Basic Clientless SSL VPN Configuration

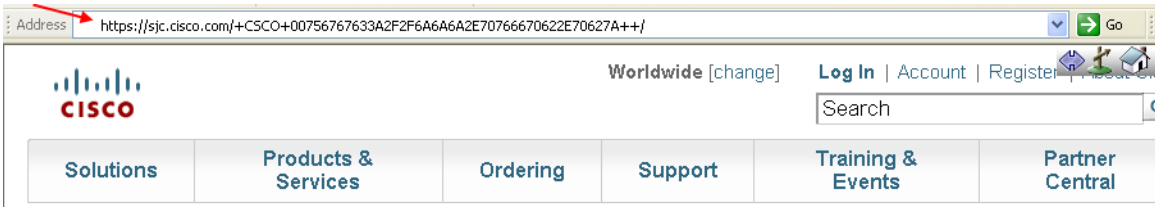
September 13, 2013

Clientless SSL VPN Security Precautions

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. Cisco recommends switching off URL Entry on these policies to prevent user confusion over what is accessible.

Figure 12-1 Example URL Entered by User

Figure 12-2 Same URL Rewritten by Security Appliance and Displayed in Browser Window



DETAILED STEPS

Step 1 Configure a group policy for all users who need Clientless SSL VPN access, and enable Clientless SSL VPN for that group policy only.

Step 2 With the group policy open, choose **General > More Options > Web ACL** and click **Manage**.

Step 3 Create a Web ACL to do one of the following:

- Permit access only to specific targets within the private network.
- Permit access only to the private network, deny Internet access, or permit access only to reputable sites.

Step 4 Assign the Web ACL to any policies (group policies, dynamic access policies, or both) that you have configured for Clientless SSL VPN access. To assign a Web ACL to a DAP, edit the DAP record, and select the Web ACL on the **Network ACL Filters** tab.

Step 5 Switch off URL Entry on the *portal page*, the page that opens upon the establishment of a browser-based connection. Click **Disable** next to URL Entry on both the group policy Portal frame and the DAP **Functions** tab. To switch off URL Entry on a DAP, use ASDM to edit the DAP record, click the **Functions** tab, and check **Disable** next to URL Entry

Step 6 Instruct users to enter external URLs in the native browser address field above the portal page or open a separate browser window to visit external sites.

Configuring Clientless SSL VPN Access

When configuring Clientless SSL VPN access, you can do the following:

- Enable or switch off ASA interfaces for Clientless SSL VPN sessions.
- Choose a port for Clientless SSL VPN connections.
- Set a maximum number of simultaneous Clientless SSL VPN sessions.

DETAILED STEPS

Step 1 To configure or create a group policy for clientless access, navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** pane.

Step 2 Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

a. Enable or switch off **Allow Access** for each ASA interface.

The Interface columns list the configured interfaces. The WebVPN Enabled field displays the status for Clientless SSL VPN on the interface. A green check next to Yes indicates that Clientless SSL VPN is enabled. A red circle next to No indicates that Clientless SSL VPN is switched off.

b. Click **Port Setting**, and enter the port number (1 to 65535) to use for Clientless SSL VPN sessions. The default is 443. If you change the port number, all current Clientless SSL VPN connections are terminated, and current users must reconnect. You will also be prompted to reconnect the ASDM session.

Step 3 Navigate to **Configuration > Remote Access VPN > Advanced > Maximum VPN Sessions**, and enter the maximum number of Clientless SSL VPN sessions to allow in the Maximum Other VPN Sessions field. Different ASA models support Clientless SSL VPN sessions as follows: ASA 5510 supports a maximum of 250; ASA 5520 maximum is 750; ASA 5540 maximum is 2500; ASA 5550 maximum is 5000.

Verifying Clientless SSL VPN Server Certificates

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 it is in fact the server you are trying to connect to. ASA 9.0 introduced support for SSL server certificate verification against a list of trusted certificate authority (CA) certificates for Clientless SSL VPN.

