

Policy Groups

- Create and Apply Clientless SSL VPN Policies for Accessing Resources, on page 1
- Connection Profile Attributes for Clientless SSL VPN, on page 1
- Group Policy and User Attributes for Clientless SSL VPN, on page 2
- Smart Tunnel Access, on page 18
- Clientless SSL VPN Capture Tool, on page 30
- Configure Portal Access Rules, on page 30
- Optimize Clientless SSL VPN Performance, on page 31

Create and Apply Clientless SSL VPN Policies for Accessing Resources

Creating and applying policies for Clientless SSL VPN that govern access to resources at an internal server requires you to assign 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, “Connection Profiles, Group Policies, and Users” for a thorough explanation of ways to simplify configuration with group policies.

Connection Profile Attributes for Clientless SSL VPN

The following table 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, “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 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.

Group Policy and User Attributes for Clientless SSL VPN

The following table provides a list of group policy and user attributes for Clientless SSL VPN that. For step-by-step instructions on configuring group policy and user attributes, see Configure Group Policy Attributes for Clientless SSL VPN Sessions, on page 4 or Configure Clientless SSL VPN Access for Specific Users, on page 11.

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 in 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.
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.
url-entry	Controls the ability of the user to enter any HTTP/HTTPS URL.

Command	Function
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.

Configure Group Policy Attributes for Clientless SSL VPN Sessions

Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. There is no need for either a software or hardware client. Clientless SSL VPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. Clientless SSL VPN uses SSL and its successor, TLS1, to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The ASA recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. By default, clientless SSL VPN is disabled.

You can customize a configuration of clientless SSL VPN for specific internal group policies.



Note The webvpn mode that you enter from global configuration mode lets you configure global settings for clientless SSL VPN sessions. The webvpn mode described in this section, which you enter from group-policy configuration mode, lets you customize a configuration of group policies specifically for clientless SSL VPN sessions.

In group-policy webvpn configuration mode, you can specify whether to inherit or customize the following parameters, each of which is described in the subsequent sections:

- customizations
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon
- deny message
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

In many instances, you define the webvpn attributes as part of configuring clientless SSL VPN, then you apply those definitions to specific groups when you configure the group-policy webvpn attributes. Enter

group-policy webvpn configuration mode by using the **webvpn** command in group-policy configuration mode. Webvpn commands for group policies define access to files, URLs and TCP applications over clientless SSL VPN sessions. They also identify ACLs and types of traffic to filter. Clientless SSL VPN is disabled by default.

To remove all commands entered in group-policy webvpn configuration mode, enter the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

webvpn

no webvpn

The following example shows how to enter group-policy webvpn configuration mode for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

Specify a Deny Message

You can specify the message delivered to a remote user who logs into a clientless SSL VPN session successfully, but has no VPN privileges, by entering the **deny-message** command in group-policy webvpn configuration mode:

```
hostname(config-group-webvpn)# deny-message value "message"
hostname(config-group-webvpn)# no deny-message value "message"
hostname(config-group-webvpn)# deny-message none
```

The **no deny-message value** command removes the message string, so that the remote user does not receive a message.

The **no deny-message none** command removes the attribute from the connection profile policy configuration. The policy inherits the attribute value.

The message can be up to 491 alphanumeric characters long, including special characters, spaces, and punctuation, but not counting the enclosing quotation marks. The text appears on the remote user's browser upon login. When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

The first command in the following example creates an internal group policy named group2. The subsequent commands modify the attributes, including the webvpn deny message associated with that policy.

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

Configure Group Policy Filter Attributes for Clientless SSL VPN Sessions

Specify whether to filter Java, ActiveX, images, scripts, and cookies from clientless SSL VPN sessions for this group policy by using the **html-content-filter** command in webvpn mode. HTML filtering is disabled by default.

To remove a content filter, enter the **no** form of this command. To remove all content filters, including a null value created by issuing the **html-content-filter** command with the **none** keyword, enter the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an html content filter, enter the **html-content-filter** command with the **none** keyword.

