URL List** tab to select and configure URL lists for user sessions.

   This tab is available only if you selected an access method other than AnyConnect Client.

h. Select the **Action** tab to configure the type of remote access permitted.

   This tab is available for all types of access methods.

Step 7 Select the **Logical Operators** tab to create multiple instances of each type of endpoint attribute. For a description of the elements on this tab, see Table 27-43 on page 27-56.

Step 8 Select the **Advanced Expressions** tab to set additional attributes for the DAP using free-form LUA. For a description of the elements on this tab, see Table 27-44 on page 27-59.

Step 9 Click **OK**.

Understanding DAP Attributes

DAP records include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding and URL lists.

DAP and AAA Attributes

DAP complements AAA services. It provides a limited set of authorization attributes that can override those AAA provides. The security appliance selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The security appliance can select multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

You can specify AAA attributes from the Cisco AAA attribute hierarchy, or from the full set of response attributes that the security appliance receives from a RADIUS or LDAP server.

AAA Attribute Definitions

Table 26-1 on page 26-22 defines the AAA selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do on the Advanced tab of the Add/Edit Dynamic Access Policy dialog box.

Table 26-1 AAA Attribute Definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Cisco	aaa.cisco.memberof	AAA	string	128	memberof value
	aaa.cisco.username	AAA	string	64	username value
	aaa.cisco.class	AAA	string	64	class attribute value
	aaa.cisco.ipaddress	AAA	number	–	framed-ip address value
	aaa.cisco.tunnelgroup	AAA	string	64	tunnel-group name
LDAP	aaa.ldap.<label>	LDAP	string	128	LDAP attribute value pair
RADIUS	aaa.radius.<number>	RADIUS	string	128	Radius attribute value pair

DAP and Endpoint Security

The security appliance obtains endpoint security attributes by using posture assessment methods that you configure. These include Cisco Secure Desktop and NAC. You can use a match of a prelogin policy, Basic Host Scan entry, Host Scan Extension, or any combination of these and any other policy attributes to assign access rights and restrictions. At minimum, configure DAPs to assign to each prelogin policy and Basic Host Scan entry.

Endpoint Assessment, a Host Scan extension, examines the remote computer for a large collection of antivirus and antispyware applications, associated definitions updates, and firewalls. You can use this feature to combine endpoint criteria to satisfy your requirements before the security appliance assigns a specific DAP to the session.

DAP and Anti-Virus, Anti-Spyware, and Personal Firewall Programs

The security appliance uses a DAP policy when the user attributes matches the configured AAA and endpoint attributes. The Prelogin Assessment and Host Scan modules of Cisco Secure Desktop return information to the security appliance about the configured endpoint attributes, and the DAP subsystem uses that information to select a DAP record that matches the values of those attributes. Most, but not all, anti-virus, anti-spyware, and personal firewall programs support active scan, which means that the programs are memory-resident, and therefore always running. Host Scan checks to see if an endpoint has a program installed, and if it is memory-resident as follows:

- If the installed program does not support active scan, Host Scan reports the presence of the software. The DAP system selects DAP records that specify the program.
- If the installed program does support active scan, and active scan is enabled for the program, Host Scan reports the presence of the software. Again the security appliance selects DAP records that specify the program.
- If the installed program does support active scan and active scan is disabled for the program, Host Scan ignores the presence of the software. The security appliance does not select DAP records that specify the program. Further, the output of the **debug trace** command, which includes a lot of information about DAP, does not indicate the program presence, even though it is installed.

Endpoint Attribute Definitions

Table 26-2 on page 26-23 defines the endpoint selection attribute names that are available for DAP use. The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do on the Advanced tab of the Add/Edit Dynamic Access Policy dialog box. The *label* variable identifies the application, filename, process, or registry entry.

Table 26-2 Endpoint Attribute Definitions

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Antispyware (Requires Cisco Secure Desktop)	endpoint.as.label.exists	Host Scan	true	–	Antispyware program exists
	endpoint.as.label.version		string	32	Antispyware description
	endpoint.as.label.description		string	128	class attribute value
	endpoint.as.label.lastupdate		integer	–	Seconds since update of antispyware definitions
Antivirus (Requires Cisco Secure Desktop)	endpoint.av.label.exists	Host Scan	true	–	Antivirus program exists
	endpoint.av.label.version		string	32	Antivirus description
	endpoint.av.label.description		string	128	class attribute value
	endpoint.av.label.lastupdate		integer	–	Seconds since update of antivirus definitions
Application	endpoint.application.clienttype	Application	string	–	Client type: CLIENTLESS ANYCONNECT IPSEC L2TP

Table 26-2 Endpoint Attribute Definitions (Continued)

File	endpoint.file.label.exists	Secure Desktop	true	–	The files exists
	endpoint.file.label.lastmodified		integer	–	Seconds since file was last modified
	endpoint.file.label.crc.32		integer	–	CRC32 hash of the file
NAC	endpoint.nac.status	NAC	string	-	User defined status string
Operating System	endpoint.os.version	Secure Desktop	string	32	Service pack for Windows
	endpoint.os.servicepack		integer	–	Operating system
Personal firewall (Requires Secure Desktop)	endpoint.fw.label.exists	Host Scan	true	–	The personal firewall exists
	endpoint.fw.label.version		string	32	Version
	endpoint.fw.label.description		string	128	Personal firewall description
Policy	endpoint.policy.location	Secure Desktop	string	64	Location value from Cisco Secure Desktop
Process	endpoint.process.label.exists	Secure Desktop	true	–	The process exists
	endpoint.process.label.path		string	255	Full path of the process
Registry	endpoint.registry.label.type	Secure Desktop	dword string	–	dword
	endpoint.registry.label.value		string	255	Value of the registry entry
VLAN	endpoint.vlan.type	CNA	sting	–	VLAN type: ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

About Advanced Expressions for AAA or Endpoint Attributes

In the text box you enter free-form LUA text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP policy file, and the security appliance processes it, discarding any expressions it cannot parse.

This option is useful for adding selection criteria other than what is possible in the AAA and endpoint attribute areas above. For example, while you can configure the security appliance to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to create appropriate logical expressions in LUA and enter them here.

Examples of DAP Logical Expressions

Study these examples for help in creating logical expressions in LUA.

- This AAA LUA expression tests for a match on usernames that begin with “b”; it uses the string library and a regular expression:

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- This endpoint expression tests for a match on CLIENTLESS OR CVC client types:

```
endpoint.application.clienttype=="CLIENTLESS" or endpoint.application.clienttype=="CVC"
```

- This endpoint expression tests for Norton Antivirus versions 10.x but excludes 10.5.x:

