Basic Clientless SSL VPN Configuration

Rewrite Each URL

By default, the ASA allows all portal traffic to all Web resources (for example HTTPS, CIFS, RDP, and plug-ins). Clientless SSL VPN rewrites each URL to one that is meaningful only to the ASA. The user cannot use this URL to confirm that they are connected to the website they requested. To avoid placing users at risk from phishing websites, assign a Web ACL to the policies configured for clientless access—group policies, dynamic access policies, or both—to control traffic flows from the portal. We recommend switching off URL Entry on these policies to prevent user confusion over what is accessible.

Figure 1: Example URL Entered by User

Figure 2: Same URL Rewritten by Security Appliance and Displayed in Browser Window

Switch Off URL Entry on the Portal Page

The portal page opens when the user establishes a browser-based connection.

Before you begin

Configure a group policy for all users who require Clientless SSL VPN access, and enable Clientless SSL VPN only for that group policy.

Procedure

Step 1 Switch to group policy clientless ssl vpn configuration mode.

webvpn

Step 2 Control the ability of the user to enter any HTTP/HTTPS URL.

url-entry

Step 3 (Optional) Switch off URL Entry.

url-entry disable

Trusted Certificate Pools

The ASA groups trusted certificates into trustpools. Trustpools can be thought of as a special case of Trustpoint representing multiple known CA certificates. The ASA includes a default bundle of certificates, similar to the bundle of certificates provided with web browsers. Those certificates are inactive until activated by the administrator by issuing the crypto ca import default command.

When connecting to a remote server with a web browser using the HTTPS protocol, the server provides a digital certificate signed by a certificate authority (CA) to identify itself. Web browsers include a collection of CA certificates which are used to verify the validity of the server certificate.

When connecting to a remote SSL-enabled server through Clientless SSL VPN, it is important to know that you can trust the remote server, and that you are connecting to the correct remote server. ASA 9.0 introduced support for SSL server certificate verification against a list of trusted certificate authority (CA) certificates for Clientless SSL VPN.

On **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool**, you can enable certificate verification for SSL connections to https sites. You can also manage the certificates in the trusted certificate pool.

Note ASA trustpools are similar to but not identical to Cisco IOS trustpools.

Configure Auto Import of Trustpool Certificates

Smart licensing uses the Smart Call Home infrastructure. When the ASA configures Smart Call Home anonymous reporting in the background, the ASA automatically creates a trustpoint containing the certificate of the CA that issued the Call Home server certificate. The ASA now supports validation of the certificate if the issuing hierarchy of the server certificate changes, without the need for customer involvement to adjust certificate hierarchy changes. You can automate the update of the trustpool bundle at periodic intervals so that Smart Call Home can remain active if the self-signed certificate of the CA server changes. This feature is not supported under multi-context deployments.

Automatic import of trustpool certificate bundles requires you to specify the URL that ASA uses to download and import the bundle. Use the following command so the import happens daily at a regular interval with the default Cisco URL and default time of 22 hours:

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

You can also enable auto import with a custom URL with the following command:

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

To give you more flexibility to set downloads during off peak hours or other convenient times, enter the following command which enables the import with a custom time:

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

Setting the automatic import with both a custom URL and custom time requires the following command:

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Show the State of the Trustpool Policy

Use the following command to see the current state of the trustpool policy:

```
show crypto ca trustpool policy
```

This command returns information like the following:

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

Clear CA Trustpool

To reset the trustpool policy to its default state, use the following command:

```
clear configure crypto ca trustpool
```

Since the automatic import of trustpoint certificates is turned off by default, using this command disables the feature.

Edit the Policy of the Trusted Certificate Pool

Procedure

Step 1 Revocation Check—Configure whether to check the certificates in the pool for revocation, and then choose whether to use CLR or OCSP and whether to make the certificate invalid if checking for revocation fails.

Step 2 Certificate Matching Rules—Select certificate maps to exempt from revocation or expiration checks. A certificate map links certificates to AnyConnect or clientless SSL connection profiles (also known as tunnel groups).

Step 3 CRL Options—Decide how often to refresh the CRL cache, between 1 and 1440 minutes (1140 minutes is 24 hours).

Step 4 Automatic Import—Cisco periodically updates the "default" list of trusted CAs. If you check Enable Automatic Import, and keep the default settings, the ASA checks for an updated list of trusted CAs on the Cisco site every 24 hours. If the list has changed, the ASA downloads and imports the new default trusted CA list.

Configure Browser Access to Plug-ins

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

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

- (Cisco-distributed plug-ins only) Unpacks the jar file specified in the URL.
- Writes the file to the ASA file system.
- Populates the drop-down list next to the URL attributes in ASDM.
- Enables the plug-in for all future Clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down list next to the Address field of the portal page.

The following shows the changes to the main menu and Address field of the portal page when you add the plug-ins described in the following sections.