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. This is a form of public key infrastructure (PKI).

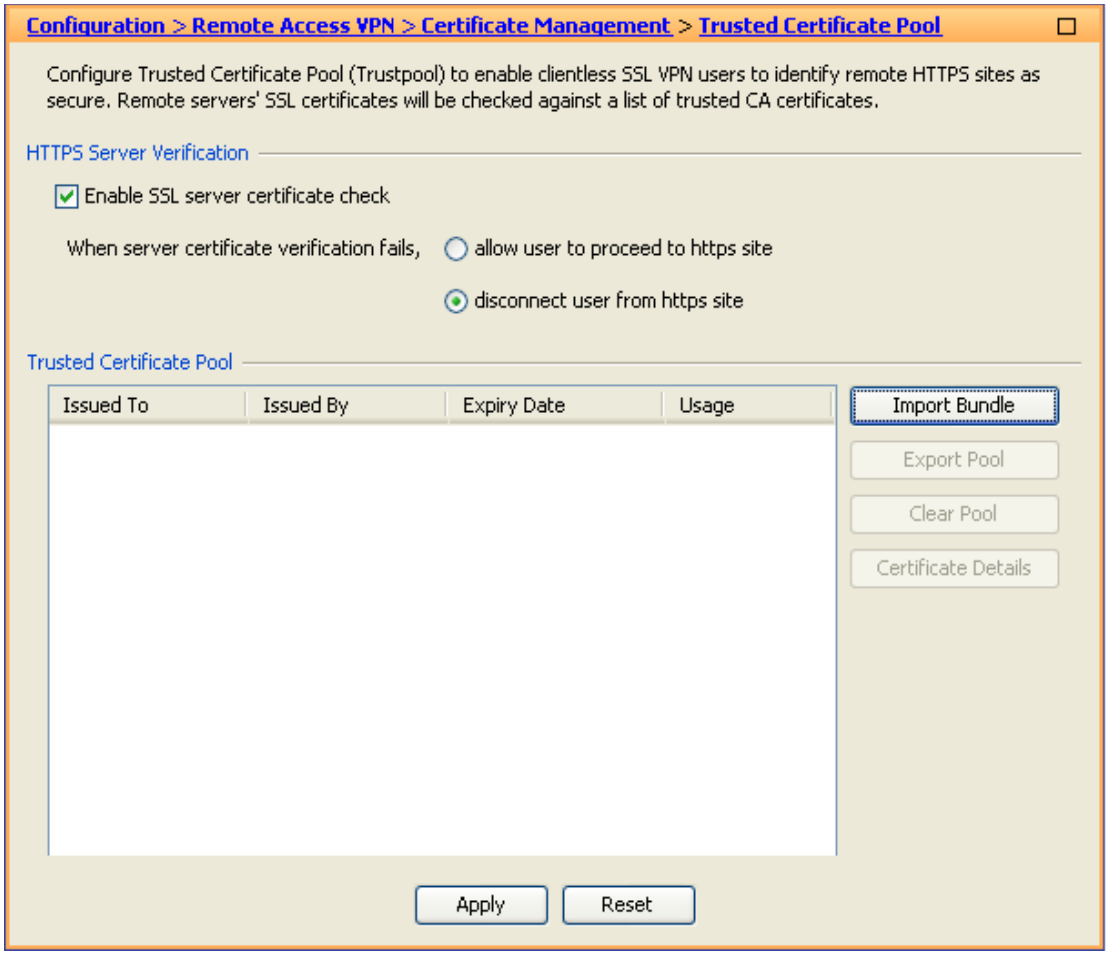
The ASA provides trusted pool certificate management facilities in the form of a trustpools. This can be thought of as a special case of trustpoint representing multiple known CA certificates. The ASA includes a default bundle of certificates, similar to that provided with Web browsers. It is inactive until activated by the administrator.

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

Enabling HTTP Server Verification

Step 1 In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**.