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or endpoint.av.NortonAV.version > "10.6"
```

DAP Connection Sequence

The following sequence outlines a typical remote access connection establishment.

1. A remote client attempts a VPN connection.
2. The security appliance performs posture assessment, using configured NAC and Cisco Secure Desktop Host Scan values.
3. The security appliance authenticates the user via AAA. The AAA server also returns authorization attributes for the user.
4. The security appliance applies AAA authorization attributes to the session, and establishes the VPN tunnel.
5. The security appliance selects DAP records based on the user AAA authorization information and the session posture assessment information.
6. The security appliance aggregates DAP attributes from the selected DAP records, and they become the DAP policy.
7. The security appliance applies the DAP policy to the session.

Related Topics

- Configuring Dynamic Access Policies, page 26-20
- Understanding Dynamic Access Policies, page 26-19
- Configuring DAP Attributes, page 26-25

Configuring DAP Attributes

The attributes you must define for a DAP policy include specifying the authorization attributes and endpoint attributes. You can also configure network and webtype ACLs, file browsing, file server entry, HTTP proxy, URL entry, port forwarding lists and URL lists.

This procedure describes how to create or edit the AAA and endpoint attributes required for a DAP policy.

Related Topics

- Understanding DAP Attributes, page 26-22

  Understanding Dynamic Access Policies, page 26-19
- Configuring Dynamic Access Policies, page 26-20

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 27-33.

Step 2 Click **Create** on the Dynamic Access policy page, or select the row of a policy in the table on the page, and click **Edit**.

The Add/Edit Dynamic Access Policy dialog box opens, displaying the Main tab. For a description of the elements on the Main tab, see Table 27-27 on page 27-36.

Step 3 Click **Create** below the table, or select a DAP entry in the table and click **Edit**. The Add/Edit DAP Entry dialog box opens. For a description of the elements on this dialog box, see Table 27-28 on page 27-41.

Step 4 Select the attribute type from the Criterion list, then enter the appropriate values. The dialog box values vary based on your selection. Options are:

- AAA Attributes Cisco; see Table 27-29 on page 27-43.
- AAA Attributes LDAP; see Table 27-30 on page 27-44.
- AAA Attributes RADIUS; see Table 27-31 on page 27-45.
- Anti-Spyware; see Table 27-32 on page 27-46.
- Anti-Virus; see Table 27-33 on page 27-47.
- Application; see Table 27-34 on page 27-48.
- File; see Table 27-36 on page 27-49.
- NAC; see Table 27-37 on page 27-50.
- Operating System; see Table 27-38 on page 27-51.
- Personal Firewall; see Table 27-39 on page 27-52.
- Policy; see Table 27-40 on page 27-53.
- Process; see Table 27-41 on page 27-54.
- Registry; see Table 27-42 on page 27-55.

Step 5 Click **OK**.

Configuring Cisco Secure Desktop Policies on ASA Devices

Cisco Secure Desktop (CSD) provides a reliable means of eliminating 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 an 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. This ensures that cookies, browser history, temporary files, and downloaded content do not remain on a system.

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.

Note A complete explanation of the capabilities and configuration of the Cisco Secure Desktop program is beyond the scope of this document. For information about configuring CSD, and what CSD can do for you, see the materials available online at http://www.cisco.com/en/US/products/ps6742/tsd_products_support_configure.html. Select the configuration guide for the CSD version you are configuring.

This procedure describes how to configure the Cisco Secure Desktop feature on an ASA device.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 26-5

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Dynamic Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Dynamic Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Dynamic Access page opens. For a description of the elements on this page, see Dynamic Access Page (ASA), page 27-33.

Step 2 In the Cisco Secure Desktop section, select **Enable** to enable CSD on the ASA device.

Step 3 In the **Package** field, specify the name of the File Object that identifies the Cisco Secure Desktop package you want to upload to the device. Click **Select** to select an existing File Object or to create a new one. For more information, see Add and Edit File Object Dialog Boxes, page 28-24.

Note The package version must be compatible with the ASA operating system version. When you create a local policy in Device view, the **Version** field indicates the CSD package version you should select. (The version is included in the package file name. For example, securedesktop-asa_k9-3.3.0.118.pkg is CSD version 3.3.0.118.) When you create a shared policy in Policy view, the **Version** field indicates the version of the CSD file you selected. For more information on version compatibility, see Understanding and Managing SSL VPN Support Files, page 26-5.

Step 4 Click **Configure** to open the Cisco Secure Desktop Manager (CSDM) Policy Editor that lets you configure CSD on the security appliance. This application is independent of Security Manager; read the CSD documentation cited above for an explanation of how to use the policy editor.

The editor contains these main items (select them in the table of contents):

- Prelogin Policies—This is a decision tree. When a user attempts a connection, the user's system is evaluated against your rules and the first rule that matches is applied. Typically, you create policies for secure locations, home locations, and insecure public locations. You can make your checks based on registry information, the presence of specific files or certificates, the workstation's operating system, or IP address.

  All editing is done through the right-click menu. Right click on boxes or + signs to activate related settings, if any.

  For end nodes, you can select these options:

  - Access Denied—Workstations that match your criteria are prevented from accessing the network.
  - Policy—You want to define a specific admission policy at this point. After naming the policy, it is added to the table of contents. Select each item in the policy and configure its settings.
  - Subsequence—You want to perform additional checks. Enter the name of the next decision tree that you want to evaluate for this workstation.

- Host scan—You can specify a set of registry entries, file names, and process names, which form a part of the basic host scan. The host scan occurs after the prelogin assessment but before the assignment of a dynamic access policy. Following the basic host scan, the security appliance uses the login credentials, the host scan results, prelogin policy, and other criteria you configure to assign a dynamic access policy. You can also enable:
  - Endpoint Assessment—The remote workstation scans for a large collection of antivirus, antispyware, and personal firewall applications, and associated updates.
  - Advanced Endpoint Assessment—Includes all of the Endpoint Assessment features, and lets you configure an attempt to update noncompliant workstations to meet the version requirements you specify. You must purchase and install a license for this feature before you can configure it.

Understanding Remote Access VPN Global Settings

On the VPN Global Settings page, you can define global settings for IKE, IPsec, NAT, and fragmentation that apply to devices in your remote access VPN.

A full description of VPN global settings is provided in Understanding VPN Global Settings, page 22-12.

Global VPN settings comprise:

- ISAKMP/IPsec settings that enable you to configure ISAKMP (IKE) and IPsec parameters that allow peers to negotiate in establishing a VPN tunnel in a remote access VPN. For more information, see Understanding ISAKMP/IPsec Settings, page 22-13.
- Network Address Translation (NAT) settings to enable devices that use internal IP addresses to send and receive data through the Internet. For more information, see Understanding NAT, page 22-13.
- General Settings, including fragmentation settings and the maximum transmission unit (MTU) handling parameters that you can configure on the devices in your remote access VPN. For more information, see Understanding Fragmentation, page 22-15.

Related Topics

- Configuring Remote Access VPN Global Settings, page 26-28
- Global Settings Page, page 27-60

Configuring Remote Access VPN Global Settings

Follow the procedure below to define global settings in your remote access VPN.

Related Topics

- Understanding Remote Access VPN Global Settings, page 26-28

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > Global Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Global Settings** from the Policy Type selector. Select an existing policy or create a new one.

The VPN Global Settings page opens. For a description of the elements on this page, see Global Settings Page, page 27-60.

Step 2 In the **ISAKMP/IPsec Settings** tab (see ISAKMP/IPsec Settings Tab, page 27-60), specify global settings for IKE and IPsec, as follows:

a. Select **Enable Keepalive** to configure IKE keepalive as the default failover and routing mechanism for your devices. (Applies to Cisco IOS routers, Catalyst 6500 /7600 devices, and PIX Firewalls version 6.3.)

b. Enter the number of seconds a device must wait between sending IKE keepalive packets.

c. Enter the number of seconds a device must wait between attempts to establish an IKE connection with the remote peer.

d. Select **Periodic** if you want to send dead-peer detection (DPD) keepalive messages, even if there is no outbound traffic to be sent (for routers except 7600).

e. Specify whether the device uses an IP address or hostname to identify itself in IKE negotiations. You can also specify to use a distinguished name (DN) to identify a user group name.

f. Specify the maximum number of SA requests allowed before IKE starts rejecting them (for routers except 7600).

g. Specify the percentage of system resources that can be used before IKE starts rejecting new SA requests (for Cisco IOS routers and Catalyst 6500 /7600 devices).

h. Select **Enable Lifetime** to configure the global lifetime settings for the crypto IPsec SAs on the devices in your remote access VPN.

i. Specify the number of seconds an SA will exist before expiring.

j. Specify the volume of traffic (in kilobytes) that can pass between IPsec peers using a given SA before it expires.

k. Specify the Xauth timeout, that is, the number of seconds the device will wait for a system response to the Xauth challenge (Cisco IOS routers and Catalyst 6500 /7600 devices).

l. Specify the maximum number of SAs that can be enabled simultaneously on the device (ASA or PIX 7.0 devices only).

m. Select **Enable IPsec via Sysopt** to specify that any packet that comes from an IPsec tunnel be implicitly trusted (PIX 6.3, PIX 7.0, and ASA devices only).

Step 3 Click the **NAT Settings** tab to define global NAT settings that apply to devices that use internal IP addresses to send and receive data through the public Internet. For a description of the elements on the **NAT Settings** tab, see NAT Settings Tab, page 27-63.

a. Select **Enable Traversal Keepalive** for the transmission of keepalive messages when a device (referred to as the middle device) located between a VPN-connected hub and spoke performs NAT on the IPsec flow.

b. Specify the interval (between 5 and 3600 seconds) between the keepalive signals sent between the spoke and the middle device to indicate that the session is active.

c. Select **Enable Traversal over TCP** (for ASA or PIX 7.0 devices only) to encapsulate both the IKE and IPsec protocols within a TCP packet, and enable secure tunneling through both NAT and PAT devices and firewalls.

d. Enter the TCP ports for which you want to enable NAT traversal (ASA or PIX 7.0 devices only).

Step 4 Click the **General Settings** tab to define fragmentation and other global settings on the devices in your remote access VPN. For a description of the elements on the **General Settings** tab, see General Settings Tab, page 27-64.

a. Select the fragmentation mode from the following options:

- **No Fragmentation**—Select if you do not want to fragment before IPsec encapsulation.
- **End to End MTU Discovery**—Select to use ICMP messages for the discovery of MTU.
- **Local MTU Handling**—Select to set the MTU locally on the devices. This option is typically used when ICMP is blocked.

See Understanding Fragmentation, page 22-15.

b. Specify the MTU size (between 68 and 65535 bytes depending on the VPN interface).

c. Select the required setting for the DF bit (for Cisco IOS routers, ASA, or PIX 7.0 devices)—**Copy**, **Set**, or **Clear**.

d. Select **Enable Fragmentation Before Encryption** (for Cisco IOS routers, ASA, or PIX 7.0 devices) to fragment before encryption, if the expected packet size exceeds the MTU (Cisco IOS routers only).

e. Select **Enable Notification on Disconnection** (for ASA or PIX 7.0 devices only) to notify qualified peers of sessions that are about to be disconnected.

f. Select **Enable Spoke-to-Spoke Connectivity** through the Hub (for ASA, or PIX 7.0 devices only) to enable direct communication between spokes in a hub-and-spoke VPN topology, in which the hub is an ASA device or a PIX Firewall version 7.0.

g. Select **Enable Default Route** (for Cisco IOS routers only) to use the device's configured external interface as the default outbound route for all incoming traffic.

Understanding Group Policies (ASA)

When you configure a remote access IPSec or SSL VPN connection, you must create user groups to which remote clients will belong. A user group policy is a set of user-oriented attribute/value pairs for remote access VPN connections that are stored either internally (locally) on the device or externally on an AAA server. The connection profile uses a user group policy that sets terms for user connections after the connection 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.

Tip Dynamic Access policies take precedence over Group policies. If a setting is not specified in a Dynamic Access policy, an ASA device checks for Group policies that specify the setting.

An ASA user group comprises the following attributes:

- Group policy source—Identifies whether the user group's attributes and values are stored internally (locally) on the security appliance or externally on an AAA server. If the user group is an external type, no other settings need to be configured for it. For more information, see ASA Group Policies Dialog Box, page 28-1.
- Client Configuration settings, which specify the Cisco client parameters for the user group in an Easy VPN or remote access VPN. For more information, see ASA Group Policies Client Configuration Settings, page 28-4.

- Client Firewall Attributes, which configure the firewall settings for VPN clients in an Easy VPN or remote access VPN. For more information, see ASA Group Policies Client Firewall Attributes, page 28-5.
- Hardware Client Attributes, which configure the VPN 3002 Hardware Client settings in an Easy VPN or remote access VPN. For more information, see ASA Group Policies Hardware Client Attributes, page 28-7.
- IPsec settings, which specify tunneling protocols, filters, connection settings, and servers for the user group in an Easy VPN or remote access VPN. For more information, see ASA Group Policies IPSec Settings, page 28-9.
- Clientless settings, which configure the Clientless mode of access to the corporate network in an SSL VPN, for the ASA user group. For more information, see ASA Group Policies SSL VPN Clientless Settings, page 28-11.
- Full Client settings, which configure the Full Client mode of access to the corporate network in an SSL VPN, for the ASA user group. For more information, see ASA Group Policies SSL VPN Full Client Settings, page 28-13.
