Configuring Policy Groups

September 13, 2013

Creating and Applying Clientless SSL VPN Policies for Accessing Resources

Creating and applying policies for Clientless SSL VPN that govern access to resources at an internal server includes the following task:

- Assigning Users to Group Policies

Assigning Users to Group Policies

Assigning users to group policies simplifies the configuration by letting you apply policies to many users. You can use an internal authentication server on the ASA or an external RADIUS or LDAP server to assign users to group policies. See Chapter 4, "Configuring Connection Profiles, Group Policies, and Users" for a thorough explanation of ways to simplify configuration with group policies.

Configuring Connection Profile Attributes for Clientless SSL VPN

Table 17-1 provides a list of connection profile attributes that are specific to Clientless SSL VPN. In addition to these attributes, you configure general connection profile attributes common to all VPN connections. For step-by-step information on configuring connection profiles, see Chapter 4, "Configuring Connection Profiles, Group Policies, and Users."

Note In earlier releases, "connection profiles" were known as "tunnel groups." You configure a connection profile with **tunnel-group** commands. This chapter often uses these terms interchangeably.

Table 17-1 Connection Profile Attributes for Clientless SSL VPN

Command	Function
`authentication`	Sets the authentication method.
`customization`	Identifies the name of a previously defined customization to apply.
`exit`	Exits from tunnel-group Clientless SSL VPN attribute configuration mode.
`nbns-server`	Identifies the name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.
`group-alias`	Specifies the alternate names by which the server can refer to a connection profile.
`group-url`	Identifies one or more group URLs. If you establish URLs with this attribute, this group is selected automatically for users when they access using these URLS.
`dns-group`	Identifies the DNS server group that specifies the DNS server name, domain name, name server, number of retries, and timeout values.
`help`	Provides help for tunnel group configuration commands.
`hic-fail-group-policy`	Specifies a VPN feature policy if you use the Cisco Secure Desktop Manager to set the Group-Based Policy attribute to "Use Failure Group-Policy" or "Use Success Group-Policy, if criteria match."
`no`	Removes an attribute value pair.
`override-svc-download`	Overrides downloading the group-policy or username attributes configured for downloading the AnyConnect VPN client to the remote user.
`pre-fill-username`	Configures username-to-certificate binding on this tunnel group.
`proxy-auth`	Identifies this tunnel-group as a specific proxy authentication tunnel group.
`radius-reject-message`	Enables the display of the RADIUS reject message on the login screen when authentication is rejected.
`secondary-pre-fill-username`	Configures the secondary username-to-certificate binding on this tunnel group.
`without-csd`	Switched off CSD for a tunnel group.

Configuring Group Policy and User Attributes for Clientless SSL VPN

Table 17-2 provides a list of group policy and user attributes for Clientless SSL VPN. For step-by-step instructions on configuring group policy and user attributes, see "Configuring Group Policies" and "Configuring Attributes for Individual Users" or in Chapter 4, "Configuring Connection Profiles, Group Policies, and Users."

Table 17-2 Group Policy and User Attributes for Clientless SSL VPN

Command	Function
activex-relay	Lets a user who has established a Clientless SSL VPN session use the browser to launch Microsoft Office applications. The applications use the session to download and upload ActiveX. The ActiveX relay remains in force until the Clientless SSL VPN session closes.
auto-sign-on	Sets values for auto sign-on, which requires that the user enter username and password credentials only once for a Clientless SSL VPN connection.
customization	Assigns a customization object to a group policy or user.
deny-message	Specifies the message delivered to a remote user who logs into Clientless SSL VPN successfully, but has no VPN privileges.
file-browsing	Enables CIFS file browsing for file servers and shares. Browsing requires NBNS (Master Browser or WINS).
file-entry	Allows users to enter file server names to access.
filter	Sets the name of the webtype access list.
hidden-shares	Controls the visibility of hidden shares for CIFS files.
homepage	Sets the URL of the Web page that displays upon login.
html-content-filter	Configures the content and objects to filter from the HTML for this group policy.
http-comp	Configures compression.
http-proxy	Configures the ASA to use an external proxy server to handle HTTP requests. **Note** Proxy NTLM authentication is not supported in **http-proxy**. Only proxy without authentication and basic authentication are supported.
keep-alive-ignore	Sets the maximum object size to ignore for updating the session timer.
port-forward	Applies a list of Clientless SSL VPN TCP ports to forward. The user interface displays the applications on this list.
post-max-size	Sets the maximum object size to post.
smart-tunnel	Configures a list of programs and several smart tunnel parameters to use smart tunnel.
sso-server	Sets the name of the SSO server.
storage-objects	Configures storage objects for the data stored between sessions.
svc	Configures SSL VPN Client attributes.
unix-auth-gid	Sets the UNIX group ID.
unix-auth-uid	Sets the UNIX user ID.
upload-max-size	Sets the maximum object size to upload.
url-entry	Controls the ability of the user to enter any HTTP/HTTPS URL.
url-list	Applies a list of servers and URLs that Clientless SSL VPN portal page displays for end-user access.
user-storage	Configures a location for storing user data between sessions.