Table 1: Effects of Plug-ins on the Clientless SSL VPN Portal Page

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
ica	Citrix MetaFrame Services	ica://

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
rdp	Terminal Servers	rdp://
rdp2*	Terminal Servers Vista	rdp2://
ssh,telnet	Secure Shell	ssh://
	Telnet Services (supporting v1 and v2)	telnet://
vnc	Virtual Network Computing services	vnc://

* Not a recommended plug-in.

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

The plug-ins support single sign-on (SSO).

Prerequisites with Plug-Ins

- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.
- The minimum access rights required for remote use belong to the guest privilege mode.
- Plug-ins require ActiveX or Oracle Java Runtime Environment (JRE). See the Supported VPN Platforms, Cisco ASA 5500 Series compatibility matrices for version requirements.

Restrictions with Plug-Ins

Note The remote desktop protocol plug-in does not support load balancing with a session broker. Because of the way the protocol handles the redirect from the session broker, the connection fails. If a session broker is not used, the plug-in works.

- The plug-ins support single sign-on (SSO). They use the *same* credentials entered to open the Clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the options to perform SSO on different fields such as the internal domain password or on an attribute on a RADIUS or LDAP server.
- A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.

- If you use stateless failover instead of stateful failover, clientless features such as bookmarks, customization, and dynamic access-policies are not synchronized between the failover ASA pairs. In the event of a failover, these features do not work.

Prepare the Security Appliance for a Plug-in

Before you begin

Ensure that Clientless SSL VPN is enabled on an ASA interface.

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

Procedure

Step 1 Show whether Clientless SSL VPN is enabled on the ASA.

show running-config

Step 2 Install an SSL certificate onto the ASA interface and provide a fully-qualified domain name (FQDN) for remote user connection.

Install Plug-ins Redistributed by Cisco

Cisco redistributes the following open-source, Java-based components to be accessed as plug-ins for Web browsers in Clientless SSL VPN sessions.

Before you begin

Ensure Clientless SSL VPN is enabled on an interface on the ASA. To do so, enter the **show running-config** command.

Table 2: Plug-ins Redistributed by Cisco

Protocol	Description	Source of Redistributed Plug-in *
RDP	Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2. Supports Remote Desktop ActiveX Control. We recommend using this plug-in that supports both RDP and RDP2. Only versions up to 5.1 of the RDP and RDP2 protocols are supported. Version 5.2 and later are not supported.	http://properjavardp.sourceforge.net/
RDP2	Accesses Microsoft Terminal Services hosted by Windows Vista and Windows 2003 R2. Supports Remote Desktop ActiveX Control. This legacy plug-in supports only RDP2. We do not recommend using this plug-in; instead, use the RDP plug-in above.	
SSH	The Secure Shell-Telnet plug-in lets the remote user establish a Secure Shell (v1 or v2) or Telnet connection to a remote computer. Because keyboard-interactive authentication is not supported by JavaSSH, it cannot be supported with SSH plugin (used to implement different authentication mechanisms).	http://javassh.org/
VNC	The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing (also known as VNC server or service) turned on. This version changes the default color of the text and contains updated French and Japanese help files.	http://www.tightvnc.com/

* Consult the plug-in documentation for information on deployment configuration and restrictions.

These plug-ins are available on the Cisco Adaptive Security Appliance Software Download site.

Note The ASA does not retain the **import webvpn plug-in protocol** command in the configuration. Instead, it loads the contents of the `csco-config/97/plugin` directory automatically. A secondary ASA obtains the plug-ins from the primary ASA.

Procedure

Step 1 Install the plug-in onto the flash device of the ASA.

import webvpn plug-in protocol [**rdp** | **rdp2** | [**ssh** | **telnet**] | **vnc**] *URL*

Note Do not enter this command once for SSH and once for Telnet. When typing **ssh,telnet** , do not insert a space. This provides plug-in access to both Secure Shell and Telnet services.

Example:

The following example shows entering the hostname or address of the TFTP or FTP server and the path to the plug-in, where URL is the remote path to the plug-in .jar file.

```
hostname# import webvpn plug-in protocol ssh,telnet
tftp://local_tftp_server/plugins/ssh-plugin.jar
Accessing
tftp://local_tftp_server/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

Step 2 (Optional) Switch off and remove Clientless SSL VPN support for a plug-in, as well as removing it from the flash drive of the ASA.

revert webvpn plug-in protocol *protocol*

Example:

```
hostname# revert webvpn plug-in protocol rdp
```

Provide Access to a Citrix XenApp Server

As an example of how to provide Clientless SSL VPN browser access to third-party plug-ins, this section describes how to add Clientless SSL VPN support for the Citrix XenApp Server Client.

With a Citrix plug-in installed on the ASA, Clientless SSL VPN users can use a connection to the ASA to access Citrix XenApp services.

A stateful failover does not retain sessions established using the Citrix plug-in. Citrix users must reauthenticate after failover.

Create and Install the Citrix Plug-in

Before you begin

You must prepare the security application for a plug-in.

You must configure the Citrix Web Interface software to operate in a mode that does not use the (Citrix) "secure gateway." Otherwise, the Citrix client cannot connect to the Citrix XenApp Server.

Procedure

Step 1 Download the ica-plugin.zip file from the Cisco Software Download website.

This file contains files that Cisco customized for use with the Citrix plug-in.

Step 2 Download the Citrix Java client from the Citrix site.

In the download area of the Citrix website, choose Citrix Receiver, and Receiver for Other Platforms, and click Find. Click the Receiver for Java hyperlink and download the archive.

Step 3 Extract the following files from the archive, and then add them to the ica-plugin.zip file:

- JICA-configN.jar
- JICAEngN.jar

Step 4 Ensure the EULA included with the Citrix Java client grants you the rights and permissions to deploy the client on your Web servers.

Step 5 Install the plug-in by using ASDM, or entering the following CLI command in privileged EXEC mode:

import webvpn plug-in protocol ica URL

URL is the hostname or IP address and path to the ica-plugin.zip file.

Note Adding a bookmark is required to provide SSO support for Citrix sessions. We recommend that you use URL parameters in the bookmark the provide convenient viewing, for example:

ica://10.56.1.114/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768

Step 6 Establish an SSL VPN clientless session and click the bookmark or enter the URL for the Citrix server.

Use the Client for Java Administrator's Guide as needed.

View the Plug-ins Installed on the Security Appliance

Procedure

Step 1 List the Java-based client applications available to users of Clientless SSL VPN.

Example:

```
hostname# show import webvpn plug
ssh
rdp
vnc
ica
```

Step 2 Include hash and date of the plug-in.

Example:

```
hostname show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tues, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTs PnjdBoo= Tues, 15 Sep 2009 23:23:56 GMT
```

Configure Port Forwarding

Port forwarding lets users access TCP-based applications over a Clientless SSL VPN connection. Such applications include the following:

- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express
- Perforce
- Sametime
- Secure FTP (FTP over SSH)
- SSH
- Telnet
- Windows Terminal Service
- XDDTS

Other TCP-based applications may also work, but we have not tested them. Protocols that use UDP do not work.

Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. You may choose to use port forwarding because you have built earlier configurations that support this technology.

Consider the following alternatives to port forwarding:

- Smart tunnel access offers the following advantages to users:
  - 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.

- Unlike port forwarding and smart tunnel access, a plug-in does not require the client application to be installed on the remote computer.

When configuring port forwarding on the ASA, you specify the port the application uses. When configuring smart tunnel access, you specify the name of the executable file or its path.

Prerequisites for Port Forwarding

- Ensure Oracle Java Runtime Environment (JRE) 1.5.x or later is installed on the remote computers to support port forwarding (application access) and digital certificates.
- Browser-based users of Safari on Mac OS X 10.5.3 must identify a client certificate for use with the URL of the ASA, once with the trailing slash and once without it, because of the way Safari interprets URLs. For example,
  - https://example.com/
  - https://example.com

  For details, go to the Safari, Mac OS X 10.5.3: Changes in client certificate authentication.
- Users of Microsoft Windows Vista or later who use port forwarding or smart tunnels must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the **Tools > Internet Options > Security** tab. Vista (or later) users can also switch off Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.

Restrictions for Port Forwarding

- Port forwarding supports only TCP applications that use static TCP ports. Applications that use dynamic ports or multiple TCP ports are not supported. For example, SecureFTP, which uses port 22, works over Clientless SSL VPN port forwarding, but standard FTP, which uses ports 20 and 21, does not.
- Port forwarding does not support protocols that use UDP.
- Port forwarding does not support Microsoft Outlook Exchange (MAPI) proxy. However, you can configure smart tunnel support for Microsoft Office Outlook in conjunction with Microsoft Outlook Exchange Server.
- A stateful failover does not retain sessions established using Application Access (either port forwarding or smart tunnel access). Users must reconnect following a failover.
- Port forwarding does not support connections to personal digital assistants.
- Because port forwarding requires downloading the Java applet and configuring the local client, and because doing so requires administrator permissions on the local system, it is unlikely that users will be able to use applications when they connect from public remote systems.

  The Java applet displays in its own window on the end user HTML interface. It shows the contents of the list of forwarded ports available to the user, as well as which ports are active, and amount of traffic in bytes sent and received.

- The port forwarding applet displays the local port and the remote port as the same when the local IP address 127.0.0.1 is being used and cannot be updated by the Clientless SSL VPN connection from the

ASA. As a result, the ASA creates new IP addresses 127.0.0.2, 127.0.0.3, and so on for local proxy IDs. Because you can modify the hosts file and use different loopbacks, the remote port is used as the local port in the applet. To connect, you can use Telnet with the hostname, without specifying the port. The correct local IP addresses are available in the local hosts file.

Configure DNS for Port Forwarding

Port forwarding forwards the domain name of the remote server or its IP address to the ASA for resolution and connection. In other words, the port forwarding applet accepts a request from the application and forwards it to the ASA. The ASA makes the appropriate DNS queries and establishes the connection on behalf of the port forwarding applet. The port forwarding applet only makes DNS queries to the ASA. It updates the host file so that when a port forwarding application attempts a DNS query, the query redirects to a loopback address. Configure the ASA to accept the DNS requests from the port forwarding applet as follows:

Procedure

Step 1 Enter the dns server-group mode and configure a DNS server group named example.com.

Example:

```
hostname(config)# dns server-group example.com
```

Step 2 Specify the domain name. The default domain-name setting is DefaultDNS.

Example:

```
hostname(config-dns-server-group)# domain-name example.com
```

Step 3 Resolve the domain name to an IP address.

Example:

```
hostname(config-dns-server-group)# name-server 192.168.10.10
```

Step 4 Switch to Clientless SSL VPN configuration mode.

webvpn

Step 5 Switch to tunnel-group Clientless SSL VPN configuration mode.

tunnel-group webvpn

Step 6 Specify the domain name that the tunnel groups will use. By default, the security appliance assigns the default Clientless SSL VPN group as the default tunnel group for clientless connections. Follow this instruction if the ASA uses that tunnel group to assign settings to the clientless connections. Otherwise, follow this step for each tunnel configured for clientless connections.

Example:

```
asa2(config-dns-server-group)# exit
asa2(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
asa2(config-tunnel-webvpn)# dns-group example.com
```

Make Applications Eligible for Port Forwarding

The Clientless SSL VPN configuration of each ASA supports *port forwarding lists*, each of which specifies local and remote ports used by the applications for which to provide access. Because each group policy or username supports only one port forwarding list, you must group each set of ca supported into a list.

Procedure

Step 1 Display the port forwarding list entries already present in the ASA configuration.

show run webvpn port-forward

Step 2 Switch to Clientless SSL VPN configuration mode.

webvpn

Following the configuration of a port forwarding list, assign the list to group policies or usernames, as described in the next section.

Assign a Port Forwarding List

You can add or edit a named list of TCP applications to associate with users or group policies for access over Clientless SSL VPN connections. For each group policy and username, you can configure Clientless SSL VPN to do one of the following:

Note These options are mutually exclusive for each group policy and username. Use only one.

- Start port forwarding access automatically upon user login.

Before you begin

Before initiating the **port-forward enable** *list name* command, the user is required to start port forwarding manually, using **Application Access** > **Start Applications** on the Clientless SSL VPN portal page.

These 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 **port-forward** command from the group policy or username configuration.

Procedure

Step 1 Start port forwarding automatically upon user login.

port-forward auto-start <*list name*>

Step 2 Enable or prevent port forwarding upon user login.

port-forward enable <*list name*>

port-forward disable

Step 3 (Optional) Remove a **port-forward** command from the group policy or username configuration, which then inherits the [**no**] **port-forward** command from the default group policy. The keywords following the **no port-forward** command are optional; however, they restrict the removal to the named **port-forward** command.

no port-forward [**auto-start** <*list name*> | **enable** <*list name*> | **disable**]

Automate Port Forwarding

To start port forwarding automatically upon user login, enter the following commands:

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode.

webvpn

Step 2 Switch to group-policy or username Clientless SSL VPN configuration mode.

group-policy webvpn or **username webvpn**

Step 3 Start port forwarding automatically upon user login.

port-forward auto-start *list_name*

list_name names the port forwarding list already present in the ASA Clientless SSL VPN configuration. You cannot assign more than one port forwarding list to a group policy or username.

Example:

The following example assigns the port forwarding list named apps1 to the group policy.

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward auto-start apps1
```

Step 4 Display the port forwarding list entries present in the ASA configuration.

show run webvpn port-forward

Step 5 (Optional) Remove the port-forward command from the group policy or username and reverts to the default.

no port-forward

Enable and Switch off Port Forwarding

By default, port forwarding is switched off.

Procedure

Step 1 Enable port forwarding.

You do not have to start port forwarding manually if you entered **port-forward auto-start** *list_name*, where *list_name* is the name of the port forwarding list already present in the ASA Clientless SSL VPN configuration. You cannot assign more than one port forwarding list to a group policy or username.

port-forward [**enable** l<*list name*> | **disable**]

Example:

The following example assigns the port forwarding list named apps1 to the group policy.