- General settings that are required for Clientless/Port Forwarding in an SSL VPN. For more information, see ASA Group Policies SSL VPN Settings, page 28-15.
- DNS/WINS settings that define the DNS and WINS servers and the domain name that should be pushed to remote clients associated with the ASA user group. For more information, see ASA Group Policies DNS/WINS Settings, page 28-18.
- Split tunneling that lets a remote client conditionally direct packets over an IPsec or SSL VPN tunnel in encrypted form or to a network interface in clear text form. For more information, see ASA Group Policies Split Tunneling Settings, page 28-19.
- Remote access or SSL VPN session connection settings for the ASA user group. For more information, see ASA Group Policies Connection Settings, page 28-20.

Related Topics

- Creating Group Policies (ASA), page 26-31
- Group Policies Page, page 27-66

Creating Group Policies (ASA)

Use the Group Policies page to create group policies for ASA devices used in remote access IPSec or SSL VPNs.

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > Group Policies** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Group Policies (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Group Policies page opens. For a description of the elements on this page, see Group Policies Page, page 27-66.

Step 2 Click **Create** to open a dialog box from which you can select a user group from a list of predefined ASA user group objects, or create new ones if necessary.

Step 3 Select the required ASA user group from the list and click **OK**, or if the required ASA user group does not exist, create it by clicking **Create**.

The Add ASA User Group dialog box appears, displaying a list of settings that you can configure for the ASA user group object. For a description of the elements on this dialog box, see ASA Group Policies Dialog Box, page 28-1.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Select whether to store the ASA user group's attributes and values locally on the device, or on an external server.

Note If you selected to store the ASA user group's attributes on an external server, you do not need to configure any Technology settings. After you specify the AAA server group that will be used for authentication and a password to the AAA server, click **OK** and then select the group in the object selector and click **OK** to add it to the policy.

Step 6 If you selected to store the ASA user group's attributes locally on the device, select the type of VPN for which you are creating the ASA user group from the **Technology** list.

Step 7 To configure the user group for an Easy VPN/IPSec VPN, from the Easy VPN/IPSec VPN folder in the Settings pane:

a. Select **Client Configuration** to configure the Cisco client parameters. For a description of these settings, see ASA Group Policies Client Configuration Settings, page 28-4.

b. Select **Client Firewall Attributes** to configure the firewall settings for VPN clients. For a description of these settings, see ASA Group Policies Client Firewall Attributes, page 28-5.

c. Select **Hardware Client Attributes** to configure the VPN 3002 Hardware Client settings. For a description of these settings, see ASA Group Policies Hardware Client Attributes, page 28-7.

d. Select **IPsec** to specify tunneling protocols, filters, connection settings, and servers. For a description of these settings, see ASA Group Policies IPSec Settings, page 28-9.

Step 8 To configure the user group for an SSL VPN, from the SSL VPN folder in the Settings pane:

a. Select **Clientless** to configure the Clientless mode of access to the corporate network in an SSL VPN. For a description of these settings, see ASA Group Policies SSL VPN Clientless Settings, page 28-11.

b. Select **Full Client** to configure the Full Client mode of access to the corporate network in an SSL VPN. For a description of these settings, see ASA Group Policies SSL VPN Full Client Settings, page 28-13.

c. Select **Settings** to configure the general settings that are required for clientless and thin client (port forwarding) access modes in an SSL VPN. For a description of these settings, see ASA Group Policies SSL VPN Settings, page 28-15.

Step 9 Specify the following settings for an ASA user group in an Easy VPN/IPSec VPN and SSL VPN configuration, in the Settings pane:

a. Select **DNS/WINS** to define the DNS and WINS servers and the domain name that should be pushed to clients associated with the ASA user group. For a description of these settings, see ASA Group Policies DNS/WINS Settings, page 28-18.

b. Select **Split Tunneling** to allow a remote client to conditionally direct encrypted packets through a secure tunnel to the central site and simultaneously allow clear text tunnels to the Internet through a network interface. For a description of these settings, see ASA Group Policies Split Tunneling Settings, page 28-19.

c. Select **Connection Settings** to configure the SSL VPN connection settings for the ASA user group, such as the session and idle timeouts, including the banner text. For a description of these settings, see ASA Group Policies Connection Settings, page 28-20.

Step 10 Click **OK**.

Step 11 Select the ASA user group from the list and click **OK**.

Configuring Public Key Infrastructure Policies

This procedure describes how to specify the CA servers that will be used to create a Public Key Infrastructure (PKI) policy in your remote access VPN.

Note In remote access VPNs, digital certificates are used for user authentication. When creating or editing a PKI enrollment object, you must configure each remote component (spoke) with the name of the user group to which it connects.

Before You Begin

- For IOS devices, make sure the selected device has release 12.3(7)T or later.
- Please read Prerequisites for Successful PKI Enrollment, page 22-28.

Related Topics

- Understanding Public Key Infrastructure Policies, page 22-26
- Prerequisites for Successful PKI Enrollment, page 22-28
- Public Key Infrastructure Page, page 27-66

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > Public Key Infrastructure** from the Policy selector.
- (Policy view) Select **Remote Access VPN > Public Key Infrastructure** from the Policy Type selector. Select an existing policy or create a new one.

The Public Key Infrastructure page opens. For a description of the elements on this page, see Public Key Infrastructure Page, page 27-66.

Step 2 Select the required CA servers from the Available CA Servers list and click **>>**.

If the required CA server is not included in the list, click **Create** to open the PKI Enrollment dialog box which enables you to create or edit a PKI enrollment object.

Keep the following in mind:

- When creating or editing a PKI enrollment object, make sure you configure each remote component (spoke) with the name of the user group to which it connects. You specify this information in the Organization Unit (OU) field in the Certificate Subject Name tab of the PKI Enrollment Editor dialog box. In addition, the certificate issued to the client should have OU as the name of the user group. For more information, see PKI Enrollment Dialog Box, page 28-33.

- Remote clients should also be configured to use digital certificates for user authentication during IKE negotiations, by specifying the user group name when configuring ISAKMP settings (see Configuring Remote Access VPN Global Settings, page 26-28).
- To save the RSA key pairs and the CA certificates permanently between reloads to flash memory on a PIX version 6.3, you must configure the **ca save all** command. You can do this manually on the device or by using a FlexConfig (see Chapter 7, "Managing FlexConfigs").

Working with IPSec VPN Policies

Certain policies need to be configured for IPSec VPNs.

This section contains the following topics:

Understanding Certificate to Connection Profile Map Policies (ASA)

Certificate to connection profile map policies are used for enhanced certificate authentication on ASA devices.

A certificate to connection profile map policy is a unique identification, made up of individual fields that can be used as the identifier when matching users to a connection profile.

Certificate to connection profile map policies let you define rules to match a user's certificate to a permission group based on specified fields. To establish authentication, you can use any field of the certificate, or you can have all certificate users share a permission group.

To match user permission groups based on fields of the certificate, you define rules that specify the fields to match for a group and then enable each rule for that selected group. A connection profile must already exist in the configuration before you can create a rule for it.

After you define rules, you must configure a certificate group matching policy to define the method for identifying the permission groups of certificate users. You can match the group from the DN rules, the Organization Unit (OU) field, the IKE identity, or the peer IP address. You can use any or all of these methods.

Related Topics

- Configuring Certificate to Connection Profile Map Policies (ASA), page 26-35
- Certificate to Connection Profile Maps > Policies Page, page 27-67

Configuring Certificate to Connection Profile Map Policies (ASA)

This procedure describes how to configure a Certificate to Connection Profile policy for a remote client trying to connect to an ASA server device.

Before You Begin

- Make sure a connection profile has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Understanding Certificate to Connection Profile Map Policies (ASA), page 26-34

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > IPSec VPN > Certificate to Connection Profile Maps > Policies** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > Certificate to Connection Profile Maps > Policies** from the Policy Type selector. Select an existing policy or create a new one.

The Certificate to Connection Profile Map Policies page opens. For a description of the elements on this page, see Certificate to Connection Profile Maps > Policies Page, page 27-67.

Step 2 Select any, or all, of the following check boxes:

- Use **Configured Rules to Match a Certificate to a Group** to configure the server to use the configured certificate to establish authentication.
- Use **Certificate Organization Unit (OU) Field to Determine the Group** to configure the server to use the OU field to establish authentication.
- Use **IKE Identify to Determine the Group** to configure the server to use the IKE identity to establish authentication.
- Use **Peer IP address to Determine the Group** to configure the server to use the peer IP address to establish authentication.

Understanding Certificate to Connection Profile Map Rules (ASA)

When configuring certificate group matching, you must define rules to match a remote client's certificate to a permission group, based on fields in the connection profile.

To match user permission groups based on fields of the certificate, you define rules that specify the fields to match for a group and then enable each rule for that selected group. A tunnel group must already exist in the configuration before you can create and map a rule to it.

After defining the certificate to connection profile map rules, you must configure a certificate group matching policy to define the method for identifying the permission groups of certificate users. For more information, see Configuring Certificate to Connection Profile Map Policies (ASA), page 26-35.

Note A connection profile must already exist in the configuration before you can create and map a certificate to connection profile map rule to it. If you unassign a connection profile after creating a certificate to connection profile map rule, the rules that are mapped to the connection profile are unassigned. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Certificate to Connection Profile Map Rules (ASA), page 26-36
- Certificate to Connection Profile Maps > Rules Page, page 27-68

Configuring Certificate to Connection Profile Map Rules (ASA)

This procedure describes how to configure the Certificate to Connection Profile Map rules and parameters for any remote client trying to connect to an ASA server device.

Before You Begin

- Make sure a connection profile has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.
- Make sure that you select **Use Configured Rules to Match a Certificate to a Group** in the Certificate to Connection Profile Maps Policies policy. See Configuring Certificate to Connection Profile Map Policies (ASA), page 26-35.

Related Topics

- Understanding Certificate to Connection Profile Map Rules (ASA), page 26-35
- Connection Profiles Page, page 27-18

Step 1 (Device view only) With an ASA device selected, select **Remote Access VPN > IPSec VPN > Certificate to Connection Profile Maps > Rules** from the Policy selector. The Certificate to Connection Profile Map Rules page is displayed. For a description of the elements on this page, see Certificate to Connection Profile Maps > Rules Page, page 27-68.

Step 2 Click **Add Row** beneath the maps table in the upper pane to configure the priority and connection profile mapping for your matching rules. The Map Rule dialog box opens. For a description of the elements on this page, see Map Rule Dialog Box (Upper Table), page 27-69.

Step 3 Select a connection profile from the list.

Step 4 Enter the priority number for the matching rule. A lower number has higher priority.

Step 5 Enter a name for the map.

Step 6 Click **OK**. The map is displayed in the upper table of the page.

Step 7 Select the map created in the upper table to display the details in the table in the lower pane.

Step 8 Click **Add Row** beneath the table in the lower pane to configure the certificate to connection profile matching rule that must be satisfied in order for a remote client to connect to the device using the profile in this map. The Map Rule dialog box opens. For a description of the elements on this page, see Map Rule Dialog Box (Lower Table), page 27-70.

Step 9 Select the certificate field from the list.

Step 10 Select the component of the certificate that you wish to configure.

Step 11 Select the operator of the rule.

Step 12 Enter the value for which the rule is testing.

Step 13 Click **OK**. The rule parameters are displayed in the lower pane of the page.

Step 14 In the **Default Connection Profile** field, select the connection profile that should be used for users who do not meet any of the map rules.

Understanding IKE Proposals in Remote Access VPNs

Internet Key Exchange (IKE), also called ISAKMP, is the negotiation protocol that enables two hosts to agree on how to build an IPsec security association. To configure your device for remote access VPNs, you must specify the encryption algorithm, authentication algorithm, and key exchange method that the device should use when negotiating a VPN connection with the remote clients.

An IKE proposal is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

For more information on IKE concepts, see Understanding IKE, page 22-1.

On the IKE Proposal page, you can select the IKE proposals to assign to your remote access VPN server. You can create and edit IKE proposals.

Related Topics

- Configuring IKE Proposals on a Remote Access VPN Server, page 26-37
- IKE Proposal Page, page 27-73

Configuring IKE Proposals on a Remote Access VPN Server

This procedure describes how to specify the IKE proposals you want to assign to your remote access VPN server.

Related Topics

- Understanding IKE Proposals in Remote Access VPNs, page 26-37

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > IPSec VPN > IKE Proposal** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > IKE Proposal** from the Policy Type selector. Select an existing policy or create a new one.