Figure 12-3 Enabling HTTPS Server Verification in the ASDM



Step 2 Select the **Enable SSL Certificate Check** check box.

Step 3 Click **Disconnect User From HTTPS Site** to disconnect if the server could not be verified. Alternatively, click **Allow User to Proceed to HTTPS Site** to allow the user to continue the connection, even if the check failed.

Step 4 Click **Apply** to save your changes.

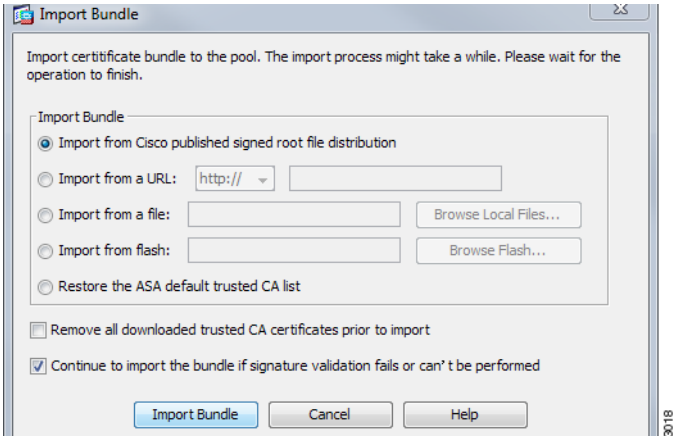
Importing a Certificate Bundle

You can import individual certificates or bundles of certificates from various locations in one of the following formats:

- x509 certificates in DER format wrapped in a pkcs7 structure.
- A file of concatenated x509 certificates in PEM format (complete with PEM header).

Step 1 In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**.

Step 2 Click **Import Bundle**.



Step 3 Select the location of the bundle:

- If the bundle is stored on your computer, click **Import From a File**, and click **Browse Local Files** and navigate to the bundle.
- If the bundle is stored on the ASA flash file system, click **Import From Flash**, and click **Browse Flash** and navigate to the file.
- If the bundle is hosted on a server, click **Import From a URL**, select the protocol from the list, and enter the URL in the field.
- Continue to import the bundle if signature validation fails or cannot be performed allows you to import the bundle, and fix individual certificate errors later. Uncheck this to have the entire bundle fail if any of the certificates fails.

Step 4 Click **Import Bundle**. Alternatively, click **Cancel** to abandon your changes.

Note You can select the **Remove All Downloaded Trusted CA Certificates Prior to Import** check box to clear the trustpool before importing a new bundle.

Exporting the Trustpool

When you have correctly configured the trustpool, you should export the pool. This will enable you to restore the trustpool to this point, for example to remove a certificate that was added to the trustpool after the export. You can export the pool to the ASA flash file system or your local file system.

In the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, and click **Export Pool**.

Step 1 Click **Export to a File**.

Step 2 Click **Browse Local Files**.

Step 3 Navigate to the folder where you want to save the trustpool.

Step 4 Enter a unique memorable name for the trustpool in the **File Name** box.

Step 5 Click **Select**.

Step 6 Click **Export Pool** to save the file. Alternatively, click **Cancel** to stop saving.

Removing Certificates

To remove all certificates, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Clear Pool**.

Note Before clearing the trustpool you should export the current trustpool to enable you to restore your current settings.

Restoring the Default Trusted Certificate Authority List

To restore the default trusted certificate authority (CA) list, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Restore Default Trusted CA List** and click **Import Bundle**.

Updating the Trustpool

The trustpool should be updated if either of the following conditions exists:

- Any certificate in the trustpool is due to expire or has been re-issued.
- The published CA certificate bundle contains additional certificates that are required by a specific application.

A full update will replace all the certificates in the trustpool.

A practical update enables you to add new certificates or replace existing certificates.

Removing a Certificate Bundle

Clearing the trustpool will remove all certificates that are not part of the default bundle.