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward enable apps1
```

Step 2 Display the port forwarding list entries.

show running-config port-forward

Step 3 (Optional) Remove the port-forward command from the group policy or username and revert to the default.

no port-forward

Step 4 (Optional) Switch off port forwarding.

port-forward disable

Configure File Access

Clientless SSL VPN serves remote users with HTTPS portal pages that interface with proxy CIFS and/or FTP clients running on the ASA. Using either CIFS or FTP, Clientless SSL VPN provides users with network access to the files on the network, to the extent that the users meet user authentication requirements and the file properties do not restrict access. The CIFS and FTP clients are transparent; the portal pages delivered by Clientless SSL VPN provide the appearance of direct access to the file systems.

When a user requests a list of files, Clientless SSL VPN queries the server designated as the master browser for the IP address of the server containing the list. The ASA gets the list and delivers it to the remote user on a portal page.

Clientless SSL VPN lets the user invoke the following CIFS and FTP functions, depending on user authentication requirements and file properties:

- Navigate and list domains and workgroups, servers within a domain or workgroup, shares within a server, and files within a share or directory.
- Create directories.
- Download, upload, rename, move, and delete files.

The ASA uses a master browser, WINS server, or DNS server, typically on the same network as the ASA or reachable from that network, to query the network for a list of servers when the remote user clicks **Browse Networks** in the menu of the portal page or on the toolbar displayed during the Clientless SSL VPN session.

The master browser or DNS server provides the CIFS/FTP client on the ASA with a list of the resources on the network, which Clientless SSL VPN serves to the remote user.

Note Before configuring file access, you must configure the shares on the servers for user access.

CIFS File Access Requirement and Limitation

To access `\\server\share\subfolder\personal` folder, the user must have a minimum of read permission for all parent folders, including the share itself.

Use Download or Upload to copy and paste files to and from CIFS directories and the local desktop. The Copy and Paste buttons are intended for remote to remote actions only, not local to remote, or remote to local.

If you drag and drop a file from a web folder to a folder on your workstation, you might get what appears to be a temporary file. Refresh the folder on your workstation to update the view and show the transferred file.

The CIFS browse server feature does not support double-byte character share names (share names exceeding 13 characters in length). This only affects the list of folders displayed, and does not affect user access to the folder. As a workaround, you can pre-configure the bookmark(s) for the CIFS folder(s) that use double-byte share names, or the user can enter the URL or bookmark of the folder in the format cifs://server/<long-folder-name>. For example:

```
cifs://server/Do you remember?
cifs://server/Do%20you%20remember%3F
```

Add Support for File Access

Note The procedure describes how to specify the master browser and WINS servers. As an alternative, you can use ASDM to configure URL lists and entries that provide access to file shares.

Adding a share in ASDM does not require a master browser or a WINS server. However, it does not provide support for the Browse Networks link. You can use a hostname or an IP address to refer to ServerA when entering the nbns-server command. If you use a hostname, the ASA requires a DNS server to resolve it to an IP address.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode.

webvpn

Step 2 Switch to tunnel-group Clientless SSL VPN configuration mode.

tunnel-group webvpn

Step 3 Browse a network or domain for each NetBIOS Name Server (NBNS).

nbns-server {*IPaddress* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

- **master** is the computer designated as the master browser. The master browser maintains the list of computers and shared resources. Any NBNS server you identify with this command without entering the master portion of the command must be a Windows Internet Naming Server (WINS). Specify the master browser first, then specify the WINS servers. You can specify up to three servers, including the master browser, for a connection profile.
- *timeout* is the number of seconds the ASA waits before sending the query again, to the same server if it is the only one, or another server if there are more than one. The default timeout is 2 seconds; the range is 1 to 30 seconds.
- *retries* is the number of times to retry queries to the NBNS server. The ASA recycles through the list of servers this number of times before sending an error message. The default value is 2; the range is 1 through 10.

Example:

```
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.20 master
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.41
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.47
```

Step 4 Display the NBNS servers already present in the connection profile configuration.

show tunnel-group webvpn-attributes

Step 5 (Optional) Specify the character set to encode in Clientless SSL VPN portal pages delivered to remote users. By default, the encoding type set on the remote browser determines the character set for Clientless SSL VPN portal pages, so you need to set the character encoding only if it is necessary to ensure proper encoding on the browser.

character-encoding *charset*

charset is a string consisting of up to 40 characters, and is equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

Example:

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color.

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
```

Step 6 (Optional) Specify the encoding for Clientless SSL VPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings.

file-encoding {*server-name* | *server-ip-address*} *charset*

Example:

The following example sets the file-encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias “CP860”) characters.