Configuring 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.## Configuring Smart Tunnel Access

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:

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.

Why 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

See the *Supported VPN Platforms, Cisco ASA 5500 Series*, for the platforms and browsers supported by ASA Release 9.0 smart tunnels.

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

- ActiveX or Oracle Java Runtime Environment (JRE) 4 update 15 or later (JRE 6 or later recommended) on Windows must be enabled on the browser.

  ActiveX pages require that you enter the **activex-relay** command on the associated group policy. If you do so or assign a smart tunnel list to the policy, and the browser proxy exception list on the endpoint specifies a proxy, the user must add a “shutdown.webvpn.relay.” entry to this list.
- 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.

Restrictions

- 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 Mac OS X 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 Mac OS X, 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 Mac OS X:
  - 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.
- Mac OS X 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).

Adding 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.

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.

Restrictions

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

DETAILED STEPS

The following smart tunnel commands are available to each group policy and username. The configuration of each group policy and username supports only one of these commands at a time, so when you enter one, the ASA replaces the one present in the configuration of the group policy or username in question with the new one, or in the case of the last command, simply removes the **smart-tunnel** command already present in the group policy or username.

	Command	Purpose
Step 1	**smart-tunnel auto-start** *list* OR **smart-tunnel enable** *list* OR **smart-tunnel disable** OR **no smart-tunnel [auto-start list | enable list | disable]**	Starts smart tunnel access automatically upon user login. Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access > Start Smart Tunnels** button on the Clientless SSL VPN portal page. Prevents smart tunnel access. Removes a **smart-tunnel** command from the group policy or username configuration, which then inherits the [**no**] **smart-tunnel** command from the default group-policy. The keywords following the **no smart-tunnel** command are optional, however, they restrict the removal to the named **smart-tunnel** command.
Step 2	Refer to Automating Smart Tunnel Access for the required option.	

Configuring and Applying Smart Tunnel Policy

The smart tunnel policy requires a per group policy/username configuration. Each group policy/username references a globally configured list of networks. When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the use of 2 CLIs: one configures the network (a set of hosts), and the other uses the specified smart-tunnel network to enforce a policy on a user. The following commands create a list of hosts to use for configuring smart tunnel policies:

DETAILED STEPS

	Command	Purpose
Step 1	**webvpn**	Switches to Clientless SSL VPN configuration mode.
Step 2	**[no] smart-tunnel network** *network name* **ip** *ip netmask*	Creates a list of hosts to use for configuring smart tunnel policies. *network name* is the name to apply to the tunnel policy. *ip* is the IP address of the network. *netmask* is the netmask of the network.
Step 3	**[no] smart-tunnel network** *network name* **host** *host mask*	Establishes the hostname mask, such as *.cisco.com.
Step 4	**[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]** OR **[no] smart-tunnel tunnel-policy {excludespecified | tunnelspecified}** *network* ***name*** **| tunnelall]**	Applies smart tunnel policies to a particular group or user policy. *network name* is a list of networks to be tunneled. *tunnelall* makes everything tunneled (encrypted). *tunnelspecified* tunnels only networks specified by network name. *excludespecified* tunnels only networks that are outside of the networks specified by network name.