You cannot remove the default bundle. To clear the trustpool, in the ASDM, navigate to **Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool**, then click **Clear Pool**.

Java Code Signer

Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin.

Choose the configured certificate to employ in Java object signing from the drop-down list.

To configure a Java Code Signer, choose Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer.

Java objects which have been transformed by Clientless SSL VPN can subsequently be signed using a PKCS12 digital certificate associated with a trustpoint. In the Java Trustpoint pane, you can configure the Clientless SSL VPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location.

To import a trustpoint, choose **Configuration > Properties > Certificate > Trustpoint > Import**.

Configuring Browser Access to Plug-ins

The following sections describe the integration of browser plug-ins for Clientless SSL VPN browser access:

- Preparing the Security Appliance for a Plug-in, page 12-8
- Installing Plug-ins Redistributed by Cisco, page 12-8
- Providing Access to a Citrix XenApp Server, page 12-10

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 menu 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 menu next to the Address field of the portal page.

Table 12-1 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.

* Not a recommended plug-in.

Table 12-1 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://
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://

When the user in a Clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.The plug-ins support single sign-on (SSO). Refer to the "Configuring SSO with the HTTP Form Protocol" section on page 16-6 for implementation details.

Prerequisites

- 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 compatibility matrix for version requirements.

Restrictions

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.

Preparing the Security Appliance for a Plug-in

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

Prerequisites

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

Restrictions

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.

Go to the section that identifies the type of plug-in to provide for Clientless SSL VPN access.

- Installing Plug-ins Redistributed by Cisco, page 12-8
- Providing Access to a Citrix XenApp Server, page 12-10

Installing 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.

Prerequisites

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

Table 12-2 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. **Note** This legacy plug-in supports only RDP2. We do not recommend using this plug-in; instead, use the RDP plug-in above.	http://properjavardp.sourceforge.net/
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. **Note** 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.

DETAILED STEPS

Step 1 Create a temporary directory named plugins on the computer you use to establish ASDM sessions with the ASA, and download the required plug-ins from the Cisco website to the plugins directory.

Step 2 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.

This pane displays the currently loaded plug-ins that are available to Clientless SSL sessions. The hash and date of these plug-ins are also provided.

Step 3 Click **Import**.

The Import Client-Server Plug-in dialog box opens.

Step 4 Use the following descriptions to enter the Import Client-Server Plug-in dialog box field values.

- Plug-in Name—Select one of the following values:
  - **ica** to provide plug-in access to Citrix MetaFrame or Web Interface services.
  - **rdp** to provide plug-in access to Remote Desktop Protocol services.
  - **ssh,telnet** to provide plug-in access to *both* Secure Shell and Telnet services.
  - **vnc** to provide plug-in access to Virtual Network Computing services.

Note Any undocumented options in this menu are experimental and are not supported.

- Select the location of the plugin file—Select one of the following options and insert a path into its text field.
  - Local computer—Enter the location and name of the plug-in into the associated Path field, or click **Browse Local Files** and navigate to the plug-in, choose it, then click **Select**.
  - Flash file system—Enter the location and name of the plug-in into the associated Path field, or click **Browse Flash** and navigate to the plug-in, choose it, then click **OK**.
  - Remote Server—Choose **ftp**, **tftp**, or **HTTP** from the drop-down menu next to the associated Path attribute, depending on which service is running on the remote server. Enter the hostname or address of the server and the path to the plug-in into the adjacent text field.

Step 5 Click **Import Now**.

Step 6 Click **Apply**.

The plug-in is now available for future Clientless SSL VPN sessions.

Providing 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.

To provide access to the Citrix plug-in, follow the procedures in the following sections.

- Preparing the Citrix XenApp Server for Clientless SSL VPN Access
- Creating and Installing the Citrix Plug-in

Preparing the Citrix XenApp Server for Clientless SSL VPN Access

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.

Note If you are not already providing support for a plug-in, you must follow the instructions in the "Preparing the Security Appliance for a Plug-in" section on page 12-8 before using this section.

