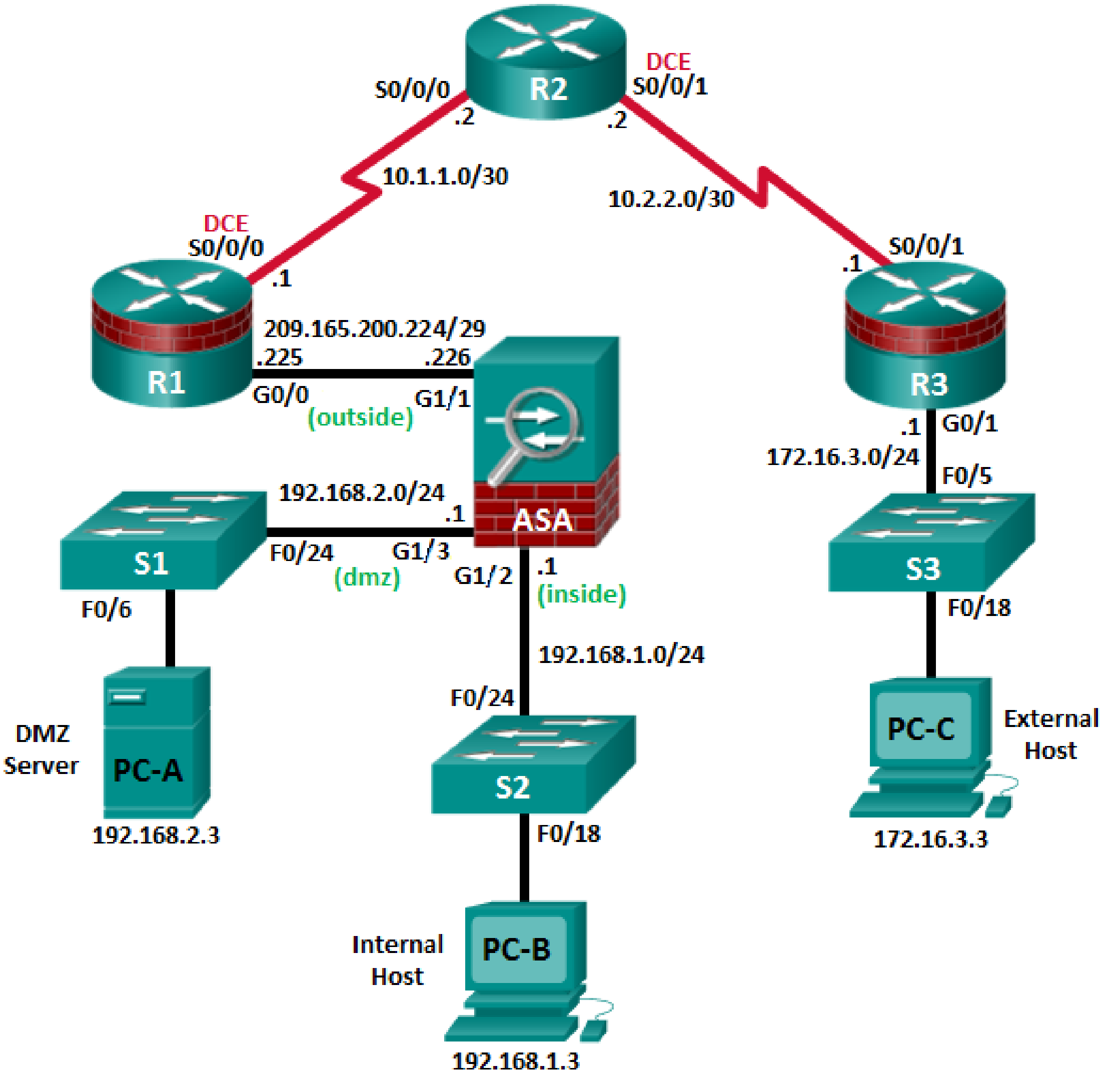
CCNA Security

Chapter 10 – Configure Clientless Remote Access SSL VPNs Using ASDM

This lab has been updated for use on NETLAB+

Topology



Note: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA Gi1/1
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	Gi1/2	192.168.1.1	255.255.255.0	NA	S2 F0/24
	Gi1/1	209.165.200.226	255.255.255.248	NA	R1 G0/0
	Gi1/3	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Basic Router/Switch/PC Configuration

- Configure basic settings for routers.
- Configure PC host IP settings.
- Verify connectivity.
- Save the basic running configuration for each router and switch.

Part 2: Access the ASA Console and ASDM

- Access the ASA console.
- Clear the previous ASA configuration settings.
- Bypass Setup mode.
- Configure the ASA by using the CLI script.
- Access ASDM.

Part 3: Configuring Clientless SSL VPN Remote Access Using ASDM

- Start the VPN wizard.
- Configure the SSL VPN user interface.
- Configure AAA user authentication.
- Configure the VPN group policy.
- Configure a bookmark list (clientless connections only).
- Review the configuration summary and deliver the commands to the ASA.
- Verify the ASDM SSL VPN connection profile.

- Verify VPN access from the remote host.
- Access the web portal page.
- View the clientless remote user session using the ASDM Monitor.

Background / Scenario

In addition to stateful firewall and other security features, the ASA can provide both site-to-site and remote access VPN functionality. The ASA provides two main deployment modes that are found in Cisco SSL remote access VPN solutions:

- **Clientless SSL VPN**—Clientless, browser-based VPN that lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser and built-in SSL to protect VPN traffic. After authentication, users are presented with a portal page and can access specific, predefined internal resources from the portal.
- **Client-Based SSL VPN**—Provides full-tunnel SSL VPN connection, but requires a VPN client application to be installed on the remote host. After authentication, users can access any internal resource as if they were physically on the local network. The ASA supports both SSL and IPsec client-based VPNs.

In Part 1 of this lab, you will configure the topology and non-ASA devices. In Part 2, you will prepare the ASA for ASDM access. In Part 3, you will use the ASDM VPN wizard to configure a clientless SSL remote access VPN and verify access using a remote PC with a browser.

Your company has two locations connected to an ISP. Router R1 represents a CPE device managed by the ISP. Router R2 represents an intermediate Internet router. Router R3 connects users at the remote branch office to the ISP. The ASA is an edge security device that connects the internal corporate network and DMZ to the ISP while providing NAT services to inside hosts.

Management has asked you to provide VPN access, using the ASA as a VPN concentrator, to teleworkers. They want you to test the clientless access model, using SSL and a browser for client access.

Note: The router commands and output in this lab are from a Cisco 1941 router with Cisco IOS Release 15.4(3)M2 (with a Security Technology Package license). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5506 with an 8-port integrated router, running OS version 9.8(1), Adaptive Security Device Manager (ASDM) version 7.8(1), and comes with a Base license.

Part 1: Basic Router/Switch/PC Configuration

In Part 1, you will configure basic settings on the routers such as interface IP addresses and static routing.

Note: Do not configure any ASA settings at this time.

Step 1: Configure R1 using the CLI script.

a. In this step, you will use the following CLI script to configure basic settings on R1. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

   Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

   Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

```
enable
config t
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/0
 ip address 209.165.200.225 255.255.255.248
 no shut
exit
int serial 0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
crypto key generate rsa general-keys modulus 1024
```

Step 2: Configure R2 using the CLI script.

a. In this step, you will use the following CLI script to configure basic settings on R2. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

```
enable
config t
hostname R2
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0
 logging synchronous
exit
interface serial 0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
exit
interface serial 0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 2000000
 no shut
exit
ip route 209.165.200.224 255.255.255.248 Serial0/0/0
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

Step 3: Configure R3 using the CLI script.

a. In this step, you will use the following CLI script to configure basic settings on R3. Copy and paste the basic configuration script commands listed below. Observe the messages as the commands are applied to ensure that there are no warnings or errors.

