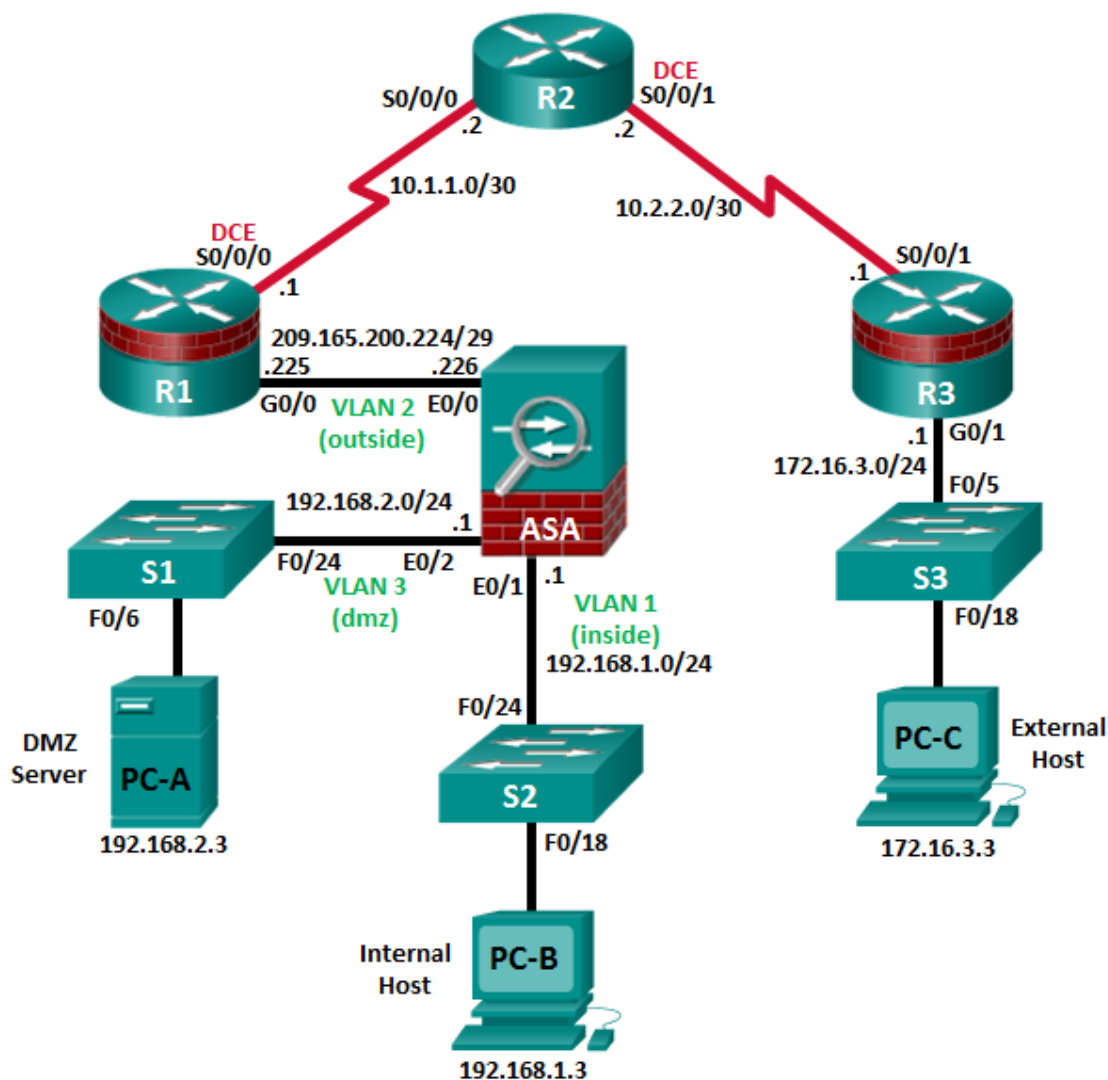


## CCNA Security

## Chapter 10 – Configure Clientless Remote Access SSL VPNs Using ASDM

## 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 E0/0
	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	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA	R1 G0/0
	VLAN 3 (E0/2)	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

- Cable the network and clear previous device settings, as shown in the topology.
- 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 output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5505 with an 8-port integrated switch, running OS version 9.2(3) and ASDM version 7.4(1) and comes with a Base license that allows a maximum of three VLANs.

**Note:** Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

## Required Resources

- 1 ASA 5505 (OS version 9.2(3) and ASDM version 7.4(1) and Base license or comparable)
- 3 routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology package license)
- 3 switches (Cisco 2960 or comparable) (not required)
- 3 PCs (Windows 7 or Windows 8.1, with SSH Client software installed)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

## Part 1: Basic Router/Switch/PC Configuration

In Part 1, you will set up the network topology and 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: Cable the network and clear previous device settings.

Attach the devices shown in the topology diagram and cable as necessary. Ensure that the routers and switches have been erased and have no startup configurations.

### Step 2: Configure R1 using the CLI script.

- 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.

```
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 3: 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.

