Policy Groups

Note **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**. Limited support will continue on releases prior to 9.17(1). Further guidance will be provided regarding migration options to more robust and modern solutions (for example, remote Duo Network Gateway, AnyConnect, remote browser isolation capabilities, and so on).

Smart Tunnel Access

The following sections describe how to enable smart tunnel access with Clientless SSL VPN sessions, specify the applications to be provided with such access, and provide notes on using it.

To configure smart tunnel access, you create a smart tunnel list containing one or more applications eligible for smart tunnel access, and the endpoint operating system associated with the list. Because each group policy or local user policy supports one smart tunnel list, you must group the nonbrowser-based applications to be supported into a smart tunnel list. After creating a list, you assign it to one or more group policies or local user policies.

The following sections describe smart tunnels and how to configure them:

• Enable and Switch Off Smart Tunnel Access, on page 11
• Configure Smart Tunnel Log Off, on page 11

About Smart Tunnels

A smart tunnel is a connection between a TCP-based application and a private site, using a clientless (browser-based) SSL VPN session with the security appliance as the pathway, and the ASA as a proxy server. You can identify applications for which to grant smart tunnel access, and specify the local path to each application. For applications running on Microsoft Windows, you can also require a match of the SHA-1 hash of the checksum as a condition for granting smart tunnel access.

Lotus SameTime and Microsoft Outlook are examples of applications to which you may want to grant smart tunnel access.

Configuring smart tunnels requires one of the following procedures, depending on whether the application is a client or is a web-enabled application:

- Create one or more smart tunnel lists of the client applications, then assign the list to the group policies or local user policies for whom smart tunnel access is required.
- Create one or more bookmark list entries that specify the URLs of the web-enabled applications eligible for smart tunnel access, then assign the list to the group policies or local user policies for whom smart tunnel access is required.

You can also list web-enabled applications for which to automate the submission of login credentials in smart tunnel connections over Clientless SSL VPN sessions.

Benefits of Smart Tunnels

Smart tunnel access lets a client TCP-based application use a browser-based VPN connection to access a service. It offers the following advantages to users, compared to plug-ins and the legacy technology, port forwarding:

- Smart tunnel offers better performance than plug-ins.
- Unlike port forwarding, smart tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
- Unlike port forwarding, smart tunnel does not require users to have administrator privileges.

The advantage of a plug-in is that it does not require the client application to be installed on the remote computer.

Prerequisites for Smart Tunnels

See the Supported VPN Platforms, Cisco ASA 5500 Series, for the platforms and browsers supported by smart tunnels.

The following requirements and limitations apply to smart tunnel access on Windows:

- ActiveX or Oracle Java Runtime Environment (JRE 6 or later recommended) on Windows must be enabled on the browser.

- Only Winsock 2, TCP-based applications are eligible for smart tunnel access.
- For Mac OS X only, Java Web Start must be enabled on the browser.
- Smart tunnel is incompatible with IE's Enhanced Protected Mode.

Guidelines for Smart Tunnels

- Smart tunnel supports only proxies placed between computers running Microsoft Windows and the security appliance. Smart Tunnel uses the Internet Explorer configuration, which sets system-wide parameters in Windows. That configuration may include proxy information:
  - If a Windows computer requires a proxy to access the ASA, then there must be a static proxy entry in the client's browser, and the host to connect to must be in the client's list of proxy exceptions.
  - If a Windows computer does not require a proxy to access the ASA, but does require a proxy to access a host application, then the ASA must be in the client's list of proxy exceptions.

