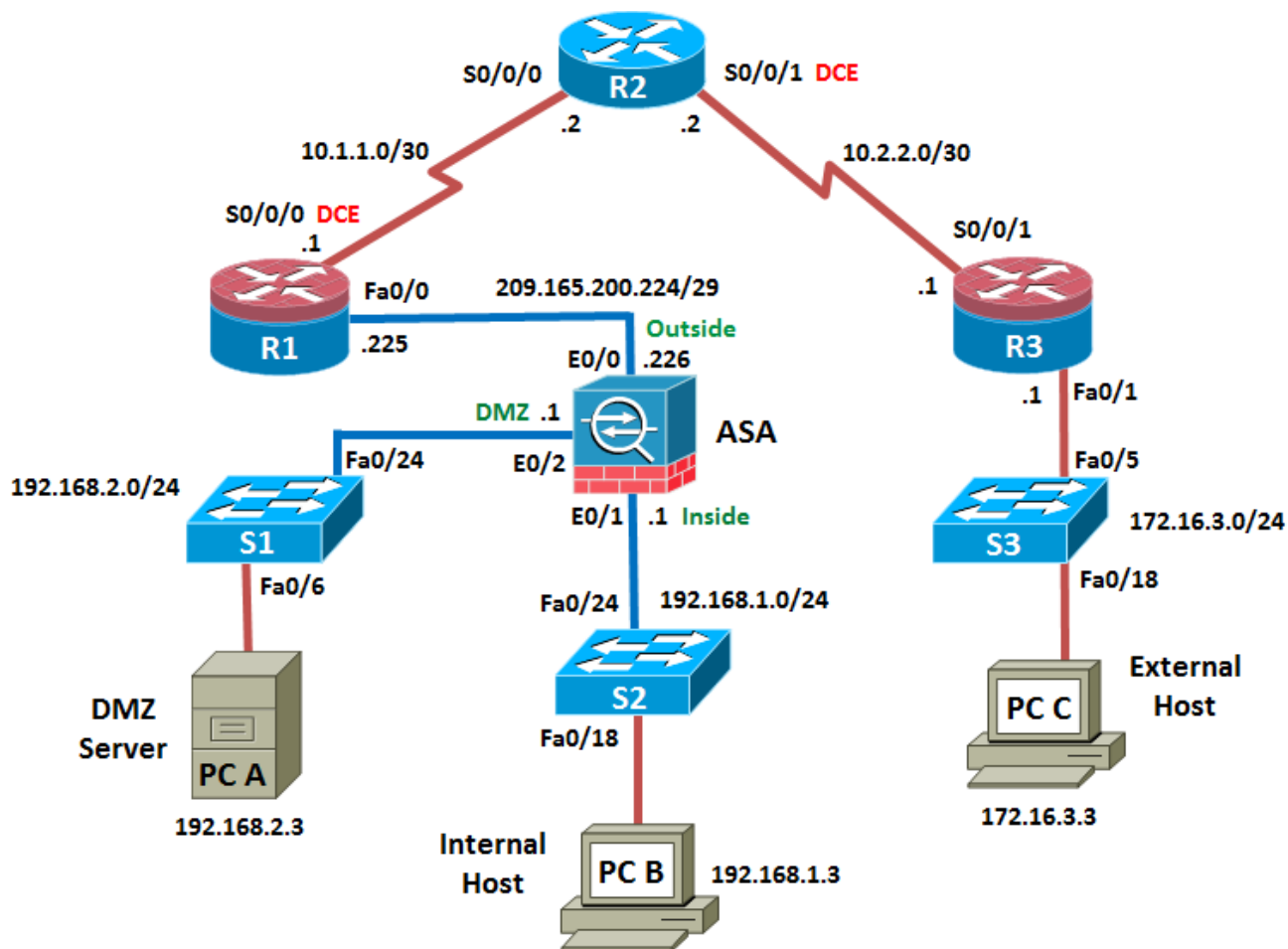


Chapter 10 Lab G: Configuring ASA 5510 Clientless and AnyConnect Remote Access SSL VPNs Using ASDM

Topology



Note: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/0	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	FA0/1	172.16.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	E0/0 (outside)	209.165.200.226	255.255.255.248	NA	R1 FA0/0
	E0/1 (inside)	192.168.1.1	255.255.255.0	NA	S2 FA0/24
	E0/2 (dmz)	192.168.2.1	255.255.255.0	NA	S1 FA0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 FA0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 FA0/18

Objectives

Part 1: Lab Setup

- Cable the network as shown in the topology.
- Configure hostnames, and interface IP addresses for routers, switches, and PCs.
- Configure static routing, including default routes, between R1, R2, and R3.
- Verify connectivity between hosts, switches, and routers.

Part 2: Accessing the ASA Console and Preparing for VPN configuration

- Access the ASA console.
- Clear previous configuration settings.
- Load the ASA CLI command script to configure basic settings.
- Access ASDM.

Part 3: Configuring Clientless SSL VPN Remote Access Using ASDM

- Configure the SSL VPN interface connection profile.
- Configure Local AAA user authentication.
- Configure the group policy.
- Configure a bookmark list for intranet URLs.
- Verify access to the VPN portal.
- Monitor the clientless SSL VPN connection.

Part 4: Configuring AnyConnect Client SSL VPN Remote Access Using ASDM

- Clear Clientless SSL VPN configuration from Part 3.
- Configure the SSL VPN interface connection profile.
- Configure the VPN encryption protocol.

- Configure the AnyConnect client image to upload.
- Configure Local AAA user authentication.
- Configure the client address pool.
- Configure the DNS server and NAT exempt.
- Configure AnyConnect client deployment.
- Verify VPN access and AnyConnect client upload.
- Monitor the AnyConnect SSL VPN connection.

Background / Scenario

In addition to statefull 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 the 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. In Part 4 you will configure an AnyConnect client-based SSL remote access VPN and verify connectivity.

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 CPE 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 both the clientless access model, using SSL and a browser for client access, and the client-based model using SSL and the Cisco AnyConnect client.

Note: The routers used with this lab are Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). The switches are Cisco WS-C2960-24TT-L with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). Other routers, switches, and Cisco IOS versions can be used. However, results and output may vary.

The ASA used with this lab is a Cisco model 5510 with four FastEthernet routed interfaces, running OS version 8.4(2) and ASDM version 6.4(5), and comes with a Base license that allows a maximum of 50 VLANs.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 3 switches (Cisco 2960 or comparable)
- 1 ASA 5510 (OS version 8.4(2) and ASDM version 6.4(5) and Base license or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with CCP, PuTTY SSH client (Web server optional)
- PC-B: Windows XP, Vista, or Windows 7 with PuTTY SSH client and Java 6 (ASDM loaded on the PC is optional)
- PC-C: Windows XP, Vista, or Windows 7 with Internet Explorer, CCP, PuTTY SSH client

- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers and ASA via the console

Note: Use of a browser other than Internet Explorer 7 or newer on remote PC-C may produce results different from those shown in this lab. It may be necessary to create an exception when connecting to the ASA over the remote access VPN.

Part 1: Basic Router/Switch/PC Configuration

In Part 1 of this lab, 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. Make sure that the routers and switches have been erased and have no startup configurations.

Step 2: Configure basic settings for routers and switches.

- Configure host names as shown in the topology for each router.
- Configure router interface IP addresses as shown in the IP Addressing Table.
- Configure a clock rate for routers with a DCE serial cable attached to their serial interface.
- Configure the host name for the switches. Other than host name, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

Step 3: Configure static routing on the routers.

- Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```
- Configure a static route from R2 to the R1 Fa0/0 subnet (connected to ASA interface E0/0) and a static route from R2 to the R3 LAN.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

Step 4: Enable the HTTP server on R1 and set the enable and vty passwords.

- Enable HTTP access to R1 using the `ip http server` command in global config mode. Also set the VTY password to cisco.
- Configure the same settings on R2 and R3. Router R1 is shown here as an example.

```
R1(config)# ip http server
R1(config)# enable password class

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login

R1(config)# line con 0
```

```
R1(config-line)# password cisco
R1(config-line)# login
```

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 connected to it. However, PC-C should be able to ping the R1 interface Fa0/0. From PC-C, ping the R1 Fa0/0 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 Fa0/0 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: Access the ASA console.

- Accessing the ASA via the console port is the same as with a Cisco router or switch. Connect to the ASA Console port with a rollover cable.
- Use a terminal emulation program such as TeraTerm or HyperTerminal to access the CLI, and use the serial port settings of 9600 baud, eight data bits, no parity, one stop bit, and no flow control.
- If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.
- Enter privileged mode with the **enable** command and password (if set). By default the password is blank so you can just press **Enter**. If the password has been changed to that specified in this lab, the password will be **class**. In addition, the hostname and prompt will be **CCNAS-ASA>**, as shown here. The default ASA hostname and prompt is **ciscoasa>**.

```
CCNAS-ASA> enable
Password: class (or press Enter if none set)
```

Step 2: Clear the previous ASA configuration settings.

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

```
CCNAS-ASA# write erase
Erase configuration in flash memory? [confirm]
[OK]
CCNAS-ASA#
```

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

- Use the **reload** command to restart the ASA. This will cause the ASA to come up in CLI Setup mode. If you see the message **System config has been modified. Save? [Y]es/[N]o:**, respond with "N".

```
CCNAS-ASA# reload
Proceed with reload? [confirm] <enter>
CCNAS-ASA#
***
```

```
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
```

<output omitted>

Step 3: Bypass setup mode.

When the ASA completes the reload process, it should detect that the startup-config file is missing and go into Setup mode. If it does not come up in this mode, repeat Step 2.

- a. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with **"no."**

```
Pre-configure Firewall now through interactive prompts [yes]? no
```

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

```
ciscoasa> enable
Password: <enter>
```

Step 4: Configure the ASA by using the CLI script.

In this step you will use the modified running-config from Lab 10E to preconfigure basic settings, the firewall and DMZ.

- a. Other than the defaults that the ASA automatically inserts, ensure with the use of the **show run** command that there is no previous configuration in the ASA.
- b. Enter CLI global configuration mode. When prompted to enable anonymous call-home reporting, respond **"no."**

```
ciscoasa# conf t
ciscoasa(config)#
```

- c. Copy and paste the Pre-VPN Configuration Script commands listed below at the ASA global config mode prompt to bring it to the point where you can start configuring the SSL VPNs.
- d. Observe the messages as the commands are applied to ensure that there are no warnings or errors. If prompted to replace the RSA keypair, respond **"yes."**
- e. After script commands have been applied, 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.

Lab 10G Pre-VPN Configuration Script:

```
hostname CCNAS-ASA
!
domain-name ccnasecurity.com
!
enable password class
passwd cisco
!
interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 209.165.200.226 255.255.255.248
  no shut
!
interface Ethernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shut
!
interface Ethernet0/2
  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 admin password cisco123
!
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 type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
```

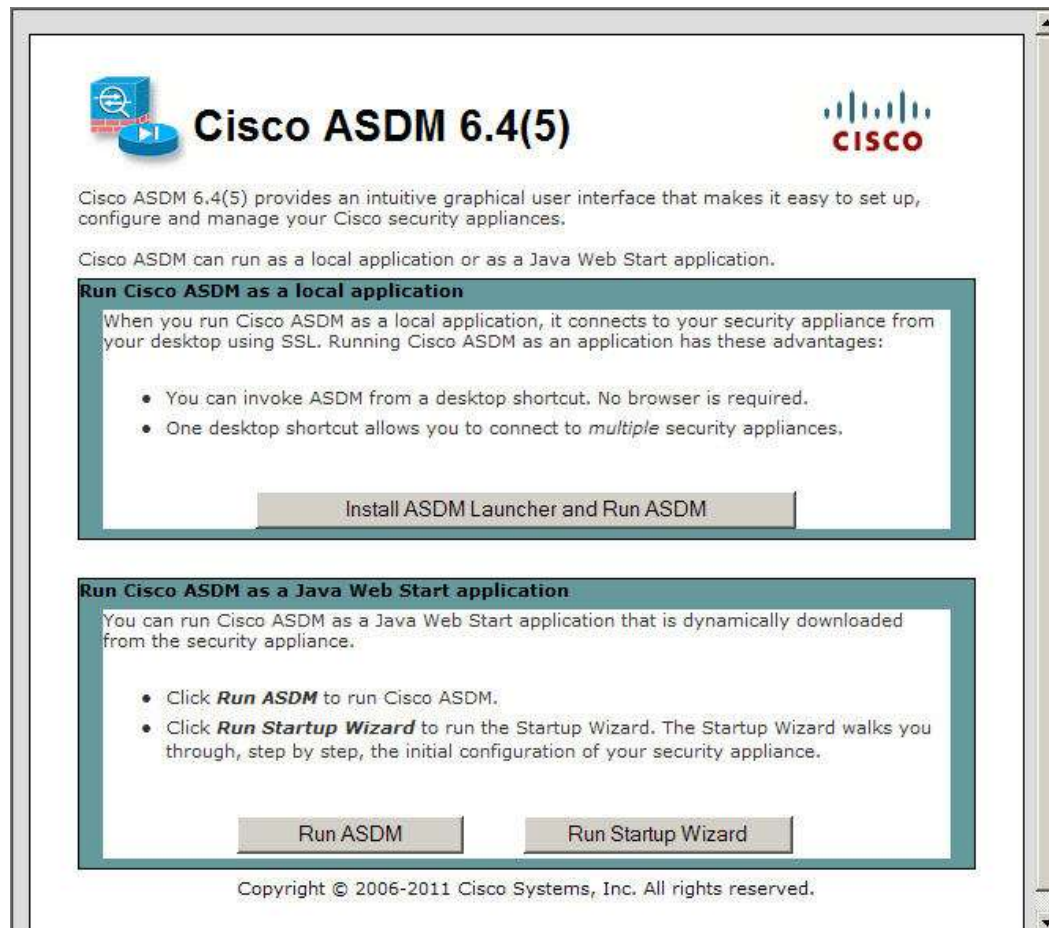
```
message-length maximum 512
policy-map global_policy
class inspection_default
inspect icmp
!
prompt hostname context
no call-home reporting anonymous
!
crypto key generate rsa modulus 1024
```

Step 5: Access ASDM.