```
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 4: 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.

```
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 5: 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 6: 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 7: 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 2.

- 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 kept 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 Ethernet0/0
  switchport access vlan 2
  no shut
!
interface Ethernet0/1
  switchport access vlan 1
  no shut
!
interface Ethernet0/2
  switchport access vlan 3
  no shut
!
```

```
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
  no forward interface Vlan1
  nameif dmz
  security-level 70
  ip address 192.168.2.1 255.255.255.0
!
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
```

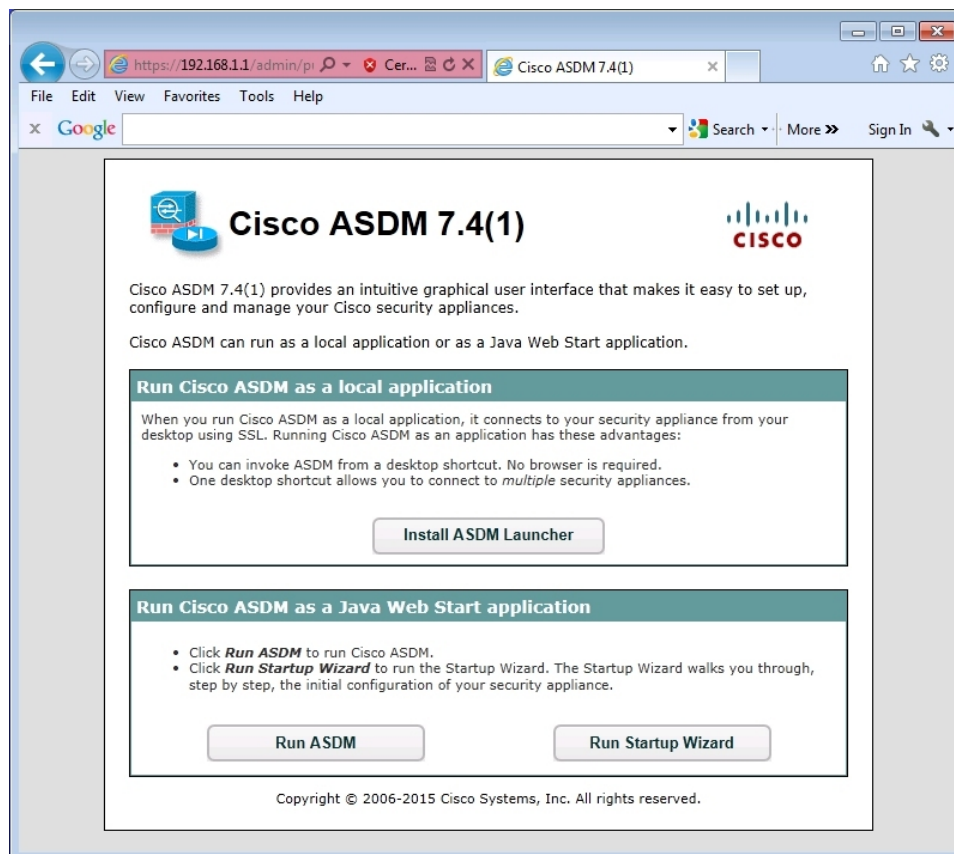
- d. At the privileged EXEC mode prompt, issue the **write mem** (or **copy run start**) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.

#### 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.



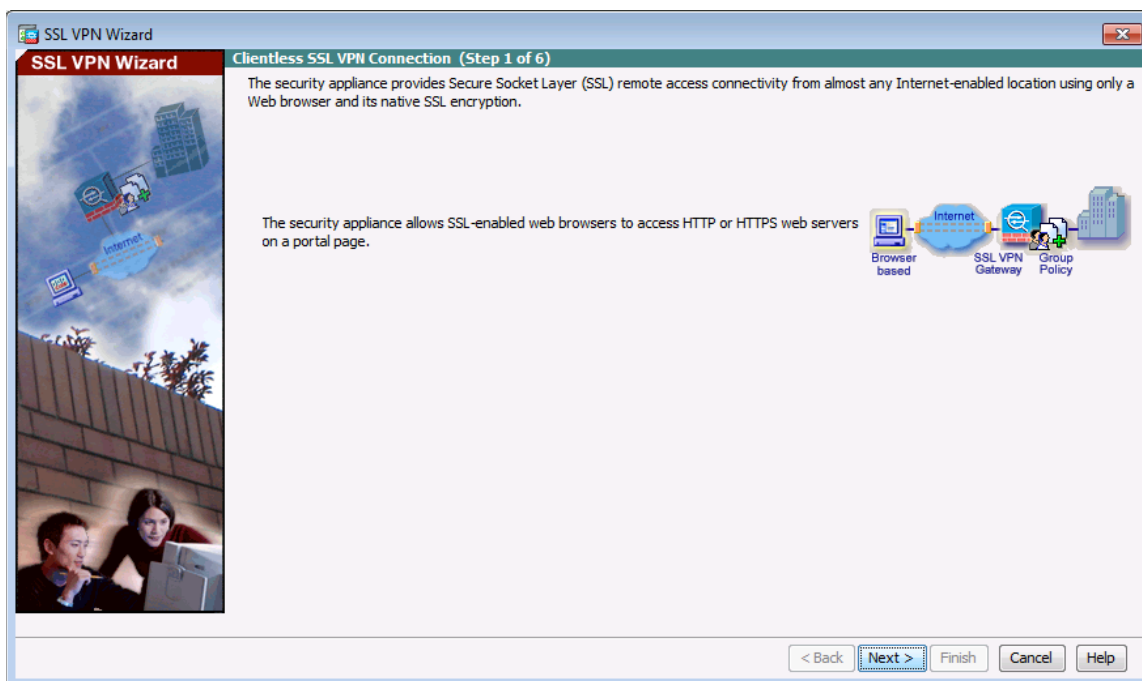
- c. Log in as user **admin01** with password **admin01pass**.



## 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 SSL VPN wizard Clientless SSL VPN Connection screen displays.



- 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).

The screenshot shows the 'SSL VPN Wizard' window, specifically the 'SSL VPN Interface (Step 2 of 6)' screen. The window has a sidebar on the left with a graphic of a globe and a person at a computer. The main area contains the following configuration options:

- Connection Profile Name:** A text box containing 'SSL-VPN'.
- The interface users access for SSL VPN connections.**
- SSL VPN Interface:** A dropdown menu showing 'outside'.
- Digital Certificate**
  - Text: 'When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.'
  - Certificate:** A dropdown menu showing '-- None --' and a 'Manage ...' button.
- Accessing the Connection Profile**
  - Text: '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** (with an empty text box)
  - ☐ **Display Group Alias list at the login page**
- Information** (highlighted in yellow)
  - URL to access SSL VPN Service: <https://209.165.200.226>
  - URL to access ASDM: <https://209.165.200.226/admin>

At the bottom right, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- b. Click **Next** to continue.