Using the command a second time overrides the previous setting.

```
hostname(config-group-webvpn)# html-content-filter {java | images | scripts |
cookies | none}

hostname(config-group-webvpn)# no html-content-filter [java | images | scripts |
 cookies | none]
```

The table below describes the meaning of the keywords used in this command.

Table 2: filter Command Keywords

Keyword	Meaning
cookies	Removes cookies from images, providing limited ad filtering and privacy.
images	Removes references to images (removes <IMG> tags).
java	Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags).
none	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
scripts	Removes references to scripting (removes <SCRIPT> tags).

The following example shows how to set filtering of JAVA and ActiveX, cookies, and images for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
hostname(config-group-webvpn)#
```

Specify the User Home Page

Specify a URL for the web page that displays when a user in this group logs in by using the **homepage** command in group-policy webvpn configuration mode. There is no default home page.

To remove a configured home page, including a null value created by issuing the **homepage none** command, enter the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, enter the **homepage none** command.

The **none** keyword indicates that there is no home page for clientless SSL VPN sessions. It sets a null value, thereby disallowing a home page and prevents inheriting an home page.

The *url-string* variable following the keyword **value** provides a URL for the home page. The string must begin with either http:// or https://.

```
hostname(config-group-webvpn)# homepage {value url-string | none}
hostname(config-group-webvpn)# no homepage
hostname(config-group-webvpn)#
```

Configure Auto-Signon

The **auto-signon** command is a single sign-on method for users of clientless SSL VPN sessions. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. The typical precedence behavior applies where username supersedes group, and group supersedes global. The mode you choose depends upon the desired scope of authentication.

To disable auto-signon for a particular user to a particular server, use the **no** form of the command with the original specification of IP block or URI. To disable authentication to all servers, use the **no** form without arguments. The **no** option allows inheritance of a value from the group policy.

The following example, entered in group-policy webvpn configuration mode, configures auto-signon for the user named anyuser, using basic authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

The following example commands configure auto-signon for users of clientless SSL VPN sessions, using either basic or NTLM authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/*
auth-type all
hostname(config-group-webvpn)#
```

The following example commands configure auto-signon for users of clientless SSL VPN sessions, using either basic or NTLM authentication, to the server with the IP address 10.1.1.0, using subnet mask 255.255.255.0:

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-group-webvpn)#
```

Specify the ACL for Clientless SSL VPN Sessions

Specify the name of the ACL to use for clientless SSL VPN sessions for this group policy or username by using the **filter** command in webvpn mode. Clientless SSL VPN ACLs do not apply until you enter the **filter** command to specify them.

To remove the ACL, including a null value created by issuing the **filter none** command, enter the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting filter values, enter the **filter value none** command.

ACLs for clientless SSL VPN sessions do not apply until you enter the **filter** command to specify them.

You configure ACLs to permit or deny various types of traffic for this group policy. You then enter the **filter** command to apply those ACLs for clientless SSL VPN traffic.

```
hostname(config-group-webvpn)# filter {value ACLname | none}
hostname(config-group-webvpn)# no filter
```

The **none** keyword indicates that there is no **webvpntype** ACL. It sets a null value, thereby disallowing an ACL and prevents inheriting an ACL from another group policy.

The *ACLname* string following the keyword **value** provides the name of the previously configured ACL.

Note Clientless SSL VPN sessions do not use ACLs defined in the **vpn-filter** command.

The following example shows how to set a filter that invokes an ACL named acl_in for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
hostname(config-group-webvpn)#
```

Apply a URL List

You can specify a list of URLs to appear on the clientless SSL VPN home page for a group policy. First, you must create one or more named lists by entering the **url-list** command in global configuration mode. To apply a list of servers and URLs for clientless SSL VPN sessions to a particular group policy, allowing access to the URLs in a list for a specific group policy, use the name of the list or lists you create there with the **url-list** command in group-policy webvpn configuration mode. There is no default URL list.

To remove a list, including a null value created by using the **url-list none** command**,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a URL list, use the **url-list none** command. Using the command a second time overrides the previous setting:

```
hostname(config-group-webvpn)# url-list {value name | none} [index]
hostname(config-group-webvpn)# no url-list
```

The table below shows the **url-list** command parameters and their meanings.