```
enable
config t
hostname R3
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
username admin01 algorithm-type scrypt secret admin01pass
ip domain name ccnasecurity.com
line con 0
 login local
 exec-timeout 5 0
 logging synchronous
exit
line vty 0 4
 login local
 transport input
 exec-timeout 5 0
 logging synchronous
exit
interface gigabitethernet 0/1
 ip address 172.16.3.1 255.255.255.0
 no shut
exit
int serial 0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shut
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
crypto key generate rsa general-keys modulus 1024
```

Step 4: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing table.

Step 5: Verify connectivity.

Because the ASA is the focal point for the network zones and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the R1 interface G0/0. From PC-C, ping the R1 G0/0 IP address (**209.165.200.225**). If these pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 G0/0 and S0/0/0, you have demonstrated that static routing is configured and functioning correctly.

Step 6: Save the basic running configuration for each router and switch.

Part 2: Accessing the ASA Console and ASDM

Step 1: Clear the previous ASA configuration settings.

a. Use the **write erase** command to remove the **startup-config** file from flash memory.

   Note: The **erase startup-config** IOS command is not supported on the ASA.

b. Use the **reload** command to restart the ASA. This causes the ASA to display in CLI Setup mode. If you see the `System config has been modified. Save? [Y]es/[N]o:` message, type **n**, and press **Enter**.

Step 2: Bypass Setup mode.

When the ASA completes the reload process, it should detect that the startup configuration file is missing and go into Setup mode. If it does not come up in this mode, repeat Step 1.

a. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with **no**.

b. Enter privileged EXEC mode with the **enable** command. The password should be blank (no password).

Step 3: Configure the ASA by using the CLI script.

In this step, you will use a CLI script to configure basic settings, the firewall and DMZ.

a. Other than the defaults that the ASA automatically inserts, use the **show run** command to confirm that there is no previous configuration in the ASA.

b. Enter global configuration mode. When prompted to enable anonymous call-home reporting, respond **no**.

c. Copy and paste the Pre-VPN Configuration Script commands listed below at the ASA global configuration mode prompt to start configuring the SSL VPNs.

   Observe the messages as the commands are applied to ensure that there are no warnings or errors. If prompted to replace the RSA key pair, respond **yes**.

```
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password cisco12345
!
interface Gi1/1
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
 no shut
!
interface Gi1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shut
!
interface Gi1/3
```