**Step 3: Configure AAA user authentication.**

- On the User Authentication screen, click **Authenticate using the local user database**.
- Enter the user name **SSL-VPN-USER** with password **cisco12345**.
- 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:

Password:

Confirm Password:

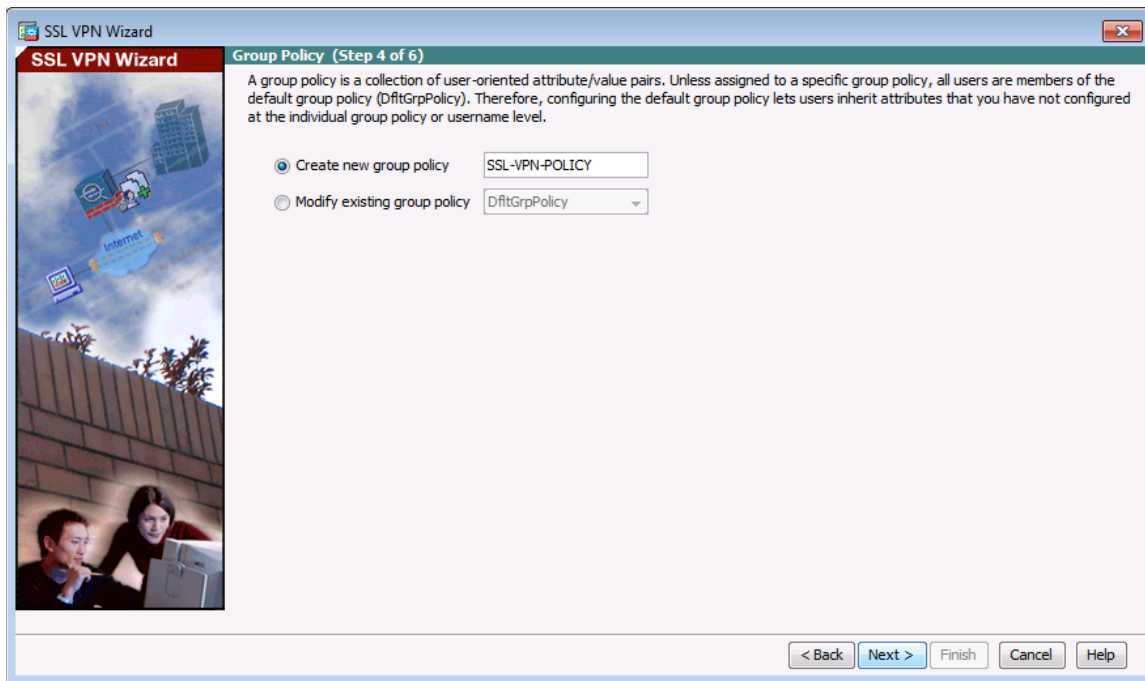
admin01

< Back Next > Finish Cancel Help

**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.)

**Note:** By default, the created user group policy inherits its settings from the DfltGrpPolicy. These settings may be modified after the wizard has been completed by navigating to the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** submenu.



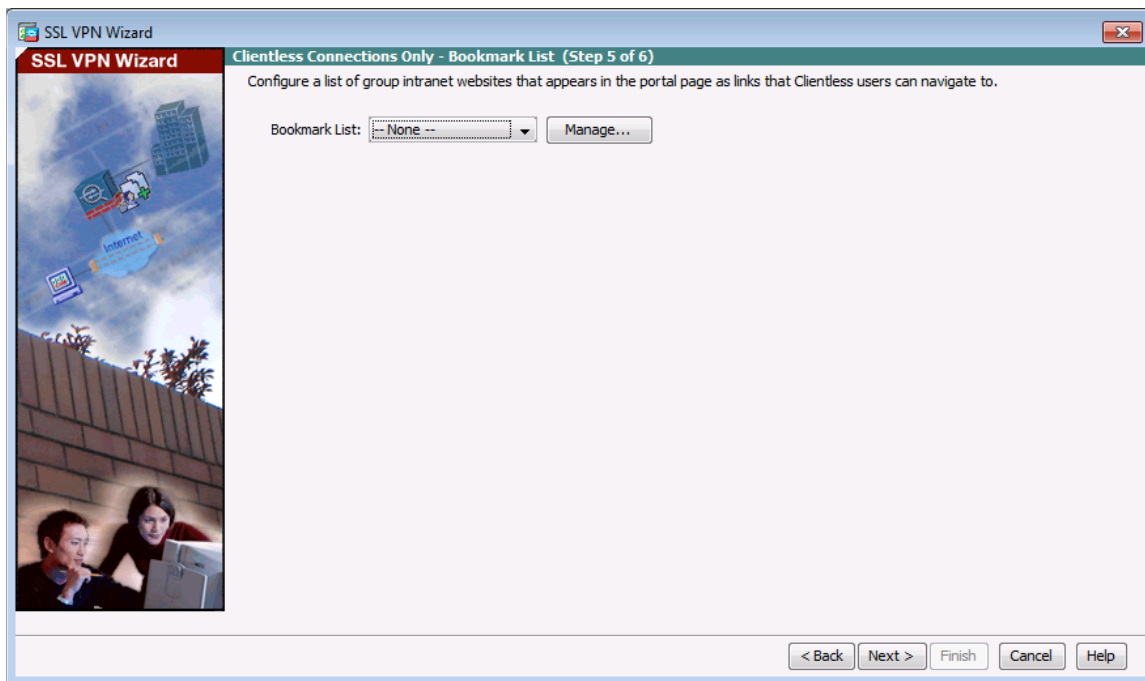
- b. Click **Next** to continue.