Creating and Installing the Citrix Plug-in

DETAILED STEPS

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, select **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.

Configuring Port Forwarding

The following sections describe port forwarding and how to configure it:

- Information About Port Forwarding, page 12-12
- Configuring DNS for Port Forwarding
- Making Applications Eligible for Port Forwarding
- Adding/Editing a Port Forwarding Entry
- Assigning a Port Forwarding List
- Enabling and Switching off Port Forwarding

Information About 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

- The remote host must be running a 32-bit version of one of the following:
  - Microsoft Windows Vista, Windows XP SP2 or SP3; or Windows 2000 SP4.
  - Apple Mac OS X 10.4 or 10.5 with Safari 2.0.4(419.3).
  - Fedora Core 4
- The remote host must also be running Oracle Java Runtime Environment (JRE) 5 or later.
- 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.
- 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. If JRE 1.4.x is running and the user authenticates with a digital certificate, the application fails to start because JRE cannot access the Web browser certificate store.

Restrictions

- 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.

Configuring 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.

Step 1 Click **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

The default Clientless SSL VPN group entry is the default connection profile used for clientless connections.

Step 2 Highlight the default Clientless SSL VPN group entry, then click **Edit** if your configuration uses it for clientless connections. Otherwise, highlight a connection profile used in your configuration for clientless connections, then click **Edit**.

The Basic window opens.

Step 3 Scan to the DNS area and select the DNS server from the drop-down list. Note the domain name, disregard the remaining steps, and go to the next section if ASDM displays the DNS server to use. You need to enter the same domain name when you specify the remote server while configuring an entry in the port forwarding list. Continue with the remaining steps if the DNS server is not present in the configuration.

Step 4 Click **Manage** in the DNS area.

The Configure DNS Server Groups window opens.

Step 5 Click **Configure Multiple DNS Server Groups**.

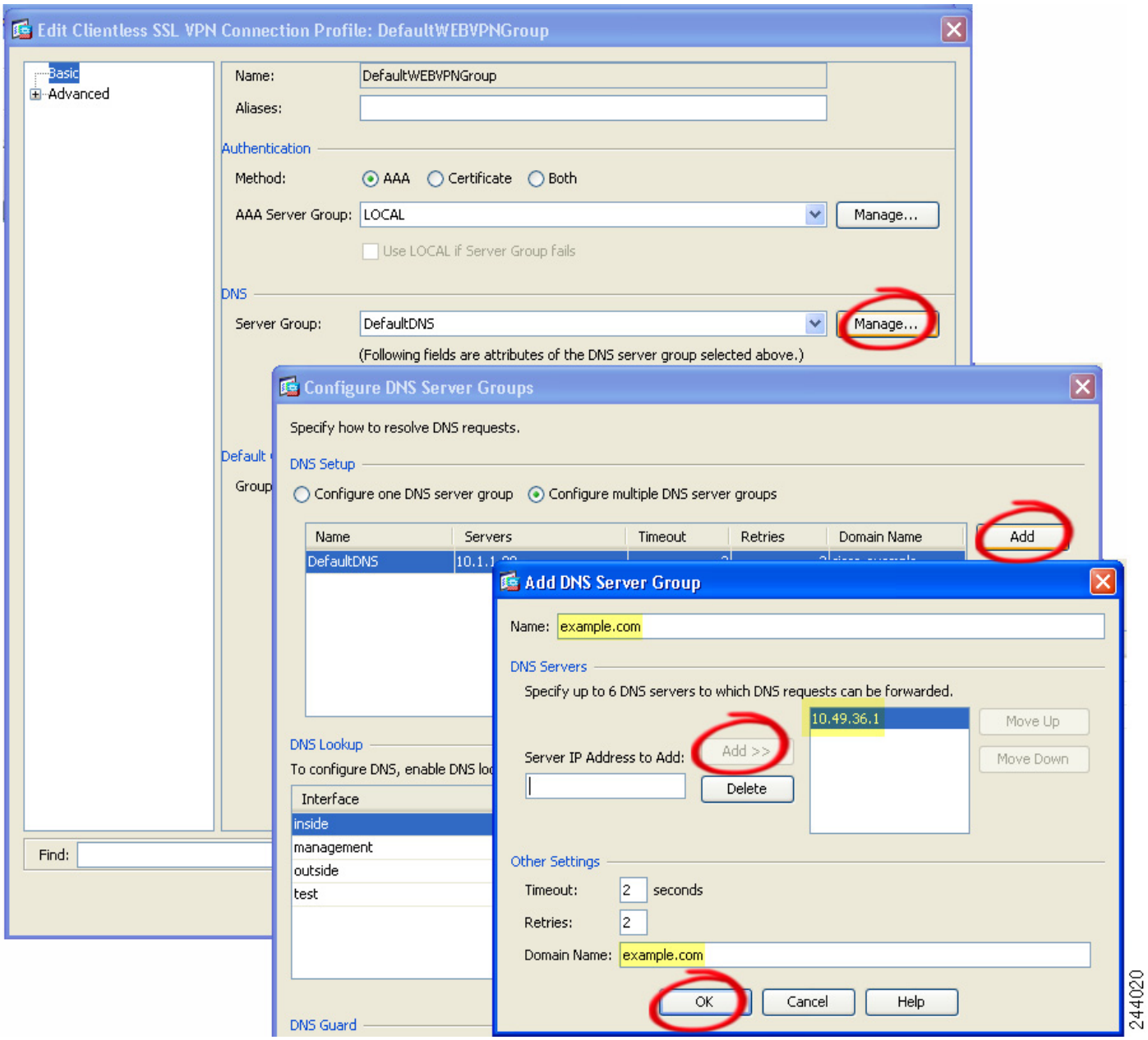
A window displays a table of DNS server entries.