- a. Open a browser on PC-B and test HTTPS access to the ASA by entering **https://192.168.1.1**.

Note: Be sure to specify the HTTPS protocol in the URL.

- b. After entering the URL above, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings. At the ASDM welcome page, click the **Run ASDM** button. The ASDM-IDM Launcher will display. Login as user **admin** with password **cisco123**. ASDM will load the current configuration into the GUI.

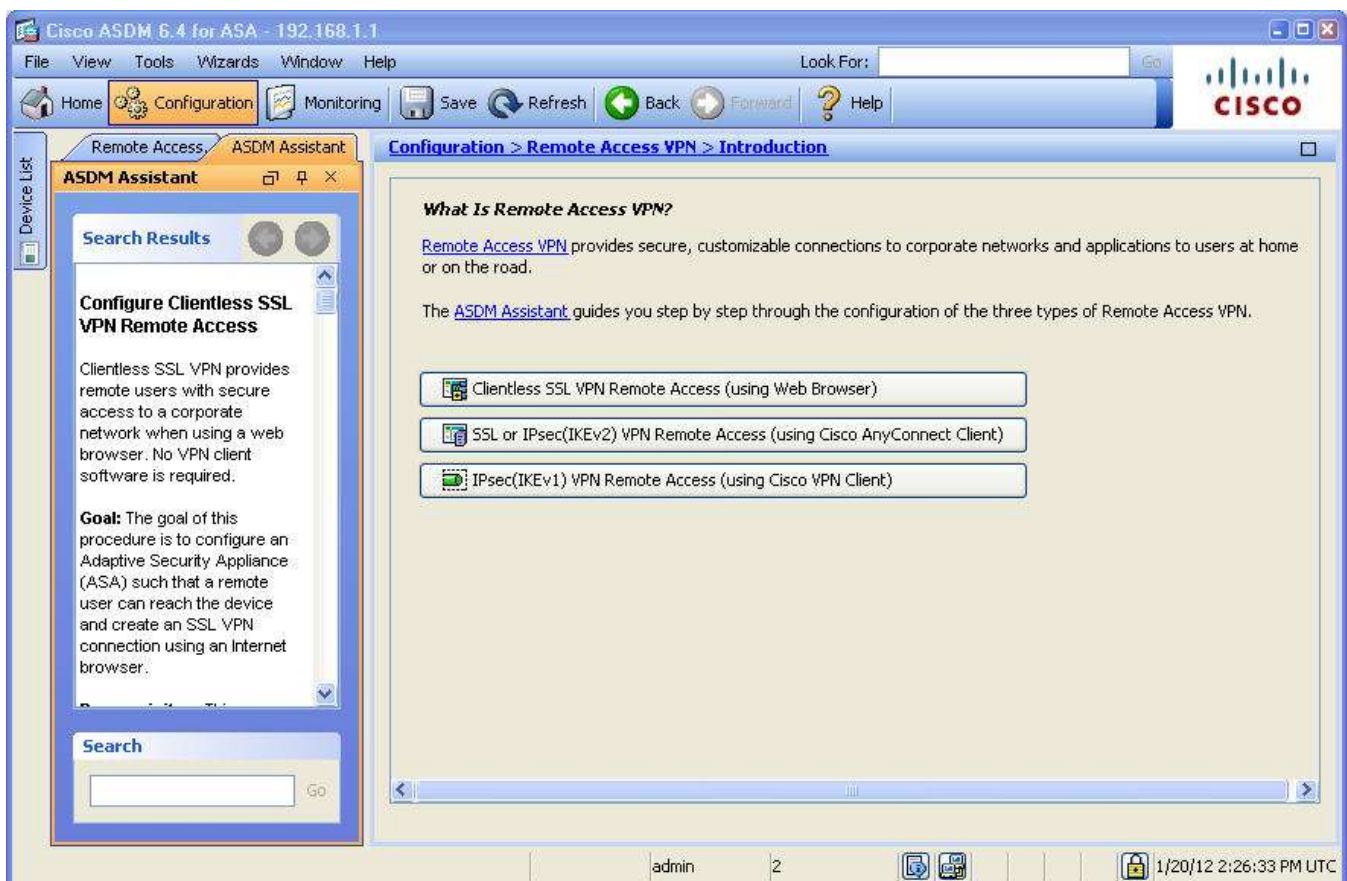




Part 3: Configuring Clientless SSL VPN Remote Access Using ASDM

Step 1: Review the Remote Access VPN ASDM Assistant.

- a. From the menu bar, choose the **Configuration** button and click **Remote Access VPN** to display the Introduction screen. From here you can access information on how to create any of the three types of remote access VPNs.



- b. Click the button **Clientless SSL VPN Remote Access (using Web Browser)** to access the ASDM Assistant. Read through the information provided to get a better understanding of the process for creating this type of VPN.

Step 2: Start the VPN wizard.

- a. From the ASDM main menu at the top of the browser window, select the **Wizards > VPN Wizards > Clientless SSL VPN wizard**. The SSL VPN wizard Clientless SSL VPN Connection screen is displayed.
- b. Review the on-screen text and topology diagram, and then click **Next** to continue.



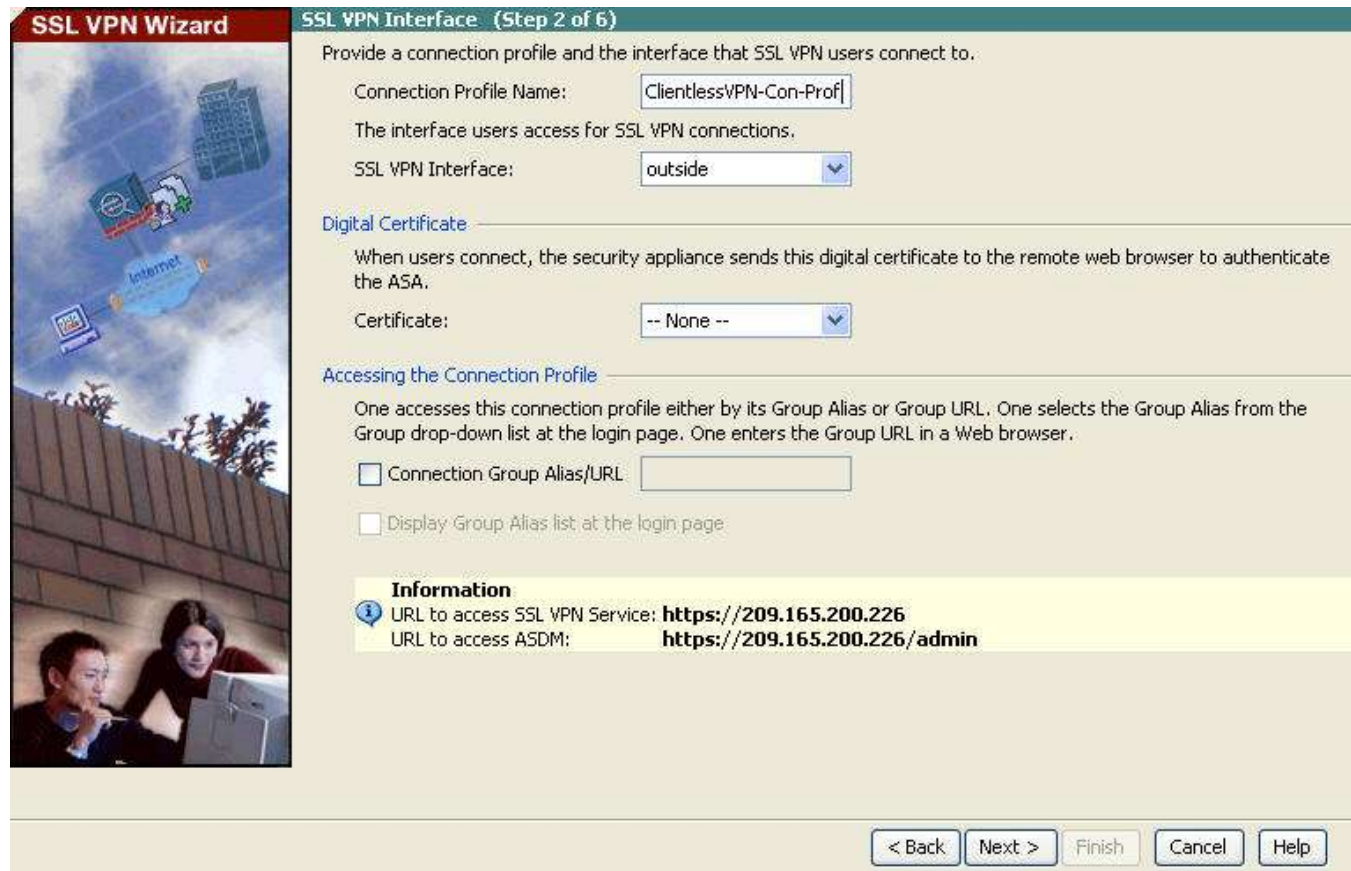
Step 3: Configure the SSL VPN user interface.

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

Note: By default, the ASA will use 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 (login) and for Cisco ASDM access (to access the Cisco ASDM software).

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



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:

The interface users access for SSL VPN connections.

SSL VPN Interface:

Digital Certificate

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

Certificate:

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

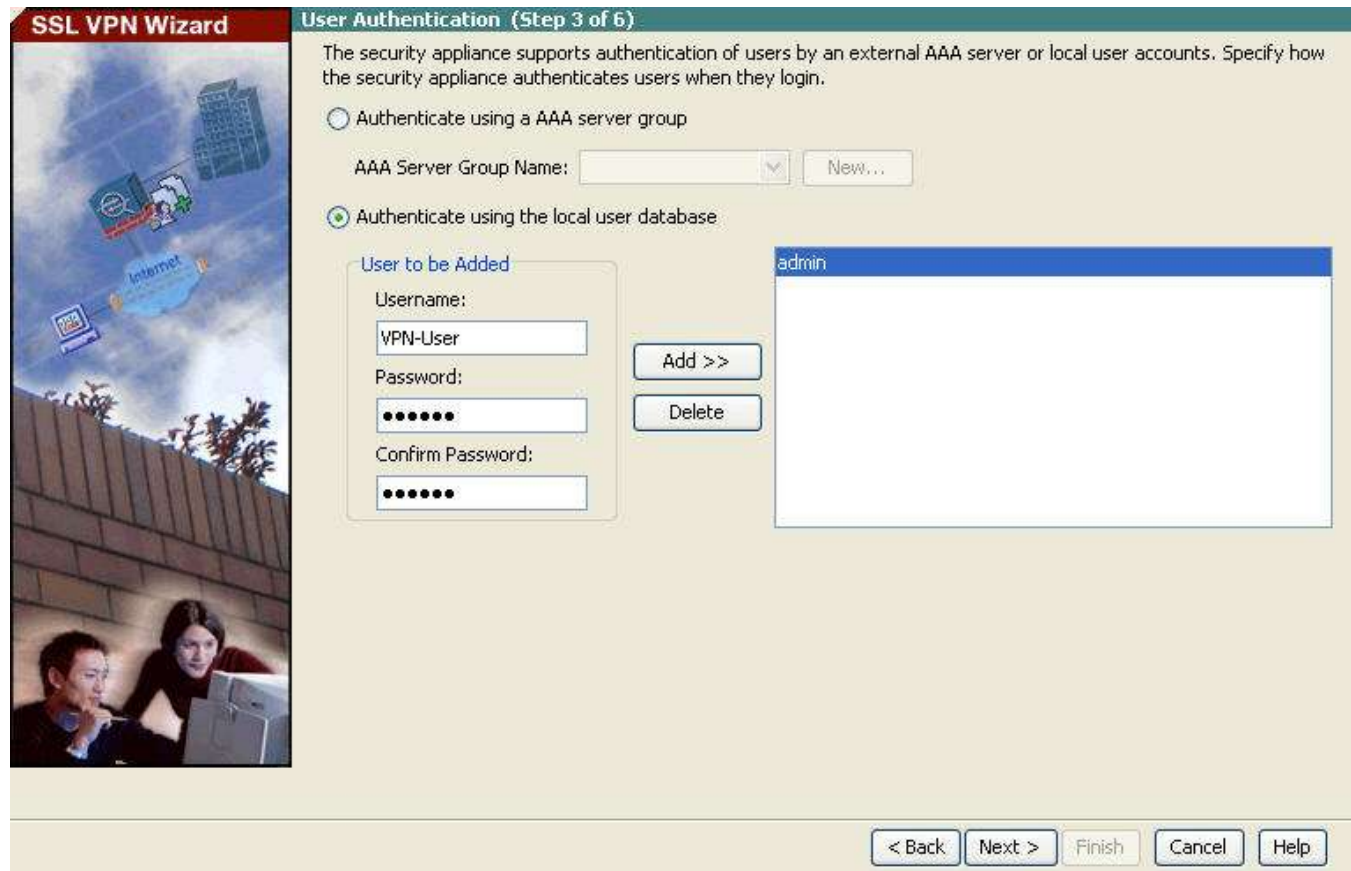
URL to access SSL VPN Service: <https://209.165.200.226>

URL to access ASDM: <https://209.165.200.226/admin>

< Back Next > Finish Cancel Help

Step 4: Configure AAA user authentication.

On the User Authentication screen, click **Authenticate using the local user database**, enter the user name **VPN-User** with a password of **remote**. 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:

admin

< Back Next > Finish Cancel Help

Step 5: Configure the VPN group policy.