Configuring and Applying a Smart Tunnel Tunnel Policy

Like the split tunnel configuration in the SSL VPN client, the smart tunnel policy is a per group-policy/username configuration. Each group policy/username references a globally configured list of networks:

Command	Purpose
[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]** or **[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified}** *network name* **| tunnelall]**	References a globally configured list of networks. *network name* is a list of networks to be tunneled. *tunnelall* makes everything tunneled (encrypted). tunnelspecified tunnels only networks specified by network name. excludespecified tunnels only networks that are outside of the networks specified by network name.

Command	Purpose
ciscoasa(config-webvpn)# [no] smart-tunnel network *network name* **ip** *ip netmask* **ciscoasa(config-webvpn)# [no] smart-tunnel network** *network name* **host** *host mask*	Applies a tunnel policy to a group-policy/user policy. One command specifies host and the other specifies network IPs; use only one. *network name*—name of network to apply to tunnel policy *ip address*—IP address of a network *netmask*—netmask of a network *host mask*—hostname mask, such as *.cisco.com
Example: ciscoasa(config-webvpn)# **smart-tunnel network inventory ip 10.5.2.2** ciscoasa(config-webvpn)# **smart-tunnel network inventory host www.example.com**	Smart tunnel policy configuration is a good option when a vendor wants to provide a partner with clientless access to an internal inventory server page upon login without going through the clientless portal first. Creates a tunnel policy that contains only one host (assuming the inventory pages are hosted at www.example.com (10.5.2.2), and you want to configure both IP address and name for the hosts).
ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**	Applies the tunnel-specified tunnel policy to the partner's group policy.
(Optional) ciscoasa(config-group-webvpn)# **homepage value http://www.example.com** ciscoasa(config-group-webvpn)# h**omepage use-smart-tunnel**	Specifies the group policy home page and enables smart tunnel on it. Without writing a script or uploading anything, an administrator can specify which homepage to connect with via smart tunnel.
(Optional) ciscoasa(config-webvpn)# **smart-tunnel notification-icon**	By default, configuration of a smart tunnel application is not necessary because all processes initiated by the browser with smart tunnel enabled have access to the tunnel. However, because no portal is visible, you may want to enable the logout notification icon.

Creating a Smart Tunnel Auto Sign-On Server List

Command	Purpose
webvpn	Switches to Clientless SSL VPN configuration mode.
smart-tunnel auto-sign-on *list* [*use-domain*] [**realm** *realm-string*] [**port** *port-num*]{**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	Use for each server to add to the server list • *list*—names the list of remote servers. Use quotation marks around the name if it includes a space. The string can be up to 64 characters. The ASA creates the list if it is not already present in the configuration. Otherwise, it adds the entry to the list. Assign a name that will help you to distinguish. • use-domain (optional)—Adds the Windows domain to the username if authentication requires it. If you enter this keyword, ensure you specify the domain name when assigning the smart tunnel list to one or more group policies, or usernames. • *realm*—Configures a realm for the authentication. Realm is associated with the protected area of the website and is passed back to the browser either in the authentication prompt or in the HTTP headers during authentication. Once auto-sign is configured 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 • *port*—Specifies which port performs auto sign-on. For Firefox, if no port number is specified, auto sign is performed on HTTP and HTTPS, accessed by the default port numbers 80 and 443 respectively. • *ip*—Specifies the server by its IP address and netmask. • *ip-address*[*netmask*]—Identifies the sub-network of hosts to auto-authenticate to. • *host*—Specifies the server by its hostname or wildcard mask. Using this option protects the configuration from dynamic changes to IP addresses. • *hostname-mask*—Specifies which hostname or wildcard mask to auto-authenticate to.
(Optional) [**no**] **smart-tunnel auto-sign-on** *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}	Removes an entry from the list of servers, specifying both the list and IP address or hostname as it appears in the ASA configuration.

Command	Purpose
`show running-config webvpn smart-tunnel`	Displays the smart tunnel auto sign-on list entries.
`config-webvpn`	Switches to config-webvpn configuration mode.
`smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0`	Adds all hosts in the subnet and adds the Windows domain to the username if authentication requires it.
(Optional) `no smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0`	Removes that entry from the list and the list named HR if the entry removed is the only entry in the list.
`no smart-tunnel auto-sign-on HR`	Removes the entire list from the ASA configuration.
`smart-tunnel auto-sign-on intranet host *.example.com`	Adds all hosts in the domain to the smart tunnel auto sign-on list named intranet.
`no smart-tunnel auto-sign-on intranet host *.example.com`	Removes that entry from the list.