The IKE Proposal page opens. For a description of the elements on this page, see IKE Proposal Page, page 27-73.

Step 2 On the IKE Proposal page, select the required IKE proposals from the Available IKE Proposals list, and click >>.

IKE proposals are objects. If the required IKE proposal is not included in the list, click **Create** to open the IKE Editor dialog box that enables you to create or edit an IKE proposal object. For more information, see Table 28-17 on page 28-27.

Understanding IPsec Proposals in Remote Access VPNs

An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peer(s), and other parameters that might be necessary to define an IPsec SA.

When configuring an IPsec proposal, you must define the external interface through which the remote access clients connect to the server, and the encryption and authentication algorithms that protect the data in the VPN tunnel. You can also select a group authorization (Group Policy Lookup) method that defines the order in which group policies are searched (on the local server or on external AAA servers) and a user authentication (Xauth) method that defines the order in which user accounts are searched.

For more information on IPsec tunnel concepts, see Understanding IPsec Tunnel Policies, page 22-5. For information about user accounts, see Defining Accounts and Credential Policies, page 53-14.

On the IPsec Proposal page, you can view the default IPsec proposal that is available for assignment to your remote access VPN. From this page, you can create a new IPsec proposal or edit the default

When you create or edit an IPsec proposal, you can also configure:

- A VPN Services Module (VPNSM) interface IPsec VPN Shared Port Adapter (VPN SPA) on a Catalyst 6500/7600 device (see VPNSM/VPN SPA Settings Dialog Box, page 27-80).
- VRF-Aware IPsec on a router or Catalyst 6500/7600 device (see Dynamic VTI/VRF Aware IPsec Tab (IPsec Proposal Editor), page 27-81).
- A dynamic virtual interface on an IOS router (see PVC Dialog Box—QoS Tab, page 52-60).

Using Dynamic Virtual Template Interfaces in Remote Access VPNs (IOS)

IOS devices allow dynamic virtual template interfaces (VTIs), which provide highly secure and scalable connectivity for remote-access VPNs, replacing dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels. You can use dynamic VTIs for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is duplicated from a virtual template configuration, which includes the IPsec configuration and any features configured on the virtual template interface. Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. They enable dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. Dynamic VTI simplifies VRF-Aware IPsec deployment, as the VRF is configured on the interface.

When this feature is enabled, Security Manager implicitly creates the virtual template interface for the selected device in a remote access VPN. All you must do is provide the IP address on the server that will be used as the virtual template interface, or use an existing loopback interface. The virtual template interface is created on the remote client without an IP address.

You can configure dynamic VTI when configuring an IPsec proposal on your remote access VPN server.

Note You can configure dynamic VTI only on routers running Cisco IOS Release 12.4(2)T and later, except 7600 devices.

You can configure dynamic VTI with or without VRF-Aware IPsec.

You can also configure dynamic VTI in a site-to-site Easy VPN topology. For more information, see Understanding Easy VPN, page 24-1.

Related Topics

- Configuring an IPsec Proposal on a Remote Access VPN Server, page 26-39
- IPsec Proposal Page, page 27-74

Configuring an IPsec Proposal on a Remote Access VPN Server

This procedure describes how to create or edit an IPsec proposal for your remote access VPN server. Keep the following in mind:

- On a Catalyst 6500/7600, you can also configure a VPN Services Module (VPNSM) interface or VPN SPA, a Firewall Services Module with a VPN Services Module, and/or VRF Aware IPsec
- If the device is a router IOS version 12.4(2)T or later, except 7600 device, you can configure a dynamic virtual interface on it.
- If the device is a PIX 7.0+, ASA, or IOS router except 7600, you can also configure reverse route injection on the crypto map.

Related Topics

- PVC Dialog Box—QoS Tab, page 52-60
- Understanding VRF-Aware IPsec, page 21-13
- Understanding IPsec Proposals in Remote Access VPNs, page 26-38
- IPsec Proposal Editor Dialog Box (for PIX and ASA Devices), page 27-75
- IPsec Proposal Editor Dialog Box (for IOS Routers and Catalyst 6500/7600 Devices), page 27-77
- VPNSM/VPN SPA Settings Dialog Box, page 27-80
- Understanding IPsec Tunnel Policies, page 22-5

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal** from the Policy Type selector. Select an existing policy or create a new one.

The IPsec Proposal page opens. For a description of the elements on this page, see IPsec Proposal Page, page 27-74.

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

Note The elements in IPsec Proposal Editor dialog box differ depending on the selected device.

Step 3 If the selected device is a PIX 7.0+ or an ASA device:

a. Select the external interface through which remote access clients will connect to the server.

b. Select the transform set or sets to be used for your tunnel policy.

c. If you do not want to configure Reverse Route Injection (RRI) on the device's crypto map, select the None option from the list.

The default option, Standard, creates routes based on the destination information defined in the crypto map access control list (ACL). For more information, see About Reverse Route Injection, page 22-8.

d. If required, enable the configuration of Network Address Translation Traversal (NAT-T) on an ASA device. See Understanding NAT, page 22-13.

e. For a PIX device, specify the AAA or Xauth user authentication method to define the order in which user accounts are searched.

f. Click **OK** to save your definitions and close the dialog box.

For a description of the elements on the IPsec Proposal Editor dialog box, see Table 27-57 on page 27-76.

Step 4 If the selected device is a Cisco IOS router, Catalyst 6500/7600, or PIX 6.3 device, the IPsec Proposal Editor dialog box opens displaying the General tab.

Note The IPsec Proposal Editor dialog box displays two tabs—General and Dynamic VTI/VRF Aware IPsec. If the selected device is a Catalyst 6500/7600, the FWSM Settings tab is also displayed.

a. In the General tab (for a description of the elements in the General tab, see Table 27-58 on page 27-78):

- Specify the external interface through which remote access clients will connect to the server.

Note **Important:** If the selected device is a Catalyst 6500/7600, specify the inside VLAN that serves as the inside interface to the VPN Services Module (VPNSM) or VPN SPA. Click **Select** to open a dialog box in which you define the settings that enable you to configure a VPNSM or VPN SPA. For a description of the elements in the VPNSM/VPN SPA Settings dialog box, see Table 27-59 on page 27-80

For information about configuring a VPNSM, see Configuring VPNSM or VPN SPA/VSPA Endpoint Settings, page 21-38.

For information about configuring a VPN SPA, see Configuring VPNSM or VPN SPA/VSPA Endpoint Settings, page 21-38.

- Select the transform sets to be used for your tunnel policy.
- If required, enable reverse route injection (RRI) to ensure that a static route is created on the device for each assigned address to the client.
- To configure reverse route injection (RRI) on the device's crypto map, select the required option from the Reverse Route Injection list. For more information, see About Reverse Route Injection, page 22-8.
- Select an AAA authorization method list to use for defining the order in which the group policies are searched. Group policies can be configured on the local server or on an external AAA server.
- Select the AAA or Xauth user authentication method to use for defining the order in which user accounts are searched.

b. Click the **Dynamic VTI/VRF Aware IPsec** tab to configure a dynamic virtual interface, VRF-Aware IPsec settings, or both on the device. For a description of the elements on this tab, see Table 27-60 on page 27-82.

Step 5 After you finish creating or editing your IPsec proposal, click **OK** to save your changes and close the IPsec Proposal Editor dialog box.

Understanding High Availability in Remote Access VPNs (IOS)

In remote access VPNs, High Availability (HA) is supported on Cisco IOS routers running IP over LANs.

In Security Manager, High Availability (HA) is supported by the creation of an HA group made up of two or more hub devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. By sharing a virtual IP address, the hubs in the HA group present the appearance of a single virtual device or default gateway to the hosts on a LAN. One hub in the HA group is always active and assumes the virtual IP address, while the others are standby hubs. The hubs in the group watch for hello packets from active and standby devices. If the active device becomes unavailable for any reason, a standby hub takes ownership of the virtual IP address and takes over the hub functionality. This transfer is seamless and transparent to hosts on the LAN, and to the peering devices.

Stateful SwitchOver (SSO) is used to ensure that state information is shared between the HSRP devices in the HA group. If a device fails, the shared state information enables the standby device to maintain IPsec sessions without having to re-establish the tunnel or renegotiate the security associations.

Note When configuring an HA group, you must provide an inside virtual IP that matches the subnet of one of the interfaces on the device, in addition to a VPN virtual IP that matches the subnet of one of the device's interfaces and is configured with an IPsec proposal. See Configuring an IPsec Proposal on a Remote Access VPN Server, page 26-39.

A remote access VPN server device on which HA is configured cannot be configured as a hub in a site-to-site VPN topology on which HA is configured, using the same outside interface that was used for the remote access VPN server.

For a description of the High Availability page, on which you can provide information for configuring an HA group, see Table 27-54 on page 27-72.

Related Topics

- Configuring a High Availability Policy, page 26-41
- High Availability Page, page 27-71
- Configuring an IPsec Proposal on a Remote Access VPN Server, page 26-39

Configuring a High Availability Policy

This procedure describes the steps required to configure a high availability policy on an IOS router in your remote access VPN.

Before You Begin:

- Make sure an IPsec proposal is configured on the device.

Related Topics

- Understanding High Availability in Remote Access VPNs (IOS), page 26-41

Step 1 Do one of the following:

- (Device view) With an IOS device selected, select **Remote Access VPN > IPSec VPN > High Availability** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > High Availability** from the Policy Type selector. Select an existing policy or create a new one.

The High Availability page opens. For a description of the elements on this page, see High Availability Page, page 27-71.

Step 2 Specify the virtual IP addresses (and subnet masks) that represent the inside interface and the VPN interface of the HA group, in the relevant fields.

Note You must provide an inside virtual IP that matches the subnet of one of the interfaces on the device, in addition to a VPN virtual IP that matches the subnet of one of the device's interfaces and is configured with an IPsec proposal; otherwise an error is displayed.

Step 3 Specify the hello interval and hold time, in seconds.

Step 4 Specify the standby number of the inside hub interface that matches the internal virtual IP subnet, and the outside hub interface that matches the external virtual IP subnet, for the hubs in the HA group. The numbers must be within the range of 0-255.

Note Inside and outside standby group numbers must be different.

Step 5 Specify the IP address of the inside interface of the remote peer device which acts as the failover server.

Understanding User Group Policies (IOS)

When you configure a remote access VPN server, 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 VPN. User groups simplify system management, enabling you to quickly configure VPN access for large numbers of users.

For example, in a typical remote access VPN, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. User group policies provide the flexibility to do so securely.

Remote clients must have the same group name as the user group configured on the VPN server so that they can connect to the device; otherwise, a connection cannot be established. When a remote client establishes a connection to the VPN server, the group policies for that user group are pushed to all clients belonging to the same user group. You can configure user groups on the local remote access VPN server and external AAA servers.

Note The remote access VPN server on which you define a user group policy can be a Cisco IOS router, PIX 6.3 Firewall, or 6500 /7600 device.

On the User Group Policy page, you can specify the user groups you want to assign to your remote access VPN server. You can create and edit user group policies. You can open the User Group Policy page from the Remote Access Configuration wizard or from the Remote Access VPN Policies folder.

Related Topics

- Configuring User Group Policies, page 26-43
- Add or Edit User Group Dialog Box, page 28-68

Configuring User Group Policies

This procedure describes how to specify the user groups to assign to your remote access VPN server using the User Groups option on the Policy selector.

Note You can also specify user groups using the Remote Access VPN Configuration Wizard. For more information, see Using the Remote Access VPN Configuration Wizard, page 26-9.

Related Topics

- Understanding User Group Policies (IOS), page 26-42

Step 1 Do one of the following:

- (Device view) With an IOS router, Catalyst 6500/7600, or PIX 6.3 device selected, select **Remote Access VPN > IPSec VPN > User Groups** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > User Groups (IOS/PIX6.x)** from the Policy Type selector. Select an existing policy or create a new one.

The User Groups page opens. For a description of the elements on this page, see User Group Policy Page, page 27-84.

Step 2 From the User Group Policy page, select the required user groups from the **Available User Groups list**, and click >>.

User groups are objects. If the required user group is not in the list, click **Create** to open the Add or Edit User Group Dialog Box, page 28-68 that enables you to create or edit a user group object.

Working with SSL VPN Policies

Certain policies need to be configured for SSL VPNs.

This section contains the following topics:

- Understanding SSL VPN Access Policies (ASA), page 26-44
- Configuring Other SSL VPN Settings, page 26-46
- Understanding SSL VPN Shared Licenses (ASA), page 26-58
- Configuring an SSL VPN Policy (IOS), page 26-60

Understanding SSL VPN Access Policies (ASA)

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, Datagram Transport Layer Security (DTLS) settings, the SSL VPN session timeout and maximum number of sessions. You can also specify whether to use the AnyConnect VPN Client or AnyConnect Essentials Client.

Datagram Transport Layer Security (DTLS)

Enabling Datagram Transport Layer Security (DTLS) allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with SSL connections and improves the performance of real-time applications that are sensitive to packet delays. By default, DTLS is enabled when SSL VPN access is enabled on an interface. If you disable DTLS, SSL VPN connections connect with an SSL VPN tunnel only.

Note In order for DTLS to fall back to a TLS connection, you must specify a fallback trustpoint. If you do not specify a fallback trustpoint and the DTLS connection experiences a problem, the connection terminates instead of falling back to the specified trustpoint.