  Proxy systems can be defined the client’s configuration of static proxy entry or automatic configuration, or by a PAC file. Only static proxy configurations are currently supported by Smart Tunnels.
- Kerberos constrained delegation (KCD) is not supported for smart tunnels.
- With Windows, to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.
- With HTTP-based remote access, some subnets may block user access to the VPN gateway. To fix this, place a proxy in front of the ASA to route traffic between the Web and the end user. That proxy must support the CONNECT method. For proxies that require authentication, Smart Tunnel supports only the basic digest authentication type.
- When smart tunnel starts, the ASA by default passes all browser traffic through the VPN session if the browser process is the same. The ASA only also does this if a tunnel-all policy (the default) applies. If the user starts another instance of the browser process, it passes all traffic through the VPN session. If the browser process is the same and the security appliance does not provide access to a URL, the user cannot open it. As a workaround, assign a tunnel policy that is not tunnel-all.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.
- The Mac version of smart tunnel does not support POST bookmarks, form-based auto sign-on, or POST macro substitution.
- For macOS users, only those applications started from the portal page can establish smart tunnel connections. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named csco_st. If this user profile is not present, the session prompts the user to create one.
- In macOS, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel.
- Smart tunnel does not support the following on macOS:
  - Sandboxed applications (verify in Activity Monitor using View > Columns). For that reason, macOS 10.14 and 10.15 do not support smart tunneling.

- Proxy services.
- Auto sign-on.
- Applications that use two-level name spaces.
- Console-based applications, such as Telnet, SSH, and cURL.
- Applications using dlopen or dlsym to locate libsocket calls.
- Statically linked applications to locate libsocket calls.

- macOS requires the full path to the process and is case-sensitive. To avoid specifying a path for each username, insert a tilde (~) before the partial path (e.g., ~/bin/vnc).
- A new method for smart-tunnel support in the Chrome browser on Mac and Windows devices is now in place. A Chrome Smart Tunnel Extension has replaced the Netscape Plugin Application Program Interfaces (NPAPIs) that are no longer supported on Chrome.

  If you click on the smart tunnel enabled bookmark in Chrome without the extension already being installed, you are redirected to the Chrome Web Store to obtain the extension. New Chrome installations will direct the user to the Chrome Web Store to download the extension. The extension downloads the binaries from ASA that are required to run smart tunnel.

  Chrome's default download location needs to point to the current user's Downloads folder. Or, if Chrome's download setup is 'Ask every time' the user should choose the Downloads folder when asked.

  Your usual bookmark and application configuration while using smart tunnel is unchanged other than the process of installing the new extension and specifying the download location.

Configure a Smart Tunnel (Lotus Example)

Note These example instructions provide the minimum instructions required to add smart tunnel support for an application. See the field descriptions in the sections that follow for more information.

Procedure

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access** > **Portal** > **Smart Tunnels**.

Step 2 Double-click the smart tunnel list to add an application to; or click **Add** to create a list of applications, enter a name for this list in the List Name field, and click **Add**.

For example, click **Add** in the Smart Tunnels pane, enter Lotus in the List Name field, and click **Add**.

Step 3 Click **Add** in the Add or Edit Smart Tunnel List dialog box.

Step 4 Enter a string in the Application ID field to serve as a unique index to the entry within the smart tunnel list.

Step 5 Enter the filename and extension of the application into the Process Name dialog box.

The following table shows example application ID strings and the associated paths required to support Lotus.

Table 1: Smart Tunnel Example: Lotus 6.0 Thick Client with Domino Server 6.5.5

Application ID Example	Minimum Required Process Name
lotusnotes	notes.exe
lotusnlnotes	nlnotes.exe
lotusntaskldr	ntaskldr.exe
lotusnfileret	nfileret.exe

Step 6 Select **Windows** next to OS.

Step 7 Click **OK**.

Step 8 Repeat for each application to add to the list.

Step 9 Click **OK** in the Add or Edit Smart Tunnel List dialog box.

Step 10 Assign the list to the group policies and local user policies to provide smart tunnel access to the associated applications, as follows:

- To assign the list to a group policy, choose **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal** and choose the smart tunnel name from the Smart Tunnel List drop-down.
- To assign the list to a local user policy, choose **Configuration > Remote Access VPN> AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the Smart Tunnel List drop-down.

Simplify Configuration of Applications to Tunnel

A smart tunnel application list is essentially a filter of what applications are granted access to the tunnel. The default is to allow access for all processes started by the browser. With a Smart Tunnel enabled bookmark, the clientless session grants access only to processes initiated by the Web browser. For non-browser applications, an administrator can choose to tunnel all applications and thus remove the need to know which applications an end user may invoke.

Note This configuration is applicable to Windows platforms only.

The following table shows the situations in which processes are granted access.