On the Group Policy screen create a new group policy named **ClientlessVPN-Grp-Pol**. When configuring a new policy, the policy name cannot contain any spaces. Click **Next** to continue.

Note: By default, the created user group policy will inherit 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.



The screenshot shows the 'SSL VPN Wizard' window, specifically the 'Group Policy (Step 4 of 6)' screen. On the left is a vertical banner with a graphic of a city skyline and a person at a computer. The main area contains a text box explaining group policies, two radio buttons for 'Create new group policy' (selected) and 'Modify existing group policy', and a text field with 'ClientlessVPN-Grp-Pol' and a dropdown menu with 'DfltGrpPolicy'. At the bottom right are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

SSL VPN Wizard

Group Policy (Step 4 of 6)

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: ClientlessVPN-Grp-Pol

☐ Modify existing group policy: DfltGrpPolicy

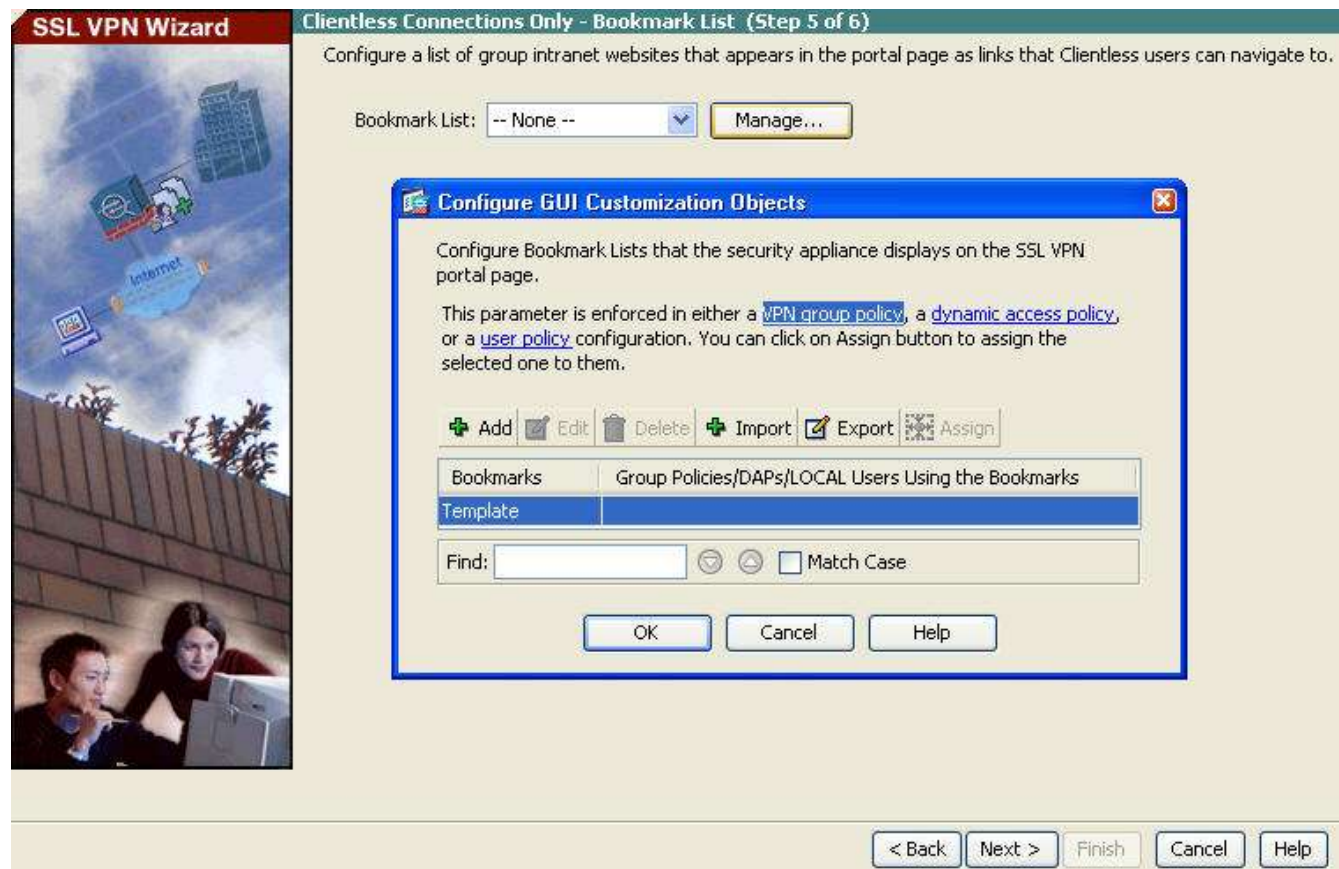
< Back Next > Finish Cancel Help

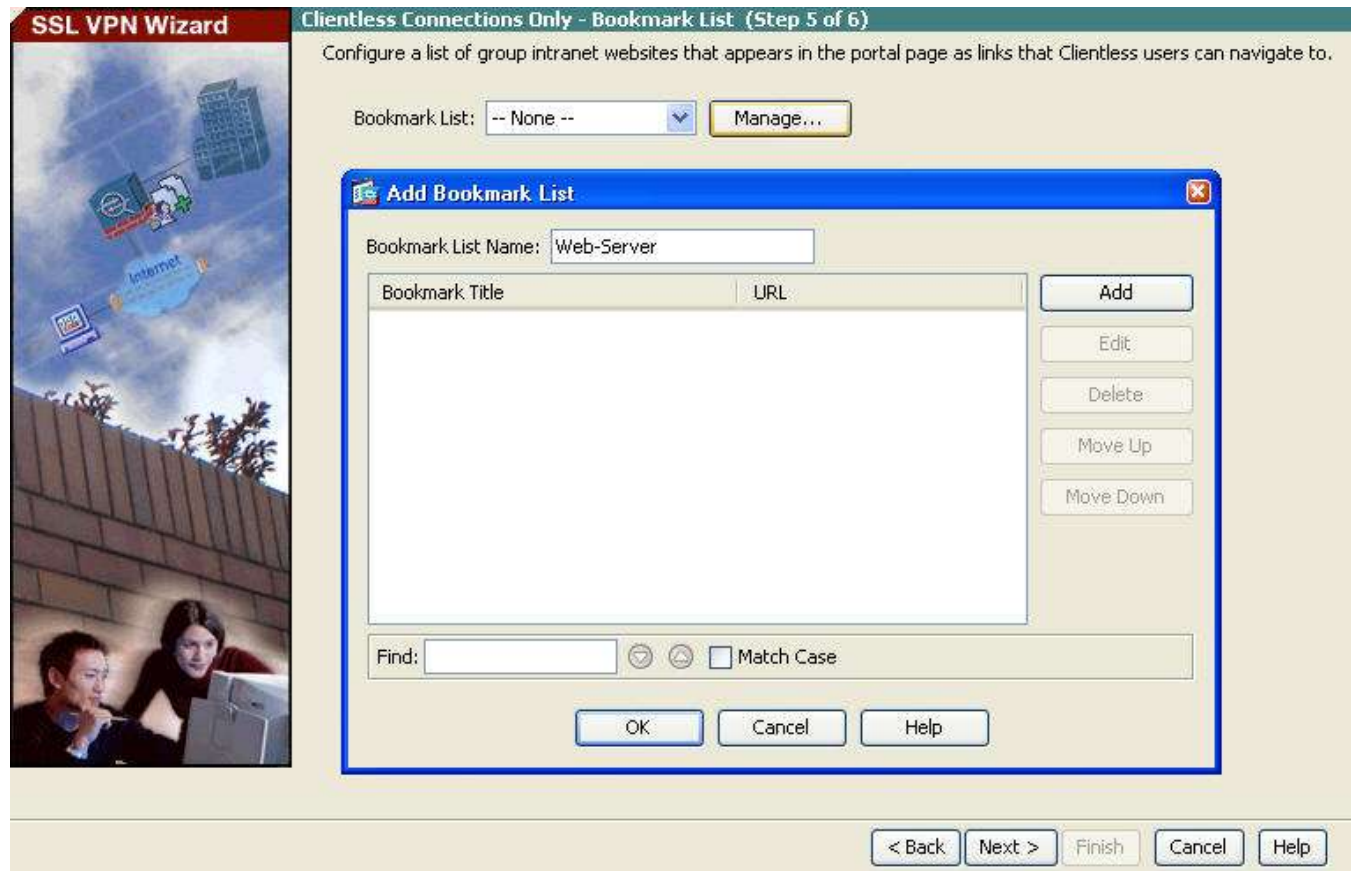
Step 6: Configure the bookmark list (clientless connections only).

A bookmark list is a set of URLs that is configured to be used in the clientless SSL VPN web portal. If there are bookmarks already listed, use the Bookmark List drop-down menu, select the bookmark of choice and click **Next** to continue with the SSL VPN wizard. However, there are no configured bookmark lists by default and therefore they must be configured by the network administrator.

- a. From the Clientless Connections Only – Bookmark List screen, click the **Manage** button to create an HTTP server bookmark in the bookmark list. 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 recreate it.





- b. From the Add Bookmark List window, click **Add** to open the Add Bookmark window. Enter **Web-Mail** as the Bookmark Title. Enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the internal IP address of the DMZ server is specified. If this server has HTTP web services and web mail installed and functional, the outside users will be able to access the server from the ASA portal when they connect.

Add Bookmark

Bookmark Title:

URL: ://

Preload Page (Optional)

Preload URL: ://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail:

☐ Enable Smart Tunnel

☒ Allow the users to bookmark the link

Advanced Options

- c. When the Bookmark Title and URL are entered, click **OK** in the Add Bookmark window to return to the Configure GUI Customization Objects window. Select the desired bookmark and click **OK** to return to the Bookmark List window. Click **Next** to continue.

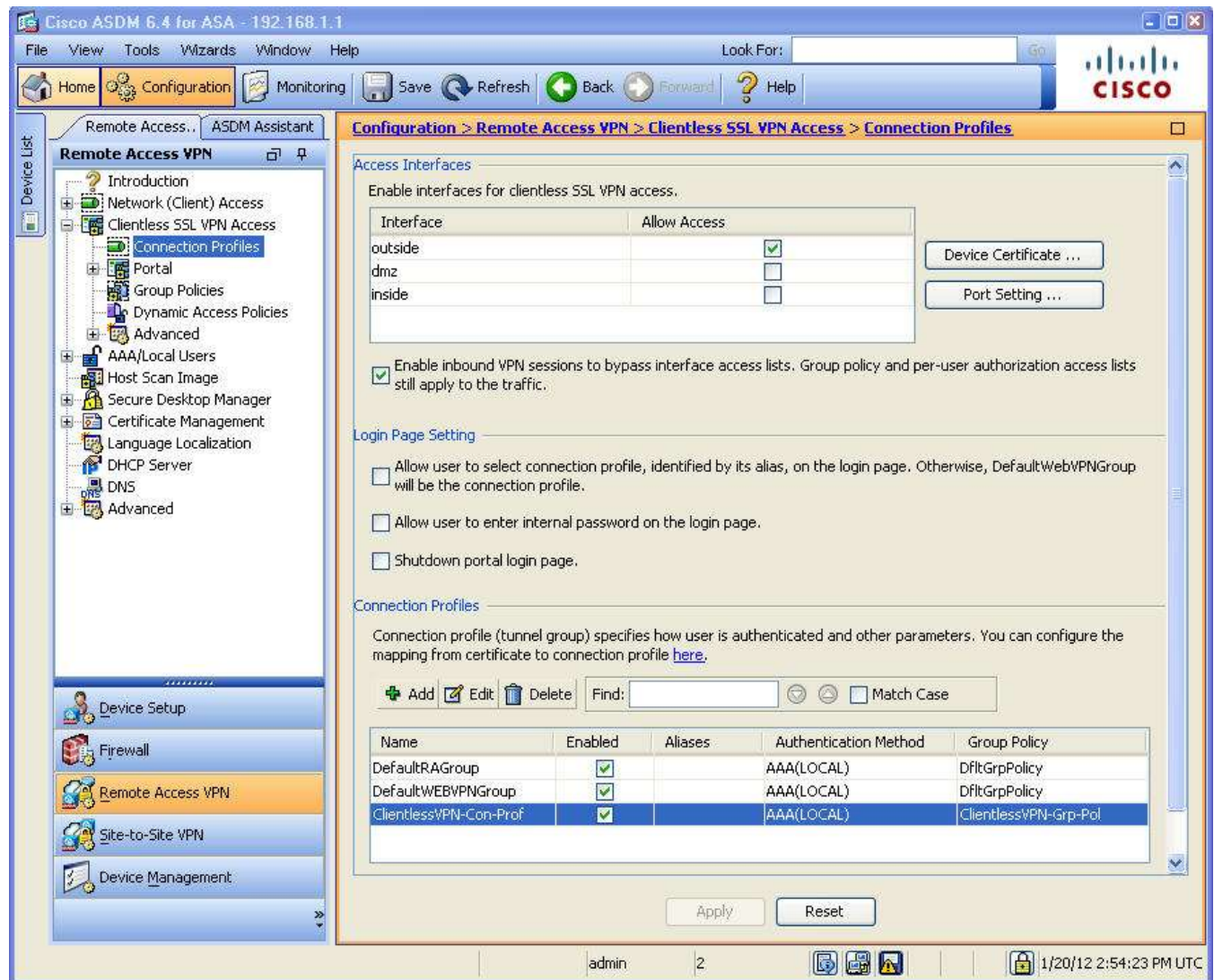
Step 7: Review the configuration summary and deliver the commands to the ASA.