Step 6 Click **Add.**

The Add DNS Server Group window opens.

Step 7 Enter a new server group name in the Name field, and enter the IP address and domain name (see Figure 12-4).

Figure 12-4 Example DNS Server Values for Port Forwarding



Note the domain name that you entered. You need it when you specify the remote server later while configuring a port forwarding entry.

Step 8 Click **OK** until the Connection Profiles window becomes active again.

Step 9 Repeat Steps 2–8 for each remaining connection profile used in your configuration for clientless connections.

Step 10 Click **Apply**.

Making 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. To display the port forwarding list entries already present in the ASA configuration, enter the following commands:

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

Adding/Editing a Port Forwarding Entry

The Add/Edit Port Forwarding Entry dialog boxes let you specify TCP applications to associate with users or group policies for access over Clientless SSL VPN connections. Assign values to the attributes in these windows as follows:

Prerequisites

The DNS name assigned to the Remote Server parameter must match the Domain Name and Server Group parameters to establish the tunnel and resolve to an IP address, per the instructions in the "Assigning a Port Forwarding List" section on page 12-16. The default setting for both the Domain and Server Group parameters is DefaultDNS.

DETAILED STEPS

Step 1 Click **Add**.

Step 2 Type a TCP port number for the application to use. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Step 3 Enter either the domain name or the IP address of the remote server. We recommend using a domain name so that you do not have to configure the client applications for the specific IP address.

Step 4 Type the well-known port number for the application.

Step 5 Type a description of the application. The maximum is 64 characters.

Step 6 (Optional) Highlight a port forwarding list and click **Assign** to assign the selected list to one or more group policies, dynamic access policies, or user policies.

Assigning 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:

- Start port forwarding access automatically upon user login.
- Enable port forwarding access upon user login, but require the user to start it manually, using **Application Access > Start Applications** on the Clientless SSL VPN portal page.

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

DETAILED STEPS

The Add or Edit Port Forwarding List dialog box lets you add or edit the following:

Step 1 Provide an alphanumeric name for the list. The maximum is 64 characters.