Situation	Smart Tunnel Enabled Bookmark	Smart Tunnel Application Access
Application list specified	Any processes that match a process name in the application list are granted access.	Only processes that match a process name in the application list are granted access.
Smart tunnel is switched off	All processes (and their child processes) are granted access.	No process is granted access.

Situation	Smart Tunnel Enabled Bookmark	Smart Tunnel Application Access
Smart Tunnel all Applications check box is checked.	All processes (and their child processes) are granted access. **Note** This includes processes initiated by non-Smart Tunnel Web pages if the Web page is served by the same browser process.	All processes owned by the user who started the browser are granted access but not child processes of those original processes.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users**.

Step 2 In the User Account window, highlight the username to edit.

Step 3 Click **Edit**. The Edit User Account window appears.

Step 4 In the left sidebar of the Edit User Account window, click **VPN Policy** > **Clientless SSL VPN**.

Step 5 Perform one of the following:

- Check the **smart tunnel_all_applications** check box. All applications will be tunneled without making a list or knowing which executables an end user may invoke for external applications.
- Or choose from the following tunnel policy options:
  - Uncheck the **Inherit** check box at the Smart Tunnel Policy parameter.
  - Choose from the network list and specify one of the tunnel options: use smart tunnel for the specified network, do not use smart tunnel for the specified network, or use tunnel for all network traffic.

Add Applications to Be Eligible for Smart Tunnel Access

The Clientless SSL VPN configuration of each ASA supports *smart tunnel lists*, each of which identifies one or more applications eligible for smart tunnel access. Because each group policy or username supports only one smart tunnel list, you must group each set of applications to be supported into a smart tunnel list.

The Add or Edit Smart Tunnel Entry dialog box lets you specify the attributes of an application in a smart tunnel list.

Procedure

Step 1 Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Smart Tunnels**, and choose a smart tunnel application list to edit, or add a new one.

Step 2 For a new list, enter a unique name for the list of applications or programs. Do not use spaces.

Following the configuration of the smart tunnel list, the list name appears next to the Smart Tunnel List attribute in the Clientless SSL VPN group policies and local user policies. Assign a name that will help you to distinguish its contents or purpose from other lists that you are likely to configure.

Step 3 Click Add and add as many applications as you need to this smart tunnel list. The parameters are described below:

- Application ID - Enter a string to name the entry in the smart tunnel list. This user-specified name is saved and then returned onto the GUI. The string is unique for the operating system. It typically names the application to be granted smart tunnel access. To support multiple versions of an application for which you choose to specify different paths or hash values, you can use this attribute to differentiate entries, specifying the operating system, and name and version of the application supported by each list entry. The string can be up to 64 characters.
- Process Name - Enter the filename or path to the application. The string can be up to 128 characters.

  Windows requires an exact match of this value to the right side of the application path on the remote host to qualify the application for smart tunnel access. If you specify only the filename for Windows, SSL VPN does not enforce a location restriction on the remote host to qualify the application for smart tunnel access.

  If you specify a path and the user installed the application in another location, that application does not qualify. The application can reside on any path as long as the right side of the string matches the value you enter.

  To authorize an application for smart tunnel access if it is present on one of several paths on the remote host, either specify only the name and extension of the application in this field; or create a unique smart tunnel entry for each path.

  Note A sudden problem with smart tunnel access may be an indication that a Process Name value is not up-to-date with an application upgrade. For example, the default path to an application sometimes changes following the acquisition of the company that produces the application and the next application upgrade.

  With Windows, to add smart tunnel access to an application started from the command prompt, you must specify “cmd.exe” in the Process Name of one entry in the smart tunnel list, and specify the path to the application itself in another entry, because “cmd.exe” is the parent of the application.
- OS—Click **Windows** or **Mac** to specify the host operating system of the application.
- Hash (Optional and only applicable to Windows)—To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1** application at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash.

  The SHA-1 hash is always 40 hexadecimal characters.

  Before authorizing an application for smart tunnel access, Clientless SSL VPN calculates the hash of the application matching the Application ID. It qualifies the application for smart tunnel access if the result matches the value of Hash.