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



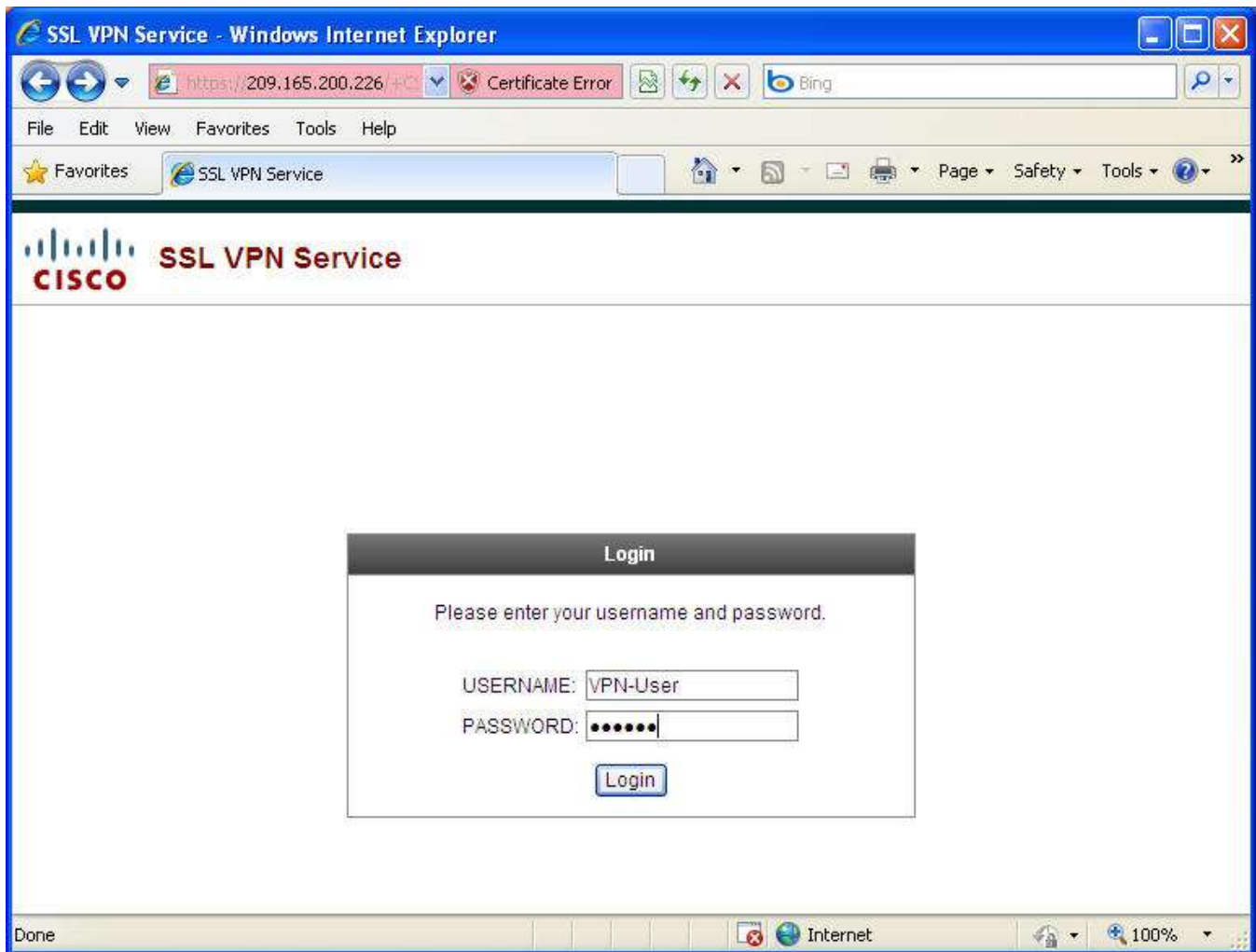
Step 8: Verify the ASDM SSL VPN connection profile.

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

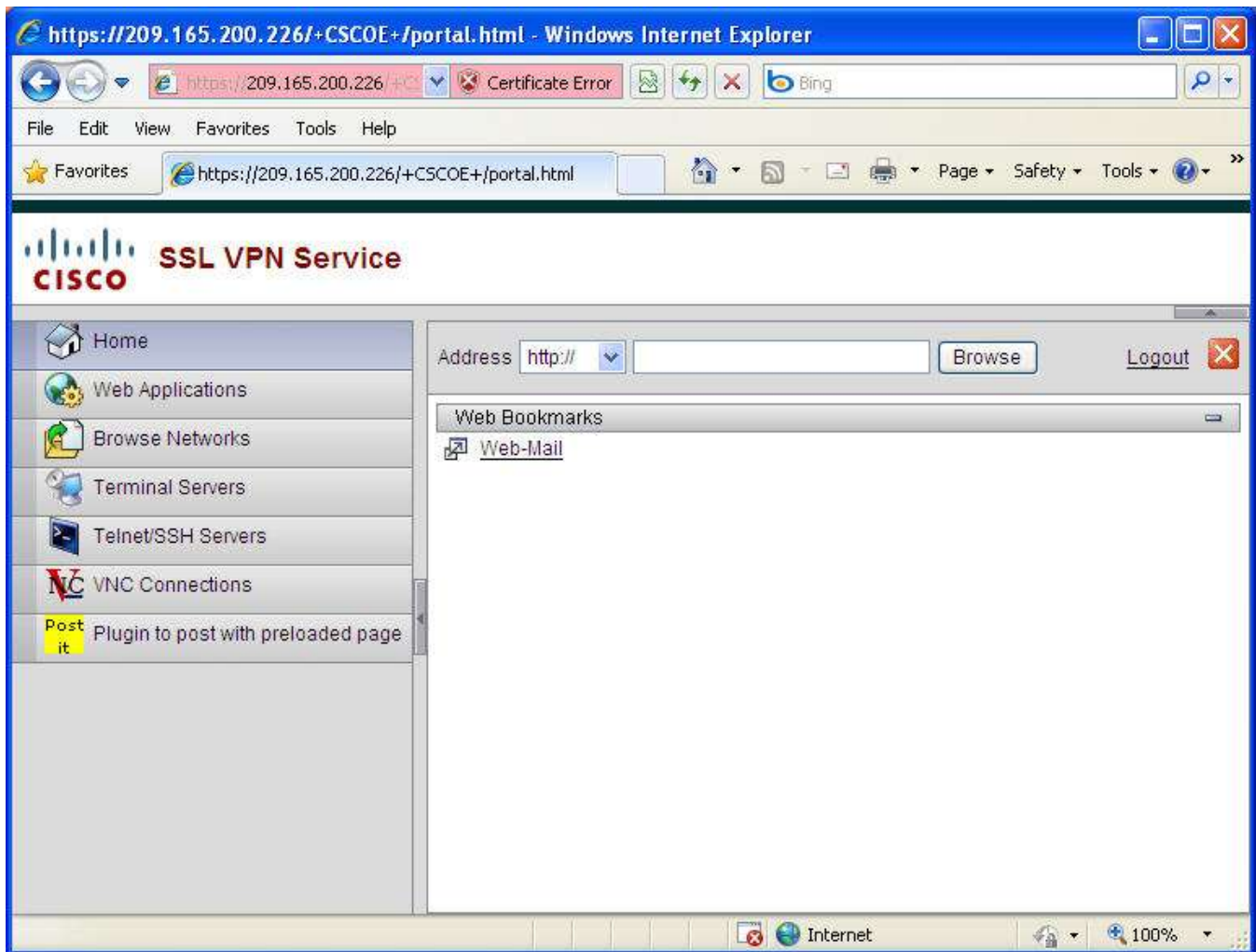


Step 9: Verify VPN access from the remote host.

- Open the browser on PC-C and enter the login URL for the SSL VPN into the address field (<https://209.165.200.226>). Be sure to use secure HTTP (HTTPS) as SSL is required to connect to the ASA. After entering the URL, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings.
- The Logon window should appear. Enter the previously configured user name **VPN-User** and password **remote** and click **Login** to continue.

**Step 10: Access the Web Portal window.**

Once the user authenticates, the ASA SSL Web portal webpage will be displayed listing 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. In this lab the web mail server is not installed.



Step 11: View the clientless remote user VPN session using 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 menu bar, click the **Monitoring** button and then choose **VPN > VPN Statistics > Sessions**. Click the **Filter By** pull-down menu and choose **Clientless SSL VPN**. You should see the VPN-User session logged in from PC-C (172.16.3.3).

Note: You may need to click the Refresh button on the menu bar to display the remote user session.

Cisco ASDM 6.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Look For: Go

Home Configuration **Monitoring** Save Refresh Back Forward Help

Device List:

- VPN
 - VPN Statistics
 - Sessions**
 - Crypto Statistics
 - Compression Statistics
 - Encryption Statistics
 - Global IKE/IPsec Statistics
 - NAC Session Summary
 - Protocol Statistics
 - VLAN Mapping Sessions
 - Clientless SSL VPN
 - 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
Browser		1	1	1

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

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration
VPN-User 172.16.3.3	ClientlessVPN-Grp-Pol DefaultWEBVPNGroup	Clientless RC4	15:01:53 UTC Fri Jan 20 2012 0h:02m:29s

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

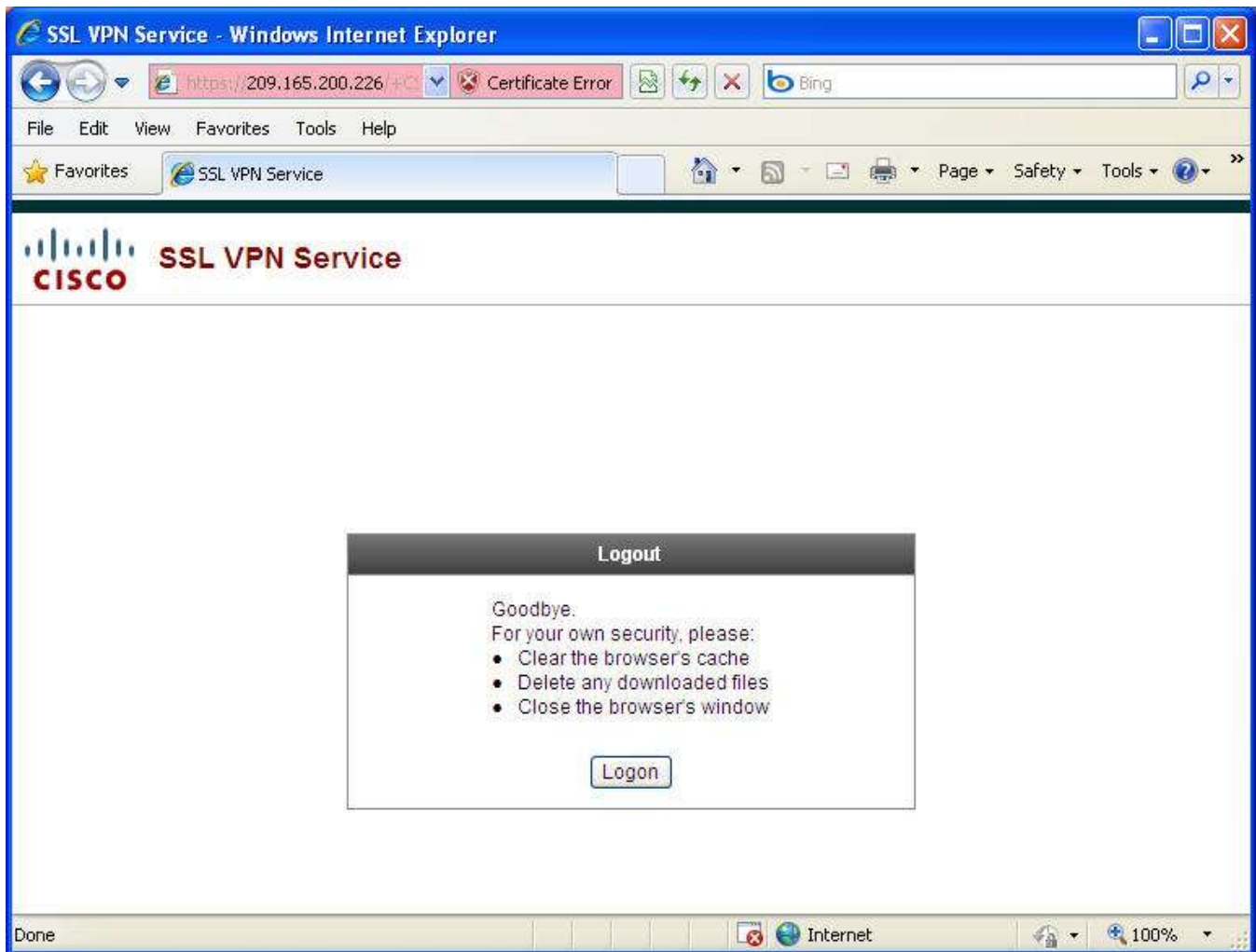
Refresh

Last Updated: 2/3/12 1:39:59 AM

Data Refreshed Successfully. admin 2 1/20/12 3:06:33 PM UTC

Step 12: Logout.

The user should log out of the web portal window 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.



Part 4: Configuring AnyConnect SSL VPN Remote Access Using ASDM

Step 1: Clear the ASA configuration and access ASDM.