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
```

Ensure Clock Accuracy for SharePoint Access

The Clientless SSL VPN server on the ASA uses cookies to interact with applications such as Microsoft Word on the endpoint. The cookie expiration time set by the ASA can cause Word to malfunction when accessing documents on a SharePoint server if the time on the ASA is incorrect. To prevent this malfunction, set the ASA clock properly. We recommend configuring the ASA to dynamically synchronize the time with an NTP server. For instructions, see the section on setting the date and time in the general operations configuration guide.

Virtual Desktop Infrastructure (VDI)

The ASA supports connections to Citrix and VMWare VDI servers.

- For Citrix, the ASA allows access through clientless portal to user's running Citrix Receiver.
- VMWare is configured as a (smart tunnel) application.

VDI servers can also be accessed through bookmarks on the Clientless Portal, like other server applications.

Limitations to VDI

- Authentication using certificates or Smart Cards is not supported for auto sign-on, since these forms of authentication do not allow the ASA in the middle.
- The XML service must be installed and configured on the XenApp and XenDesktop servers.
- Client certificate verifications, double Auth, internal passwords and CSD (all of CSD, not just Vault) are not supported when standalone mobile clients are used.

Citrix Mobile Support

A mobile user running the Citrix Receiver can connect to the Citrix server by:

- Connecting to the ASA with AnyConnect, and then connecting to the Citrix server.
- Connecting to the Citrix server through the ASA, without using the AnyConnect client. Logon credentials can include:
  - A connection profile alias (also referred to as a tunnel-group alias) in the Citrix logon screen. A VDI server can have several group policies, each with different authorization and connection settings.

- An RSA SecureID token value, when the RSA server is configured. RSA support includes next token for an invalid entry, and also for entering a new PIN for an initial or expired PIN.

Supported Mobile Devices for Citrix

- iPad—Citrix Receiver version 4.x or later
- iPhone/iTouch—Citrix Receiver version 4.x or later
- Android 2.x/3.x/4.0/4.1 phone—Citrix Receiver version 2.x or later
- Android 4.0 phone—Citrix Receiver version 2.x or later

Limitations of Citrix

Certificate Limitations

- Certificate/Smart Card authentication is not supported as means of auto sign-on.
- Client certificate verifications and CSD are not supported
- Md5 signature in the certificates are not working because of security issue, which is a known problem on iOS: http://support.citrix.com/article/CTX132798
- SHA2 signature is not supported except for Windows, as described on the Citrix website: http://www.citrix.com/
- A key size >1024 is not supported

Other Limitations

- HTTP redirect is not supported; the Citrix Receiver application does not work with redirects.
- XML service must be installed and configured on the XenApp and XenDesktop servers.

About Citrix Mobile Receiver User Logon

The logon for mobile users connecting to the Citrix server depends on whether the ASA has configured the Citrix server as a VDI server or a VDI proxy server.

When the Citrix server is configured as a VDI server:

1. Using the AnyConnect Secure Mobility Client, connect to ASA with VPN credentials.
2. Using Citrix Mobile Receiver, connect to Citrix server with Citrix server credentials (if single-signon is configured, the Citrix credentials are not required).

When the ASA is configured as a to a VDI proxy server:

1. Using Citrix Mobile Receiver, connect to the ASA entering credentials for both the VPN and Citrix server. After the first connection, if properly configured, subsequent connections only require VPN credentials.

Configure the ASA to Proxy a Citrix Server

You can configure the ASA to act as a proxy for the Citrix servers, so that connections to the ASA appear to the user like connections to the Citrix servers. The AnyConnect client is not required when you enable VDI proxy in ASDM. The following high-level steps show how the end user connects to Citrix.

Procedure

Step 1 A mobile user opens Citrix Receiver and connects to ASA's URL.

Step 2 The user provides credentials for the XenApp server and the VPN credentials on the Citrix logon screen.

Step 3 For each subsequent connection to the Citrix server, the user only needs to enter the VPN credentials.

Using the ASA as a proxy for XenApp and XenDesktop removes the requirement for a Citrix Access Gateway. XenApp server info is logged on the ASA, and displays in ASDM.

Configure the Citrix server's address and logon credentials, and assign that VDI server to a Group Policy or username. If both username and group-policy are configured, username settings override group-policy settings.

What to do next

http://www.youtube.com/watch?v=JMM2RzppaG8 - This video describes the advantages of using the ASA as a Citrix proxy.

Assign a VDI Server to a Group Policy

VDI servers are configured and assigned to Group Policies by:

- Adding the VDI server on the VDI Access pane, and assigning a group policy to the server.
- Adding a VDI server to the group policy.

If both username and group policy are configured, username settings take precedence over group policy. Enter the following:

```
configure terminal
 group-policy DfltGrpPolicy attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password
   <password>
configure terminal
 username <username> attributes
  webvpn
   vdi type <citrix> url <url> domain <domain> username <username> password
   <password>]
```

The syntax options are defined as follows:

- type—Type of VDI. For a Citrix Receiver type, this value must be *citrix*.
- url—Full URL of the XenApp or XenDesktop server including http or https, hostname, and port number, as well as the path to the XML service.

- username—Username for logging into the virtualization infrastructure server. This value can be a clientless macro.
- password—Password for logging into the virtualization infrastructure server. This value can be a clientless macro.
- domain—Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.

Use SSL to Access Internal Servers

Procedure

Step 1 Switch to group policy Clientless SSL VPN configuration mode.

webvpn

Step 2 Switch off URL entry.

url-entry disable

Clientless SSL VPN uses SSL and its successor, TLS1 to provide a secure connection between remote users and specific, supported internal resources at an internal server.

Configure Clientless SSL VPN and ASDM Ports

From version 8.0(2), the ASA supports both Clientless SSL VPN sessions and ASDM administrative sessions simultaneously on port 443 of the outside interface. You can configure these applications on different interfaces.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode.

webvpn

Step 2 Change the SSL listening port for Clientless SSL VPN.

port *port_number*

Example:

This example enables Clientless SSL VPN on port 444 of the outside interface. With this configuration, remote users initiating Clientless SSL VPN sessions enter https://<outside_ip>:444 in the browser.

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside
```

Step 3 (Privileged mode) Change the listening port for ASDM.

http server enable

Example:

This example specifies that HTTPS ASDM sessions use port 444 on the outside interface. Clientless SSL VPN is also enabled on the outside interface and uses the default port (443). With this configuration, remote users initiate ASDM sessions by entering https://<outside_ip>:444.