  Entering a hash provides a reasonable assurance that SSL VPN does not qualify an illegitimate file that matches the string you specified in the Application ID. Because the checksum varies with each version or patch of an application, the Hash you enter can only match one version or patch on the remote host. To specify a hash for more than one version of an application, create a unique smart tunnel entry for each Hash value.

Note If you enter Hash values and you need to support future versions or patches of an application with smart tunnel access, you must keep the smart tunnel list updated. A sudden problem with smart tunnel access may be an indication that the application list containing Hash values is not up-to-date with an application upgrade. You can avoid this problem by not entering a hash.

Step 4 Click **OK** to save the application, and create how ever many applications you need for this smart tunnel list.

Step 5 When you are done creating your smart tunnel list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy, choose **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add** or **Edit > Portal** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.
- To assign the list to a local user policy, choose **Config > Remote Access VPN> AAA Setup > Local Users > Add** or **Edit > VPN Policy > Clientless SSL VPN** and choose the smart tunnel name from the drop-down list next to the Smart Tunnel List attribute.

Table 2: Example Smart Tunnel Entries

Smart Tunnel Support	Application ID (Any unique string is OK.)	Process Name	OS
Mozilla Firefox.	firefox	firefox.exe	Windows
Microsoft Outlook Express.	outlook-express	msimn.exe	Windows
More restrictive alternative—Microsoft Outlook Express only if the executable file is in a predefined path.	outlook-express	\Program Files\Outlook Express\msimn.exe	Windows
Open a new Terminal window on a Mac. (Any subsequent application launched from within the same Terminal window fails because of the one-time-password implementation.)	terminal	Terminal	Mac
Start smart tunnel for a new window	new-terminal	Terminal open -a MacTelnet	Mac
Start application from a Mac Terminal window.	curl	Terminal curl www.example.com	Mac

About Smart Tunnel Lists

For each group policy and username, you can configure Clientless SSL VPN to do one of the following:

- Start smart tunnel access automatically upon user login.
- Enable smart tunnel access upon user login, but require the user to start it manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN Portal Page.

Note The smart tunnel logon options are mutually exclusive for each group policy and username. Use only one.

Create a Smart Tunnel Auto Sign-On Server List

The Smart Tunnel Auto Sign-on Server List dialog box lets you add or edit lists of servers which will automate the submission of login credentials during smart tunnel setup. Auto sign-on over a smart tunnel is available for Internet Explorer and Firefox.

Procedure

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels, and ensure that the Smart Tunnel Auto Sign-on Server List is expanded.

Step 2 Click Add, and enter a unique name for a list of remote servers that will help you to distinguish its contents or purpose from other lists that you are likely to configure. The string can be up to 64 characters. Do not use spaces.

What to do next

Note After you create a smart tunnel auto sign-on list, that list name appears next to the Auto Sign-on Server List attribute under Smart Tunnel in the Clientless SSL VPN group policy and local user policy configurations.

Add Servers to a Smart Tunnel Auto Sign-On Server List

The following steps describe how to add servers to the list of servers for which to provide auto sign-on in smart tunnel connections, and assign that list to a group policies or a local user.

Procedure

Step 1 Navigate to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Smart Tunnels**, choose one of the lists, and click **Edit**.

Step 2 Click the Add button on the Add Smart Tunnel Auto Sign-On Server List dialog to add one more smart tunnel servers.

Step 3 Enter the hostname or IP address of the server to auto-authenticate to:

- If you choose Hostname, enter a hostname or wildcard mask to auto-authenticate to. You can use the following wildcard characters:
  - * to match any number of characters or zero characters.
  - ? to match any single character.
  - [] to match any single character in the range expressed inside the brackets.
  - For example, enter *.example.com. Using this option protects the configuration from dynamic changes to IP addresses.
- If you choose IP Address, enter an IP address.

  Note Firefox does not support a host mask with wild cards, a subnet using IP addresses, or a netmask; you must use an exact hostname or IP address. For example, within Firefox, if you enter *.cisco.com, auto sign-on to host email.cisco.com will fail.

Step 4 Windows Domain (Optional)—Click to add the Windows domain to the username, if authentication requires it. If you do so, ensure you specify the domain name when assigning the smart tunnel list to one or more group policies or local user policies.

