1. CCNA Security

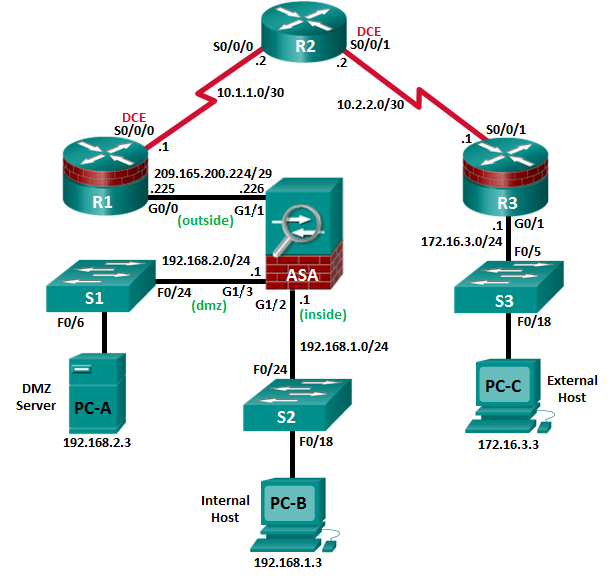
Chapter 10 – Configure Clientless Remote Access SSL VPNs Using ASDM (Instructor Version)

(ASA-5506 / Equiv)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

|  |  |
| --- | --- |
|  | **This lab has been updated for use on NETLAB+.**  [**www.netdevgroup.com**](https://www.netdevgroup.com/) |

1. Topology



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

1. 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 |

1. 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.

1. 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 VPNwizard 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.

**Instructor Note**: Instructions for erasing switches and routers are provided in Chapter 0.0.0.0. Instructions for erasing the ASA, accessing the console, and accessing ASDM are provided in this lab.

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.

* + 1. Configure R1 using the CLI script.
       1. 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

* + 1. Configure R2 using the CLI script.
       1. 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

* + 1. Configure R3 using the CLI script.
       1. 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

* + 1. **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.

* + 1. **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.

* + 1. **Save the basic running configuration for each router and switch.**

1. Accessing the ASA Console and ASDM
   * 1. Clear the previous ASA configuration settings.
        1. 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.

* + - 1. 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**.
    1. 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.

* + - 1. When prompted to preconfigure the firewall through interactive prompts (Setup mode), respond with **no**.
      2. Enter privileged EXEC mode with the **enable** command. The password should be blank (no password).
    1. 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.

* + - 1. 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.
      2. Enter global configuration mode. When prompted to enable anonymous call-home reporting, respond **no**.
      3. 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

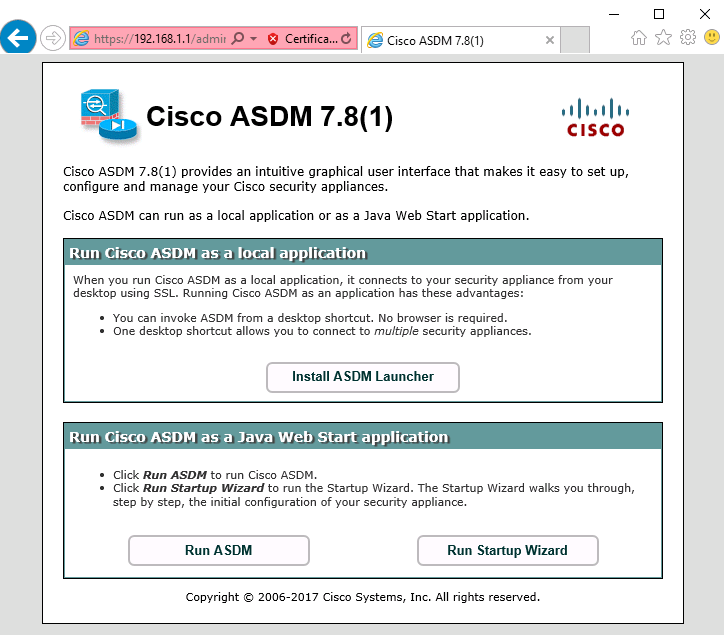
* + - 1. At the privileged EXEC mode prompt, issue the **write mem** (or **copy run start**) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.
    1. Access ASDM.
       1. Open a browser on PC-B and test the HTTPS access to the ASA by entering **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.