Table 3: url-list Command Keywords and Variables

Parameter	Meaning
index	Indicates the display priority on the home page.

Parameter	Meaning
none	Sets a null value for url lists. Prevents inheriting a list from a default or specified group policy.
value name	Specifies the name of a previously configured list of urls. To configure such a list, use the **url-list** command in global configuration mode.

The following example sets a URL list called FirstGroupURLs for the group policy named FirstGroup and specifies that this should be the first URL list displayed on the homepage:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
hostname(config-group-webvpn)#
```

Enable ActiveX Relay for a Group Policy

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 Microsoft Office documents. The ActiveX relay remains in force until the Clientless SSL VPN session closes.

To enable or disable ActiveX controls on Clientless SSL VPN sessions, enter the following command in group-policy webvpn configuration mode:

activex-relay {**enable | disable**}

To inherit the **activex-relay** command from the default group policy, enter the following command:

no activex-relay

The following commands enable ActiveX controls on clientless SSL VPN sessions associated with a given group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

Enable Application Access on Clientless SSL VPN Sessions for a Group Policy

To enable application access for this group policy, enter the **port-forward** command in group-policy webvpn configuration mode. Port forwarding is disabled by default.

Before you can enter the **port-forward** command in group-policy webvpn configuration mode to enable application access, you must define a list of applications that you want users to be able to use in a clientless SSL VPN session. Enter the **port-forward** command in global configuration mode to define this list.

To remove the port forwarding attribute from the group-policy configuration, including a null value created by issuing the **port-forward none** command, enter the **no** form of this command. The **no** option allows inheritance of a list from another group policy. To prevent inheriting a port forwarding list, enter the **port-forward** command with the **none** keyword. The **none** keyword indicates that there is no filtering. It sets a null value, thereby disallowing a filtering, and prevents inheriting filtering values.

The syntax of the command is as follows:

```
hostname(config-group-webvpn)# port-forward {value listname | none}
hostname(config-group-webvpn)# no port-forward
```

The *listname* string following the keyword **value** identifies the list of applications users of clientless SSL VPN sessions can access. Enter the port-forward command in webvpn configuration mode to define the list.

Using the command a second time overrides the previous setting.

The following example shows how to set a port-forwarding list called ports1 for the internal group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
hostname(config-group-webvpn)#
```

Configure the Port-Forwarding Display Name

Configure the display name that identifies TCP port forwarding to end users for a particular user or group policy by using the **port-forward-name** command in group-policy webvpn configuration mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** enter the **no** form of the command. The **no** option restores the default name, Application Access. To prevent a display name, enter the **port-forward none** command. The syntax of the command is as follows:

```
hostname(config-group-webvpn)# port-forward-name {value name | none}
hostname(config-group-webvpn)# no port-forward-name
```

The following example shows how to set the name, Remote Access TCP Applications, for the internal group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup internal attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP
Applications
hostname(config-group-webvpn)#
```

Configure the Maximum Object Size to Ignore for Updating the Session Timer

Network devices exchange short keepalive messages to ensure that the virtual circuit between them is still active. The length of these messages can vary. The **keep-alive-ignore** command lets you tell the ASA to consider all messages that are less than or equal to the specified size as keepalive messages and not as traffic when updating the session timer. The range is 0 through 900 KB. The default is 4 KB.

To specify the upper limit of the HTTP/HTTPS traffic, per transaction, to ignore, use the **keep-alive-ignore** command in group-policy attributes webvpn configuration mode:

```
hostname(config-group-webvpn)# keep-alive-ignore size
hostname(config-group-webvpn)#
```

The **no** form of the command removes this specification from the configuration:

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

The following example sets the maximum size of objects to ignore as 5 KB:

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

Specify HTTP Compression

Enable compression of http data over a clientless SSL VPN session for a specific group or user by entering the http-comp command in the group policy webvpn mode.