Step 5 HTTP-based Auto Sign-On (Optional)

- Authentication Realm—The realm is associated with the protected area of the website and passed back to the browser either in the authentication prompt or in the HTTP headers during authentication. Once auto-sign is configured here, and a realm string is specified, users can configure the realm string on a Web application (such as Outlook Web Access) and access Web applications without signing on.

  Use the address format used in the source code of the Web pages on the intranet. If you are configuring smart tunnel auto sign-on for browser access and some Web pages use hostnames and others use IP addresses, or you do not know, specify both in different smart tunnel auto sign-on entries. Otherwise, if a link on a Web page uses a different format than the one you specify, it fails when the user clicks it.

  Note If administrators do not know the corresponding realm, they should perform logon once and get the string from the prompt dialog.

- Port Number—Specify a port number for the corresponding hosts. For Firefox, if no port number is specified, auto sign-on is performed on HTTP and HTTPS, accessed by default port numbers 80 and 443 respectively.

Step 6 Click **OK**.

Step 7 Following the configuration of the smart tunnel auto sign-on server list, you must assign it to a group policy or a local user policy for it to become active, as follows:

- To assign the list to a group policy:
  - **a.** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies,** and open a group policy,
  - **b.** Select the Portal tab, find the Smart Tunnel area, and choose the auto sign-on server list from the drop-down list next to the Auto Sign-On Server List attribute.

- To assign the list to a local user policy:
  a. Choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**, and edit the local user to assign an auto sign-on server list to.
  b. Navigate to VPN Policy > Clientless SSL VPN, and find the Auto Sign-on Server setting under the Smart Tunnel area
  c. Uncheck Inherit, and choose a server list from the drop-down list next to the Auto Sign-On Server List attribute.

Enable and Switch Off Smart Tunnel Access

By default, smart tunnels are switched off.

If you enable smart tunnel access, the user will have to start it manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.

Configure Smart Tunnel Log Off

This section describes how to ensure that the smart tunnel is properly logged off. Smart tunnel can be logged off when all browser windows have been closed, or you can right click the notification icon and confirm log out.

Note We strongly recommend the use of the logout button on the portal. This method pertains to Clientless SSL VPNs and logs off regardless of whether smart tunnel is used or not. The notification icon should be used only when using standalone applications without the browser.

Configure Smart Tunnel Log Off when Its Parent Process Terminates

This practice requires the closing of all browsers to signify log off. The smart tunnel lifetime is now tied to the starting process lifetime. For example, if you started a smart tunnel from Internet Explorer, the smart tunnel is turned off when no iexplore.exe is running. Smart tunnel can determine that the VPN session has ended even if the user closed all browsers without logging out.

Note In some cases, a lingering browser process is unintentional and is strictly a result of an error. Also, when a Secure Desktop is used, the browser process can run in another desktop even if the user closed all browsers within the secure desktop. Therefore, smart tunnel declares all browser instances gone when no more visible windows exist in the current desktop.

Configure Smart Tunnel Log Off with a Notification Icon

You may also choose to switch off logging off when a parent process terminates so that a session survives if you close a browser. For this practice, you use a notification icon in the system tray to log out. The icon

remains until the user clicks the icon to logout. If the session has expired before the user has logged out, the icon remains until the next connection is tried. You may have to wait for the session status to update in the system tray.

Note This icon is an alternative way to log out of SSL VPN. It is not an indicator of VPN session status.

Procedure

Step 1 Choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Smart Tunnels**.

Step 2 Enable the **Click on smart-tunnel logoff** > **icon in the system tray** radio button.

Step 3 In the Smart Tunnel Networks portion of the window, check **Add** and enter both the IP address and hostname of the network which should include the icon.

Note If you right-click the icon, a single menu item appears that prompts the user to log out of the SSL VPN.

Clientless SSL VPN Capture Tool

The Clientless SSL VPN CLI includes a capture tool that lets you log information about websites that do not display properly over a WebVPN connection. The data this tool records can help your Cisco customer support representative troubleshoot problems.