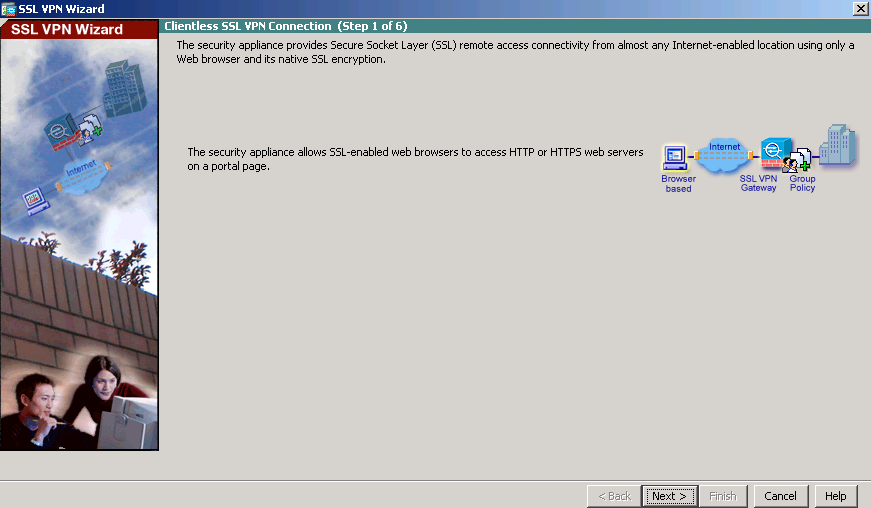
* + - 1. At the ASDM welcome page, click **Run ASDM**. The ASDM-IDM Launcher will display. Log in as user **admin01** with password **admin01pass**.

**Note:** You will need to accept all security messages and/or add the ASA IP address to the allowed list of IP addresses in Java.

If the “*Run ASDM*” button via Java is not accessible, access your ASA via **https://<ip\_address>/admin/public/asdm.jnlp** to download the JNLP file and then open the file to continue using ASDM.



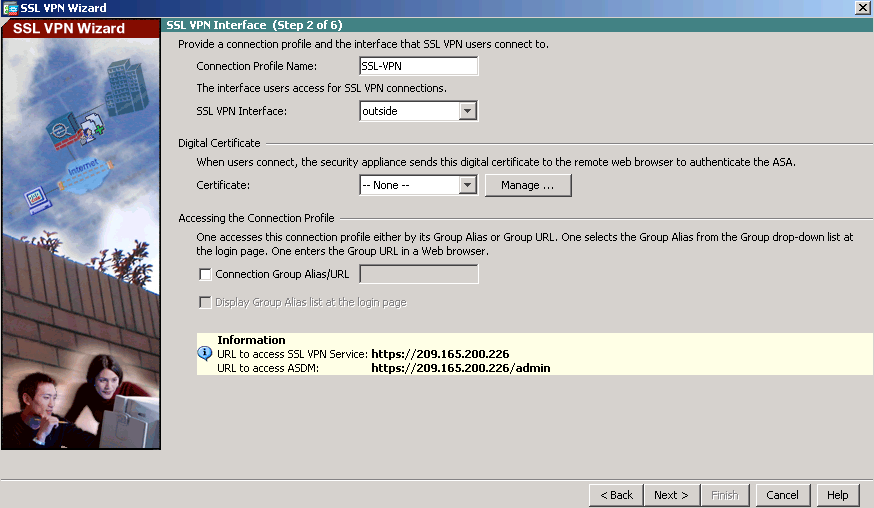
1. Configuring Clientless SSL VPN Remote Access Using ASDM
   * 1. Start the VPN wizard.
        1. On the ASDM main menu, click **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard**. The Clientless SSL VPN Connection screen displays.



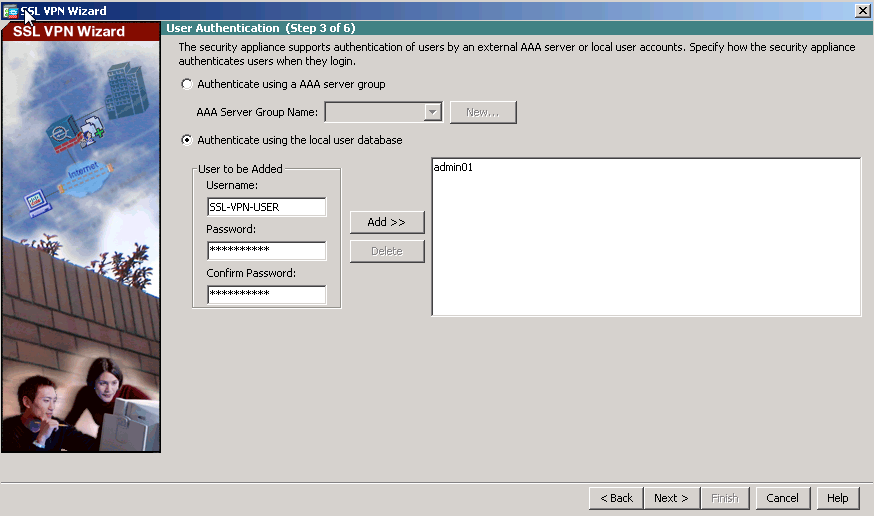
* + - 1. Review the on-screen text and topology diagram, and then click **Next** to continue.
    1. Configure the SSL VPN user interface.
       1. On the SSL VPN Interfacescreen, configure **SSL-VPN** as the Connection Profile Name, and specify **outside** as the interface to which outside users will 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.