```
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
 no shut
!
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
object network dmz-server
 host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
 nat (inside,outside) dynamic interface
!
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
username admin01 password admin01pass
!
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 10
ssh timeout 10
!
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
   inspect icmp
!
crypto key generate rsa modulus 1024
```

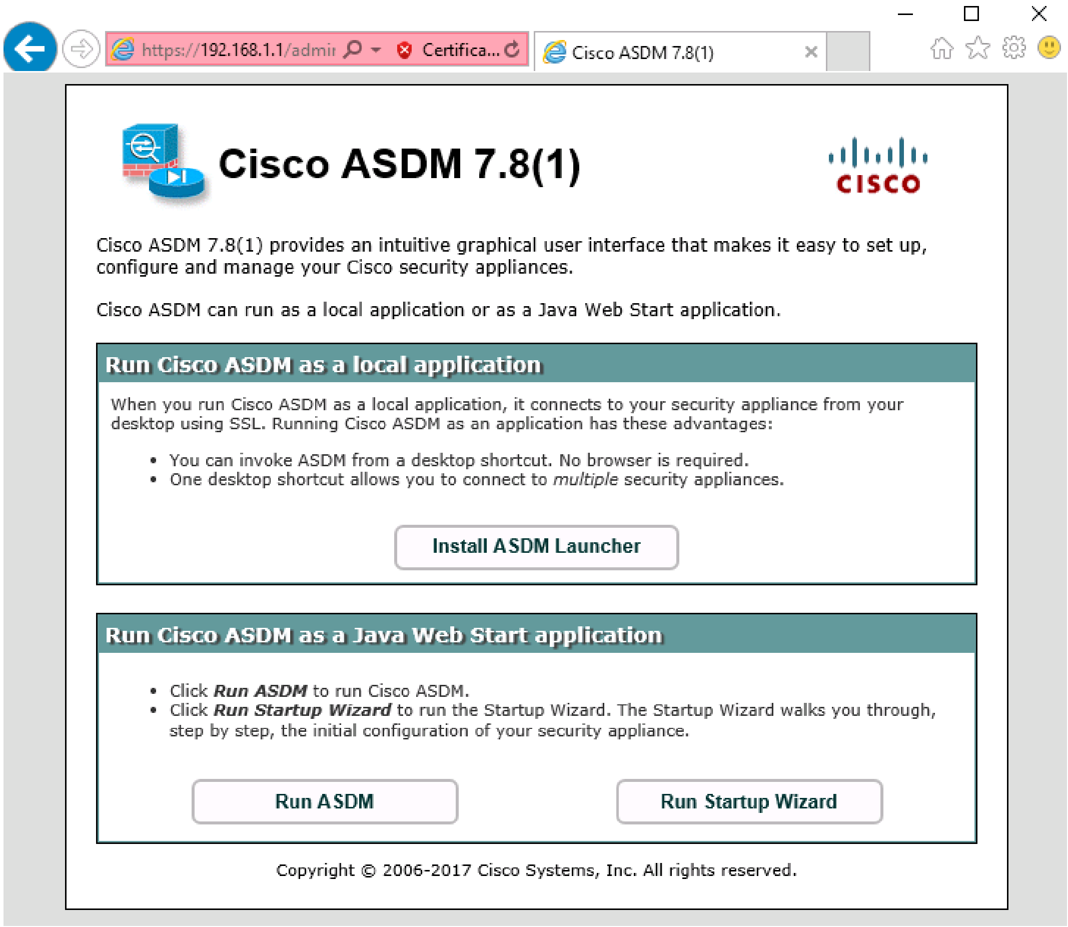
d. At the privileged EXEC mode prompt, issue the **write mem** (or **copy run start**) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.

Step 4: Access ASDM.

a. Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**. After entering the https://192.168.1.1 URL, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings.

   Note: Specify the HTTPS protocol in the URL.

b. At the ASDM welcome page, click **Run ASDM**. The ASDM-IDM Launcher will display. Log in as user **admin01** with password **admin01pass**.



Cisco ASDM 7.8(1)

Cisco ASDM 7.8(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Install ASDM Launcher

Run Cisco ASDM as a Java Web Start application

- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

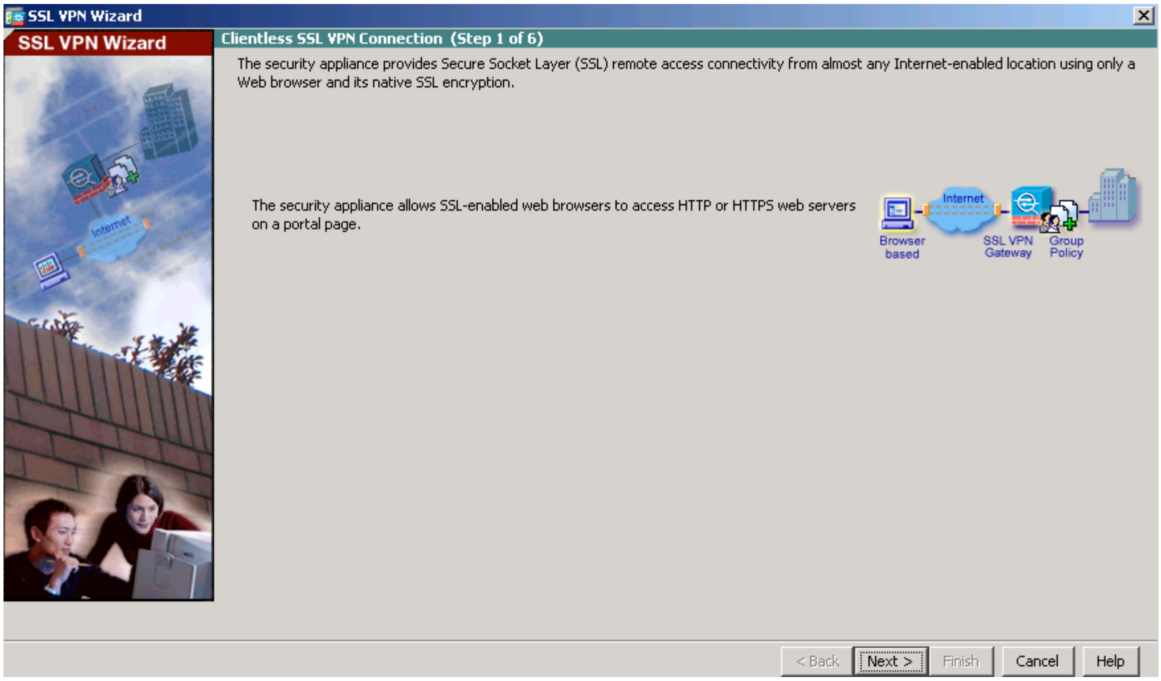
Run ASDM   Run Startup Wizard

Copyright © 2006-2017 Cisco Systems, Inc. All rights reserved.

Part 3: Configuring Clientless SSL VPN Remote Access Using ASDM

Step 1: Start the VPN wizard.

a. On the ASDM main menu, click **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard**. The Clientless SSL VPN Connection screen displays.



SSL VPN Wizard

Clientless SSL VPN Connection (Step 1 of 6)

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption.

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

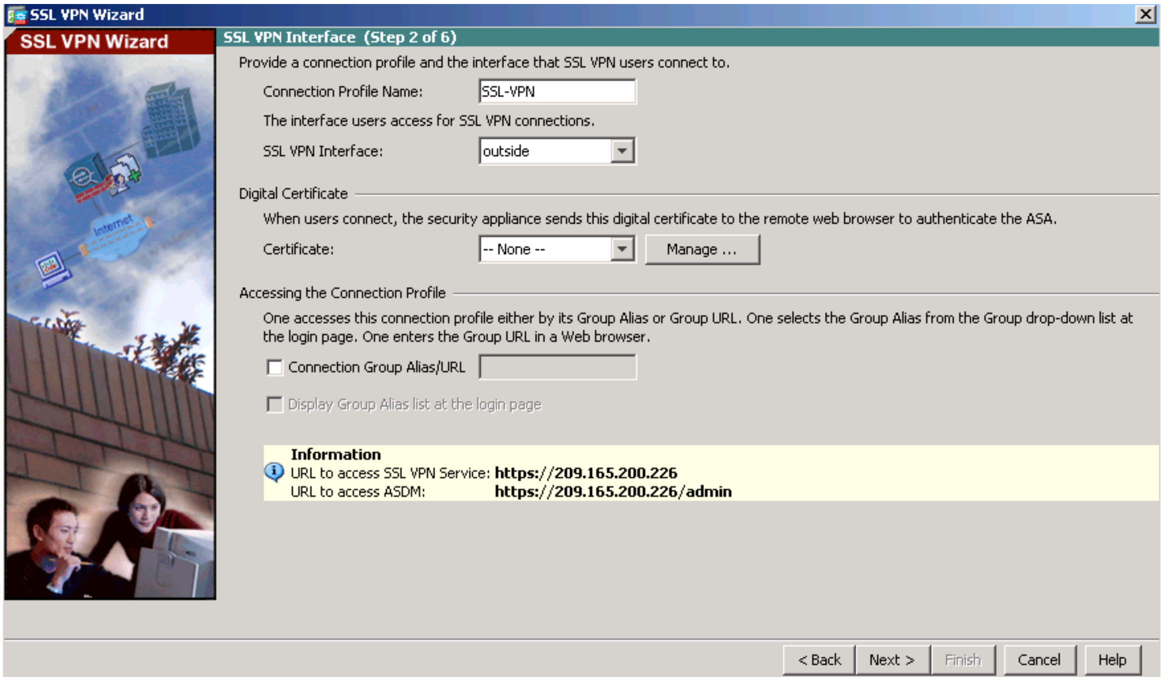
b. Review the on-screen text and topology diagram, and then click **Next** to continue.

Step 2: Configure the SSL VPN user interface.