AnyConnect SSL VPN Client

The Cisco AnyConnect SSL VPN client provides secure SSL connections to the security appliance for remote users. Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After you enter the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). (See Datagram Transport Layer Security [DTLS] above.)

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The security appliance downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

AnyConnect Essentials SSL VPN Client

AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the adaptive security appliance, that provides the full AnyConnect capability, with the following exceptions:

- No CSD (including HostScan/Vault/Cache Cleaner)
- No clientless SSL VPN
- Optional Windows Mobile Support

The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client. If this feature is disabled, the full AnyConnect VPN client is used. This feature is disabled by default.

Note This license cannot be used at the same time as the shared license for SSL VPN.

This section contains the following topics:

- Configuring an Access Policy, page 26-45

Configuring an Access Policy

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

Related Topics

- Understanding SSL VPN Client Settings, page 26-56

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Access** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Access (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Access page opens. For a description of the elements on this page, see SSL VPN Access Policy Page, page 27-85.

Step 2 From the table, you can create an interface or edit an existing one on which SSL VPN connection can be established, as follows:

a. Click **Add Row** below the table, or select a row in the table and click **Edit Row**. The Access Interface Configuration dialog box opens. For a description of the elements on this dialog box, see Table 27-63 on page 27-87.

b. Specify the interface on which you want to configure a VPN access. 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.

c. Enter or select a defined Trustpoint to be assigned to this interface.

d. If load balancing is configured, you can enter or Select a secondary, Load Balancing Trustpoint to be assigned to this interface.

e. Select Allow Access to enable VPN access via this interface. If this option is not selected, access is configured on the interface, but it is disabled.

f. Select Enable DTLS to enable DTLS connections with the AnyConnect client on the interface and allow AnyConnect VPN Clients to establish an SSL VPN connection using two simultaneous tunnels—an SSL tunnel and a DTLS tunnel.

g. Select Check Client Certification to require a valid digital certificate from the client for connection.

h. Click **OK**.

Step 3 Specify the port number 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 a separate UDP port for DTLS connections with the AnyConnect client. You can click **Select** to open the Port List Selector dialog box from which you can make your selection.

Step 5 Specify a Fallback Trustpoint to use for interfaces that do not have a trustpoint assigned.

Step 6 Specify the amount of time, in seconds, that an SSL VPN session can be idle before the security appliance terminates the session.

Step 7 Specify the maximum number of SSL VPN sessions you want to allow.

Step 8 Select **Allow Users to Select Connection Profile in Portal Page** to include a list of the configured tunnel groups on the SSL VPN end-user interface, from which users can select a connection profile when they log in.

Step 9 Select **Enable AnyConnect Access** to enable either the Cisco AnyConnect VPN Client or the legacy Cisco SSL VPN Client (SVC) on the interfaces defined on the security appliance for SSL VPN connections. For details, see Understanding SSL VPN Client Settings, page 26-56.

Step 10 Select **Enable AnyConnect Essentials** to enable the AnyConnect Essentials SSL VPN Client. For details, see Understanding SSL VPN Client Settings, page 26-56.

Configuring Other SSL VPN 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, browser plug-ins, and AnyConnect client images and profiles.

This section contains the following topics:

Understanding 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.

Related Topics

- Defining Performance Settings, page 26-47
- Performance Tab, page 27-88

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

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Performance Tab, page 27-88

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

The Other Settings page opens with the Performance tab open by default. For a description of the elements on this tab, see Performance Tab, page 27-88.

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.

Understanding 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 permit 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 Other 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.

Related Topics

- Defining Content Rewrite Rules, page 26-48
- Content Rewrite Tab, page 27-90
- Add/Edit Content Rewrite Dialog Box, page 27-91

Defining Content Rewrite Rules

This procedure shows you how to create or edit content rewrite rules.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Content Rewrite Tab, page 27-90
- Add/Edit Content Rewrite Dialog Box, page 27-91

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other 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 27-65 on page 27-90.

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 27-66 on page 27-91.

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 the name of the application or resource to which the rule applies (up to 300 characters).

Step 7 Enter the application or resource for the rule.

Step 8 Click **OK**. The Add Content Rewrite Rule dialog box closes, and the content rewrite rule is added to the table.

Understanding Encoding

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.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Encoding Tab, page 27-91
- Add/Edit File Encoding Dialog Box, page 27-93

Defining Encoding Rules

This procedure shows you how to define encoding rules for your SSL VPN.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Encoding Tab, page 27-91
- Add/Edit File Encoding Dialog Box, page 27-93

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other Settings page, click the **Encoding** Tab. For a description of the elements on this tab, see Table 27-67 on page 27-92.

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 27-68 on page 27-93.

Step 5 Enter the IP address or host name 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**.

Understanding 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 specify a proxy autoconfiguration (PAC) file to download from an HTTP proxy server; however, you may not use proxy authentication when specifying the PAC file.

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.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Defining Proxies and Proxy Bypass Rules, page 26-51
- Proxy Tab, page 27-94
- Add/Edit Proxy Bypass Dialog Box, page 27-97

Defining Proxies and Proxy Bypass Rules

This procedure shows you how to define proxies and proxy bypass rules for your SSL VPN.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Understanding Proxies and Proxy Bypass Rules, page 26-51
- Proxy Tab, page 27-94
- Add/Edit Proxy Bypass Dialog Box, page 27-97

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other Settings page, click the **Proxy** Tab. For a description of the elements on this tab, see Table 27-69 on page 27-94.

Step 3 Select the type of external proxy server to use for SSL VPN connections as follows:

- **HTTP Proxy**—Enables you to use an external proxy server to handle HTTP requests and activates all the fields beneath it that specify HTTP server properties.
- **HTTPS Proxy**—Enables you to use an external proxy server to handle HTTPS requests and activates all the fields beneath it that specify HTTPS server properties.
- **Proxy Auto-Configuration File**—Enables you to specify a proxy autoconfiguration (PAC) file to download from an HTTP proxy server to a browser.

Step 4 If you selected HTTP Proxy as the type of proxy server, do the following to set the type of configuration for the HTTP server.

a. 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.

b. 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.

c. In the Exception Address List field, enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTP proxy server. 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 Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68.

d. Specify the username to accompany each HTTP proxy request with a password to provide basic, proxy authentication.

e. Enter the password to send to the proxy server with each HTTP request. Reenter the password to confirm it.

Step 5 If you selected HTTPS Proxy as the type of proxy server, do the following to set the type of configuration for the HTTPS server.

a. 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.

b. 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.

c. In the Exception Address List field, enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the HTTPS proxy server. 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 Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68.

d. Specify the username to accompany each HTTPS proxy request with a password to provide basic, proxy authentication.

e. Enter the password to send to the proxy server with each HTTPS request. Reenter the password to confirm it.

Step 6 If you selected Proxy Auto-Configuration File as the type of proxy server, select the **Specify PAC file URL** option and specify a PAC file to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.

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 27-70 on page 27-97.

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 **Rewrite Hostname** 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**.

Understanding Plug-ins

A browser plug-in is a separate program that a web browser invokes to perform a dedicated function, such as connect a client to a server within the browser window. The security appliance lets you import plug-ins for download to remote browsers in clientless SSL VPN sessions. Of course, Cisco tests the plug-ins it redistributes, and in some cases, tests the connectivity of plug-ins we cannot redistribute. However, we do not recommend importing plug-ins that support streaming media at this time.

Note Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

The security appliance does the following when you install a plug-in onto the flash device:

- (Cisco-distributed plug-ins only) Unpacks the jar file specified in the URL.
- Writes the file to the csco-config/97/plugin directory on the security appliance file system.
- Enables the plug-in for all future clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page.

When the user in a clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

Note Some Java plug-ins may report a status of connected or online even when a session to the destination service is not set up. The open-source plug-in reports the status, not the security appliance.

Plug-in Requirements and Restrictions

Clientless SSL VPN must be enabled on the security appliance to provide remote access to the plug-ins. The minimum access rights required for remote use belong to the guest privilege mode. The plug-ins automatically install or update the Java version required on the remote computer. A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.

Before installing a plug-in, prepare the security appliance as follows:

- Make sure clientless SSL VPN ("webvpn") is enabled on an interface on the security appliance. To do so, enter the **show running-config** command.
- Install an SSL certificate onto the security appliance interface to which remote users use a fully-qualified domain name (FQDN) to connect.

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

In the Plug-in tab of the SSL VPN Global Settings page, you can view the currently configured browser plug-ins for clientless SSL VPN browser access. From this tab, you can create or edit the plug-in files, as described in the following procedure.

Providing Access to Plug-ins Redistributed by Cisco

Create a temporary directory named "plugins" on the computer you use to establish Security Manager sessions with the security appliance. Then download the plug-ins you want from the Cisco web site to the "plugins" directory. Cisco redistributes the following open-source, Java-based components to be accessed as plug-ins for web browsers in Clientless SSL VPN sessions:

- rdp-plugin.jar—The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is http://properjavardp.sourceforge.net/.
- ssh-plugin.jar—The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell or Telnet connection to a remote computer. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is http://javassh.org/.

Note The ssh-plugin.jar provides support for both SSH and Telnet protocols. The SSH client supports SSH Version 1.0.

- vnc-plugin.jar—The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes to it per the GNU General Public License. The web site containing the source of the redistributed plug-in is http://www.tightvnc.com.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 26-5
- Configuring Other SSL VPN Settings, page 26-46
- Defining Browser Plug-ins, page 26-55
- Plug-in Tab, page 27-98
- Add/Edit Plug-in Entry Dialog Box, page 27-99

Defining Browser Plug-ins

This procedure shows you how to define browser plug-ins for your SSL VPN.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other Settings page, click the **Plug-in** Tab. For a description of the elements on this tab, see Plug-in Tab, page 27-98.

Step 3 Click **Create**, or select a plug-in in the table and click **Edit**.

The Add/Edit Plug-in dialog box opens. For a description of the elements in this dialog box, see Add/Edit Plug-in Entry Dialog Box, page 27-99.

Step 4 From the Plug-in list, select the type of plug-in that you want to download from the Security Manager server to the device. For more information on the types of available plug-ins, see Understanding Plug-ins, page 26-53.

Step 5 In the Plug-in File field, enter the name of the File Object that identifies the plug-in file, or click **Select** to select an object. You can also create the File Object from the object selector. For more information, see Add and Edit File Object Dialog Boxes, page 28-24.

Step 6 Click **OK**.

Understanding SSL VPN Client Settings

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. The client gives remote users the benefits of an SSL VPN client without the need for network administrators to install and configure clients on remote computers.

Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<*address*>.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS), and optionally, Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

The AnyConnect client can be downloaded from the security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The security appliance downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user about whether to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

About AnyConnect Client Profiles

An AnyConnect client profile is a group of configuration parameters, stored in an XML file, that the client uses to configure the connection entries that appear in the client user interface. These parameters (XML tags) include the names and addresses of host computers and settings to enable additional client features.

The AnyConnect client installation includes a profile template, named *AnyConnectProfile.tmpl*, that you can edit with a text editor and use as a basis to create other profile files. You can also set advanced parameters that are not available through the user interface. The installation also includes a complete XML schema file, named *AnyConnectProfile.xsd*.