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

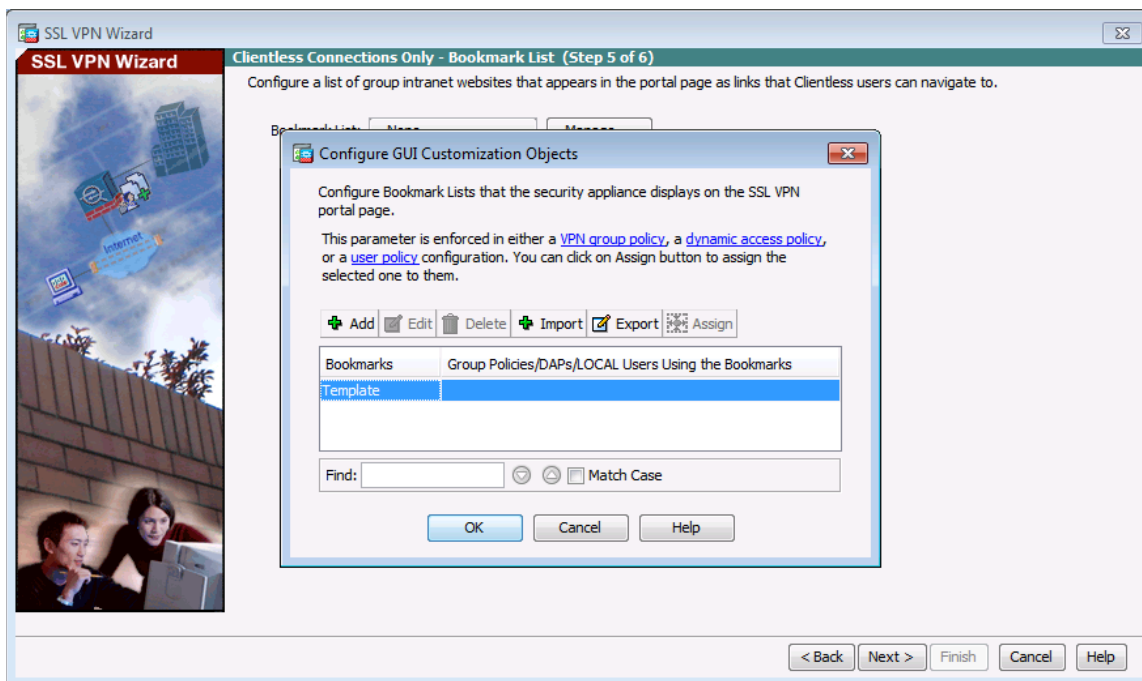
A bookmark list is a set of URLs configured to be used in the clientless SSL VPN web portal. If there are bookmarks already listed, use the **Bookmark List** drop-down list, select the bookmark of choice, and click **Next** to continue with the SSL VPN wizard.

**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.

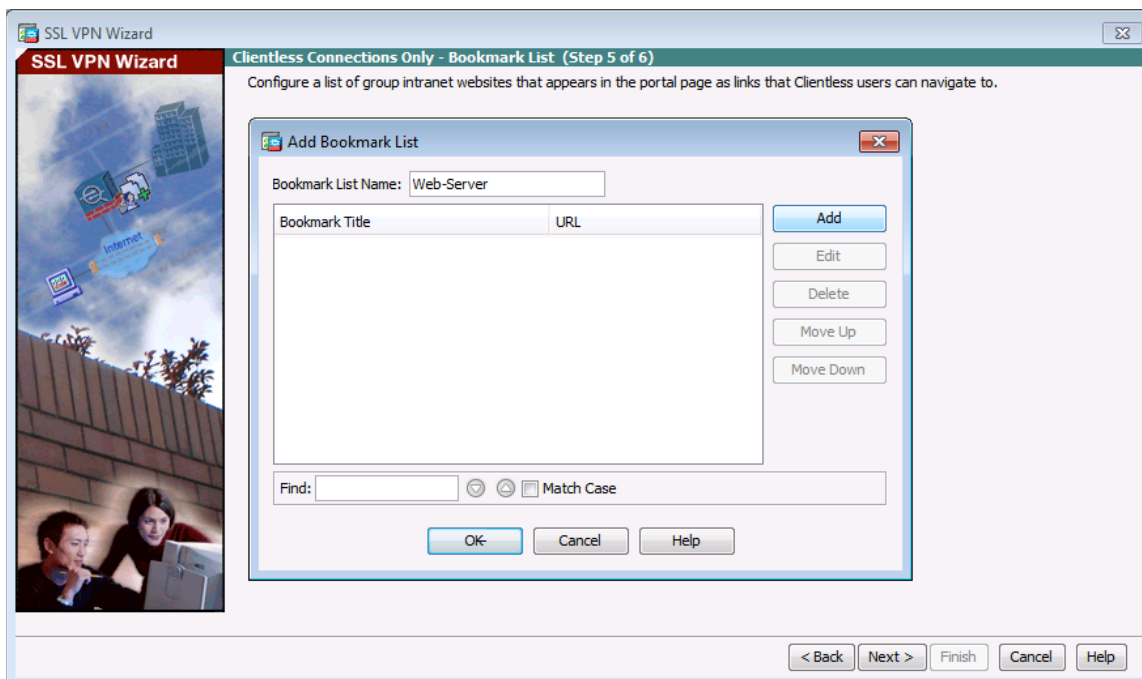


- b. In the Configure GUI Customization Objects window, click **Add** to open the Add Bookmark List window. Name the list **Web-Server**.