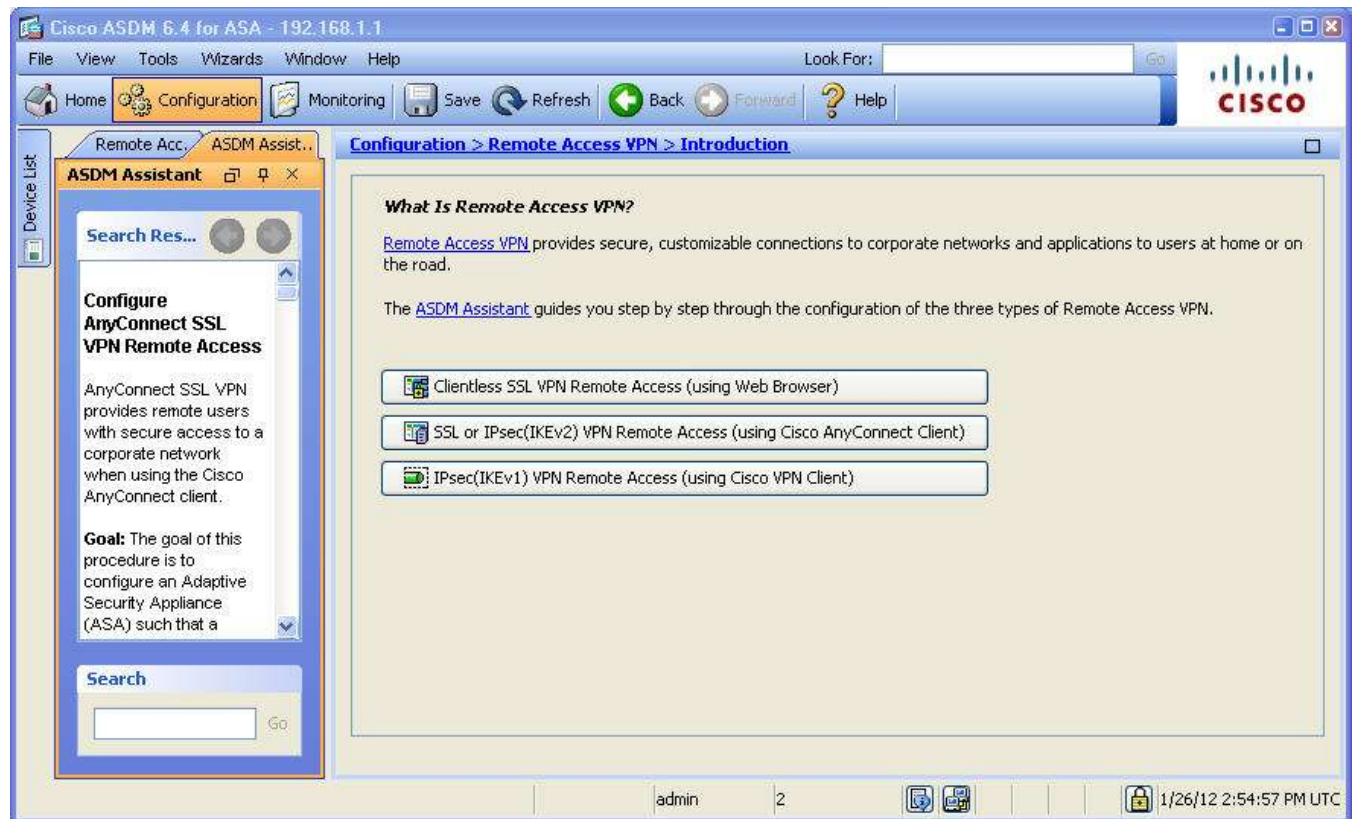
- Before beginning Part 4 of this lab, use the procedure that is described in Part 2 to remove the current VPN settings, return the ASA to its base configuration, and verify ASDM access.
- Open a browser on PC-B and test the HTTPS access to the ASA by entering `https://192.168.1.1`.

Note: Be sure to specify the HTTPS protocol in the URL.

- After entering the URL above, you should see a security warning about the security certificate of the website. Click **Continue to this website**. The ASDM welcome page will display. Click the **Run ASDM** button. When prompted, login as **admin** with a password of **cisco123**.

Step 2: Review the Remote Access VPN ASDM Assistant.

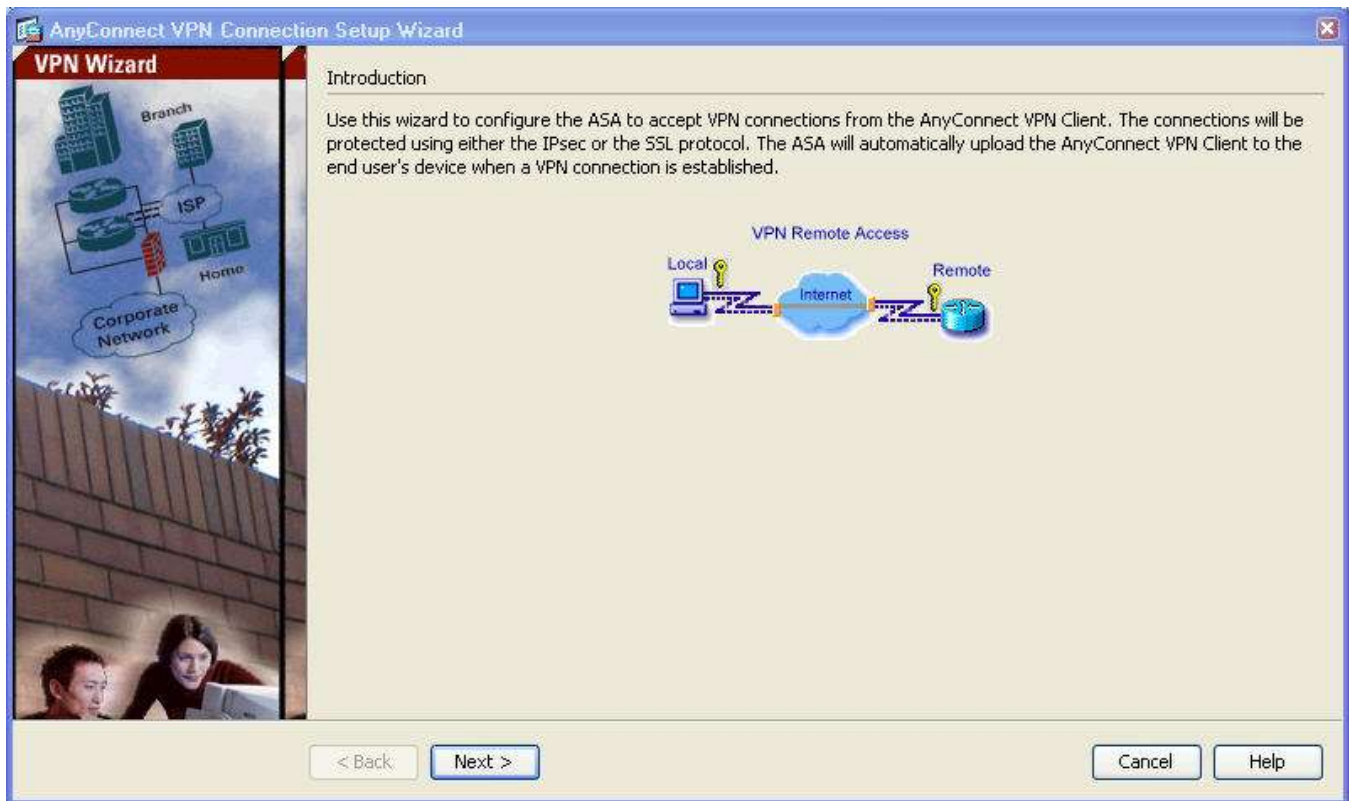
- From the ASDM menu bar, click the **Configuration** button and choose **Remote Access VPN** to display the Introduction screen. From here you can access information on how to create each of the three types of remote access VPNs that are supported by the ASA.



- b. Click the button **SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)** to access the ASDM Assistant. Read through the information provided to get a better understanding of the process for creating this type of VPN.

Step 3: Start the VPN wizard.

- a. From the ASDM main menu, choose the **Wizards > VPN Wizards > AnyConnect VPN** wizard.
- b. Review the on-screen text and topology diagram, and then click **Next** to continue.



Step 4: Configure the connection profile.

On the Connection Profile Identification screen, enter **AnyC-SSL-VPN-Con-Prof** as the Connection Profile Name and specify the **outside** interface as the VPN Access Interface. Click **Next** to continue.

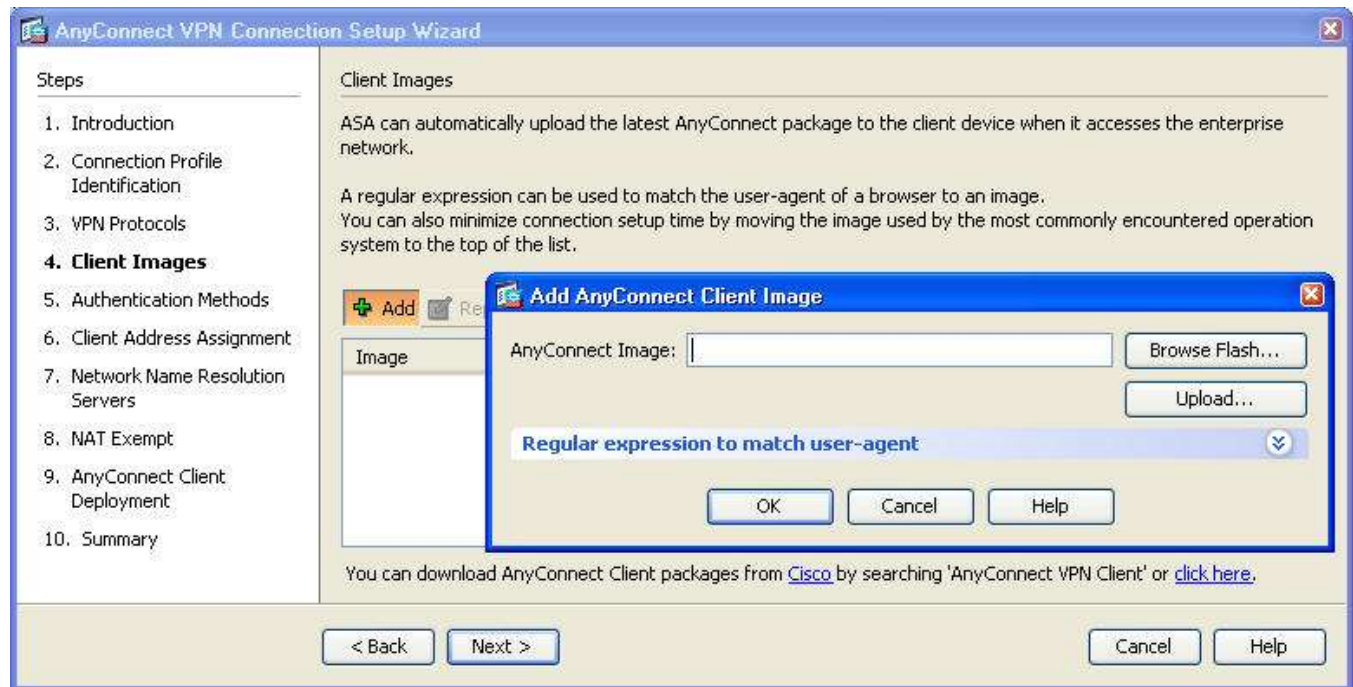


Step 5: Specify the VPN encryption protocol.

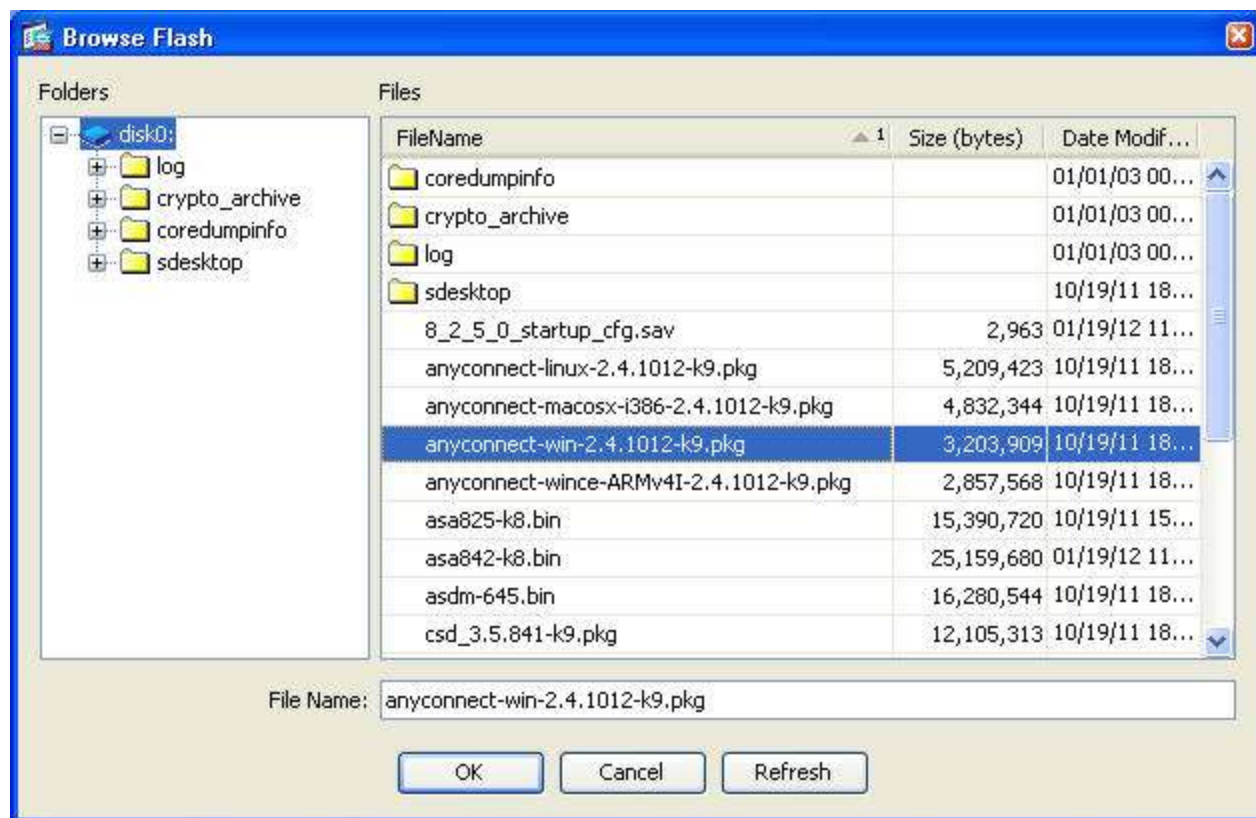
On the VPN Protocols screen, uncheck the **IPsec** protocol and leave the **SSL** check box checked. Do not specify a device certificate. Click **Next** to continue.