After creating a profile, you must load the file on the security appliance and configure the security appliance to download it to remote client PCs. After the file is loaded into cache memory, the profile is available to group policies and username attributes of client users.

Related Topics

- Understanding and Managing SSL VPN Support Files, page 26-5
- Configuring SSL VPN Client Settings, page 26-57
- SSL VPN Client Settings Tab, page 27-99

Configuring SSL VPN Client Settings

This procedure shows you how to define SSL VPN client images and profiles and configure the cache memory for the SSL VPN client and Cisco Secure Desktop images on the security appliance.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Understanding SSL VPN Client Settings, page 26-56

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other Settings page, click the **Client Settings** Tab. For a description of the elements on this tab, see SSL VPN Client Settings Tab, page 27-99.

Step 3 In the AnyConnect Client Image table, you can add a new image or edit an existing one, as follows:

- Click **Create** below the table, or select an image in the table and click **Edit**. The Add/Edit AnyConnect Client Image dialog box appears. For a description of the elements in this dialog box, see Add/Edit AnyConnect Client Image Dialog Box, page 27-101.
- In the AnyConnect Client Image field, enter the name of the File Object that identifies the AnyConnect client, or click **Select** to select an object. You can also create the File Object from the object selector. For more information, see Add and Edit File Object Dialog Boxes, page 28-24.
- Enter the order in which the security appliance downloads the client images to the remote PC. It downloads the image at the top of the table first. Therefore, you should enter a lower value for the image used by the most commonly-encountered operating system.
- Click **OK** to save the changes.

Step 4 From the AnyConnect Client Profile table, you can create a new profile or edit the path of an existing one, as follows:

- Click **Create** below the table, or select a profile in the table and click **Edit**. The Add/Edit AnyConnect Client Profile dialog box appears. For a description of the elements in this dialog box, see Add/Edit AnyConnect Client Profile Dialog Box, page 27-101.
- Enter a name for the client profile.
- In the AnyConnect Client Profile field, enter the name of the File Object that identifies the AnyConnect client profile, or click **Select** to select an object. You can also create the File Object from the object selector.
- Click **OK** to save the changes.

Step 5 In the Maximum Size field, specify the size of the cache memory in MB to be allocated for the SSL VPN client and CSD images on the device.

Defining Advanced Settings

The Advanced tab lets you configure the memory, on-screen keyboard, and internal password features on ASA devices.

Before You Begin

- Make sure a connection profile policy has been configured on the device. See Configuring Connection Profiles (ASA), page 26-18.

Related Topics

- Configuring Other SSL VPN Settings, page 26-46
- Advanced Tab, page 27-102

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Other Settings** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > Other Settings (ASA)** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 On the Other Settings page, click the **Advanced** Tab. For a description of the elements on this tab, see Table 27-76 on page 27-103.

Step 3 Specify the amount of memory that you want to allocate to the SSL VPN processes. The default percentage is 50%. If you change this setting, Cisco recommends that you specify the amount of memory in terms of percentage, because 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 In the Enable On-Screen Keyboard field, choose **On All Pages** or **On Logon Page Only** to enable the on-screen keyboard feature, as desired. Otherwise, leave it set to **Disabled**.

Step 5 Click the **Allow Users to Enter Internal Password** check box to require an additional password when accessing internal sites. This feature is useful if you require that the internal password be different from the SSL VPN password. For example, you can use a one-time password for authentication to ASA and another password for internal sites.

Understanding SSL VPN Shared Licenses (ASA)

You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of ASA devices by configuring one of the ASA devices as a shared license server, and the rest as clients. For the server license, you can share 500-50,000 licenses in increments of 500 and 50,000-1,040,000 licenses in increments of 1000.

Note The shared license cannot be used at the same time as the AnyConnect Essentials license.

This section contains the following topics:

Configuring an ASA Device as a Shared License Client

This procedures describes how to configure an ASA device as a shared license client.

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Shared License** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN >Shared License (ASA 8.2+)** from the Policy Type selector. Select an existing policy or create a new one.

The SSL VPN Shared License page appears (see SSL VPN Shared License (ASA 8.2) Page, page 27-103).

Step 2 Select **Shared License Client** as the role of the device.

Step 3 In the Shared Secret field, enter and confirm a case-sensitive string (4-128 characters) used for communicating with the shared license server.

Step 4 In the License Server field, enter the hostname of the ASA device configured as the license server.

Step 5 In the License Server Port field, enter the number of the TCP port on which the license server communicates.

Step 6 Select the role of the client:

- **Client Only**—When selected, the client acts only as the client. In this case, you must specify another device as a backup server.
- **Backup Server**—When selected, the client also acts as the backup server. In this case, you must also specify the interfaces to be used for this purpose.

Configuring an ASA Device as a Shared License Server

This procedures describe how to configure an ASA device as a shared license server.

Step 1 Do one of the following:

- (Device view) With an ASA device selected, select **Remote Access VPN > SSL VPN > Shared License** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN >Shared License (ASA 8.2+)** from the Policy Type selector. Select an existing policy or create a new one.

The SSL VPN Shared License page appears (see SSL VPN Shared License (ASA 8.2) Page, page 27-103).

Step 2 Select **Shared License Server** as the role of the device.

Step 3 In the Shared Secret field, enter and confirm a case-sensitive string (4-128 characters) used for communicating with the shared license server.

Step 4 In the License Server field, enter the hostname of the ASA device configured as the license server.

Step 5 In the License Server Port field, enter the number of the TCP port on which the license server communicates.

Step 6 In the Refresh Interval field, enter a value between 10-300 seconds to be used as the refresh interval. Default is 30 seconds.

Step 7 In the Interfaces field, enter or select the interfaces to be used for communicating with clients.

Step 8 Click the Configure Backup shared SSL VPN License Server check box to configure a backup server for the shared license server, then configure the following:

- **Backup License Server**—Server to act as a backup license server if the current one is unavailable.
- **Backup Server Serial Number**—Serial number of the backup license server.
- **HA Peer Serial Number**—(Optional) Serial number of the backup server of a failover pair.

Configuring an SSL VPN Policy (IOS)

After you create a basic SSL VPN connection on your server device using the Remote Access VPN Configuration wizard, you can modify the connection, if required, and configure additional policies and features using the SSL VPN policy on the Policy selector.

Step 1 Do one of the following:

- (Device view) With an IOS device selected, select **Remote Access VPN > SSL VPN** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > SSL VPN Policy (IOS)** from the Policy Type selector. Select an existing policy or create a new one.

The SSL VPN page appears (see SSL VPN Policy Page (IOS), page 27-105).

Step 2 Click **Add Row** on the SSL VPN Policy page, or select a row in the table and click **Edit Row**, to open the SSL VPN Context Editor Dialog Box (IOS), page 27-105.

Step 3 Configure at least the following general settings for the policy. For information on other fields, see General Tab, page 27-107.

- **Name, Domain**—For new policies, the name of the context that defines the virtual configuration of the SSL VPN. To simplify the management of multiple context configurations, make the context name the same as the domain or virtual hostname.
- **Gateway**—The SSL VPN gateway policy object that identifies the gateway device to which users will connect, including interface and port configuration. Click **Select** to select the object from a list or to create a new object.

  When you select the object, the Portal Page URL field shows the URL to which users connect.
- **Authentication Server Group**—A prioritized list of AAA server group objects that identify the AAA servers to use for authenticating users.
- **User Groups**— The user groups that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway.

  To add a user group, click **Add Row** to open a list of existing user group policy objects from which you can select the group. If the desired group does not already exist, click the **Create** button below the available groups list and create it. For more information about user group objects, see Add or Edit User Group Dialog Box, page 28-68.

Step 4 Click the **Portal Page** tab and customize the design of the login page. You can customize the title, the logo graphic, the message that appears above the login prompt, and the background and text colors.

If you want to select a different graphic, you must first copy the graphic onto the Security Manager server. You cannot select it from your workstation's hard drive.

Step 5 Click the **Secure Desktop** tab to configure Cisco Secure Desktop (CSD) software. CSD policies define entry requirements for client systems and provide a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session.

If you want to use CSD, select **Enable Cisco Secure Desktop** and click **Select** to select a Secure Desktop Configuration policy object, which defines the rules you want to use to control VPN access and host scanning. You can create a new object from the selection list. For information about configuring these objects, see Creating Cisco Secure Desktop Configuration Objects, page 26-61.

Note You must install and activate the Secure Desktop Client software on a device for your configuration to work.

Step 6 Click the **Advanced** tab to configure a maximum number of simultaneous users for the context or if you are using VRF, the name of the VRF instance that is associated with the SSL VPN context.

Step 7 Click **OK** to save your changes.

Creating Cisco Secure Desktop Configuration Objects

Cisco Secure Desktop (CSD) Configuration objects define the settings you want to use if you enable Secure Desktop in an SSL VPN policy for an IOS device (see Configuring an SSL VPN Policy (IOS), page 26-60). For ASA devices, the feature is set up as part of the Dynamic Access Policy (see Understanding Dynamic Access Policies, page 26-19 and Configuring Cisco Secure Desktop Policies on ASA Devices, page 26-26).

Cisco Secure Desktop (CSD) provides a reliable means of eliminating 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 an 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.

About Windows Locations

Windows locations let you determine how clients connect to your virtual private network, and protect it accordingly. For example, clients connecting from within a workplace LAN on a 10.x.x.x network behind a NAT device are an unlikely risk for exposing confidential information. For these clients, you might set up a CSD Windows Location named Work that is specified by IP addresses on the 10.x.x.x network, and disable both the Cache Cleaner and the Secure Desktop function for this location.

In contrast, users' home PCs might be considered more at risk to viruses due to their mixed use. For these clients, you might set up a location named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This location would require the presence of antivirus software and specific, supported operating systems to grant full access to the network.

Alternatively, for untrusted locations such as Internet cafes, you might set up a location named "Insecure" that has no matching criteria (thus making it the default for clients that do not match other locations). This location would require full Secure Desktop functions, and include a short timeout period to prevent access by unauthorized users. If you create a location and do not specify criteria, make sure it is the last entry in the Locations list.

Related Topics

- Cisco Secure Desktop on IOS Configuration Example Using SDM, http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml
- Setting Up CSD for Microsoft Windows Clients, http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html
- Creating Policy Objects, page 6-6

Step 1 Select **Tools > Policy Object Manager** to open the Policy Object Manager (see Policy Object Manager Window, page 6-3).

Step 2 Select **Cisco Secure Desktop Configuration** from the Object Type selector.

Step 3 Right-click in the work area and select **New Object** to open the Add or Edit Secure Desktop Configuration Dialog Box, page 28-21.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Select **Windows Location Settings** to create locations (such as Work, Home, or Insecure), and define the location-based settings (also called adaptive policies) for CSD.

a. For each location you want to configure, enter its name in the **Location to Add** field and click **Add** to move it to the Locations field. You can reorder the locations using the Move Up and Move Down buttons. When users connect, these locations are evaluated in order and the first one that matches is used to define the policies for the user.

When you add a location, a folder for the location is added to the table of contents. The folder and its subfolders define the policies for the location.

b. If you want all the open browser windows to close after the Secure Desktop installation, make sure to select the corresponding check box.

c. Select the required check boxes to configure a VPN Feature policy that enables web browsing, file access, port forwarding, and full tunneling, if installation or location matching fails.

Step 6 Select the folders and subfolders for the Windows locations you added and configure their settings. For detailed information about these settings, see *Setting Up CSD for Microsoft Windows Clients* at http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html.

Step 7 Select **Windows CE** to configure a VPN feature policy to enable or restrict web browsing and remote server file access for remote clients running Microsoft Windows CE.

Step 8 Select **Mac and Linux Cache Cleaner** to configure the Cache Cleaner and a VPN Feature Policy for these clients, such as enabling or restricting web browsing, remote server file access, and port forwarding.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-9.

Step 10 Click **OK** to save the object.

Customizing Clientless SSL VPN Portals

You can customize the web site and its contents that you use for the portal page for a browser-based clientless SSL VPN. ASA devices allow much more customization than IOS devices. You can create several policy objects that define the look of the web pages the user sees when logging into or out of the VPN and the home page for the portal, as well as the bookmarks and smart tunnels available to the user.