a. On the SSL VPN Interface screen, configure **SSL-VPN** as the Connection Profile Name, and specify **outside** as the interface to which outside users will connect.

Note: By default, the ASA uses a self-signed certificate to send to the client for authentication. Optionally, the ASA may be configured to use a third-party certificate that is purchased from a well-known certificate authority, such as VeriSign, to connect clients. In the event that a certificate is purchased, it may be selected in the Digital Certificate drop-down menu.

The SSL VPN Interface screen provides links in the Information section. These links identify the URLs that need to be used for the SSL VPN service access (log in) and for Cisco ASDM access (to access the Cisco ASDM software).



SSL VPN Wizard

SSL VPN Interface (Step 2 of 6)

Provide a connection profile and the interface that SSL VPN users connect to.

Connection Profile Name: SSL-VPN

The interface users access for SSL VPN connections.

SSL VPN Interface: outside

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate: -- None --

Accessing the Connection Profile

One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.

□ Connection Group Alias/URL

□ Display Group Alias list at the login page

Information
URL to access SSL VPN Service: **https://209.165.200.226**
URL to access ASDM: **https://209.165.200.226/admin**

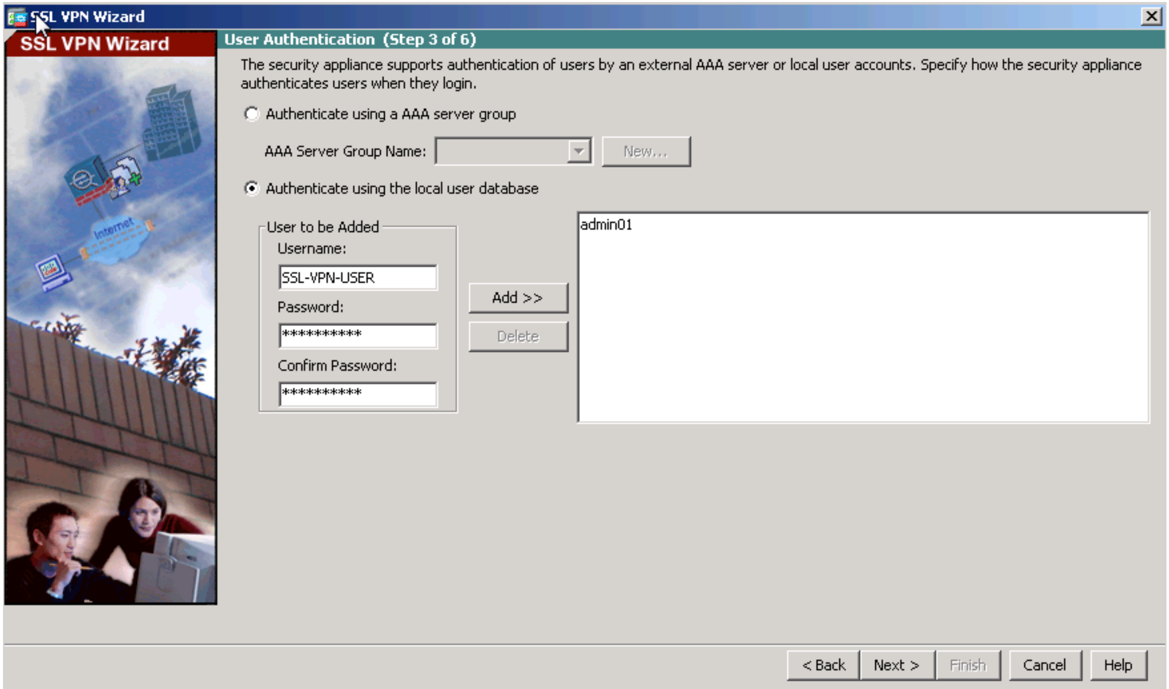
b. Click **Next** to continue.

Step 3: Configure AAA user authentication.

a. On the User Authentication screen, click **Authenticate using the local user database.**

b. Enter the user name **SSL-VPN-USER** with password **cisco12345**.

c. Click **Add** to create the new user and click **Next** to continue.



SSL VPN Wizard

User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

○ Authenticate using a AAA server group

AAA Server Group Name:

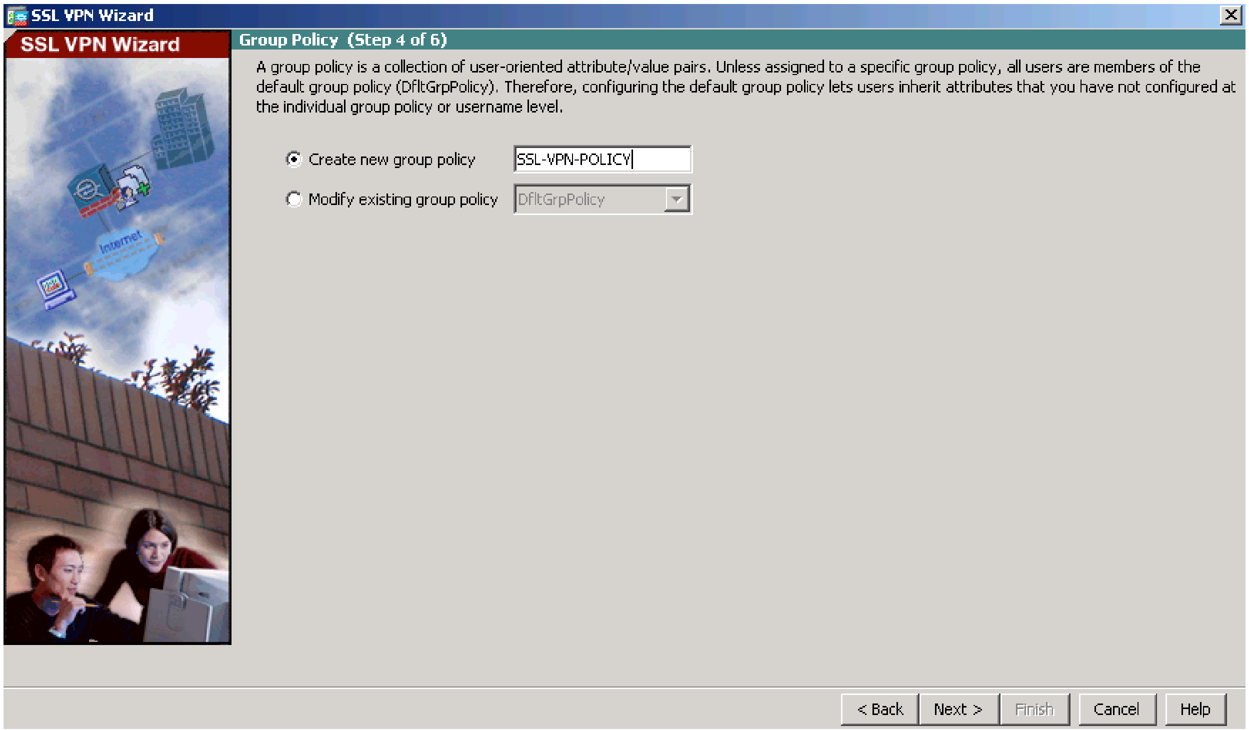
● Authenticate using the local user database

User to be Added
Username: SSL-VPN-USER
Password: **********
Confirm Password: **********

admin01