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

Use HTTPS for Clientless SSL VPN Sessions

Procedure

Step 1 Switch to clientless SSL VPN configuration mode.

Enter **webvpn**.

Step 2 Enable Clientless SSL VPN sessions on the interface called outside.

Enter **enable** *interface-name*.

Example

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

What to do next

To see the current configuration, use the **show running-config webvpn**.

To clear the current configuration, use the **clear configure webvpn**.

Configure Support for Proxy Servers

The ASA can terminate HTTPS connections and forward HTTP and HTTPS requests to proxy servers. These servers act as intermediaries between users and the public or private network. Requiring network access via a proxy server that the organization controls provides another opportunity for filtering, to assure secure network access and administrative control.

When configuring support for HTTP and HTTPS proxy services, you can assign preset credentials to send with each request for basic authentication. You can also specify URLs to exclude from HTTP and HTTPS requests.

Before you begin

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

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode.

webvpn

Step 2 Configure the ASA to use an external proxy server to handle HTTP and HTTPS requests.

http-proxy and https-proxy

Note Proxy NTLM authentication is not supported in **http-proxy**. Only proxy without authentication and basic authentication are supported.

Step 3 Configure HTTP proxy.

http-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

Step 4 Configure HTTPS proxy.

https-proxy *host* [*port*] [**exclude** *url*] [**username** *username* {**password** *password*}]

Step 5 Set the PAC file URL.

http-proxy pac *url*

Step 6 (Optional) Exclude URLs from those that can be sent to the proxy server.

exclude

Step 7 Provide the hostname or IP address for the external proxy server.

host

Step 8 Download the proxy autoconfiguration file to the ASA using a JavaScript function which identifies a proxy for each URL.

pac

Step 9 (Optional) (Only available if you specify a username) Accompanies each proxy request with a password to provide basic, proxy authentication.

password

Step 10 Send the password to the proxy server with each HTTP or HTTPS request.

password

Step 11 (Optional) Provide the port number used by the proxy server. The default HTTP port is 80. The default HTTPS port is 443. The ASA uses each of these ports if you do not specify an alternative value. The range is 1-65535.

port

Step 12 If you entered **exclude**, enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards:

- ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string.
- **?** to match any single character, including slashes and periods.
- [x-y] to match any single character in the range of x and y, where x represents one character and y represents another character in the ANSI character set.
- [**!**x-y] to match any single character that is not in the range.

Step 13 If you entered **http-proxy pac**, follow it with **http://** and type the URL of the proxy autoconfiguration file. (If you omit the **http://** portion, the CLI ignores the command.)

Step 14 (Optional) Accompany each HTTP proxy request with a username for basic, proxy authentication. Only the **http-proxy***host* command supports this keyword.

username

Step 15 Send the username to the proxy server with each HTTP or HTTPS request.

username

Step 16 Show how to configure use of an HTTP proxy server with an IP address of 209.165. 201.1 using the default port, sending a username and password with each HTTP request.

Example:

```
hostname(config-webvpn)# http-proxy 209.165.201.1 user jsmith password
mysecretdonttell
```

Step 17 Show the same command, except when the ASA receives the specific URL www.example.com in an HTTP request, it resolves the request instead of passing it on to the proxy server.

Example:

```
hostname(config-webvpn)# http-proxy 209.165.201.1 exclude www.example.com
username jsmith password mysecretdonttell
```

Step 18 Show how to specify a URL to serve a proxy autoconfiguration file to the browser.

Example:

```
hostname(config-webvpn)# http-proxy pac http://www.example.com/pac
```

The ASA Clientless SSL VPN configuration supports only one **http-proxy** and one **https-proxy** command each. For example, if one instance of the **http-proxy** command is already present in the running configuration and you enter another, the CLI overwrites the previous instance.

Note Proxy NTLM authentication is not supported in **http-proxy**. Only proxy without authentication and basic authentication is supported.

Configure SSL/TLS Encryption Protocols

Port forwarding requires the Oracle Java Runtime Environment (JRE). Port forwarding does not work when a user of Clientless SSL VPN connects with some SSL versions. Refer to the Supported VPN Platforms, Cisco ASA 5500 Series for supported JRE versions.