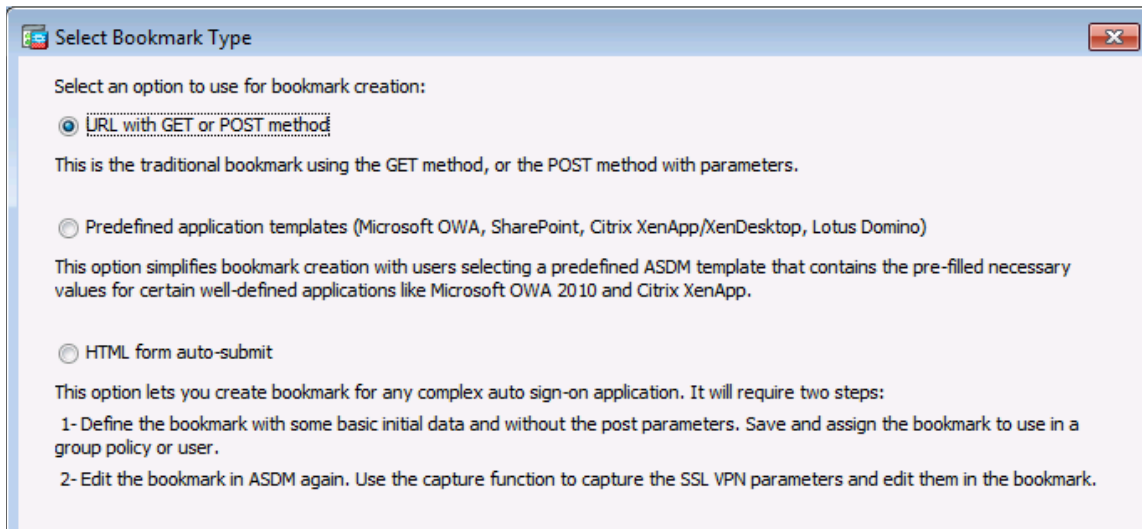


**Note:** If the Web-Server bookmark list is shown as available from a previous configuration, you can delete it in ASDM and re-create it.

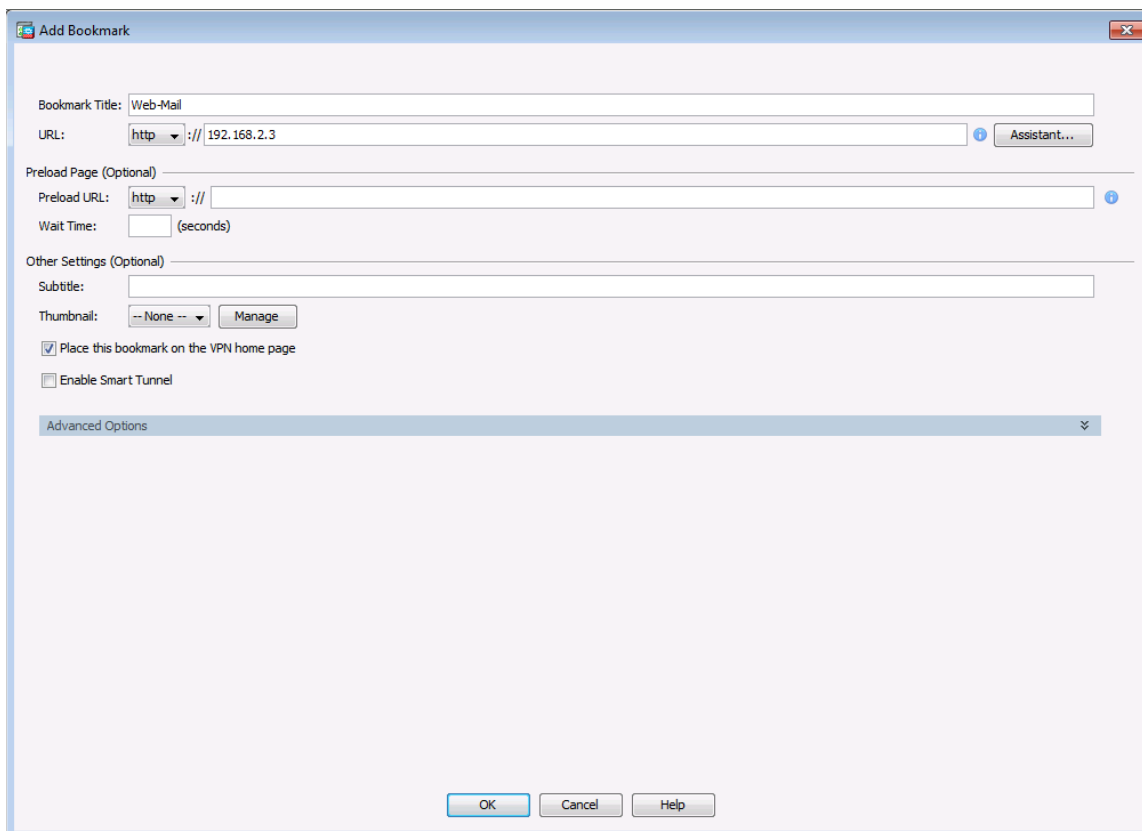
- c. In the Add Bookmark List window, click **Add** to open the Select Bookmark Type window.



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

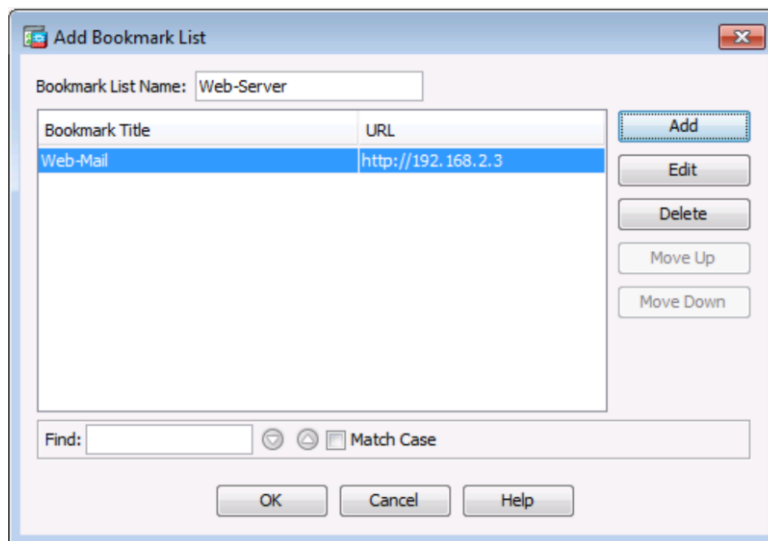


- e. Enter the bookmark title and enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the Bookmark Title of **Web-Mail** is entered and an internal IP address of **192.168.2.3** (the DMZ server) is specified. If this server has HTTP web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