Step 4: Configure the VPN group policy.

a. On the Group Policy screen, create a new group policy named **SSL-VPN-POLICY**. (When configuring a new policy, the policy name cannot contain any spaces.)



A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

● Create new group policy SSL-VPN-POLICY

○ Modify existing group policy DfltGrpPolicy

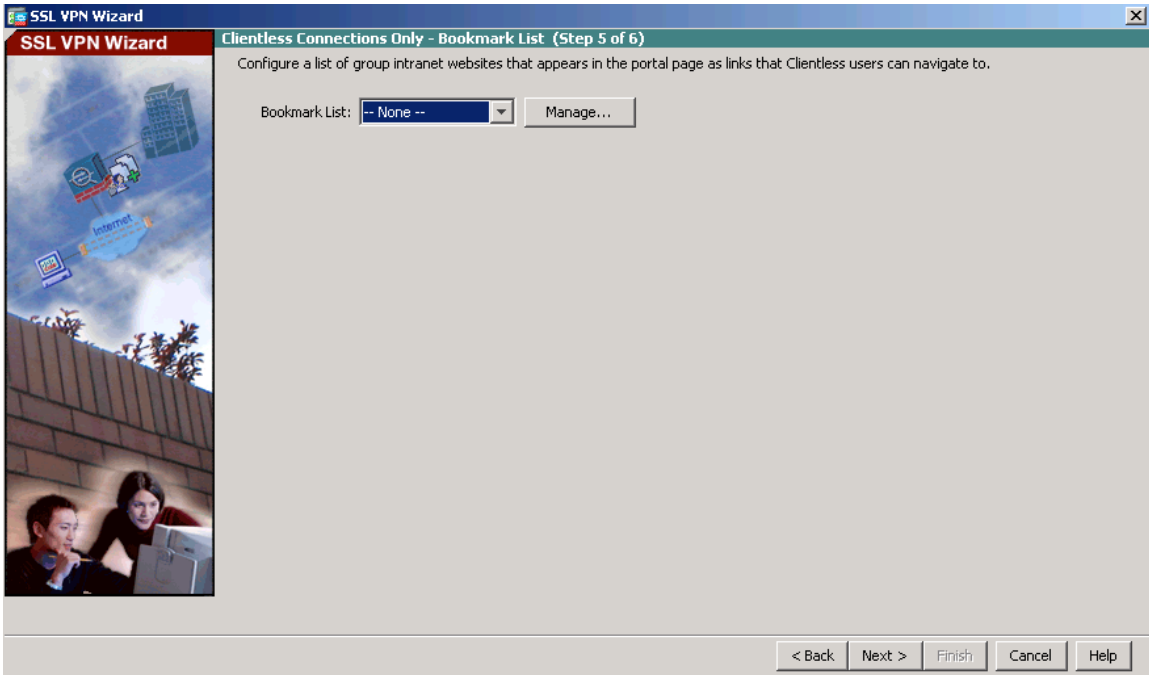
b. Click **Next** to continue.

Step 5: Configure the bookmark list (clientless connections only).

A bookmark list is a set of URLs configured to be used in the clientless SSL VPN web portal.
If there were bookmarks already listed, you would use the **Bookmark List** drop-down list, select the bookmark of choice, and click **Next** to continue with the SSL VPN wizard.

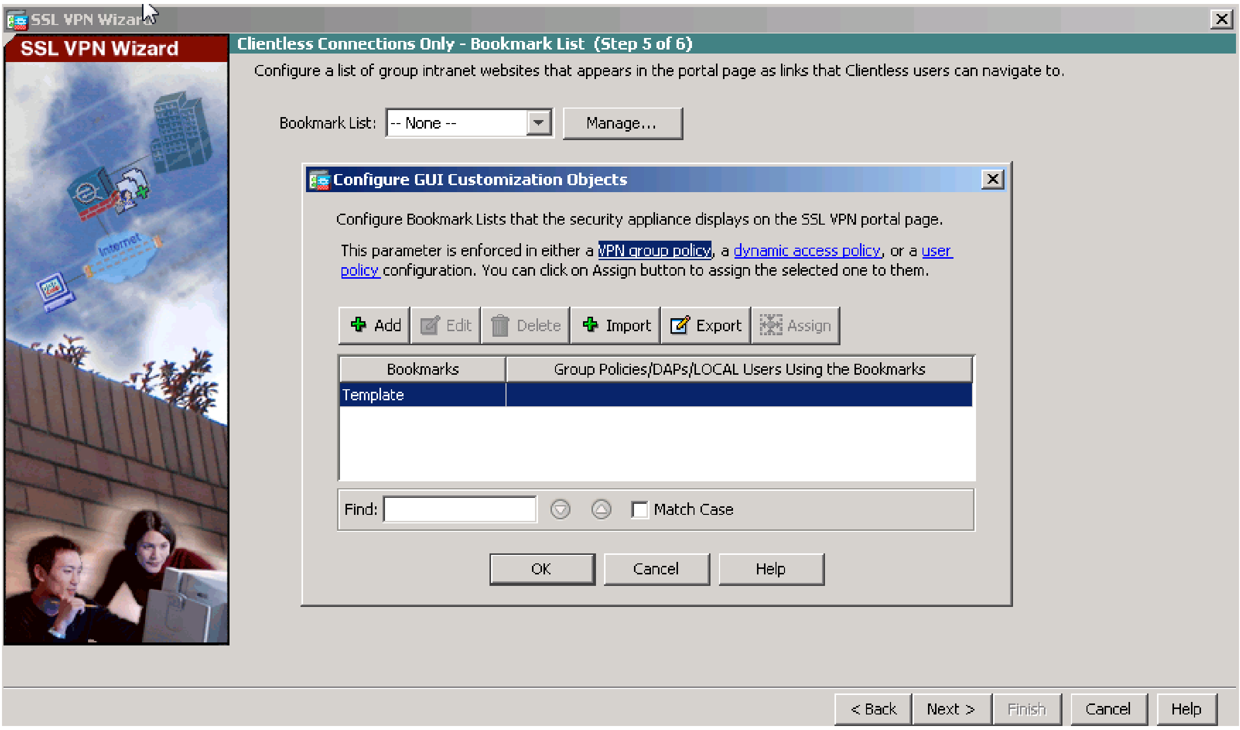
Note: There are no configured bookmark lists by default and, therefore, they must be configured by the network administrator.

a. On the Clientless Connections Only – Bookmark List screen, click **Manage** to create an HTTP server bookmark in the bookmark list.

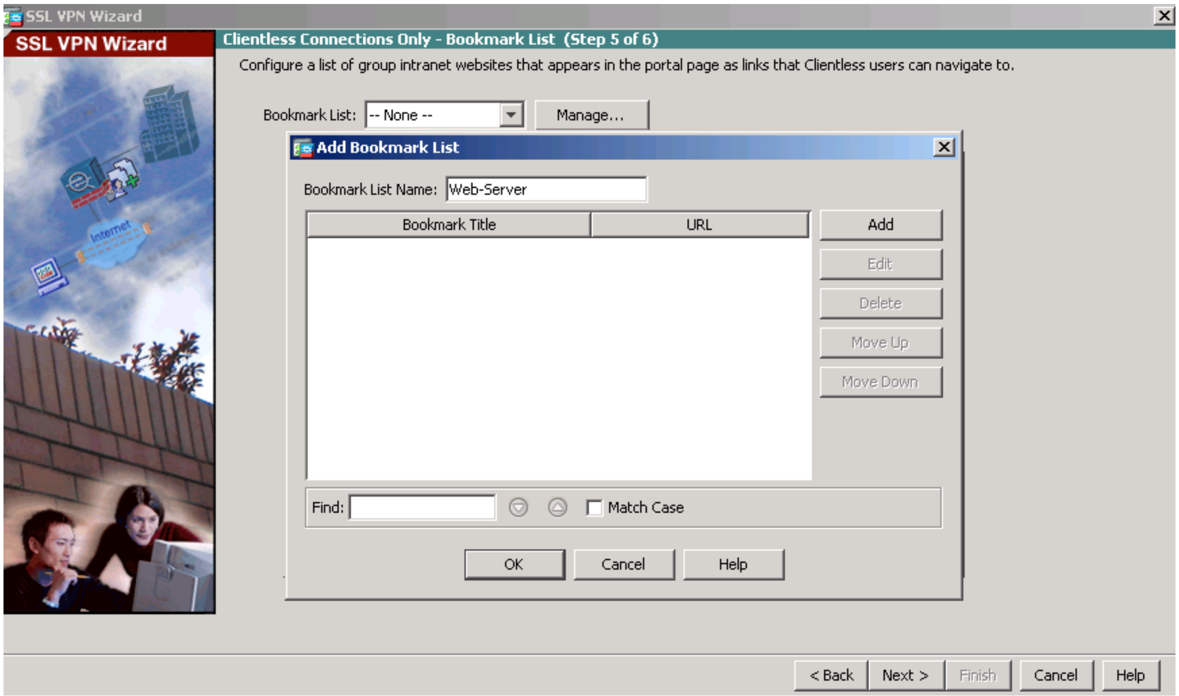

SSL VPN Wizard
SSL VPN Wizard
Clientless Connections Only - Bookmark List (Step 5 of 6)
Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.
Bookmark List: -- None --
Manage...
< Back
Next >
Finish
Cancel
Help

b. In the Configure GUI Customization Objects window, click **Add** to open the Add Bookmark List window. Name the list **Web-Server**.

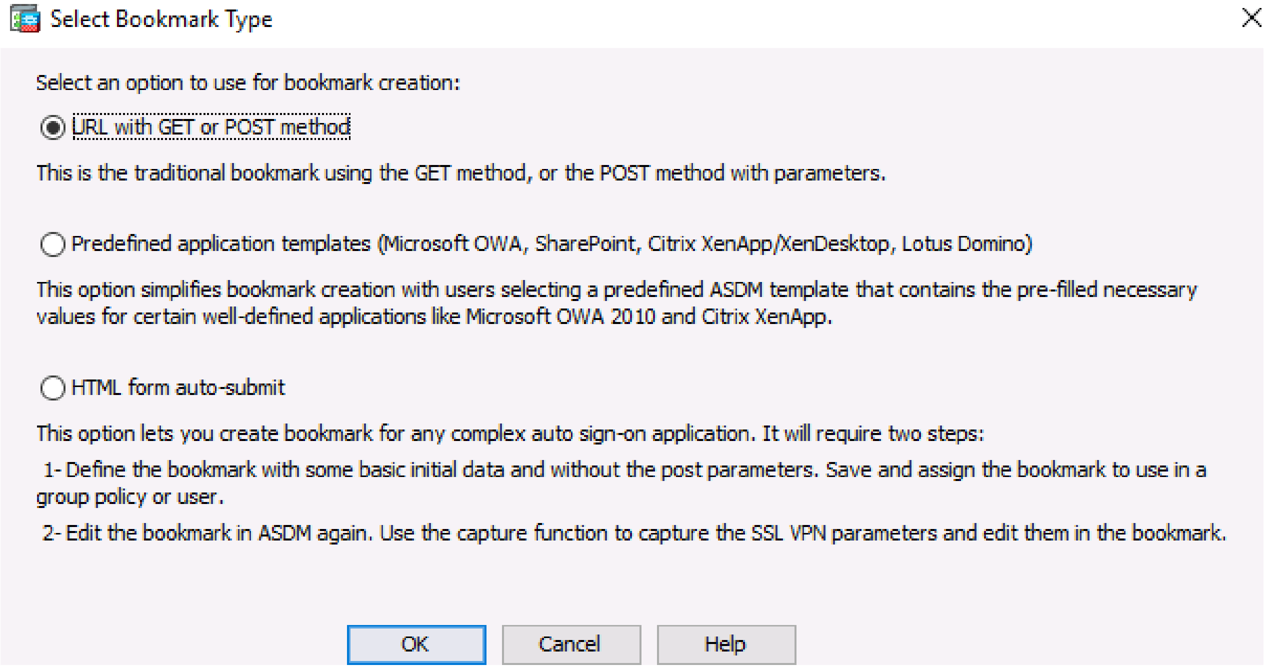
Note: If the Web-Server bookmark list is shown as available from a previous configuration, you can delete it in ASDM and re-create it.


SSL VPN Wizard
SSL VPN Wizard
Clientless Connections Only - Bookmark List (Step 5 of 6)
Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.
Bookmark List: -- None --
Manage...
Configure GUI Customization Objects
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.
Add
Edit
Delete
Import
Export
Assign
Bookmarks
Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template
Find:
Match Case
OK
Cancel
Help
< Back