```
hostname(config-group-webvpn)# http-comp {gzip | none}
hostname(config-group-webvpn)#
```

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command:

```
hostname(config-group-webvpn)# no http-comp {gzip | none}
hostname(config-group-webvpn)#
```

The syntax of this command is as follows:

- **gzip—**Specifies compression is enabled for the group or user. This is the default value.
- **none—**Specifies compression is disabled for the group or user.

For clientless SSL VPN sessions, the **compression** command configured from global configuration mode overrides the **http-comp** command configured in group policy and username webvpn modes.

In the following example, compression is disabled for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
hostname(config-group-webvpn)#
```

Configure Clientless SSL VPN Access for Specific Users

The following sections describe how to customize a configuration for specific users of clientless SSL VPN sessions. Enter username webvpn configuration mode by using the **webvpn** command in username configuration mode. Clientless SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. There is no need for either a software or hardware client. Clientless SSL VPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. Clientless SSL VPN uses SSL and its successor, TLS1, to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The ASA recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The username webvpn configuration mode commands define access to files, URLs and TCP applications over clientless SSL VPN sessions. They also identify ACLs and types of traffic to filter. Clientless SSL VPN is disabled by default. These **webvpn** commands apply only to the username from which you configure them. Notice that the prompt changes, indicating that you are now in username webvpn configuration mode.

```
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

To remove all commands entered in username webvpn configuration mode, use the **no** form of this command:

```
hostname(config-username)# no webvpn
hostname(config-username)#
```

You do not need to configure clientless SSL VPN to use e-mail proxies.



Note The webvpn mode that you enter from global configuration mode lets you configure global settings for clientless SSL VPN sessions. The username webvpn configuration mode described in this section, which you enter from username mode, lets you customize the configuration of specific users specifically for clientless SSL VPN sessions.

In username webvpn configuration mode, you can customize the following parameters, each of which is described in the subsequent steps:

- customizations
- deny message
- html-content-filter
- homepage
- filter
- url-list
- port-forward
- port-forward-name
- auto-signon
- AnyConnect Secure Mobility Client
- keep-alive ignore
- HTTP compression

The following example shows how to enter username webvpn configuration mode for the username anyuser attributes:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)#
```

Specify the Content/Objects to Filter from the HTML

To filter Java, ActiveX, images, scripts, and cookies for clientless SSL VPN sessions for this user, enter the **html-content-filter** command in username webvpn configuration mode. To remove a content filter, enter the **no** form of this command. To remove all content filters, including a null value created by issuing the **html-content-filter none** command, enter the **no** form of this command without arguments. The **no** option allows inheritance of a value from the group policy. To prevent inheriting an HTML content filter, enter the **html-content-filter none** command. HTML filtering is disabled by default.

Using the command a second time overrides the previous setting.

```
hostname(config-username-webvpn)# html-content-filter {java | images | scripts |
 cookies | none}

hostname(config-username-webvpn)# no html-content-filter [java | images | scripts
 | cookies | none]
```

The keywords used in this command are as follows:

- **cookies—**Removes cookies from images, providing limited ad filtering and privacy.
- **images—**Removes references to images (removes <IMG> tags).
- **java—**Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags).
- **none—**Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
- **scripts**—Removes references to scripting (removes <SCRIPT> tags).

The following example shows how to set filtering of JAVA and ActiveX, cookies, and images for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# html-content-filter java cookies images
hostname(config-username-webvpn)#
```

Specify the User Home Page

To specify a URL for the web page that displays when this user logs into clientless SSL VPN session, enter the **homepage** command in username webvpn configuration mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, enter the **no** form of this command. The **no** option allows inheritance of a value from the group policy. To prevent inheriting a home page, enter the **homepage none** command.

The **none** keyword indicates that there is no clientless SSL VPN home page. It sets a null value, thereby disallowing a home page and prevents inheriting a home page.

The *url-string* variable following the keyword **value** provides a URL for the home page. The string must begin with either http:// or https://.

There is no default home page.

```
hostname(config-username-webvpn)# homepage {value url-string | none}
```

```
hostname(config-username-webvpn)# no homepage
hostname(config-username-webvpn)#
```

The following example shows how to specify www.example.com as the home page for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# homepage value www.example.com
hostname(config-username-webvpn)#
```

Specify a Deny Message

You can specify the message delivered to a remote user who logs into clientless SSL VPN session successfully, but has no VPN privileges by entering the **deny-message** command in username webvpn configuration mode:

```
hostname(config-username-webvpn)# deny-message value "message"
hostname(config-username-webvpn)# no deny-message value "message"
hostname(config-username-webvpn)# deny-message none
```

The **no deny-message value** command removes the message string, so that the remote user does not receive a message.