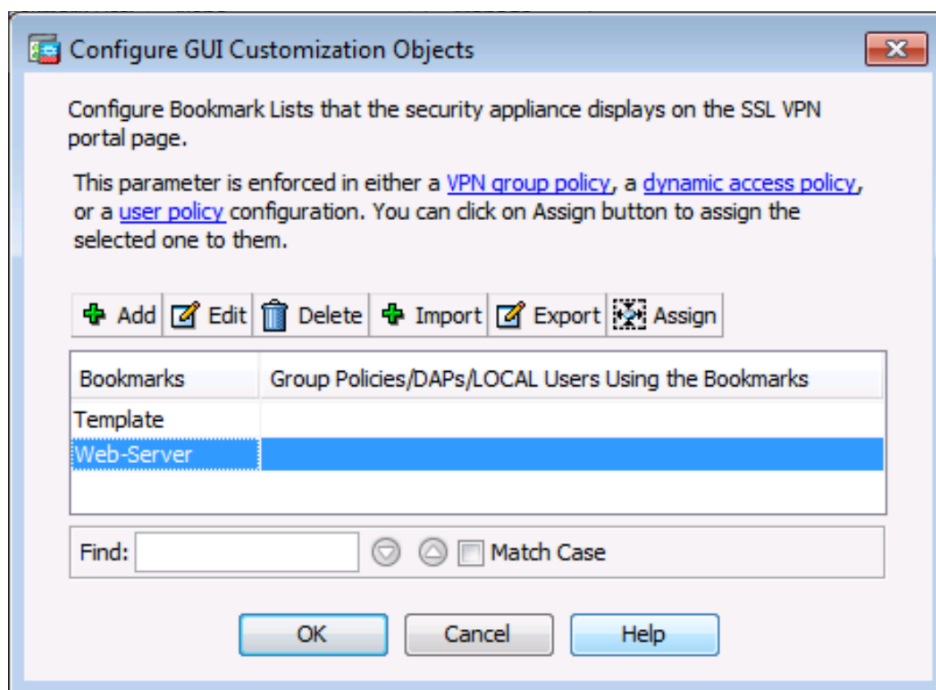




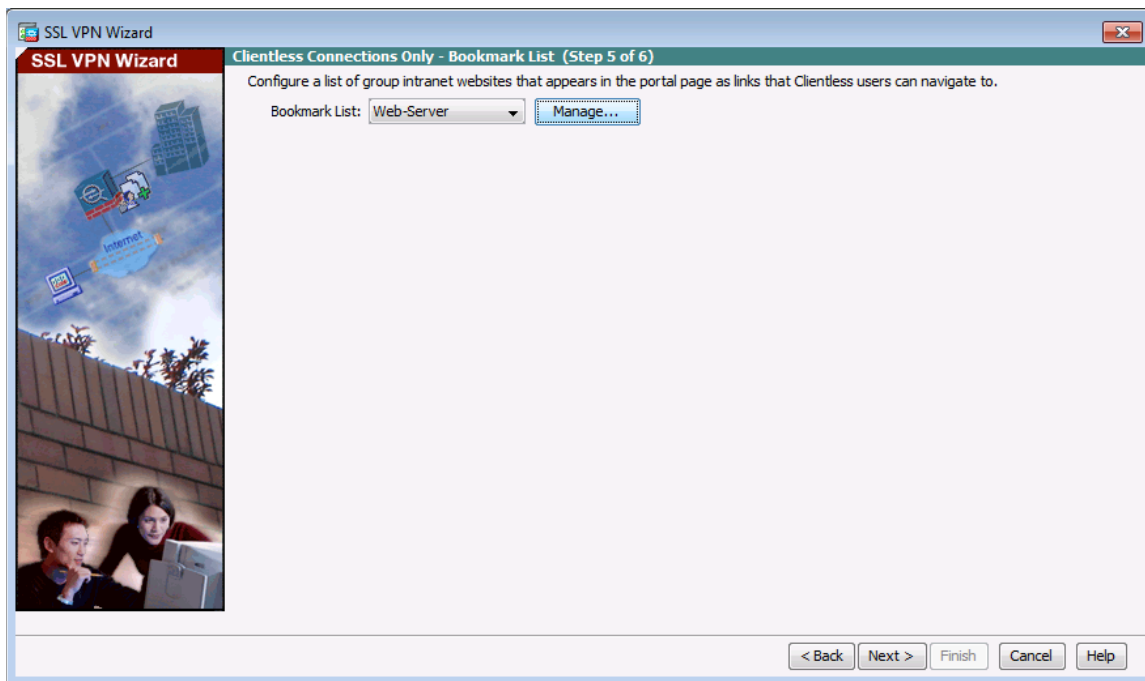
- f. Click **OK** to continue and return to the Add Bookmark List window which now displays the Web-Server bookmark title and URL.