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 described in the next section.

The next step is to add servers to the server list.

Adding 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.

Prerequisites

You must use the **smart-tunnel auto-sign-on** *list* command to create a list of servers first. You can assign only one list to a group policy or username.

Restrictions

- The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using Internet Explorer and Firefox.
- Firefox requires the administrator to specify hosts using an exact hostname or IP address (instead of a host mask with wildcards, a subnet using IP addresses, or a netmask). For example, within Firefox, you cannot enter *.cisco.com and expect auto sign-on to host email.cisco.com.

DETAILED STEPS

To enable smart tunnel auto sign-on in clientless (browser-based) SSL VPN sessions, use the following commands:

	Command	Purpose
Step 1	**webvpn**	Switches to Clientless SSL VPN configuration mode.
Step 2	**group-policy webvpn** or **username webvpn**	Switches to group-policy Clientless SSL VPN configuration mode. Switches to username Clientless SSL VPN configuration mode.
Step 3	**smart-tunnel auto-sign-on enable**	Enables smart tunnel auto sign-on Clientless SSL VPN sessions.
Step 4	(Optional) [**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]	Switches off smart tunnel auto sign-on Clientless SSL VPN session, removes it from the group policy or username, and uses the default. • *list*—The name of a smart tunnel auto sign-on list already present in the ASA Clientless SSL VPN configuration. • (Optional) *domain*—The name of the domain to be added to the username during authentication. If you enter a domain, enter the **use-domain** keyword in the list entries.
Step 5	**show running-config webvpn smart-tunnel**	Views the smart tunnel auto sign-on list entries in the SSL VPN configuration.
Step 6	**smart-tunnel auto-sign-on enable HR**	Enables the smart tunnel auto sign-on list named HR.
Step 7	**smart-tunnel auto-sign-on enable HR domain CISCO**	Enables the smart tunnel auto sign-on list named HR and adds the domain named CISCO to the username during authentication.
Step 8	**(Optional)** **no smart-tunnel auto-sign-on enable HR**	Removes the smart tunnel auto sign-on list named HR from the group policy and inherits the smart tunnel auto sign-on list command from the default group policy.

•

Automating Smart Tunnel Access

To start smart tunnel access automatically upon user login, enter the following commands:

Requirements

For Mac OS X, you must click the link for the application in the portal's Application Access panel, with or without auto-start configured.

DETAILED STEPS

	Command	Purpose
Step 1	**webvpn**	Switches to Clientless SSL VPN configuration mode.
Step 2	**group-policy webvpn** or **username webvpn**	Switches to group-policy Clientless SSL VPN configuration mode. Switches to username Clientless SSL VPN configuration mode.

Step 3	**smart-tunnel auto-start** *list*
	Example:
	`ciscoasa(config-group-policy)# webvpn`
	`ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1`
		Starts smart tunnel access automatically upon user login. *list* is the name of the smart tunnel list already present.
		Assigns the smart tunnel list named apps1 to the group policy.

Step 4	**show running-config webvpn smart-tunnel**	Displays the smart tunnel list entries in the SSL VPN configuration.
Step 5	(Optional) **no smart-tunnel**	Removes the **smart-tunnel** command from the group policy or username and reverts to the default.

Enabling and Switching Off Smart Tunnel Access

By default, smart tunnels are switched off.

DETAILED STEPS

	Command	Purpose
Step 1	**webvpn**	Switches to Clientless SSL VPN configuration mode.
Step 2	**group-policy webvpn** or **username webvpn**	Switches to group-policy Clientless SSL VPN configuration mode. Switches to username Clientless SSL VPN configuration mode.

Step 3	**smart-tunnel [enable** *list* **| disable]**
	Example:
	`ciscoasa(config-group-policy)# webvpn`
	`ciscoasa(config-group-webvpn)# smart-tunnel enable apps1`
		Enables smart tunnel access. *list* is the name of the smart tunnel list already present. You do not have to start smart tunnel access manually if you entered **smart-tunnel auto-start list** from the previous table.
		Assigns the smart tunnel list named apps1 to the group policy.