The **no deny-message none** command removes the attribute from the connection profile policy configuration. The policy inherits the attribute value.

The message can be up to 491 alphanumeric characters long, including special characters, spaces, and punctuation, but not counting the enclosing quotation marks. The text appears on the remote user's browser upon login. When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

The first command in the following example enters username mode and configures the attributes for the user named anyuser. The subsequent commands enter username webvpn configuration mode and modify the deny message associated with that user.

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-username-webvpn)
```

Apply a URL List

You can specify a list of URLs to appear on the home page for a user who has established a clientless SSL VPN session. First, you must create one or more named lists by entering the **url-list** command in global configuration mode. To apply a list of servers and URLs to a particular user of clientless SSL VPN, enter the **url-list** command in username webvpn configuration mode.

To remove a list, including a null value created by using the **url-list none** command**,** enter the **no** form of this command. The **no** option allows inheritance of a value from the group policy. To prevent inheriting a url list, enter the **url-list none** command.

```
hostname(config-username-webvpn)# url-list {listname displayname url | none}
hostname(config-username-webvpn)# no url-list
```

The keywords and variables used in this command are as follows:

- *displayname*—Specifies a name for the URL. This name appears on the portal page in the clientless SSL VPN session.
- listname—Identifies a name by which to group URLs.
- **none**—Indicates that there is no list of URLs. Sets a null value, thereby disallowing a URL list. Prevents inheriting URL list values.
- *url*—Specifies a URL that users of clientless SSL VPN can access.

There is no default URL list.

Using the command a second time overrides the previous setting.

The following example shows how to set a URL list called AnyuserURLs for the user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# url-list value AnyuserURLs
hostname(config-username-webvpn)#
```

Enable ActiveX Relay for a User

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 Microsoft Office documents. The ActiveX relay remains in force until the Clientless SSL VPN session closes.

To enable or disable ActiveX controls on Clientless SSL VPN sessions, enter the following command in username webvpn configuration mode:

activex-relay {**enable | disable**}

To inherit the **activex-relay** command from the group policy, enter the following command:

no activex-relay

The following commands enable ActiveX controls on Clientless SSL VPN sessions associated with a given username:

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay enable
hostname(config-username-webvpn)
```

Enable Application Access for Clientless SSL VPN Sessions

To enable application access for this user, enter the **port-forward** command in username webvpn configuration mode. Port forwarding is disabled by default.

To remove the port forwarding attribute from the configuration, including a null value created by issuing the **port-forward none** command, enter the **no** form of this command. The **no** option allows inheritance of a list from the group policy. To disallow filtering and prevent inheriting a port forwarding list, enter the **port-forward** command with the **none** keyword.

```
hostname(config-username-webvpn)# port-forward {value listname | none}
hostname(config-username-webvpn)# no port-forward
hostname(config-username-webvpn)#
```

The *listname* string following the keyword **value** identifies the list of applications users of clientless SSL VPN can access. Enter the **port-forward** command in configuration mode to define the list.

Using the command a second time overrides the previous setting.

Before you can enter the **port-forward** command in username webvpn configuration mode to enable application access, you must define a list of applications that you want users to be able to use in a clientless SSL VPN session. Enter the **port-forward** command in global configuration mode to define this list.

The following example shows how to configure a portforwarding list called ports1:

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward value ports1
hostname(config-username-webvpn)#
```

Configure the Port-Forwarding Display Name

Configure the display name that identifies TCP port forwarding to end users for a particular user by using the **port-forward-name** command in username webvpn configuration mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** enter the **no** form of the command. The **no** option restores the default name, Application Access. To prevent a display name, enter the **port-forward none** command.

```
hostname(config-username-webvpn)# port-forward-name {value name | none}
hostname(config-username-webvpn)# no port-forward-name
```

The following example shows how to configure the port-forward name test:

```
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# port-forward-name value test
hostname(config-username-webvpn)#
```

Configure the Maximum Object Size to Ignore for Updating the Session Timer

Network devices exchange short keepalive messages to ensure that the virtual circuit between them is still active. The length of these messages can vary. The **keep-alive-ignore** command lets you tell the ASA to consider all messages that are less than or equal to the specified size as keepalive messages and not as traffic when updating the session timer. The range is 0 through 900 KB. The default is 4 KB.