This section contains the following topics:

Configuring ASA Portal Appearance Using SSL VPN Customization Objects

An SSL VPN Customization object describes the appearance of browser-based clientless SSL VPN web pages displayed to users. This includes the Logon page displayed when they connect to the ASA security appliance, the Home page displayed after authentication, and the Logout page displayed when users log out of the SSL VPN service.

You use SSL VPN Customization objects when defining ASA group objects or Remote Access VPN Connection policies for ASA devices. You can create several customization objects and define multiple ASA group or connection profiles so that each user group sees web pages designed specifically for their use. Customization can include localizing the web pages in the languages appropriate for each group. For more information about localization, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66.

Initially, when a user first connects, the default customization object identified in the connection profile determines how the logon screen appears. If the user selects a different group from the connection profile list on the logon page, and that group has its own customization, the screen changes to reflect the customization object for the selected group. After the remote user is authenticated, the screen appearance is determined by the customization object that has been assigned to the group policy.

After you create the SSL VPN customization object as described in this procedure, you can use the object to specify the portal characteristics in these policies:

- On the **SSL VPN > Settings** page in an ASA group policy object (see ASA Group Policies SSL VPN Settings, page 28-15), which you then select in one of these policies:
  - **Remote Access VPN > Group Policies**
  - **Remote Access VPN > Connection Profiles** on the **General** tab
- In the **Remote Access VPN > Connection Profiles** policy, you can also specify the SSL VPN customization object on the **SSL** tab (see SSL Tab (Connection Profiles), page 27-29).

Related Topics

- Localizing SSL VPN Web Pages for ASA Devices, page 26-66
- Creating Policy Objects, page 6-6
- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49

Step 1 Select **Tools > Policy Object Manager** to open the Policy Object Manager (see Policy Object Manager Window, page 6-3).

Tip You can also create SSL VPN Customization objects when defining policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Step 2 Select **SSL VPN Customization** from the Object Type selector. The SSL VPN Customization page opens, displaying a list of the existing SSL VPN Customization objects.

Step 3 Right-click in the work area and select **New Object**.

The Add SSL VPN Customization dialog box appears (see Add and Edit SSL VPN Customization Dialog Boxes, page 28-49).

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Before you configure settings for the various pages, use the Preview button to view the default settings. Clicking **Preview** opens a browser window to display the current settings for the Logon page, Portal page, or Logout page, whichever one is selected in the table of contents (selecting a page within one of these folders is the same as selecting the parent folder).

Tip Click **Preview** after making any changes to settings to verify that the changes are what you desire.

Step 6 Configure the settings for the Logon page. This web page is the one users see first when connecting to the SSL VPN portal. It is used for logging into the VPN. Select the following items in the Logon Page folder in the table of contents on the left of the dialog box to view and change the settings:

- **Logon Page**—Specify the title of the web page, which is displayed in the browser's title bar.
- **Title Panel**—Determine whether the Logon page will have a title displayed in the web page itself. If you enable the title panel, you can specify the title, font, font size and weight, styles, and colors used. You can also select a File object that identifies a logo graphic. For more information about the settings, see SSL VPN Customization Dialog Box—Title Panel, page 28-52.
- **Language**—If you want to configure translation tables for other languages on the ASA device and use them, you can configure the supported languages and allow users to choose their language. For information about translation tables and localization support, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66. For more information about the settings, see SSL VPN Customization Dialog Box—Language, page 28-53.
- **Logon Form**—Configure the labels and colors used in the form that accepts user logon information. For more information about the settings, see SSL VPN Customization Dialog Box—Logon Form, page 28-55.
- **Informational Panel**—If you want to provide extra information to the user, you can enable an informational panel and add text and a logo graphic. For more information about the settings, see SSL VPN Customization Dialog Box—Informational Panel, page 28-56.

- **Copyright Panel**—If you want to include copyright information on the logon page, you can enable the copyright panel and enter your copyright statement. For more information about the settings, see SSL VPN Customization Dialog Box—Copyright Panel, page 28-56.
- **Full Customization**—If you do not want to use the security appliance's built-in logon page, even customized, you can instead enable full customization and supply your own web page. For information on creating the required file, see Creating Your Own SSL VPN Logon Page for ASA Devices, page 26-67. For more information about the settings, see SSL VPN Customization Dialog Box—Full Customization, page 28-57.

Step 7 Configure the settings for the Portal page. This is the home page for the SSL VPN portal, and is displayed after the users log in. Select the following items in the Portal Page folder in the table of contents on the left of the dialog box to view and change the settings:

- **Portal Page**—Specify the title of the web page, which is displayed in the browser's title bar.
- **Title Panel**—Determine whether the Portal page will have a title displayed in the web page itself. If you enable the title panel, you can specify the title, font, font size and weight, styles, and colors used. You can also select a File object that identifies a logo graphic. For more information about the settings, see SSL VPN Customization Dialog Box—Title Panel, page 28-52.
- **Toolbar**—Determine whether the Portal page will have a toolbar, which contains a field for entering a URL to browse. For more information about the settings, see SSL VPN Customization Dialog Box—Toolbar, page 28-58.
- **Applications**—Determine which application buttons will appear on the page. For more information about the settings, see SSL VPN Customization Dialog Box—Applications, page 28-58.
- **Custom Panes**—Determine how you want to organize the body of the Portal page. The default is a single column with no internal panes. You can create a multiple-column layout, create internal panes that display text or references to URLs, and determine in which column and row to place the panes. For more information about the settings, see SSL VPN Customization Dialog Box—Custom Panes, page 28-59.
- **Home Page**—Determine how and whether to display URL lists on the home page, and whether to use your own web page for the main body of the Portal page. For more information about the settings, see SSL VPN Customization Dialog Box—Home Page, page 28-61.

Step 8 Select **Logout Page** to configure the settings of the page displayed when a user logs out of the SSL VPN. You can configure the title, message text, fonts, and colors. For more information about the settings, see SSL VPN Customization Dialog Box—Logout Page, page 28-62.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-9.

Step 10 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-13.

Step 11 Click **OK** to save the object.

Localizing SSL VPN Web Pages for ASA Devices

Localization is the process of providing text in a language that is appropriate for the target users. When you create an SSL VPN Customization object for defining the look of browser-based clientless SSL VPN web pages hosted on an ASA device, you can configure the pages to use the desired language.

To see localized web pages correctly, users must configure their browsers to use UTF-8 encoding (for example, in Internet Explorer, select **View > Encoding > Unicode (UTF-8)**. They also must install the required fonts or language support files for their language using the Regional and Language Options control panel. On the Languages tab, click Details to install the desired languages, and select the appropriate supplemental language settings for East Asian, complex scripting, and right-left languages. On the Advanced tab, select the desired code page conversion tables. If users do not configure the browser correctly, they might see boxes instead of characters.

There are two techniques you can use to localize SSL VPN web pages that are hosted on an ASA device. These techniques are not mutually exclusive; you can use both of them. These are the techniques:

- **Configure the SSL VPN Customization object using the desired language**—When you create the SSL VPN Customization object, you can enter text for labels and messages in non-English, non-ASCII languages in UTF-8 encoding. To enter non-ASCII languages in UTF-8 encoding, you must configure Windows with the correct locale setting and have the required fonts installed. Use the Regional and Language Options control panel to configure your system and install files required for complex script or East Asian languages. If you want to type in text directly, you also need to install an appropriate keyboard; otherwise, you can use a text editor that supports the language's characters and copy and paste text from a document that contains the text you want to use.

  You can also enter non-ASCII languages into SSL VPN Bookmarks objects.

- **Configure translation tables on the ASA device to support the languages you want to make available**—To enable the security appliance to provide language translation for the portal and screens displayed to users, you must define the necessary languages in a translation table and import the table into the security appliance. The software image package for the security appliance includes a translation table template. Every language you list in an SSL VPN Customization object must have a corresponding translation table on the device. Conversely, translation tables for languages that are not listed in the SSL VPN Customization object are ignored.

  If you use this technique, you must use the ASA CLI or ASDM to configure and upload the translation tables. You cannot manage the translation tables with Security Manager. However, the SSL VPN Customization object includes settings that allow you to configure automatic browser language selection and to enable users to select their desired language. Thus, if you install translation tables for ten languages, the pages defined in the SSL VPN Customization object will be available to users in all of those languages. For more information on these settings, see SSL VPN Customization Dialog Box—Language, page 28-53.

  Although both of the following features require translation tables, they are separate and complementary:

  - **Automatic Browser Language Selection**—Automatic browser language selection attempts to select the appropriate language based on the user's browser settings. This technique does not ask for user input. In the SSL VPN Customization object, you create a list of languages that will be used in the negotiation with the browser. During a connection, the security appliance receives a list of languages (and their priorities) from the browser, and looks through your list of languages top to bottom until a match is found. If there is no match, then the language you defined in the list as the default language is used. If you do not specify a default language, English is used.

The languages on the security appliance are labels for the translation tables. The languages must mirror those of the browser, and can consist of groups of up to 8 alphanumeric characters (starting from alpha characters), separated by hyphens. For example, fr-FR-paris-univ8. However, when you add a language to the list in Security Manager, only the first two characters are available.

When looking for a match, the security appliance starts with the longest language name, and if it does not match, it discards the rightmost group of the name. For example, if the preferred language on the browser is fr-FR-paris-univ8, and the security appliance supports fr-FR-paris-univ8, fr-FR-paris, fr-FR, and fr, it matches fr-FR-paris-univ8 and uses the translated strings from that translation table. If fr is the only language on the security appliance, the security appliance considers it a match also, and uses that translation table.

For more information about setting up translation tables, see the user documentation for the ASA device and operating system or the ASDM online help.

– **Language Selector**—By enabling the language selector, you provide the user with the ability to actively select the desired language from a list of languages that you support. This technique does not rely on the browser language settings being configured correctly. The language selector is displayed on the logon page.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63
- Creating Policy Objects, page 6-6
- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49

Creating Your Own SSL VPN Logon Page for ASA Devices

You can create your own custom SSL VPN Logon page rather than use the page provided by the security appliance for browser-based clientless SSL VPNs. This is called full customization, and replaces the settings you can configure in the SSL VPN Customization policy object.

To provide your own Logon page, you must create the page, copy it to the Security Manager server, and identify the page on the Full Customization page of the SSL VPN Customization object dialog box. For information on creating SSL VPN Customization objects, see Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63.

When you enable full customization, all other settings for the Logon page configured in the policy object are ignored. When you deploy your configuration to the ASA device, Security Manager copies your custom page to the device.

The Logon page you create must include all of the HTML code required to present the page correctly, and include special Cisco HTML code that provides the functions for the login form and the Language Selector drop-down list. Keep the following in mind when you create the HTML file:

- The file extension must be **.inc**.
- All images in the custom Logon page must be present on the security appliance. Replace the file path with the keyword **/+CSCOU+/**, which is an internal directory on the ASA device. When you upload an image to the device, it is saved in this directory.
- Use the **csco_ShowLoginForm('lform')** Javascript function to add the login form to the page. This form prompts for the username, passwords, and group information. You must include this function somewhere on the page.
- Use the **csco_ShowLanguageSelector('selector')** Javascript function to add the Language Selector drop-down list to the page. You do not have to use this function if you are not supporting the use of more than one language.

Related Topics

- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 26-63
- Add and Edit SSL VPN Customization Dialog Boxes, page 28-49
- SSL VPN Customization Dialog Box—Full Customization, page 28-57

Configuring SSL VPN Bookmark Lists for ASA and IOS Devices

When you configure a browser-based clientless SSL VPN, you can define a list of bookmarks, or URLS, to include on the SSL VPN portal page. Use SSL VPN bookmarks policy objects to define bookmark lists.