**Step 6: Specify the client image to upload to AnyConnect users.**

- a. On the Client Images screen, click **Add** to specify the AnyConnect client image filename. In the Add AnyConnect Client Image window, click the **Browse Flash** button.



- b. From the Browse Flash window, select the AnyConnect package file for Windows. Click **OK** to return to the AnyConnect Client Images window and then click **OK** again. On the Client Images screen, click **Next** to continue.

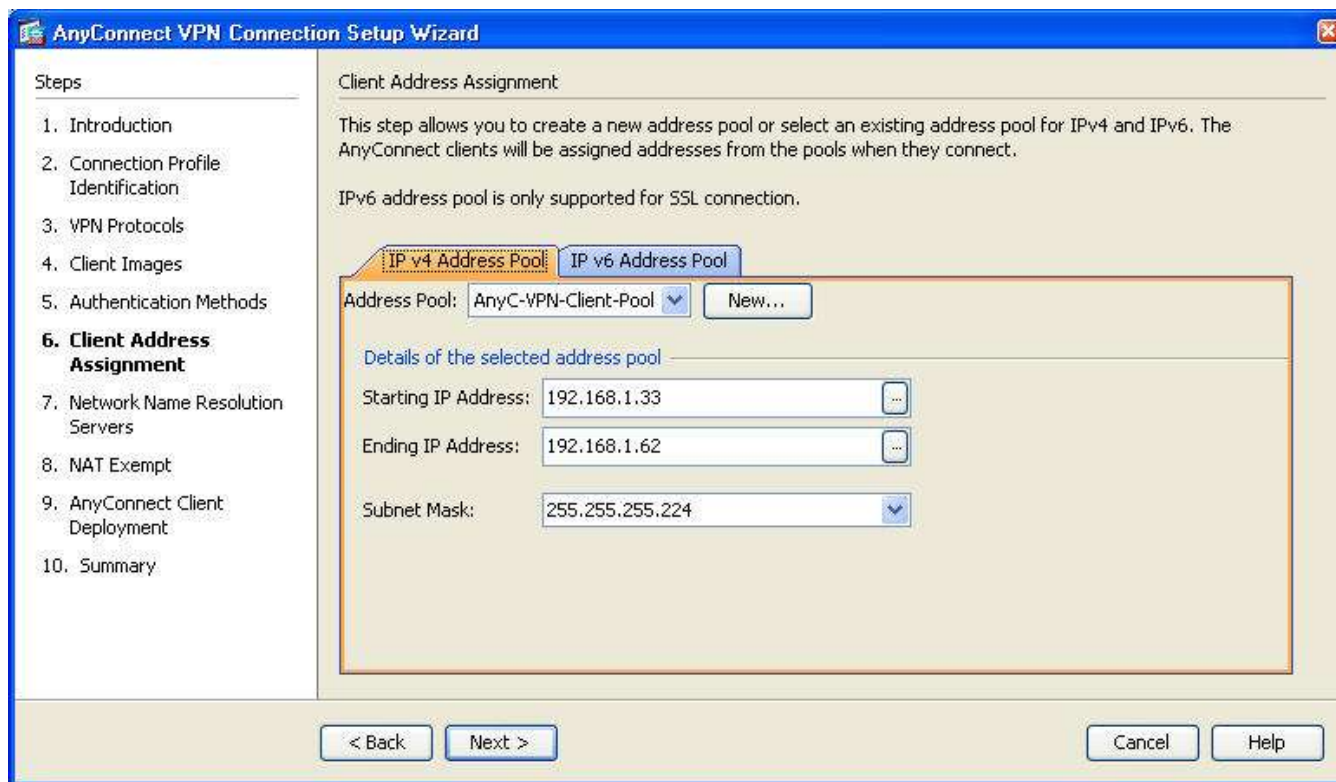


Step 7: Configure AAA local authentication.

- a. On the Authentication Methods screen, ensure that the AAA Server Group is specified as **LOCAL**.
- b. Enter a new user named **VPN-User** with a password of **remote**. Click **Add** to create the new user. Click **Next** to continue.

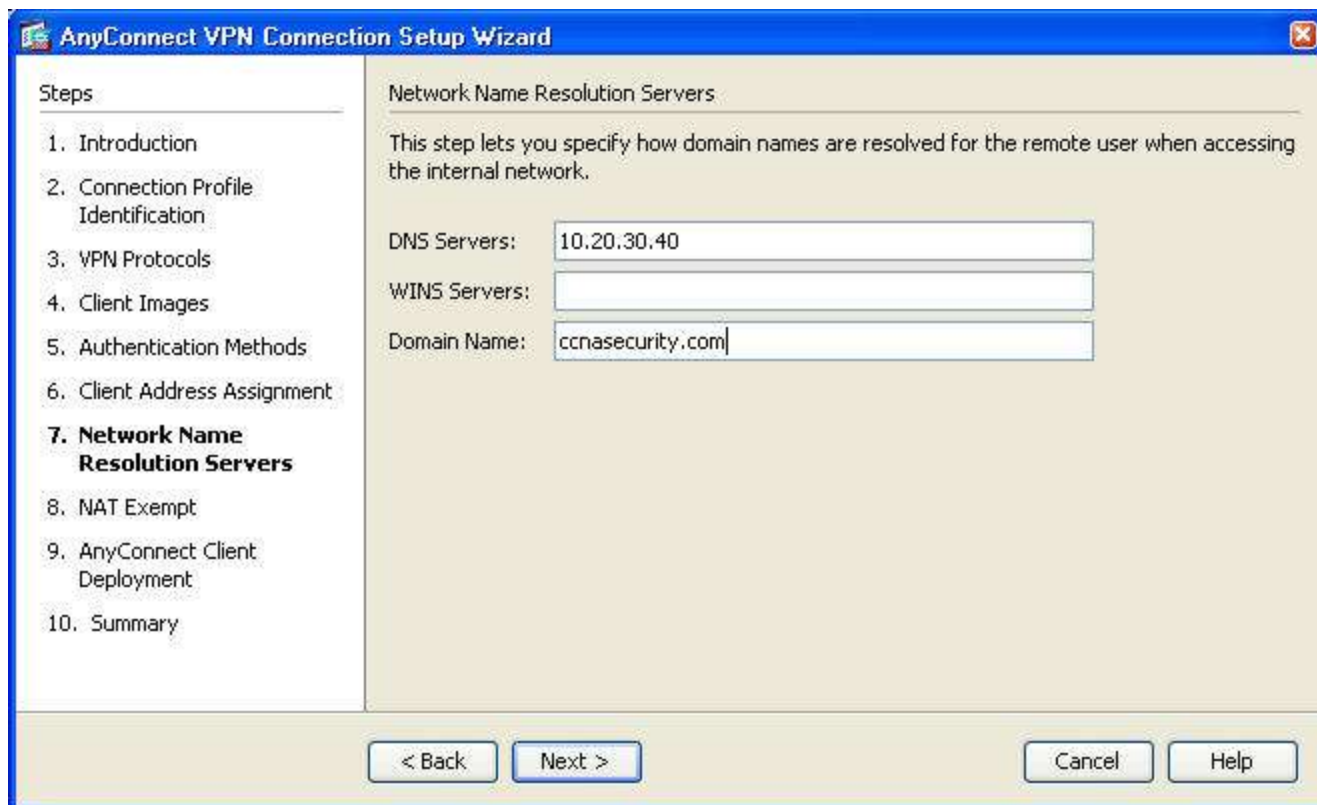
**Step 8: Configure the client address assignment.**

- a. On the Client Address Assignment screen, click **New** to create an IPv4 address pool named **AnyC-VPN-Client-Pool**. Enter a starting IP address of **192.168.1.33**, an ending IP address of **192.168.1.62** and subnet mask of **255.255.255.224**. Click **OK** to close the Add IP Pool window.
- b. Click **Next** to continue.



Step 9: Configure network name resolution.

On the Network Name Resolution Servers screen, enter the IP address of a DNS server. Leave the current domain name as **ccnasecurity.com**. Click **Next** to continue.



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. On the left, a 'Steps' list contains 10 items, with '7. Network Name Resolution Servers' highlighted. The main area is titled 'Network Name Resolution Servers' and contains the text: 'This step lets you specify how domain names are resolved for the remote user when accessing the internal network.' Below this text are three input fields: 'DNS Servers' with the value '10.20.30.40', 'WINS Servers' which is empty, and 'Domain Name' with the value 'ccnasecurity.com'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
- 7. Network Name Resolution Servers**
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 10.20.30.40

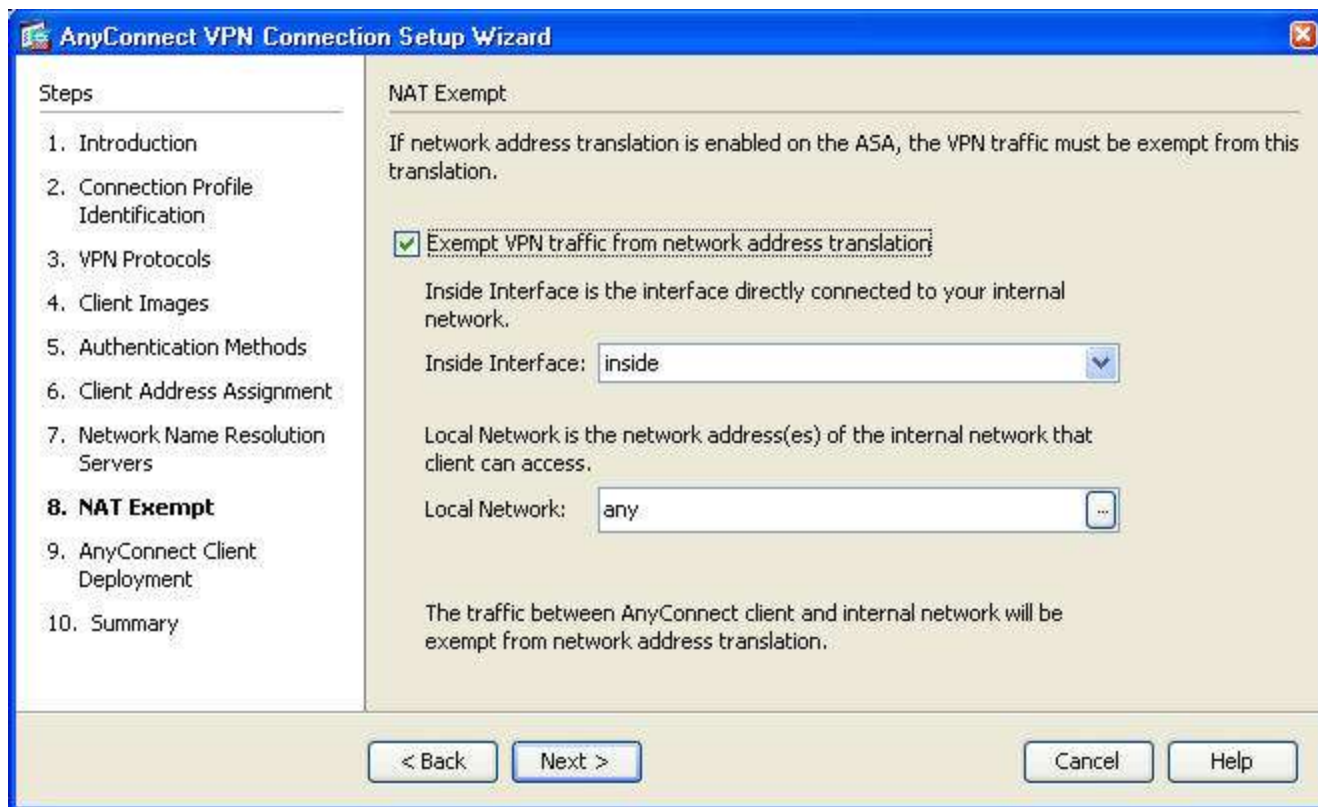
WINS Servers:

Domain Name: ccnasecurity.com

< Back Next > Cancel Help

Step 10: Exempt address translation for VPN traffic.

- a. On the NAT Exempt screen, select the checkbox for **Exempt VPN traffic from network address translation**.
- b. Leave the default entries for the Inside Interface (inside) and the Local Network (any) as they are. Click **Next** to continue.



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window, specifically the 'NAT Exempt' step. On the left, a 'Steps' pane lists 10 steps, with '8. NAT Exempt' highlighted. The main area contains the following text: 'NAT Exempt', 'If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.', a checked checkbox 'Exempt VPN traffic from network address translation', and a description of the 'Inside Interface'. Below this, the 'Inside Interface' is set to 'inside' in a dropdown menu. Another description follows for the 'Local Network', which is set to 'any' in a text field with a browse button. A summary sentence at the bottom states: 'The traffic between AnyConnect client and internal network will be exempt from network address translation.' At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignment
7. Network Name Resolution Servers
- 8. NAT Exempt**
9. AnyConnect Client Deployment
10. Summary

NAT Exempt

If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.

☒ Exempt VPN traffic from network address translation

Inside Interface is the interface directly connected to your internal network.

Inside Interface:

Local Network is the network address(es) of the internal network that client can access.