To specify the upper limit of the HTTP/HTTPS traffic, per transaction, to ignore, use the **keep-alive-ignore** command in group-policy attributes webvpn configuration mode:

```
hostname(config-group-webvpn)# keep-alive-ignore size
```

```
hostname(config-group-webvpn)#
```

The **no** form of the command removes this specification from the configuration:

```
hostname(config-group-webvpn)# no keep-alive-ignore
hostname(config-group-webvpn)#
```

The following example sets the maximum size of objects to ignore as 5 KB:

```
hostname(config-group-webvpn)# keep-alive-ignore 5
hostname(config-group-webvpn)#
```

Configure Auto-Signon

To automatically submit the login credentials of a particular user of clientless SSL VPN to internal servers using NTLM, basic HTTP authentication, or both, use the **auto-signon** command in username webvpn configuration mode.

The **auto-signon** command is a single sign-on method for users of clientless SSL VPN sessions. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. The typical precedence behavior applies where username supersedes group, and group supersedes global. The mode you choose depends upon the desired scope of authentication.

To disable auto-signon for a particular user to a particular server, use the **no** form of the command with the original specification of IP block or URI. To disable authentication to all servers, use the **no** form without arguments. The **no** option allows inheritance of a value from the group policy.

The following example commands configure auto-signon for a user of clientless SSL VPN named anyuser, using either basic or NTLM authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow uri https://*.example.com/*
 auth-type all
```

The following example commands configure auto-signon for a user of clientless SSL VPN named anyuser, using either basic or NTLM authentication, to the server with the IP address 10.1.1.0, using subnet mask 255.255.255.0:

```
hostname(config)# username anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type all
hostname(config-username-webvpn)#
```

Specify HTTP Compression

Enable compression of http data over a clientless SSL VPN session for a specific user by entering the http-comp command in the username webvpn configuration mode.

```
hostname(config-username-webvpn)# http-comp {gzip | none}
hostname(config-username-webvpn)#
```

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command:

```
hostname(config-username-webvpn)# no http-comp {gzip | none}
hostname(config-username-webvpn)#
```

The syntax of this command is as follows:

- **gzip—**Specifies compression is enabled for the group or user. This is the default value.
- **none—**Specifies compression is disabled for the group or user.

For clientless SSL VPN session, the **compression** command configured from global configuration mode overrides the **http-comp** command configured in group policy and username webvpn modes.

In the following example, compression is disabled for the username testuser:

```
hostname(config)# username testuser internal
hostname(config)# username testuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# http-comp none
hostname(config-username-webvpn)#
```

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:

- About Smart Tunnels, on page 19
- Prerequisites for Smart Tunnels, on page 19
- Guidelines for Smart Tunnels, on page 20
- Add Applications to Be Eligible for Smart Tunnel Access, on page 21
- About Smart Tunnel Lists, on page 21
- Configure and Apply Smart Tunnel Policy, on page 22
- Configure and Apply a Smart Tunnel Tunnel-Policy, on page 23
- Create a Smart Tunnel Auto Sign-On Server List, on page 24
- Add Servers to a Smart Tunnel Auto Sign-On Server List, on page 26

- Automate Smart Tunnel Access, on page 27
- Enable and Switch Off Smart Tunnel Access, on page 28
- Configure Smart Tunnel Log Off, on page 29

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.

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.
- 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.

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.

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.

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.

- **smart-tunnel auto-start** *list*

  Start smart tunnel access automatically upon user login.

- **smart-tunnel enable** *list*

  Enable 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.

- **smart-tunnel disable**

  Prevent smart tunnel access.

- **no smart-tunnel [auto-start list | enable list | disable]**

  Remove 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.

Configure and Apply 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.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Create a list of hosts to use for configuring smart tunnel policies:

[no] smart-tunnel network *network name* **ip** *ip netmask*

- *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 Establish the hostname mask, such as *.cisco.com:

[no] smart-tunnel network *network name* **host** *host mask*

Step 4 Apply smart tunnel policies to a particular group or user policy:

[no] smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* **| tunnelall]**

- *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.

Configure and Apply 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:

Procedure

Step 1 Reference a globally configured list of networks:

[no]smart-tunnel tunnel-policy [{excludespecified | tunnelspecified} *network name* | *tunnelall]*

- *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.

Step 2 Apply a tunnel policy to a group-policy/user policy:

[no] smart-tunnel network *network name* **ip** *ip netmask*

or

[no] smart-tunnel network *network name* **host** *host mask*

One command specifies host and the other specifies network IPs. Use only one.

- *network name* specifies the name of network to apply to tunnel policy
- *ip* specifies the IP address of a network
- *netmask* specifies the netmask of a network
- *host mask* specifies the hostname mask, such as *.cisco.com

Example:

Example:

Create 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-webvpn)# smart-tunnel network inventory ip 10.5.2.2
or
ciscoasa(config-webvpn)# smart-tunnel network inventory host www.example.com
```

Step 3 Apply the tunnel-specified tunnel policy to the partner's group policy:

ciscoasa(config-group-webvpn)# **smart-tunnel tunnel-policy tunnelspecified inventory**

Step 4 (Optional) Specify the group policy home page and enable smart tunnel on it.

Example:

Example:

```
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
ciscoasa(config-webvpn)# smart-tunnel notification-icon
```

Note
Without writing a script or uploading anything, an administrator can specify which homepage to connect with via smart tunnel.

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.

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.

Create a Smart Tunnel Auto Sign-On Server List

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Use for each server to add to the server list:

smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

- *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.

Step 3 (Optional) Remove an entry from the list of servers, specifying both the list and IP address or hostname as it appears in the ASA configuration:

no smart-tunnel auto-sign-on *list* [**use-domain**] [**realm** *realm-string*] [**port** *port-num*] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

Step 4 Display the smart tunnel auto sign-on list entries:

show running-config webvpn smart-tunnel

Step 5 Switch to config-webvpn configuration mode:

config-webvpn

Step 6 Add all hosts in the subnet and adds the Windows domain to the username if authentication requires it:

smart-tunnel auto-sign-on HR use-domain ip 93.184.216.119 255.255.255.0

Step 7 (Optional) Remove 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 use-domain ip 93.184.216.119 255.255.255.0

Step 8 Remove the entire list from the ASA configuration:

no smart-tunnel auto-sign-on HR

Step 9 Add all hosts in the domain to the smart tunnel auto sign-on list named intranet:

smart-tunnel auto-sign-on intranet host *.example.com

Step 10 Remove that entry from the list:

no smart-tunnel auto-sign-on intranet host *.example.com

Note
After configuring 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.For more information, see, Add Servers to a Smart Tunnel Auto Sign-On Server List, on page 26

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.

Before you begin

- 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.



Note The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using Internet Explorer and Firefox.

- If you are using Firefox, make sure that you 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.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Switch to group-policy Clientless SSL VPN configuration mode:

group-policy webvpn

Step 3 Switch to username Clientless SSL VPN configuration mode.

username webvpn

Step 4 Enable smart tunnel auto sign-on Clientless SSL VPN sessions:

smart-tunnel auto-sign-on enable

Step 5 (Optional) Switch off smart tunnel auto sign-on Clientless SSL VPN session, remove it from the group policy or username, and use the default:

[**no**] **smart-tunnel auto-sign-on enable** *list* [**domain** *domain*]