Authenticate with Digital Certificates

SSL uses digital certificates for authentication. The ASA creates a self-signed SSL server certificate when it boots; or you can install in the ASA an SSL certificate that has been issued in a PKI context. For HTTPS, this certificate must then be installed on the client.

Restrictions of Digital Certificates Authentication

Email clients such as MS Outlook, MS Outlook Express, and Eudora lack the ability to access the certificate store.

For more information on authentication and authorization using digital certificates, see the section on using certificates and user login credentials in the general operations configuration guide.

Configure Browser Access to Client-Server Plug-ins

The Client-Server Plug-in table displays the plug-ins the ASA makes available to browsers in Clientless SSL VPN sessions.

To add, change, or remove a plug-in, do one of the following:

- To add a plug-in, click **Import**. The Import Plug-ins dialog box opens.
- To remove a plug-in, choose it and click **Delete**.

About Installing Browser Plug-ins

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

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

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

The following table shows the changes to the main menu and address field of the portal page when you add the plug-ins described in the following sections.

Table 3: Effects of Plug-ins on the Clientless SSL VPN Portal Page

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
ica	Citrix Client	citrix://
rdp	Terminal Servers	rdp://
rdp2	Terminal Servers Vista	rdp2://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

Note A secondary ASA obtains the plug-ins from the primary ASA.

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

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

Prerequisites for Installing Browser Plug-ins

- The plug-ins do not work if the security appliance configures the clientless session to use a proxy server.

  Note The remote desktop protocol plug-in does not support load balancing with a session broker. Because of the way the protocol handles the redirect from the session broker, the connection fails. If a session broker is not used, the plug-in works.

- The plug-ins support single sign-on (SSO). They use the *same* credentials entered to open the Clientless SSL VPN session. Because the plug-ins do not support macro substitution, you do not have the options to perform SSO on different fields such as the internal domain password or on an attribute on a RADIUS or LDAP server.
- To configure SSO support for a plug-in, you install the plug-in, add a bookmark entry to display a link to the server, and specify SSO support when adding the bookmark.
- The minimum access rights required for remote use belong to the guest privilege mode.

Requirements for Installing Browser Plug-ins

- Per the GNU General Public License (GPL), Cisco redistributes plug-ins without having made any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.
- Clientless SSL VPN must be enabled on the ASA to provide remote access to the plug-ins.
- A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.
- Plug-ins require that ActiveX or Oracle Java Runtime Environment (JRE) is enabled on the browser. There is no ActiveX version of the RDP plug-in for 64-bit browsers.

Set Up RDP Plug-in

To set up and use an RDP plug-in, you must add a new environment variable.

Procedure

Step 1 Right-click **My Computer** to access the System Properties, and choose the **Advanced** tab.

Step 2 On the Advanced tab, choose the environment variables button.

Step 3 In the new user variable dialog box, enter the RF_DEBUG variable.

Step 4 Verify the new Environment Variable in the user variables section.

Step 5 If you used the client computer with versions of Clientless SSL VPN before version 8.3, you must remove the old Cisco Portforwarder Control. Go to the C:/WINDOWS/Downloaded Program Files directory, right-click portforwarder control, and choose **Remove**.

Step 6 Clear all of the Internet Explorer browser cache.

Step 7 Launch your Clientless SSL VPN session and establish an RDP session with the RDP ActiveX Plug-in.

You can now observe events in the Windows Application Event viewer.

Prepare the Security Appliance for a Plug-in

Procedure

Step 1 Ensure that Clientless SSL VPN is enabled on an ASA interface.

Step 2 Install an SSL certificate onto the ASA interface to which remote users use a fully-qualified domain name (FQDN) to connect.

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

Configure the ASA to Use the New HTML File

Procedure

Step 1 Import the file and images as Web Content.

import webvpn webcontent <*file*> <*url*>

Example:

```
hostname# import webvpn webcontent /+CSCOU+/login.inc tftp://209.165.200.225/login.inc
!!!!* Web resource `+CSCOU+/login.inc' was successfully initialized
hostname#
```

Step 2 Export a customization template.

export webvpn customization <*file*> <*URL*>

Example:

```
hostname# export webvpn customization template tftp://209.165.200.225/sales_vpn_login
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
%INFO: Customization object 'Template' was exported to tftp://10.21.50.120/sales
_vpn_login
```

Step 3 Change the full customization mode tag in the file to enable.

Example:

This example supplies the URL of the login file stored in the ASA memory.

```
<full-customization>
          <mode>enable</mode>
          <url>/+CSCOU+/login.inc</url>
      </full-customization>
```

Step 4 Import the file as a new customization object.

Example:

```
hostname# import webvpn customization sales_vpn_login tftp://10.21.50.120/sales_vpn_login$
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
%INFO: customization object 'sales_vpn_login' was successfully imported
```

Step 5 Apply the customization object to a Connection Profile (tunnel group).

Example:

```
hostname(config)# tunnel-group Sales webvpn-attributes
hostname(config-tunnel-webvpn)#customization sales_vpn_login
```