Step 2 Enter which local port listens for traffic for the application. You can use a local port number only once for a listname. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Note Enter the IP address or DNS name of the remote server. We recommend using a domain name so that you do not have to configure the client applications for the specific IP address.

Step 3 Enter the remote port that listens for traffic for the application.

Step 4 Describe the TCP application. The maximum is 64 characters.

Enabling and Switching off Port Forwarding

By default, port forwarding is switched off.

If you enable port forwarding, the user will have to start it manually, using **Application Access > Start Applications** on the Clientless SSL VPN portal page.

Configuring 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.

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
```

Adding Support for File Access

Configure file access as follows:

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.

For a complete description of these commands, see the *Cisco Security Appliance Command Reference*.

Ensuring 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

- 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

- 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

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.

Configuring 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.

1. A mobile user opens Citrix Receiver and connects to ASA's URL.
2. The user provides credentials for the XenApp server and the VPN credentials on the Citrix logon screen.
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.

Additional Information

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

Configuring a VDI Server

For one server:

1. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access

2. Check Enable VDI Server Proxy, and configure the VDI server.

To assign several group policies to a VDI server:

1. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. Check Configure All VDI Servers.
3. Add a VDI Server, and assign one or more group policies.

Configuring a VDI Proxy Server

For one VDI server assigned to one group policy:

1. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. Check Enable VDI Server Proxy, and configure the VDI server.

To assign several group policies to a VDI server:

1. Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > VDI Access
2. Check Configure All VDI Servers.
3. Add a VDI Server, and assign one or more group policies.

Assigning 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.

Step 1 Browse to Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies.

Step 2 Edit the DfltGrpPolicy and expand the More options menu from the left-side menu.

Step 3 Choose **VDI Access**. Click **Add** or **Edit** to provide VDI server details.

- Server (Host Name or IP Address)—Address of the XenApp or XenDesktop server. This value can be a clientless macro.
- Port Number (Optional)—Port number for connecting to the Citrix server. This value can be a clientless macro.
- Active Directory Domain Name—Domain for logging into the virtualization infrastructure server. This value can be a clientless macro.
- Use SSL Connection—Check the checkbox if you want the server to connect using SSL.
- 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.

•

	Command	Purpose
Step 1	`webvpn`	Switches to group policy Clientless SSL VPN configuration mode.
Step 2	`url-entry disable`	Switches off URL Entry.

Note

Configuring ACLs

ACLs constrain user access to specific networks, subnets, hosts, and Web servers. The Web ACLs table displays the filters configured on the ASA application to the Clientless SSL VPN traffic. The table shows the name of each access control list (ACL) and, below and indented to the right of the ACL name, the ACEs (access control entries) assigned to the ACL.

Each ACL permits or denies access to specific networks, subnets, hosts, and Web servers. Each ACE specifies one rule that serves the function of the ACL.

Guidelines

If you do not define any filters, all connections are permitted.

Restrictions

- The ASA supports only an inbound ACL on an interface.
- At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an ACE (access control entry), the ASA denies it. ACEs are referred to as rules in this topic.

DETAILED STEPS

Web ACLs are configured on the page **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

Step 1 Click **Add ACL** to add an ACL or ACE. To insert a new ACE before or after an existing ACE, click **Insert** or **Insert After**.

Step 2 Click **Edit** to highlight the ACE to change.

Step 3 Highlight the ACL or ACE to remove and click **Delete**. When you delete an ACL, you must delete all of its ACEs. No warning is provided and it is not possible to recover deleted ACL or ACEs.

Step 4 Use the **Move Up** and **Move Down** buttons to change the order of ACLs or ACEs. The ASA checks ACLs to be applied to Clientless SSL VPN sessions and their ACEs in the sequence determined by their position in the ACLs list until it finds a match.