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

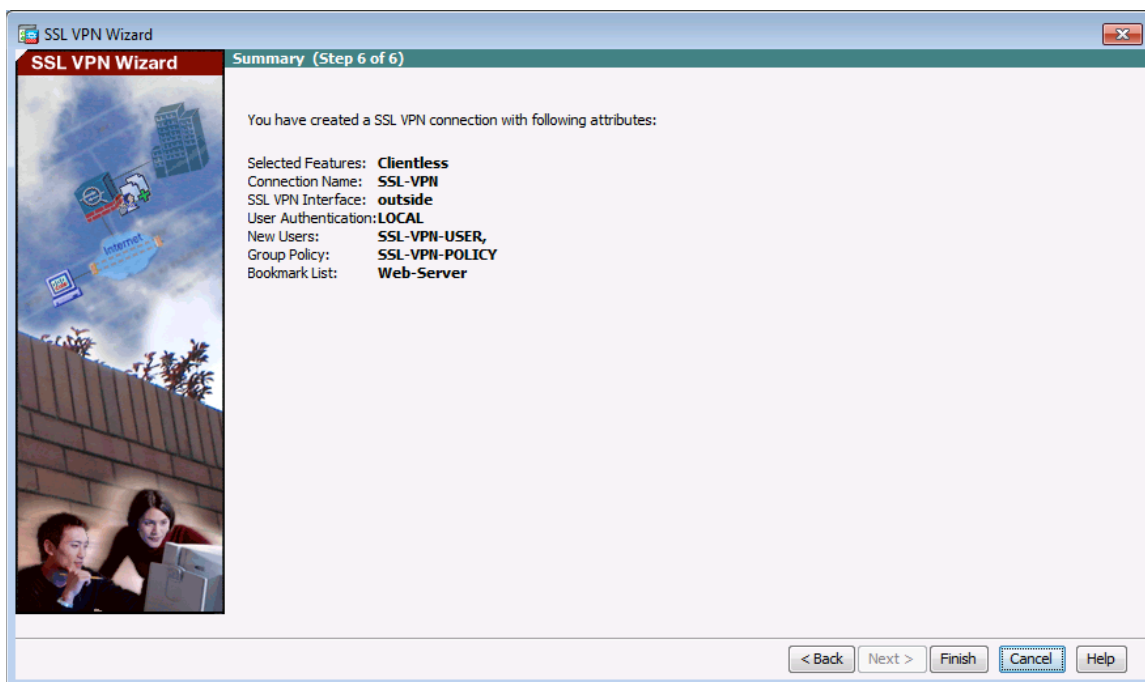


- h. Click **OK** to continue and return to the Bookmark List window and click **Next** to continue.



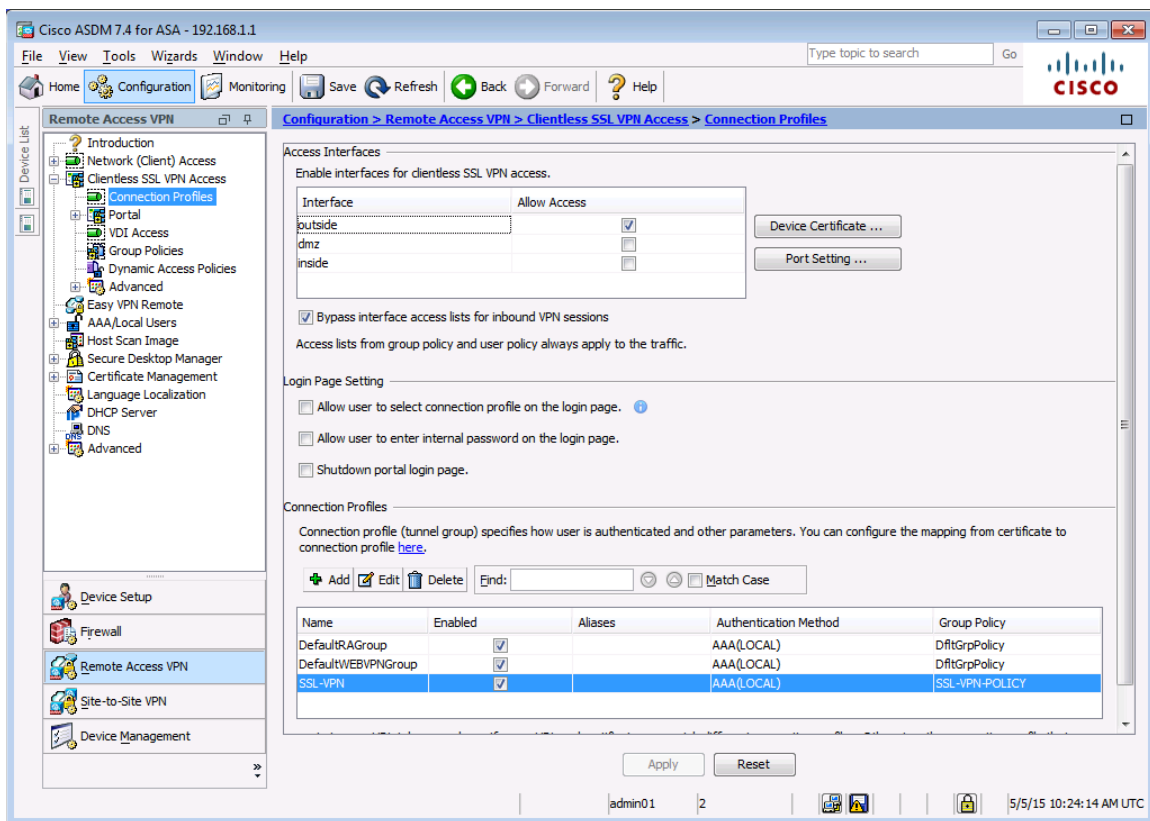
### Step 6: Review the configuration summary and deliver the commands to the ASA.