You can create SSL VPN bookmark objects for SSL VPNs hosted on IOS devices or ASA devices. However, these device types allow different bookmark configurations, the ASA device allowing more configuration options than IOS devices. Besides allowing more configuration options, you can also create bookmarks for ASA devices in non-English, non-ASCII languages. For more information on localizing the bookmarks and portal for ASA devices, see Localizing SSL VPN Web Pages for ASA Devices, page 26-66.

After you create the SSL VPN bookmark object as described in this procedure, you can use the object to specify the bookmark object in the **Portal Web Pages** or **Bookmarks** fields in these policies:

- ASA devices—On the **SSL VPN > Clientless** page in an ASA group policy object (see ASA Group Policies SSL VPN Clientless Settings, page 28-11), which you then select in one of these policies:
  - **Remote Access VPN > Group Policies**
  - **Remote Access VPN > Connection Profiles** on the **General** tab
- ASA devices—In the **Remote Access VPN > Dynamic Access** policy, you can specify the SSL VPN bookmark object on the **Main > Bookmarks** tab (see Main Tab, page 27-36).
- IOS devices—On the **Clientless** page in a user group policy object configured for SSL VPN (see User Group Dialog Box—Clientless Settings, page 28-78), which you then select in the **Remote Access VPN > SSL VPN** policy on the **General** tab.

Related Topics

- Creating Group Policies (ASA), page 26-31
- Configuring Dynamic Access Policies, page 26-20
- Understanding Connection Profiles (ASA), page 26-18
- Configuring an SSL VPN Policy (IOS), page 26-60
- Creating Policy Objects, page 6-6
- Policy Object Manager Window, page 6-3

Step 1 Select **Tools > Policy Object Manager** to open the Policy Object Manager (see Policy Object Manager Window, page 6-3).

Tip You can also create SSL VPN bookmark objects when you define policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Step 2 Select **SSL VPN Bookmarks** from the Object Type selector. The SSL VPN Bookmarks page opens, displaying a list of the existing SSL VPN bookmark objects.

Step 3 Right-click in the work area, then select **New Object**.

The Add SSL VPN Bookmark dialog box appears (see Add or Edit Bookmarks Dialog Boxes, page 28-46).

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 If you are creating the object for an SSL VPN hosted on an IOS device, you can enter a name for the heading that is displayed above the bookmarks list in the **Bookmarks Heading (IOS)** field.

Step 6 The Bookmarks table displays any URLs that are defined for the object. To add a bookmark, click the **Add Row** button below the table; to edit an existing bookmark, select it and click the **Edit Row** button.

The Add/Edit SSL VPN Bookmark Entry dialog box opens. For more information about the fields on this dialog box, see Add and Edit Bookmark Entry Dialog Boxes, page 28-47.

- In the **Bookmark Option** field, select whether you are defining a bookmark (**Enter Bookmark**) or adding bookmarks from another SSL VPN bookmark object (**Include Existing Bookmarks**). If you are including an existing object, enter the object's name or click **Select** to select it from a list of existing objects.
- If you are creating the object for use on an IOS device, enter the title of the bookmark, which is displayed to users, and the URL. Be careful to select the correct protocol for the URL. Click **OK** to add the bookmark to the table of bookmarks.
- If you are creating the object for use on an ASA device, you have many more options. Besides the title and the URL, you can define a subtitle and image icon for the bookmark plus other options.

Tip If you choose the protocols RDP, SSH, Telnet, VNC, or ICA, you must configure the plug-in for the protocol in the **Remote Access VPN > SSL VPN > Other Settings** policy (see SSL VPN Other Settings Page, page 27-88).

You can also configure the bookmark to use the Post method rather than the Get method. If you use Post, you must configure the post parameters by clicking **Add Row** beneath the Post Parameters table. For more information on Post parameters, see these topics:

- Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks, page 26-70
- Add and Edit Post Parameter Dialog Boxes, page 28-49

Click **OK** to add the bookmark to the table of bookmarks.

Step 7 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-9.

Step 8 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-13.

Step 9 Click **OK** to save the object.

Using the Post URL Method and Macro Substitutions in SSL VPN Bookmarks

One of the options you have for configuring bookmarks on an SSL VPN hosted on an ASA device is the method used by a URL, either Get or Post. The Get method is the standard method; a user clicks the URL and is taken to the web page. The Post method is useful when processing the data might involve changes to it, for example, storing or updating data, ordering a product, or sending e-mail.

If you choose the Post URL method, you must configure Post parameters for bookmark entries. Because these are often personalized resources that contain the user ID and password or other input parameters, you might need to define clientless SSL VPN macro substitutions.

Clientless SSL VPN macro substitutions let you configure users for access to personalized resources that contain the user ID and password or other input parameters. Examples of such resources include bookmark entries, URL lists, and file shares.

Note For security reasons, password substitutions are disabled for file access URLs (cifs://). Also for security reasons, use caution when introducing password substitutions for web links, especially for non-SSL instances.

You can use the following macro substitutions:

- **Logon Information Substitutions**— The security appliance obtains values for these substitutions from the SSL VPN Logon page. It recognizes these strings in user requests, and replaces them with the value specific to the user before it passes the request on to a remote server.

  These are the available macro substitutions:

  - CSCO_WEBVPN_USERNAME

    The username used to log into the SSL VPN.

  - CSCO_WEBVPN_PASSWORD

    The password used to log into the SSL VPN.

  - CSCO_WEBVPN_INTERNAL_PASSWORD

    The internal resource password entered when logging into the SSL VPN.

  - CSCO_WEBVPN_CONNECTION_PROFILE

    The connection profile associated with the user group selected when logging into the SSL VPN.

  For example, if a URL list contains the link http://someserver/homepage/CSCO_WEBVPN_USERNAME.html, the security appliance translates it to the following unique links:

  - For USER1 the link becomes http://someserver/homepage/USER1.html
  - For USER2 the link is http://someserver/homepage/USER2.html

  In the following example, cifs://server/users/CSCO_WEBVPN_USERNAME lets the security appliance map a file drive to specific users:

  - For USER1 the link becomes cifs://server/users/USER1
  - For USER2 the link is cifs://server/users/USER2

- **RADIUS/LDAP Vendor-Specific Attributes (VSAs)**—These substitutions let you set substitutions configured on either a RADIUS or an LDAP server. These are the available macro substitutions:
  - CSCO_WEBVPN_MACRO1
  - CSCO_WEBVPN_MACRO2

For information on configuring bookmarks, see Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 26-68.

Configuring SSL VPN Smart Tunnels for ASA Devices

A smart tunnel is a connection between an application running on a user's workstation and a private site. The connection uses a clientless (browser-based) SSL VPN session with the security appliance as the pathway and proxy server. Smart tunnels do not require the user to connect the application to the local port, so the application can gain access to the network without giving the user administrative privileges, as is required for full tunnel support. If you do not otherwise configure the network to allow access to an application, you can create a smart tunnel for those applications that you want to support.

You can configure smart tunnel access to an application under the following conditions:

- The application is a Winsock 2, TCP-based application and there is a browser plug-in for the application. Cisco distributes plug-ins for some applications for use in clientless SSL VPN, including SSH (for both SSH and Telnet sessions), RDP, and VNC. You must supply or obtain plug-ins for any other applications. Configure plug-ins in the **Remote Access VPN > SSL VPN > Other Settings** policy on the Plug-Ins tab.
- The user's workstation is running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000.

  Users of Microsoft Windows Vista who use smart tunnels (or port forwarding) must add the URL of the ASA device to the Trusted Site zone. Configure the Trusted Site zone in Internet Explorer (**Tools > Internet Options**, **Security** tab).
- The user's browser must be enabled with Java, Microsoft ActiveX, or both.
- If the user's workstation requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. In this configuration, smart tunnels support only basic authentication.

Tip A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

You configure smart tunnel access for an application by creating an SSL VPN smart tunnel list policy object and including that object in an ASA group policy object. You then assign the ASA group policy object to a device in the **Remote Access VPN > Group Policies** policy.

Related Topics

- Understanding Group Policies (ASA), page 26-30
- Creating Policy Objects, page 6-6
- Policy Object Manager Window, page 6-3

Step 1 Create an SSL VPN smart tunnel list policy object:

a. Select **Tools > Policy Object Manager** to open the Policy Object Manager (see Policy Object Manager Window, page 6-3), and select **SSL VPN Smart Tunnel Lists** from the table of contents.

Tip You can also create SSL VPN smart tunnel list objects when you create or edit the ASA group policy object. For more information, see Selecting Objects for Policies, page 6-2.

b. Click the **Add Object** button to open the Add and Edit Smart Tunnel List Dialog Boxes, page 28-65.

c. Enter a name for the object, up to 64 characters.

d. Add the applications to which you are granting smart tunnel access to the table of applications (click the **Add Row** button to open the Add and Edit A Smart Tunnel Entry Dialog Boxes, page 28-66). Consider the following:

- Enter an application name that is easy to understand and include version numbers if you support more than one version. For example, Microsoft Outlook.
- For the application path, the simplest and easiest to maintain option is to enter only the filename, for example, outlook.exe. This allows the user to install the application in any folder. Enter the full path if you want to enforce a specific installation structure.
- Hash values are optional, but you can use them to prevent spoofing. Without hash values, a user can rename an application to a supported filename; the security appliance checks only the filename and path (if specified). However, if you enter hash values, you must maintain them as users apply patches or application upgrades. For specific information on determining hash values, see Add and Edit A Smart Tunnel Entry Dialog Boxes, page 28-66.

Click **OK** to save the entry.

e. You can also incorporate other SSL VPN smart list objects into the object. This allows you to create a core set of smart list objects that you can use repeatedly in other objects.

f. Click **OK** to save the object.

Step 2 Configure the ASA group policy object to use the SSL VPN smart tunnel list object:

a. Edit (or create) the ASA group policy object either from the Policy Object Manager Window, page 6-3 or the **Remote Access VPN > Group Policies** policy. The object must be configured to support SSL VPNs. (You can also edit these objects from the **Remote Access VPN > Connection Profiles** policy from an individual profile, or the **Connection Profiles** policy for an EasyVPN topology.)

b. Select the **SSL VPN > Clientless** folder from the table of contents to open ASA Group Policies SSL VPN Clientless Settings, page 28-11.

c. Enter the name of the SSL VPN smart tunnel list object in the **Smart Tunnel** field.

d. Select **Auto Start Smart Tunnel** to automatically start smart tunnels for the applications when the user connects to the SSL VPN portal.

If you do not select this option, users must start smart tunnel access using the **Application Access > Start Smart Tunnels** button on the clientless SSL VPN portal page.

Configuring WINS/NetBIOS Name Service (NBNS) Servers To Enable File System Access in SSL VPNs

Clientless SSL VPN uses WINS and the Common Internet File System (CIFS) protocol to access or share files, printers, and other machine resources on remote systems. The ASA or IOS device uses a proxy CIFS client to provide this access transparently; users appear to have direct access to the file systems (subject to individual file and user permissions).

When users attempt a file-sharing connection to a Windows computer by using its computer name, the file server they specify corresponds to a specific WINS name that identifies a resource on the network. The security appliance queries WINS or NetBIOS name servers to map WINS names to IP addresses. SSL VPN requires NetBIOS to access or share files on remote systems.

You use WINS server list policy objects to configure the list of WINS servers that are used to resolve these Microsoft file-directory share names. The WINS server list objects define the NetBIOS Name Service (NBNS) server list on the device (using the **nbns-list** and **nbns-server** commands) for Common Internet File System (CIFS) name resolution.

After creating the WINS server list policy object, you can configure it in the following policies and policy objects, and also select the file access services that you want to allow:

- ASA devices—In the **Remote Access VPN > Connection Profiles** policy, specify the WINS server list object on the **SSL** tab (see SSL Tab (Connection Profiles), page 27-29).

  Select the file access options on the **SSL VPN > Clientless** page in an ASA group policy object (see ASA Group Policies SSL VPN Clientless Settings, page 28-11), which you then select in one of these policies:

  - **Remote Access VPN > Group Policies**
  - **Remote Access VPN > Connection Profiles** on the **General** tab
- IOS devices—On the **Clientless** page in a user group policy object configured for SSL VPN (see User Group Dialog Box—Clientless Settings, page 28-78), which you then select in the **Remote Access VPN > SSL VPN** policy on the **General** tab.

Related Topics

- Creating Policy Objects, page 6-6

Step 1 Select **Tools > Policy Object Manager** to open the Policy Object Manager Window, page 6-3.

Tip You can also create WINS server list objects when defining policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Step 2 Select **WINS Server Lists** from the Object Type selector.

The WINS Server List page opens, displaying the currently defined WINS server list objects.

Step 3 Right-click in the work area and select **New Object** to open the Add or Edit WINS Server List Dialog Box, page 28-84.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Click the **Add Row** button below the table, or select a server in the table and click **Edit Row**, to configure the WINS servers defined in the object. Configure these settings:

- **Server**—The IP address of the WINS server. You can select a network/host object or enter the address directly.
- **Set as Master Browser**—Select this option if the server is a master browser, which maintains the list of computers and shared resources.

Other fields are optional; change them if you want non-default values. For more information, see Add or Edit WINS Server Dialog Box, page 28-85.

Click **OK** to save your changes.

Step 6 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-9.

Step 7 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-13.

Step 8 Click **OK** to save the object.