Next >
Finish
Cancel
Help

c. In the Add Bookmark List window, click **Add** to open the Select Bookmark Type window.


SSL VPN Wizard
SSL VPN Wizard
Clientless Connections Only - Bookmark List (Step 5 of 6)
Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.
Bookmark List: -- None --
Manage...
Add Bookmark List
Bookmark List Name: Web-Server
Bookmark Title
URL
Add
Edit
Delete
Move Up
Move Down
Find:
Match Case
OK
Cancel
Help
< Back
Next >
Finish
Cancel
Help

d. As shown in the figure, the ASDM can create three types of bookmarks. Select the **URL with GET or POST method**, click **OK.**


Select Bookmark Type

Select an option to use for bookmark creation:

● URL with GET or POST method

This is the traditional bookmark using the GET method, or the POST method with parameters.

○ Predefined application templates (Microsoft OWA, SharePoint, Citrix XenApp/XenDesktop, Lotus Domino)

This option simplifies bookmark creation with users selecting a predefined ASDM template that contains the pre-filled necessary values for certain well-defined applications like Microsoft OWA 2010 and Citrix XenApp.

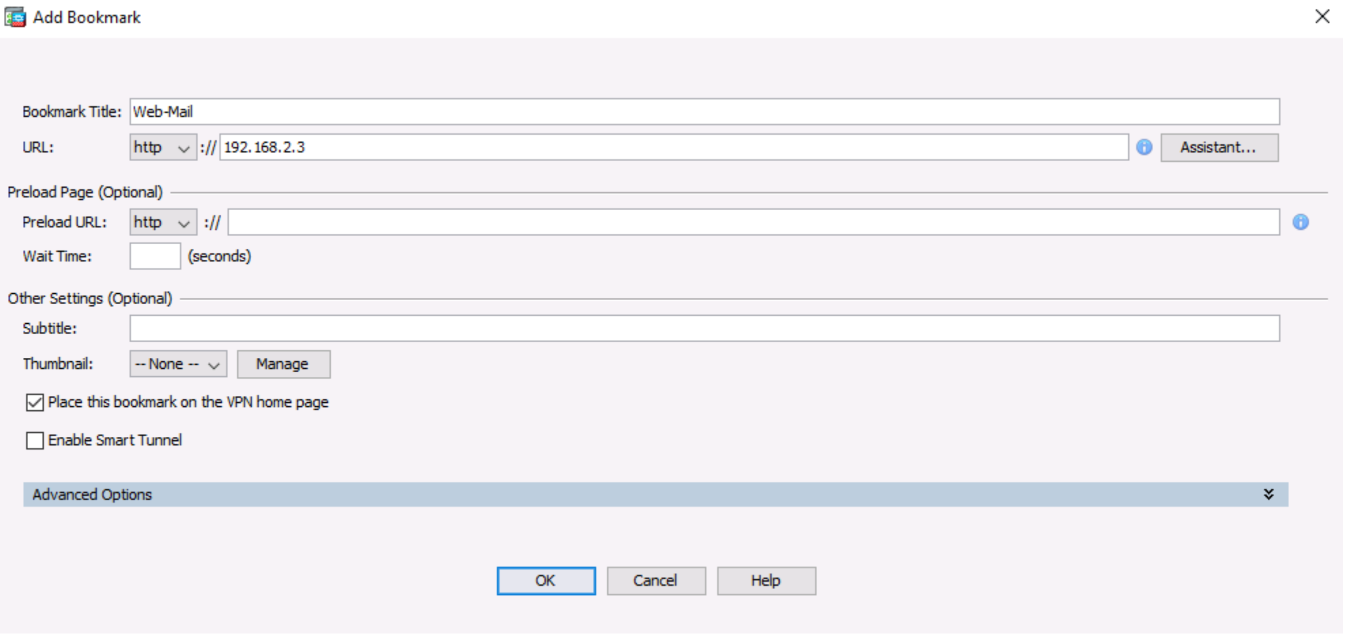
○ HTML form auto-submit

This option lets you create bookmark for any complex auto sign-on application. It will require two steps:

1- Define the bookmark with some basic initial data and without the post parameters. Save and assign the bookmark to use in a group policy or user.

2- Edit the bookmark in ASDM again. Use the capture function to capture the SSL VPN parameters and edit them in the bookmark.

e. Enter the bookmark title and enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the Bookmark Title of **Web-Mail** is entered and an internal IP address of **192.168.2.3** (the DMZ server) is specified. If this server has HTTP web services with web mail installed and functional, the outside users are able to access the server from the ASA portal when they connect.


Add Bookmark

Bookmark Title: Web-Mail

URL: http :// 192.168.2.3

Preload Page (Optional)

Preload URL: http ://