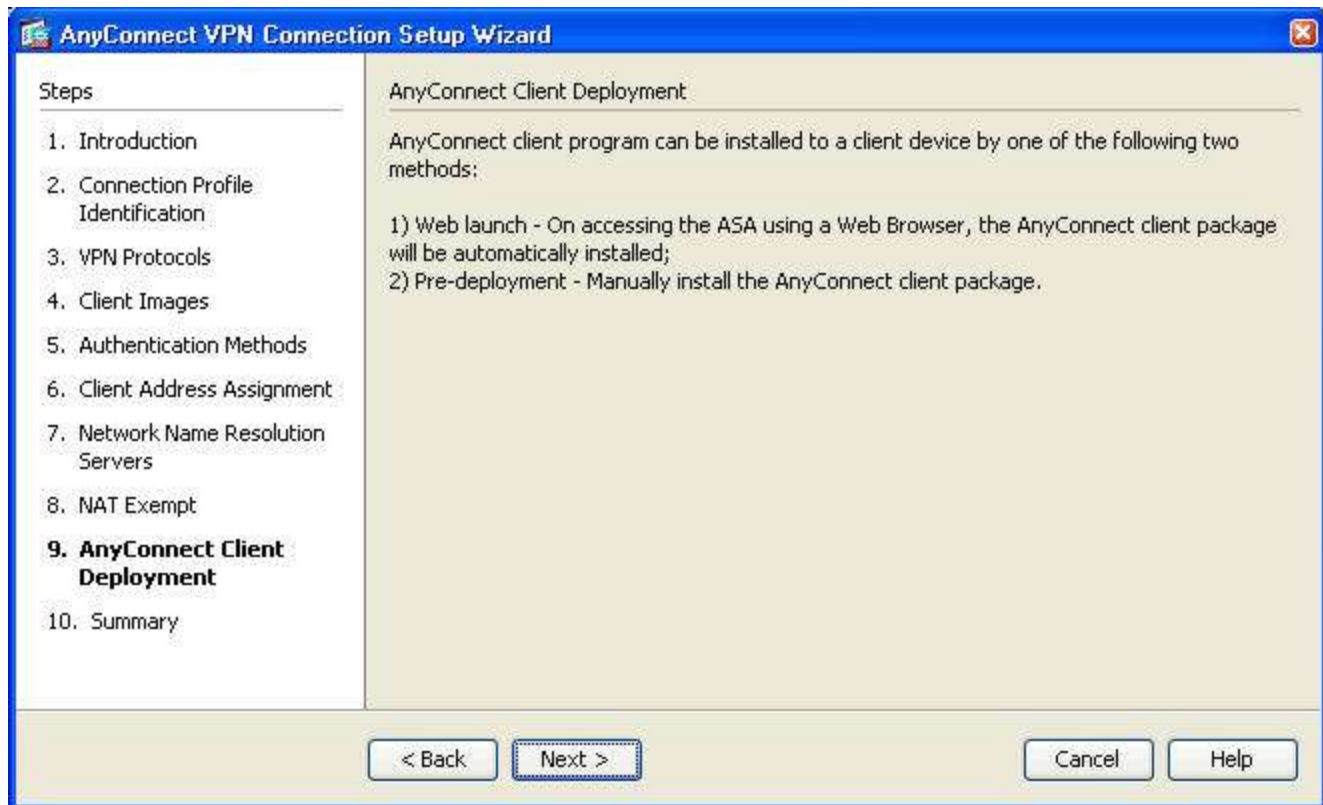
Local Network:

The traffic between AnyConnect client and internal network will be exempt from network address translation.

< Back Next > Cancel Help

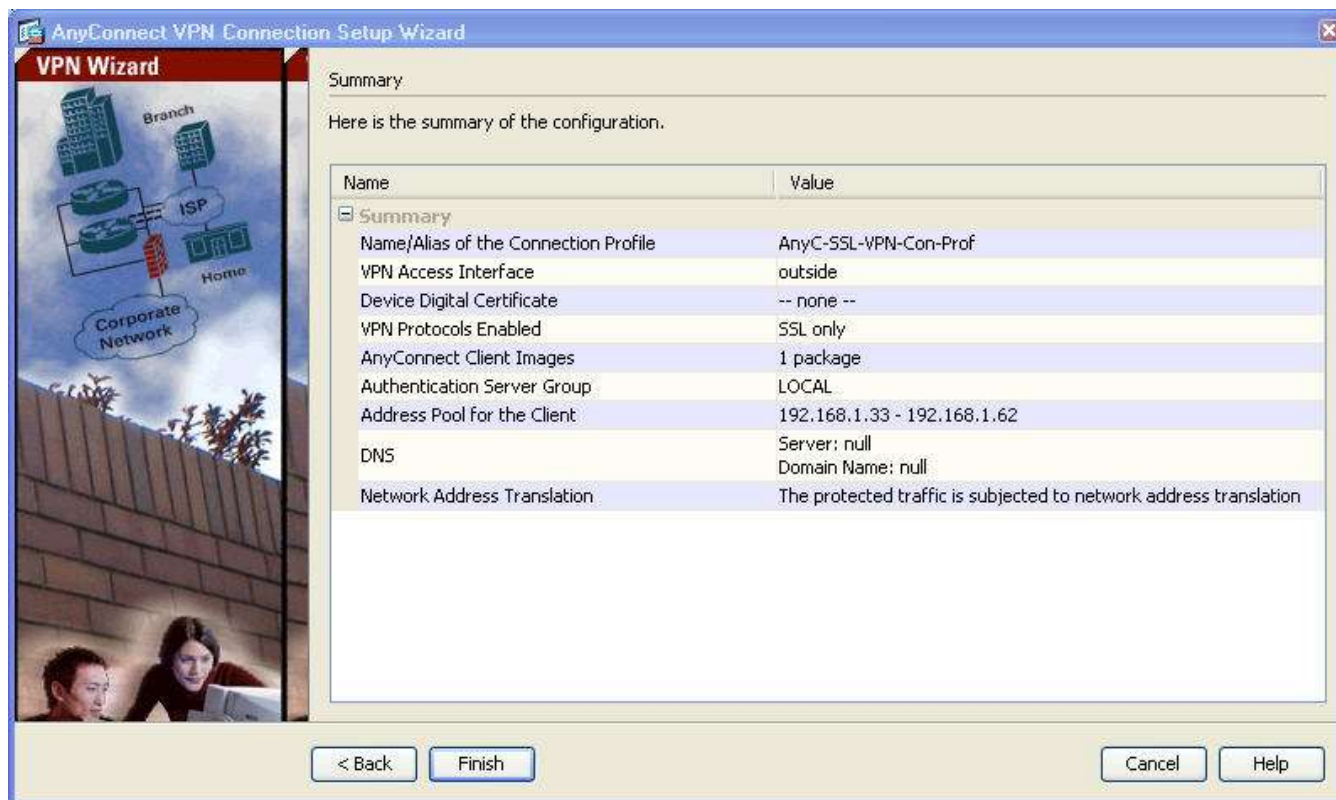
Step 11: AnyConnect client deployment.

On the AnyConnect Client Deployment screen, read the text describing the options and then click **Next** to continue.



Step 12: Review the Summary screen and apply the configuration to the ASA

On the Summary screen, review the configuration description and then click **Finish** to send the commands to the ASA.



Step 13: Verify the AnyConnect client profile.

After the configuration is delivered to the ASA, the AnyConnect Connection Profiles screen is displayed.

The screenshot shows the Cisco ASA configuration interface for 'AnyConnect Connection Profiles'. The left sidebar lists various configuration options under 'Remote Access VPN'. The main pane displays the configuration for 'AnyConnect Connection Profiles'.

Access Interfaces

☒ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☒ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

☒ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ 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](#).

Buttons: Add, Edit, Delete, Find: Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyC-SSL-VPN-Con-Prof	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyC-SSL-VPN-Con-Prof	AAA(LOCAL)	GroupPolicy_AnyC-SSL-VPN-Con-Prof

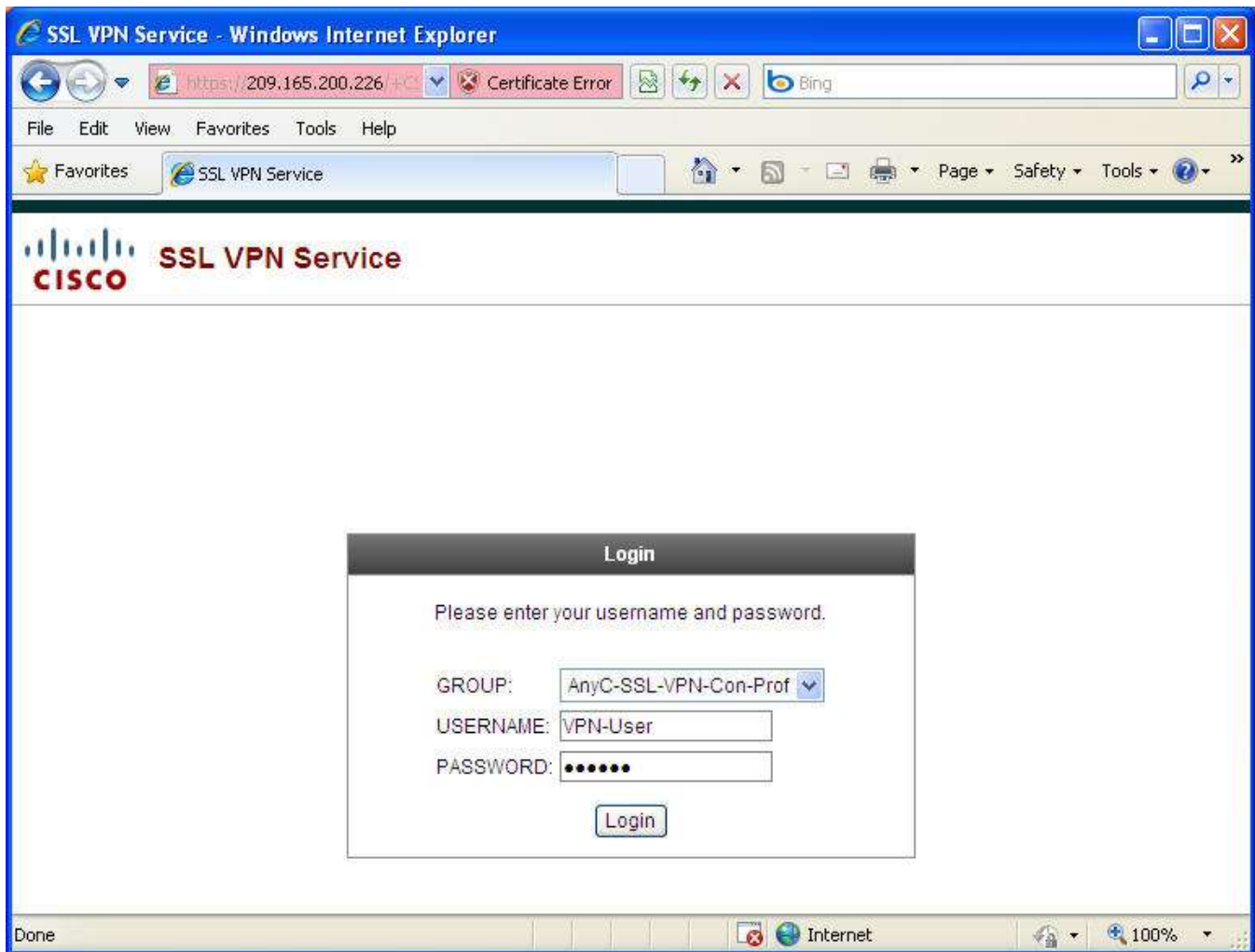
Buttons: Apply, Reset

admin 2 1/27/12 1:45:38 PM UTC

Step 14: Log in from the remote host.

Initially you will establish a clientless SSL VPN connection to the ASA in order to download the AnyConnect client software.

Open a web browser on PC-C and enter the login URL **https://209.165.200.226** for the SSL VPN into the address field. Because SSL is required to connect to the ASA, be sure to use secure HTTP (HTTPS). After entering the URL, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings. Enter the previously created username **VPN-User** with password **remote** and click **Login** to continue.