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

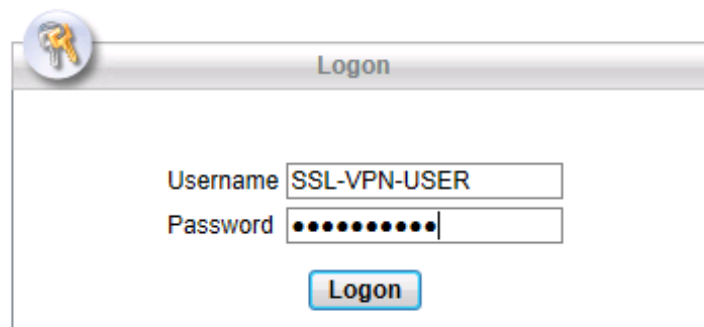


**Step 7: Verify the ASDM SSL VPN connection profile.**

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

**Step 8: Verify VPN access from the remote host.**

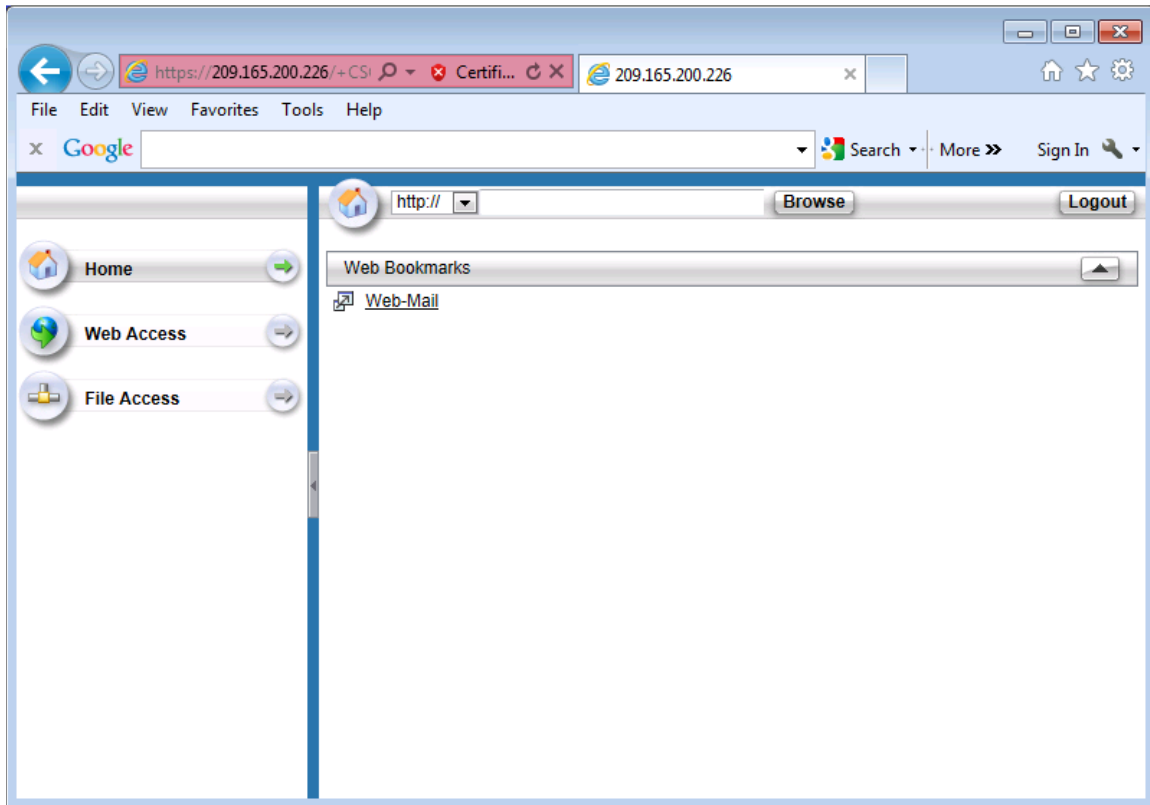
- Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (**https://209.165.200.226**). Use secure HTTP (HTTPS) because SSL is required to connect to the ASA.
- The Logon window should display. Enter the previously configured username **SSL-VPN-USER** and password **cisco12345**, and click **Logon** to continue.



**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.



### 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 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN Statistics

Sessions

Crypto Statistics

Compression Statistics

Encryption Statistics

Global IKE/Ipsec Statistics

Protocol Statistics

VLAN Mapping Sessions

Clientless SSL VPN

Easy VPN Client

VPN Connection Graphs

WSA Sessions

Interfaces

VPN

Routing

Properties

Logging

Monitoring > VPN > VPN Statistics > Sessions

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

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

Username	Group Policy	Protocol	Login Time	Bytes Tx	Bytes Rx
IP Address	Connection Profile	Encryption	Duration		
SSL-VPN-USER	SSL-VPN-POLICY	Clientless	14:46:21 UTC Tue May 5 2015	285328	36674
172.16.3.3	DefaultWEBVPNGroup	Clientless: (1)RC4	0h:01m:58s		

Details Logout Ping

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

Logout By: -- All Sessions -- Logout Sessions Refresh

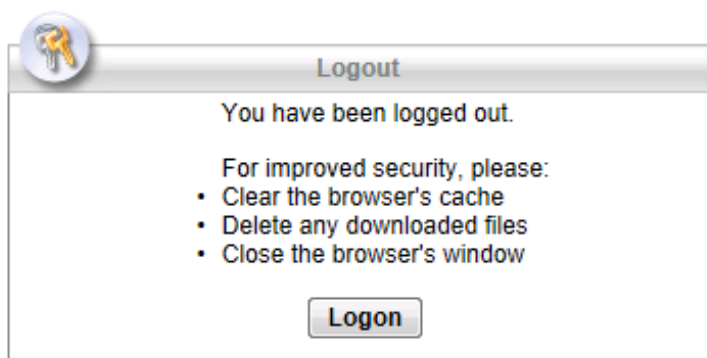
Last Updated: 5/5/15 7:51:42 AM

Data Refreshed Successfully.

admin01 2 5/5/15 10:24:14 AM UTC

### 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 (See Step 10). 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.



## 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)
<b>Note:</b> 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.				