The output of the Clientless SSL VPN capture tool consists of two files:

- mangled.1, 2,3, 4... and so on, depending on the Web page activity. The mangle files record the html actions of the VPN Concentrator transferring these pages on a Clientless SSL VPN connection.
- original.1,2,3,4... and so on, depending on the Web page activity. The original files are the files the URL sent to the VPN Concentrator.

To open and view the files output by the capture tool, go to Administration | File Management. Zip the output files and send them to your Cisco support representative.

Note Using the Clientless SSL VPN capture tool does impact VPN Concentrator performance. Ensure you switch off the capture tool after you have generated the output files.

Configure Portal Access Rules

This enhancement allows customers to configure a global Clientless SSL VPN access policy to permit or deny Clientless SSL VPN sessions based on the data present in the HTTP header. If the ASA denies a Clientless SSL VPN session, it returns an error code to the endpoint immediately.

The ASA evaluates this access policy before the endpoint authenticates to the ASA. As a result, in the case of a denial, fewer ASA processing resources are consumed by additional connection attempts from the endpoint.

Procedure

Step 1 Start ASDM and choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Portal Access Rule**.

The Portal Access Rule window opens.

Step 2 Click **Add** to create a portal access rule or choose an existing rule and click **Edit** > **.**

The Add (or Edit) Portal Access Rule dialog box opens.

Step 3 Enter a rule number from 1 to 65535 in the Rule Priority field.

Rules are processed in order of priority from 1 to 65535.

Step 4 In the User Agent field, enter the name of the user agent to find in the HTTP header.

- Surround the string with wildcards (*) to generalize the string; for example, *Thunderbird*. We recommend using wildcards in your search string. Without wildcards, the rule may not match any strings or it may match many fewer strings than you expect.
- If your string contains a space, ASDM automatically adds quotes to the beginning and end of the string when it saves the rule. For example, if you enter `my agent`, ASDM will save the string as `"my agent"`. ASA will then search for matches of `my agent`.

  Do not add quotes to a string with spaces unless you require the ASA to match the quotes you added to the string. For example, if you enter `"my agent"` ASDM will save the string as `"\"my agent\'"` and try to find a match for `"my agent"` and it will not find `my agent`.
- To use wildcards with a string that contains a space, start and end the entire string with wildcards, for example, `*my agent*` and ASDM will automatically surround that string with quotes when it saves the rule.

Step 5 In the Action field, choose either **Deny** or **Permit**.

The ASA will deny or permit a Clientless SSL VPN connection based on this setting.

Step 6 Enter an HTTP message code in the Returned HTTP Code field.

The HTTP message number 403 is pre-populated in the field and is the default value for portal access rules. The allowed range of message codes is 200 to 599.

Step 7 Click **OK**.

Step 8 Click **Apply**.

Optimize Clientless SSL VPN Performance

The ASA provides several ways to optimize Clientless SSL VPN performance and functionality. Performance improvements include caching and compressing Web objects. Functionality tuning includes setting limits on content transformation and proxy-bypass. APCF provides an additional method of tuning content transformation.

Configure Content Transformation

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

Some Web resources require highly individualized treatment. The following sections describe functionality that provides such treatment. Subject to the requirements of your organization and the Web content involved, you may use one of these features.

Use Proxy Bypass

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

You can 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 may need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you may need to use multiple pathmask statements to exhaust the possibilities.

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

You can set rules for when the ASA performs little or no content rewriting:

Procedure

Step 1 Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxy Bypass**.

Step 2 Select the Interface name for proxy bypass.

Step 3 Specify either a port or a URI for proxy bypass:

- Port—(radio button) Click to use a port for proxy bypass. The valid port numbers are 20000 to 21000.
- Port (field)—Enter a high-numbered port for the ASA to reserve for proxy bypass.
- Path Mask—(radio button) Click to use a URL for proxy bypass.
- Path Mask—(Field) Enter a URL for proxy bypass. It can contain a regular expression.

Step 4 Define target URLs for proxy bypass:

- URL—(drop-down list) Click either http or https as the protocol.
- URL (text field)—Enter a URL for which to apply a proxy bypass.

Step 5 Specify the content to rewrite. The choices are none or a combination of XML, links, and cookies.

- XML—Check to rewrite XML content.
- Hostname—Check to rewrite links.