**Step 15: Accept the security certificate (if required).**

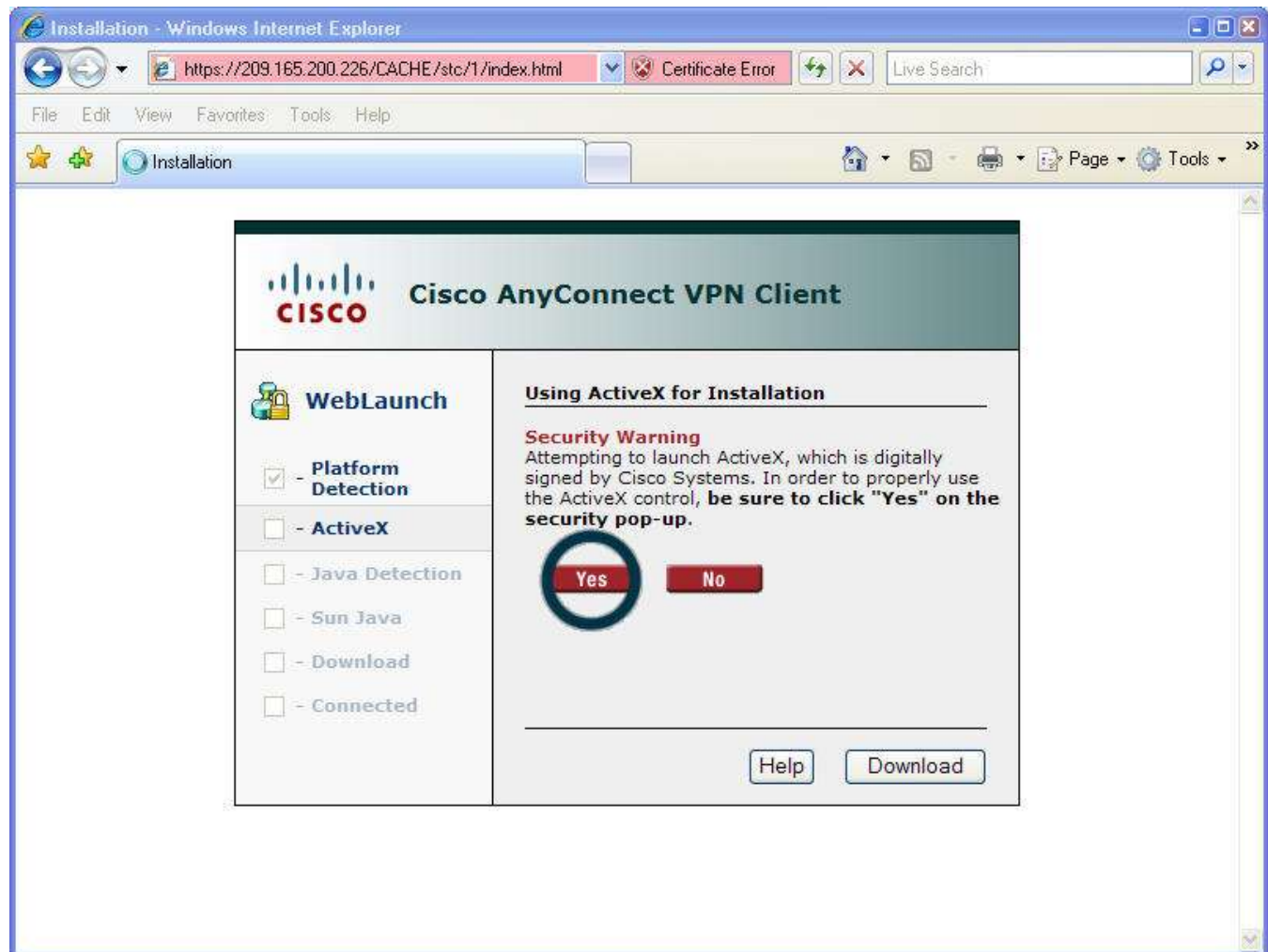
The ASA may request confirmation that this is a trusted site. If requested, then click **Yes** to proceed.

Step 16: Perform platform detection (if required).

The ASA will begin a software auto-download process consisting of a series of compliance checks for the target system. The ASA performs the platform detection by querying the client system in an attempt to identify the type of client connecting to the security appliance. Based on the platform that is identified, the proper software package may be auto-downloaded.

Step 17: Install AnyConnect (if required).

If the AnyConnect client must be downloaded, then a security warning will be displayed on the remote host. Then the ASA will detect whether ActiveX is available on the host system. For ActiveX to operate properly with the Cisco ASA, it is important that the security appliance is added as a trusted network site. ActiveX will be used for client download in the event that a web portal is not in use.

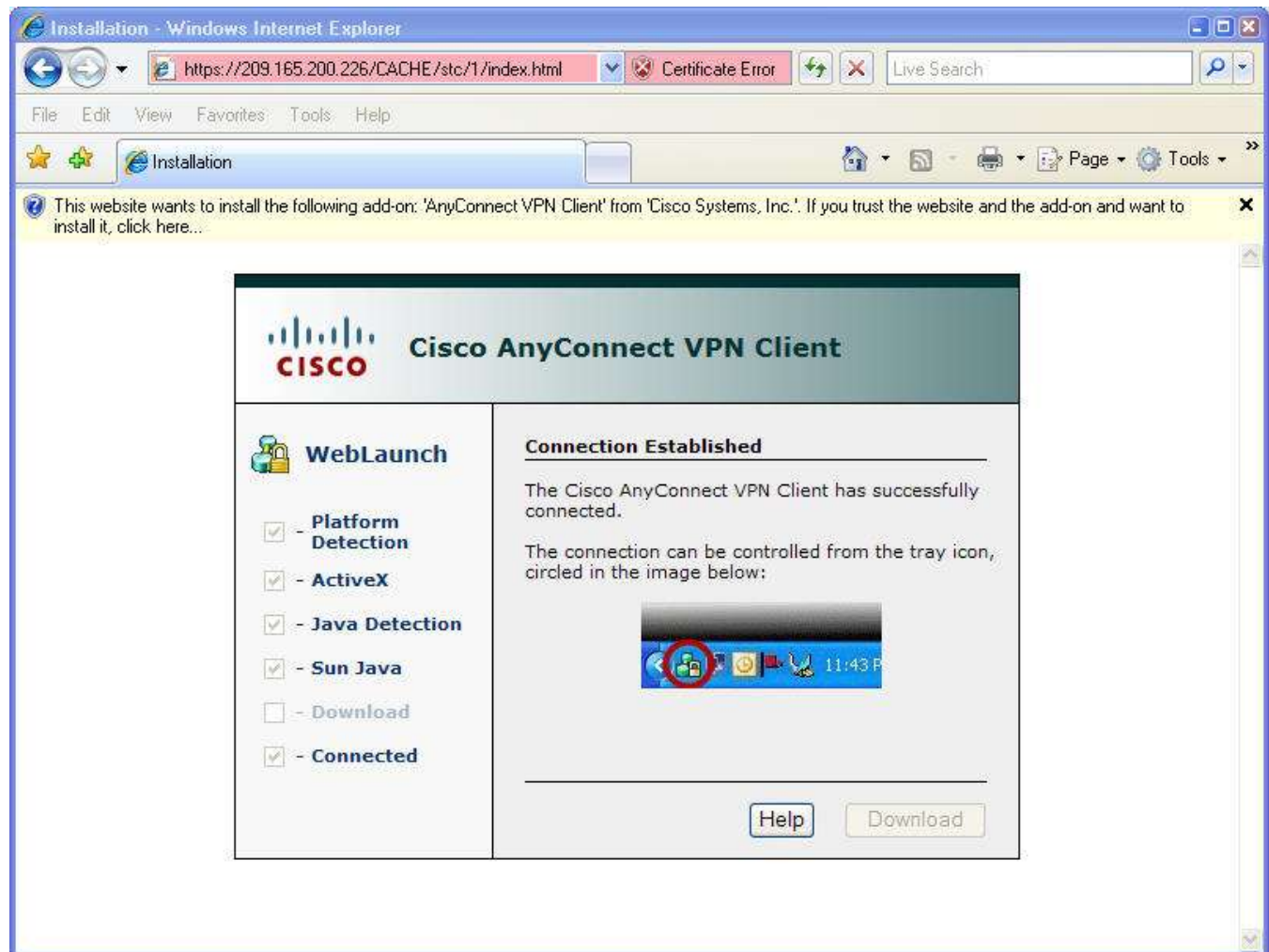


To continue, choose **Install**. If requested, click **Yes**. The VPN Client Installer will begin and another security alert window may appear. If required, click **Yes** to continue and accept the security certificate.



Step 18: Client connection is established with the ASA.

Once the client completes the auto-download of the Cisco AnyConnect SSL VPN Client, the web session will automatically launch the Cisco AnyConnect SSL VPN Client and will attempt to log the user into the network using the same credentials that are supplied when logging into the web portal.



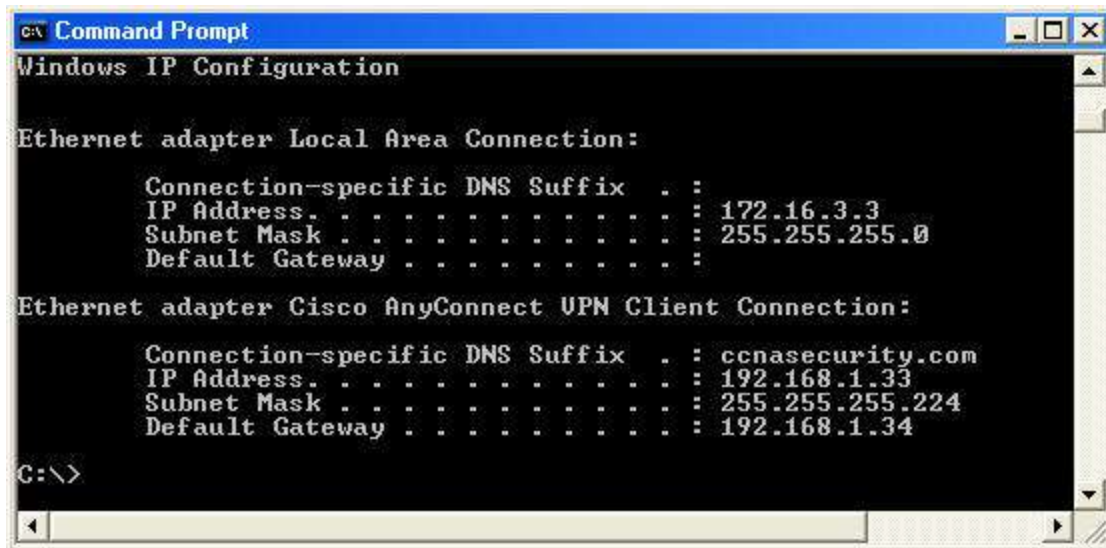
Step 19: Confirm VPN connectivity.

When the full tunnel SSL VPN connection is established, an icon will appear in the system tray that signifies that the client has successfully connected to the SSL VPN network.

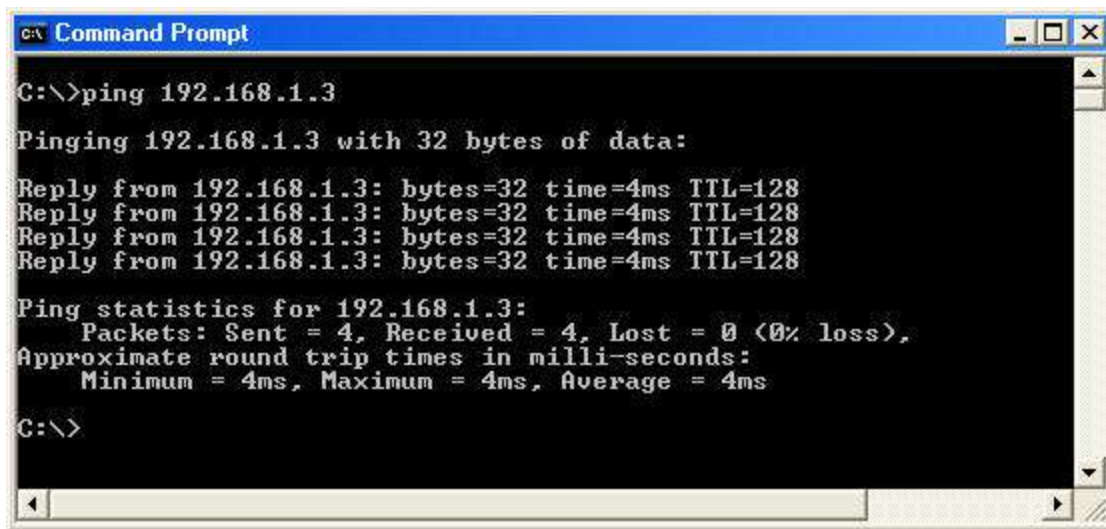
- a. Display connection statistics and information by double-clicking the **AnyConnect** icon in the system tray. This client interface may also be used to log out the user. Note the inside IP address that is assigned to the client from the VPN pool (192.168.1.33-.62).



- b. From a command prompt on remote host PC-C, verify the IP addressing using the `ipconfig` command. There should be two IP addresses listed. One is for the PC-C remote host local IP address (172.16.3.3) and the other is the IP address assigned by the ASA for the SSL VPN tunnel (192.168.1.33).



- c. From remote host PC-C, ping inside host PC-B (192.168.1.3) to verify connectivity.



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\>
```

Note: Future SSL VPN sessions may be launched through the web portal or through the installed Cisco AnyConnect SSL VPN Client.



Step 20: Use the ASDM Monitor to view the AnyConnect remote user session.

While the remote user at PC-C is still logged in using the AnyConnect client, you can view the session statistics using ASDM monitor.

From the menu bar, click the **Monitoring** button and then choose **VPN > VPN Statistics > Sessions**. Click the **Filter By** pull-down menu and choose **AnyConnect Client**. You should see the **VPN-User** session logged in from PC-C, which has been assigned an inside network IP address of 192.168.1.33 by the ASA.

Note: You may need to click the **Refresh** button on the menu bar to display the remote user session.

The screenshot shows the Cisco ASDM 6.4 interface for ASA - 192.168.1.1. The left sidebar is expanded to show the **VPN** section, with **Sessions** selected. The main content area displays the **Monitoring > VPN > VPN Statistics > Sessions** page. At the top, there is a summary table:

Type	Active	Cumulative	Peak Concurrent	Inactive
AnyConnect Client	1	1	1	0
SSL/TLS/DTLS	1	1	1	0

Below this is a **Filter By:** dropdown menu set to **AnyConnect Client**, with a **Filter** button. The main table lists the session details:

Username	IP Address	Group Policy	Connection Profile	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
VPN-User	192.168.1.33	GroupPolicy_AnyC-SSL-VPN-Con-Prof	AnyC-SSL-VPN-Con-Prof	Clientless SSL-Tunnel	DTLS-Tunnel	13:50:56 UTC Fri Jan 27 2012	0h:13m:44s	2414721	33838

Buttons for **Details**, **Logout**, and **Ping** are available for the selected session. Below the table, there is a **Logout By:** dropdown menu set to **-- All Sessions --**, a **Logout Sessions** button, and a **Refresh** button. A note states: "To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu." The status bar at the bottom shows "Data Refreshed Successfully.", the user "admin", and the time "1/27/12 2:06:27 PM UTC".

Reflection:

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

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

3. 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 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	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)
2800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	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.				