Step 5 Click **+** to expand or **-** to collapse the list of ACEs under each ACL. The priority of the ACEs under each ACL is displayed. The order in the list determines priority.

Step 6 (Optional) Click **Find** to search for a Web ACL. Start typing in the field, and the tool searches the beginning characters of every field for a match. You can use wild cards to expand your search. For example, typing *sal* in the Find field matches a Web ACL named sales but not a customization object named wholesalers. If you type **sal* in the Find field, the search finds the first instance of either sales or wholesalers in the table.

Use the up and down arrows to skip up or down to the next string match. Check the **Match Case** check box to make your search case sensitive.

Step 7 (Optional) Highlight a Web ACL and click **Assign** to assign the selected Web ACL to one or more VPN group policies, dynamic access policies, or user policies.

Step 8 When you create an ACE, by default it is enabled. Clear the check box to switch off an ACE.

The IP address or URL of the application or service to which the ACE applies is displayed. The TCP service to which the ACE applies is also displayed. The Action field displays whether the ACE permits or denies Clientless SSL VPN access. The time range associated with the ACE and the logging behavior (either switched off or with a specified level and time interval) is also displayed.

Adding or Editing ACEs

An access control entry (or "access rule") controls access to specific URLs and services. You can configure multiple ACEs for an ACL. ACLs apply ACEs in priority order, acting on the first match.

DETAILED STEPS

Step 1 Permit or deny access to specific networks, subnets, hosts, and Web servers specified in the **Filter Group** field.

Step 2 Specify a URL or an IP address to which to apply the filter (permit or deny user access):

- URL—Applies the filter to the specified URL.
- Protocols (unlabeled)—Specifies the protocol part of the URL address.
- ://x—Specifies the URL of the Web page to which to apply the filter.
- TCP—Applies the filter to the specified IP address, subnet, and port.
- IP Address—Specifies the IP address to which to apply the filter.
- Netmask—Lists the standard subnet mask to apply to the address in the IP Address field.
- Service—Identifies the service (such as https, kerberos, or any) to be matched. Displays a list of services from which you can select the service to display in the Service field.
- Boolean operator (unlabeled)—Lists the Boolean conditions (equal, not equal, greater than, less than, or range) to use in matching the service specified in the service field.

Step 3 The Rule Flow Diagram graphically depicts the traffic flow using the filter. This area may be hidden.

Step 4 Specify the logging rules. The default is Default Syslog.

- Logging—Choose to enable a specific logging level.
- Syslog Level—Grayed out until you select Enable for the Logging attribute. Enables you select the type of syslog messages the ASA displays.
- Log Interval—Lets you select the number of seconds between log messages.
- Time Range—Lets you select the name of a predefined time-range parameter set.

Configuration Examples for ACLs for Clientless SSL VPN

Examples

Here are examples of ACLs for Clientless SSL VPN:

Action	Filter	Effect
Deny	url http://*.yahoo.com/	Denies access to all of Yahoo!
Deny	url cifs://fileserver/share/directory	Denies access to all files in the specified location.
Deny	url https://www.example.com/ directory/file.html	Denies access to the specified file.
Permit	url https://www.example.com/directory	Permits access to the specified location
Deny	url http://*:8080/	Denies HTTPS access to anywhere via port 8080.
Deny	url http://10.10.10.10	Denies HTTP access to 10.10.10.10.
Permit	url any	Permits access to any URL. Usually used after an ACL that denies url access.

Configuring 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**.The following sections describe the integration of browser plug-ins for Clientless SSL VPN browser access:

- About Installing Browser Plug-ins
- Preparing the Security Appliance for a Plug-in
- Installing Plug-ins Redistributed by Cisco

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 menu 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 menu next to the Address field of the portal page.

Table 12-3 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 12-3 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 select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

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

Before installing the first plug-in, you must follow the instructions in the next section.

Prerequisites

- 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

- 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) 1.4.2 (or later) is enabled on the browser. There is no ActiveX version of the RDP plug-in for 64-bit browsers.

RDP Plug-in ActiveX Debug Quick Reference

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

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.

Preparing the Security Appliance for a Plug-in

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.