	Command	Purpose
Step 4	`show running-config webvpn smart-tunnel`	Dislpays the smart tunnel list entries in the SSL VPN configuration.
Step 5	(Optional) `no smart-tunnel`	Removes the **smart-tunnel** command from the group policy or local user policy and reverts to the default group policy.
Step 6	(Optional) `smart-tunnel disable`	Switches off smart tunnel access.

Configuring 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.

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.

DETAILED STEPS

	Command	Purpose
Step 1	`[no] smart-tunnel notification-icon`	Allows administrators to turn on the notification icon on a global basis. This command configures log out properties and controls whether the user is presented with a logout icon for logging out, as opposed to having logout triggered by closing browser windows. This command also controls logging off when a parent process terminates, which is automatically turned on or off when the notification icon is turned on or off. **notification-icon** is the keyword that specifies when to use the icon for logout. **Note** The no version of this command is the default, in which case, closing all browser windows logs off the SSL VPN session. **Note** Portal logout still takes effect and is not impacted.
Step 2	`*.webvpn.`	When using a proxy and adding to the proxy list exception, ensures that smart tunnel is properly closed when you log off, regardless of icon usage or not.

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.

Configuring 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:

- Configuring a Certificate for Signing Rewritten Java Content
- Switching Off Content Rewrite

- Using Proxy Bypass

Subject to the requirements of your organization and the Web content involved, you may use one of these features.

Configuring a Certificate for Signing Rewritten Java Content

Java objects that have been transformed by Clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint.

DETAILED STEPS

	Command	Purpose
Step 1	**crypto ca import**	Imports a certificate.
Step 2	**ava-trustpoint** **Example:t** ciscoasa(config)# **crypto ca import mytrustpoint pkcs12 mypassphrase** Enter the base 64 encoded PKCS12. End with the word "quit" on a line by itself. [PKCS12 data omitted] **quit** INFO: Import PKCS12 operation completed successfully. ciscoasa(config)# **webvpn** ciscoasa(config)# **java-trustpoint mytrustpoint**	Employs a certificate. Shows the creation of a trustpoint named mytrustpoint and its assignment to signing Java objects.

Switching Off Content Rewrite

You may not want some applications and Web resources, for example, public websites, to go through the ASA. The ASA therefore lets you create rewrite rules that let users browse certain sites and applications without going through the ASA. This is similar to split-tunneling in an IPsec VPN connection.

	Command	Purpose
Step 1	**webvpn**	Switches to Clientless SSL VPN configuration mode.
Step 2	**rewrite**	Specifies applications and resources to access outside a clientless SSLN VPN tunnel. You can use this command multiple times.
Step 3	**disable**	Used in combination with the **rewrite** command. The rule order number is important because the security appliance searches rewrite rules by order number, starting with the lowest, and applies the first rule that matches.

Using 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 use the **proxy-bypass** command multiple times. The order in which you configure entries 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*.

DETAILED STEPS

	Command	Purpose
Step 1	`webvpn`	Switches to Clientless SSL VPN configuration mode.
Step 2	`proxy-bypass`	Configures proxy bypass.

Configuring 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.

Prerequisites

Log on to the ASA and enter global configuration mode. In global configuration mode, the ASA displays this prompt:

```
hostname(config)#
```

DETAILED STEPS

	Command	Purpose
Step 1	**webvpn** **Example:** `ciscoasa(config)# webvpn`	Enter Clientless SSL VPN configuration mode.

Step 2	**portal-access-rule** *priority* [{**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}
	
	Example:
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*`
	
	`hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match "*my agent*"`
		Permit or deny the creation of a Clientless SSL VPN session based on an HTTP header code or a string in the HTTP header.
		
		The second example shows the proper syntax for specifying a string with a space. Surround the string with wildcards (*) and then quotes (" ").

Optimizing 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. These sections explain these features:

- Configuring Caching
- Configuring Content Transformation

Configuring Caching

Caching enhances Clientless 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 Clientless SSL VPN and the remote servers, with the result that many applications run much more efficiently.

By default, caching is enabled. You can customize the way caching works for your environment by using the caching commands in cache mode.