- *list*—The name of a smart tunnel auto sign-on list already present in the ASA Clientless SSL VPN configuration.
- *domain (optional)*—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 6 View the smart tunnel auto sign-on list entries in the SSL VPN configuration:

show running-config webvpn smart-tunnel

Step 7 Enable the smart tunnel auto sign-on list named HR:

smart-tunnel auto-sign-on enable HR

Step 8 Enable the smart tunnel auto sign-on list named HR and adds the domain named CISCO to the username during authentication:

smart-tunnel auto-sign-on enable HR domain CISCO

Step 9 (Optional) Remove 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:

no smart-tunnel auto-sign-on enable HR

Automate Smart Tunnel Access

To start smart tunnel access automatically upon user login, perform the following steps:

Before you begin

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

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Switch to group-policy Clientless SSL VPN configuration mode:

group-policy webvpn

Step 3 Switch to username Clientless SSL VPN configuration mode:

username webvpn

Step 4 Start smart tunnel access automatically upon user login:

smart-tunnel auto-start *list*

list is the name of the smart tunnel list already present.

Example:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
```

This assigns the smart tunnel list named apps1 to the group policy.

Step 5 Display the smart tunnel list entries in the SSL VPN configuration:

show running-config webvpn smart-tunnel

Step 6 Remove the smart-tunnel command from the group policy or username and reverts to the default:

no smart-tunnel

Enable and Switch Off Smart Tunnel Access

By default, smart tunnels are switched off.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Switch to group-policy Clientless SSL VPN configuration mode:

group-policy webvpn

Step 3 Switch to username Clientless SSL VPN configuration mode:

username webvpn

Step 4 Enable smart tunnel access:

smart-tunnel [enable *list* **| disable]**

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.

Example:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
```

This example assigns the smart tunnel list named apps1 to the group policy.

Step 5 Display the smart tunnel list entries in the SSL VPN configuration:

show running-config webvpn smart-tunnel

Step 6 Remove the smart-tunnel command from the group policy or local user policy and reverts to the default group policy:

no smart-tunnel

Step 7 Switch off smart tunnel access:

smart-tunnel disable

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.

Procedure

Step 1 Allow administrators to turn on the notification icon on a global basis:

[no] smart-tunnel notification-icon

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.

The *no* version of this command is the default, in which case, closing all browser windows logs off the SSL VPN session.

Portal logout still takes effect and is not impacted.

Step 2 When using a proxy and adding to the proxy list exception, ensure that smart tunnel is properly closed when you log off, regardless of icon usage or not.

***.webvpn.**

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.

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

You can 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. The ASA evaluates this access policy before authenticating the endpoint. If ASA denies a clientless SSL VPN session according to the access policy, it returns an error code to the endpoint immediately.

Before you begin

Log in to the ASA and enter the global configuration mode.

Procedure

Step 1 Enter the clientless SSL VPN configuration mode using the following command:

webvpn

Step 2 Permit or deny a clientless SSL VPN session based on an HTTP header code or a string in the HTTP header using the following command:

portal-access-rule *priority* {**permit** | **deny** [**code** *code*]} {**any** | **user-agent match** *string*}

Table 4: portal-access-rule Command Keywords and Variables

Parameter	Description
priority	Specifies the priority of the rule.
permit	Permits a clientless SSL VPN connection based on this setting.
deny	Denies a clientless SSL VPN connection based on this setting.
code *code*	Specifies the HTTP message code. The range is from 200 to 599.
user-agent match *string*	Specifies a string that identifies the application, operating system, vendor, and or version of the requesting user agent.

- To specify a string, start and end the string with wildcards (*). Without wildcards, the rule may not match any strings or it may match many fewer strings than you expect. For example, *Thunderbird*.
- To specify a string with a space, start and end the string with wildcards (*) and then add quotes (“ ”) to the beginning and end. In the second example, `my agent` is the 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*"
```

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 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.

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.

Configure 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.

Procedure

Step 1 Import a certificate:

crypto ca import

Step 2 Employ a certificate:

ava-trustpoint

Example:

```
hostname(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.
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
```

This example shows the creation of a trustpoint named mytrustpoint and its assignment to signing Java objects.

Switch 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.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Specify applications and resources to access outside a clientless SSLN VPN tunnel:

rewrite

You can use this command multiple times.

Step 3 Use in combination with the rewrite command:

disable

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.

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 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*.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Configure proxy bypass:

proxy-bypass