Wait Time: (seconds)

Other Settings (Optional)

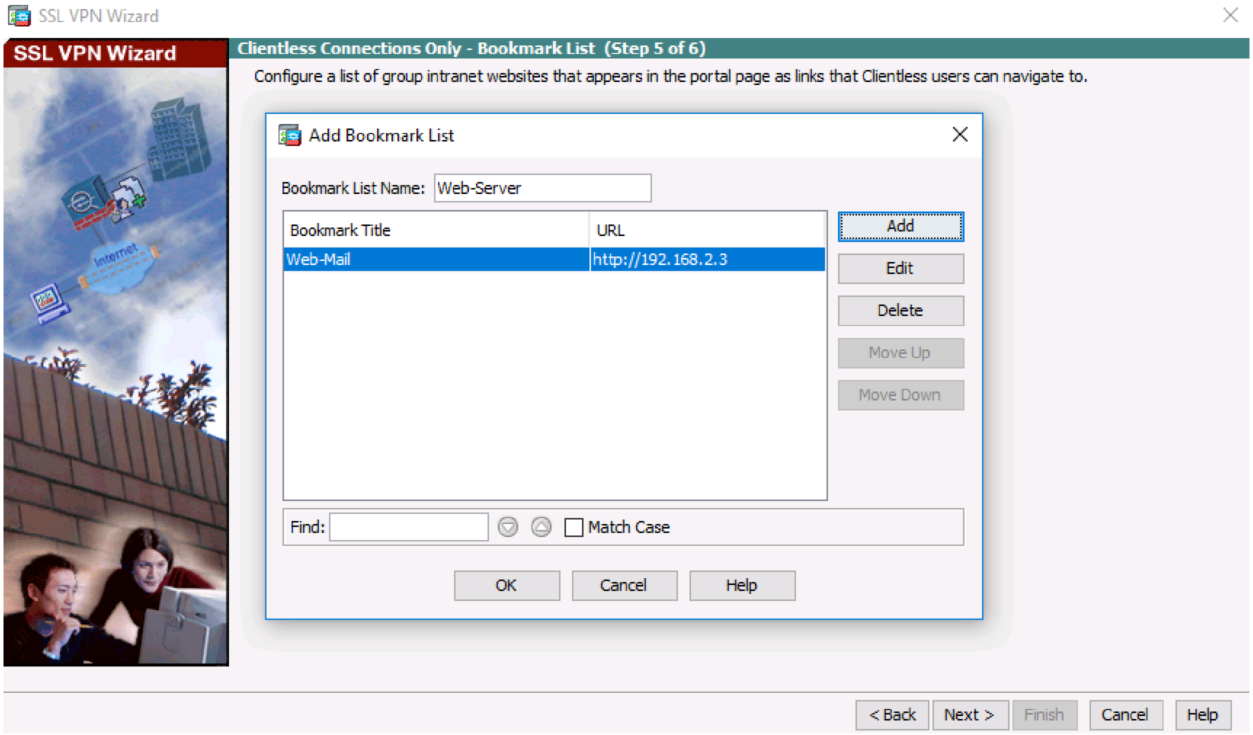
Subtitle:

Thumbnail: -- None --

☑ Place this bookmark on the VPN home page

☐ Enable Smart Tunnel

f. Click **OK** to continue and return to the Add Bookmark List window which now displays the Web-Server bookmark title and URL.


SSL VPN Wizard

Clientless Connections Only - Bookmark List (Step 5 of 6)

Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.

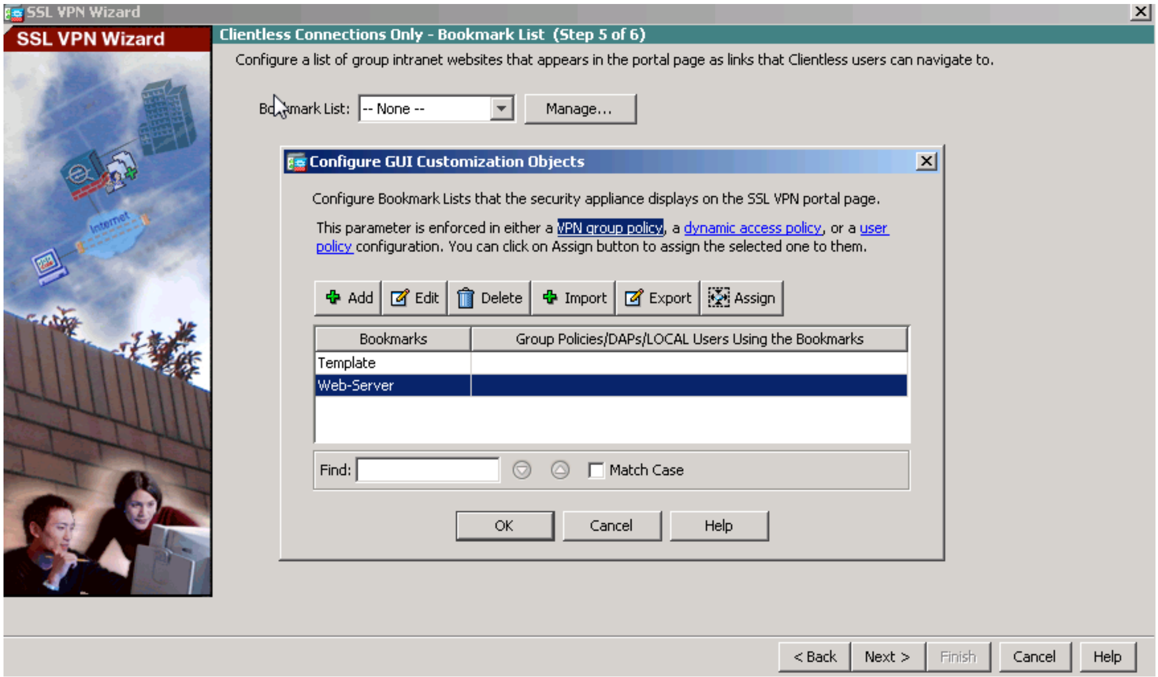
Add Bookmark List

Bookmark List Name: Web-Server

Bookmark Title	URL
Web-Mail	http://192.168.2.3

Find: ☐ Match Case

g. Click **OK** to continue and return to the Configure GUI Customization Objects window which now displays the Web-Server bookmark.



Clientless Connections Only - Bookmark List (Step 5 of 6)

Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.

Bookmark List: -- None --

Configure GUI Customization Objects

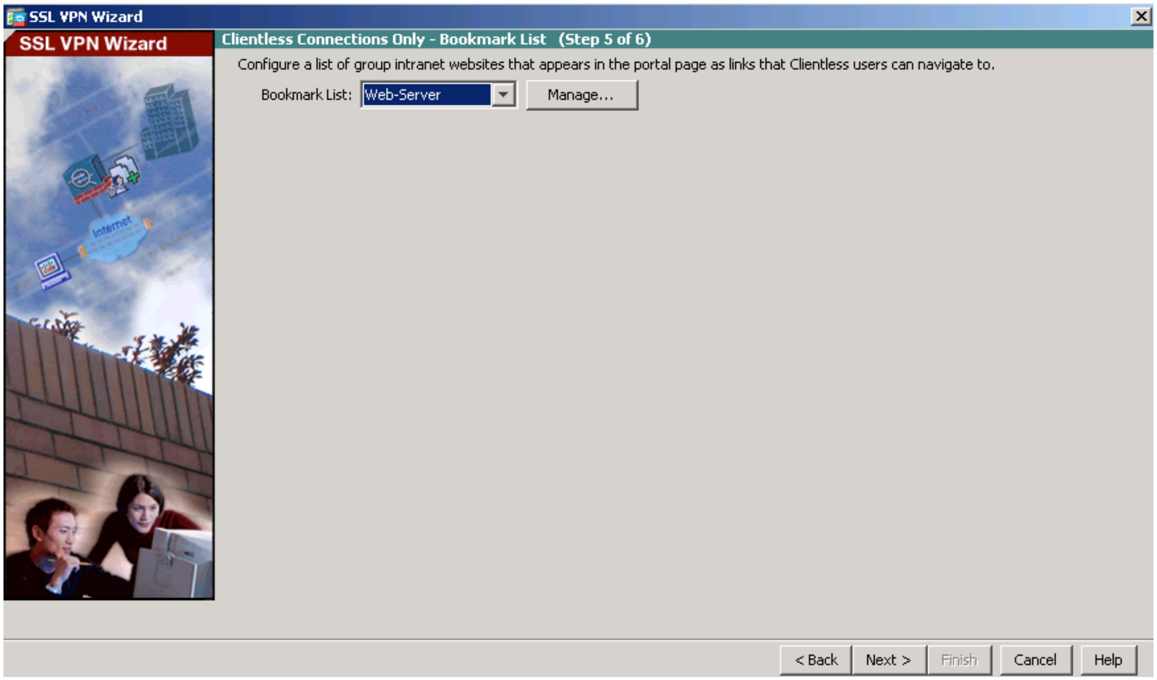
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

This parameter is enforced in either a VPN group policy, a dynamic access policy, or a user policy configuration. You can click on Assign button to assign the selected one to them.

Bookmarks	Group Policies/DAPs/LOCAL Users Using the Bookmarks
Template	
Web-Server	

Find: □ Match Case

h. Click **OK** to continue and return to the Bookmark List window and click **Next** to continue.



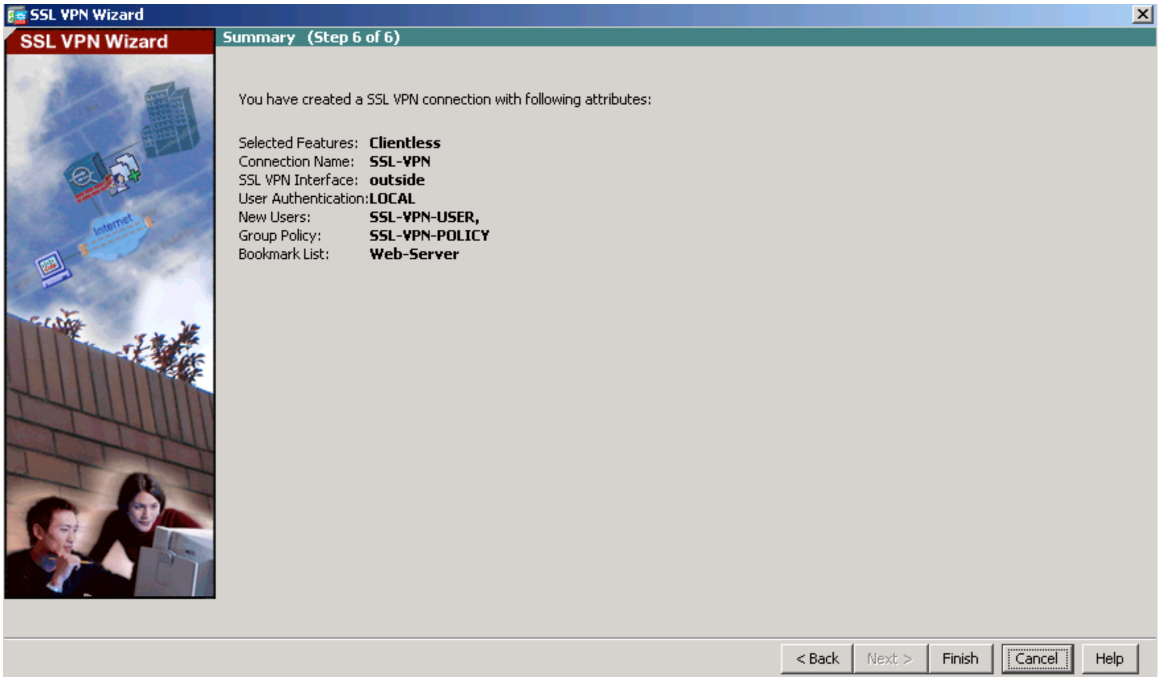
Clientless Connections Only - Bookmark List (Step 5 of 6)

Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.

Bookmark List: Web-Server

Step 6: Review the configuration summary and deliver the commands to the ASA.

The Summary page is displayed next. Verify that the information configured in the SSL VPN wizard is correct. Click **Back** to make changes, or click **Cancel** and restart the VPN wizard. Click **Finish** to complete the process and deliver the commands to the ASA

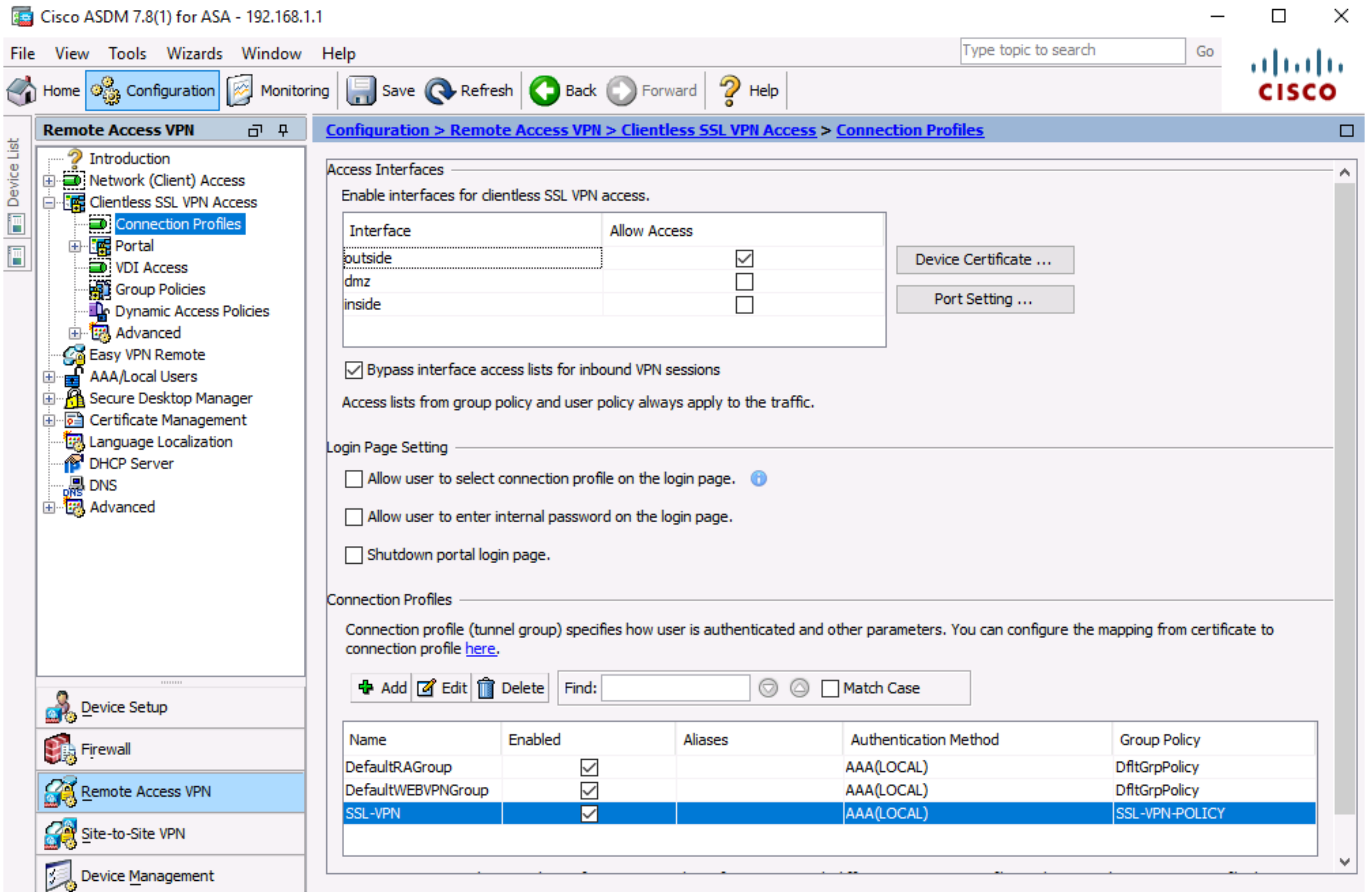


You have created a SSL VPN connection with following attributes:

```
Selected Features:  Clientless
Connection Name:    SSL-VPN
SSL VPN Interface:  outside
User Authentication:LOCAL
New Users:          SSL-VPN-USER,
Group Policy:       SSL-VPN-POLICY
Bookmark List:      Web-Server
```

Step 7: Verify the ASDM SSL VPN connection profile.

In ASDM, click **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**. In this window, the VPN configuration can be verified and edited.



Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	☑
dmz	□
inside	□

Device Certificate ... Port Setting ...

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

□ Allow user to select connection profile on the login page.

□ Allow user to enter internal password on the login page.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

Add Edit Delete Find: □ Match Case

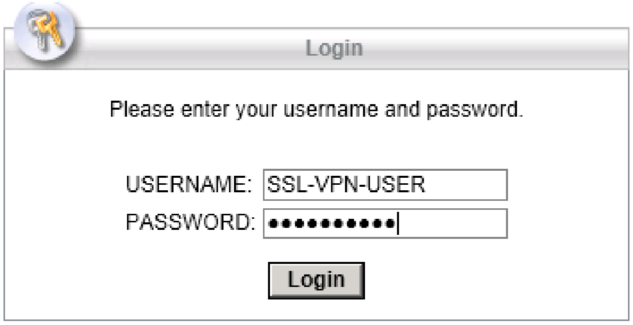
Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	☑		AAA(LOCAL)	DfltGrpPolicy
SSL-VPN	☑		AAA(LOCAL)	SSL-VPN-POLICY

Step 8: Verify VPN access from the remote host.

a. Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (**https://209.165.200.226**). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA.

Note: If you encounter a prompt stating that the connection is not trusted or secure, accept the self-signed certificate to continue.

b. The Logon window should display. Enter the previously configured username **SSL-VPN-USER** and password **cisco12345,** and click **Logon** to continue.



Please enter your username and password.

USERNAME: SSL-VPN-USER

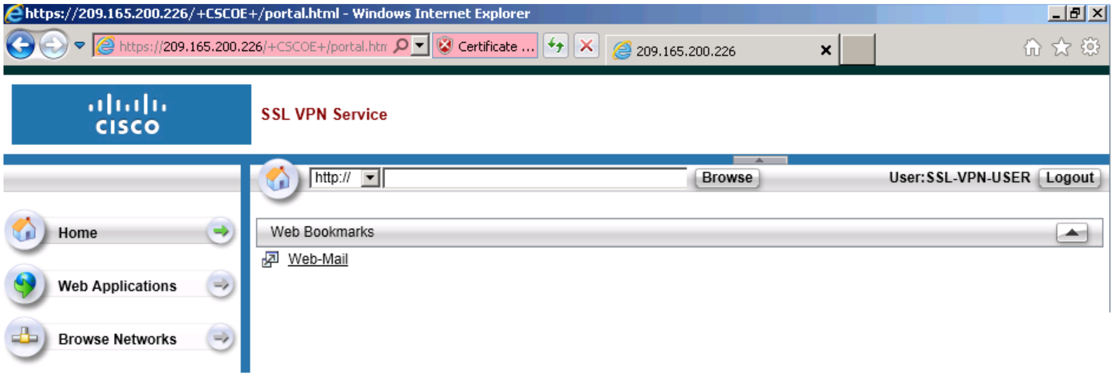
PASSWORD: ●●●●●●●●●●

Login

Step 9: Access the web portal window.

After the user authenticates, the ASA SSL web portal page lists the various bookmarks previously assigned to the profile. If the Bookmark points to a valid server IP address or hostname that has HTTP web services installed and functional, the outside user will be able to access the server from the ASA portal.

Note: In this lab, the web mail server is not installed.



https://209.165.200.226/+CSCOE+/portal.html - Windows Internet Explorer

https://209.165.200.226/+CSCOE+/portal.htm

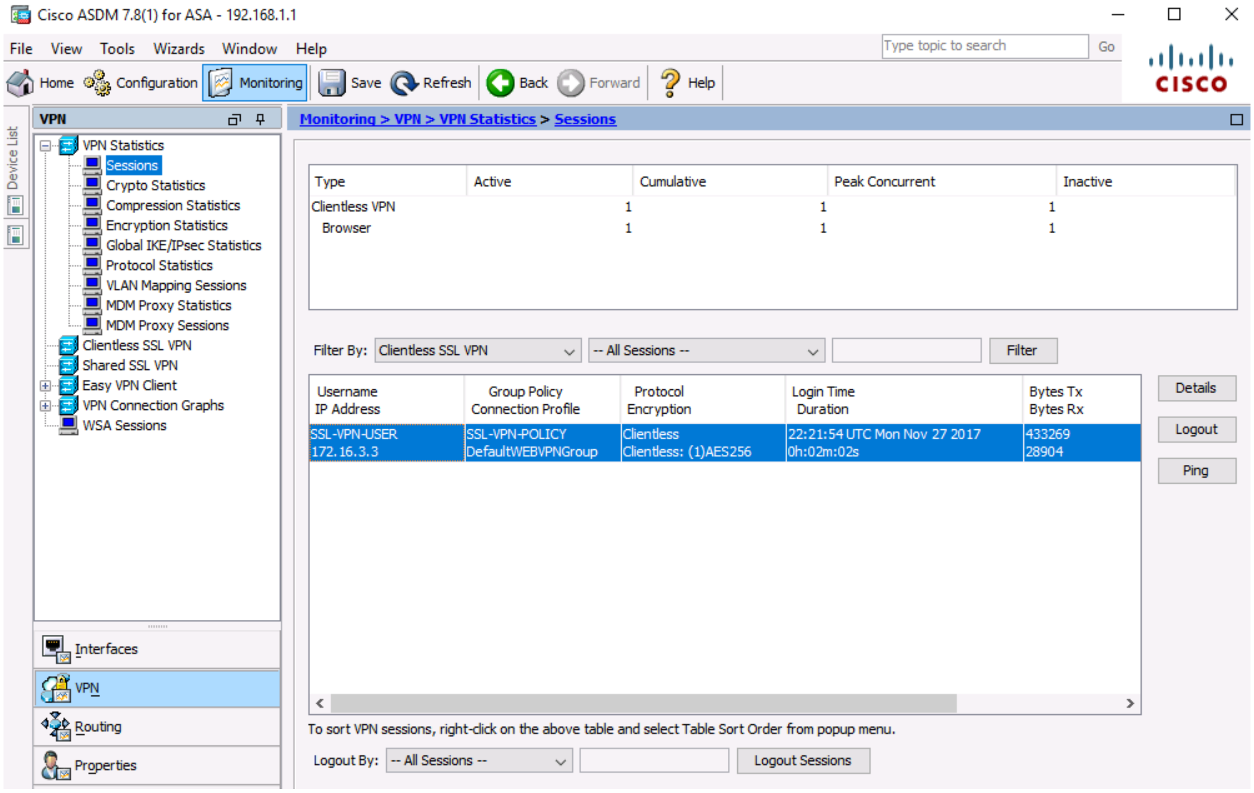
User:SSL-VPN-USER

Step 10: View the clientless remote user session using the ASDM Monitor.

While the remote user at PC-C is still logged in and on the ASA portal page, you can view the session statistics using ASDM monitor.

From the ASDM menu bar on PC-B, click **Monitoring** and then select **VPN** > **VPN Statistics** > **Sessions**. Click the **Filter By** pull-down list and select **Clientless SSL VPN**. You should see the SSL-VPN-USER session logged in from PC-C (172.16.3.3).

Note: You may need to click **Refresh** to display the remote user session.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1

Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Clientless VPN	1	1	1	
Browser	1	1	1	

Filter By: Clientless SSL VPN -- All Sessions --

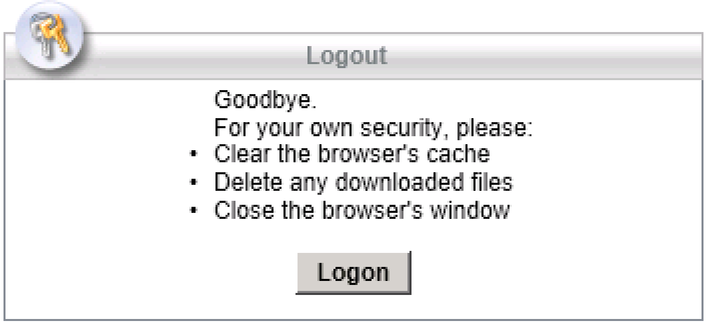
Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
SSL-VPN-USER 172.16.3.3	SSL-VPN-POLICY DefaultWEBVPNGroup	Clientless Clientless: (1)AES256	22:21:54 UTC Mon Nov 27 2017 0h:02m:02s	433269 28904

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Step 11: Log out of the web portal page.

The user should log out of the web portal window on PC-C using the **Logout** button when done. However, the web portal will also time out if there is no activity. In either case a logout window will be displayed informing users that for additional security, they should clear the browser cache, delete the downloaded files, and close the browser window.



Goodbye.
For your own security, please:

- Clear the browser's cache
- Delete any downloaded files
- Close the browser's window

Reflection

1. What are some benefits of clientless vs. client-based VPNs?

____

____

____

____

____

____

2. What are some differences when using SSL as compared to IPsec for remote access tunnel encryption?

____

____

____

____

____

____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.