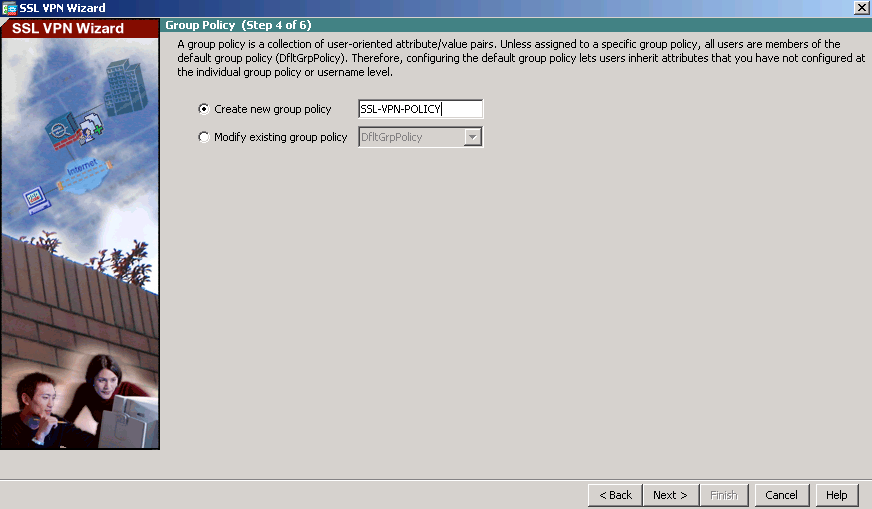
The SSL VPN Interface screen provides links in the Information section. These links identify the URLs that need to be used for the SSL VPN service access (log in) and for Cisco ASDM access (to access the Cisco ASDM software).



* + - 1. Click **Next** to continue.
    1. Configure AAA user authentication.
       1. On the User Authenticationscreen, click **Authenticate using the local user database.**
       2. Enter the user name **SSL-VPN-USER** with password **cisco12345**.
       3. Click **Add** to create the new user and click **Next** to continue.



* + 1. Configure the VPN group policy.
       1. 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.)

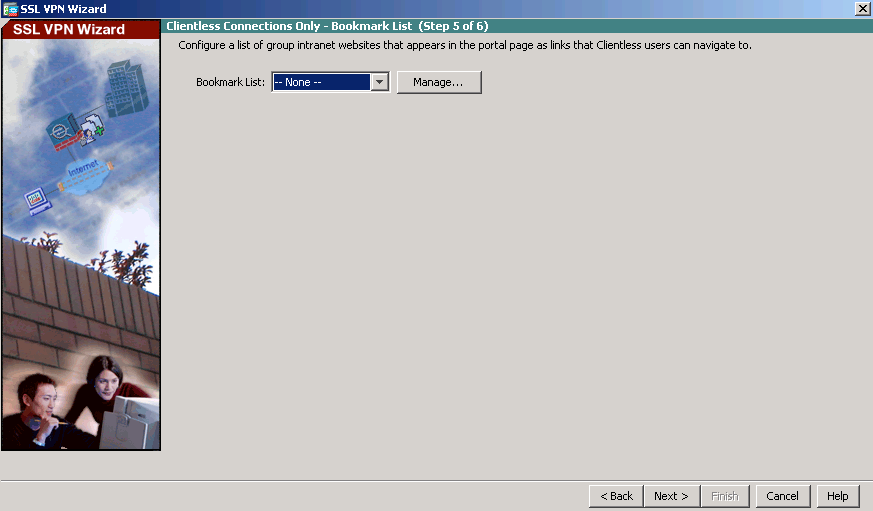


* + - 1. Click **Next** to continue.
    1. Configure the bookmark list (clientless connections only).

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.

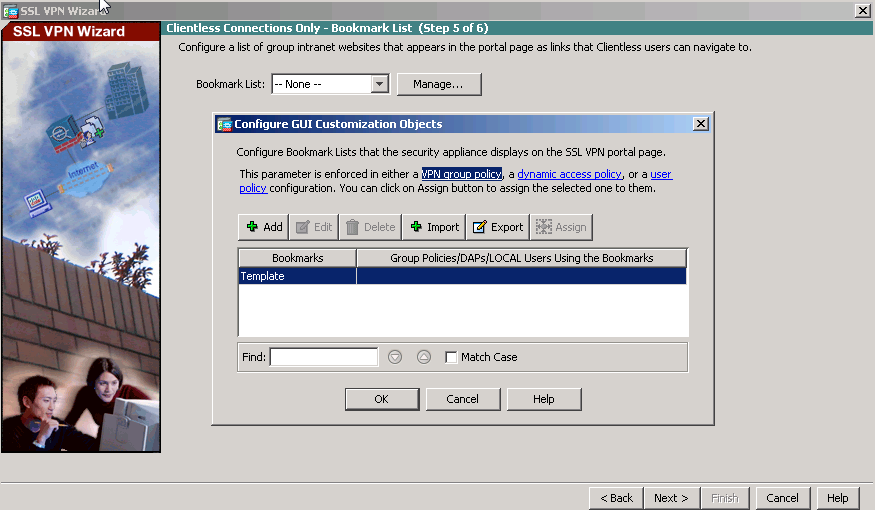
**Note:** There are no configured bookmark lists by default and, therefore, they must be configured by the network administrator.

* + - 1. On the Clientless Connections Only – Bookmark List screen, click **Manage** to create an HTTP server bookmark in the bookmark list.

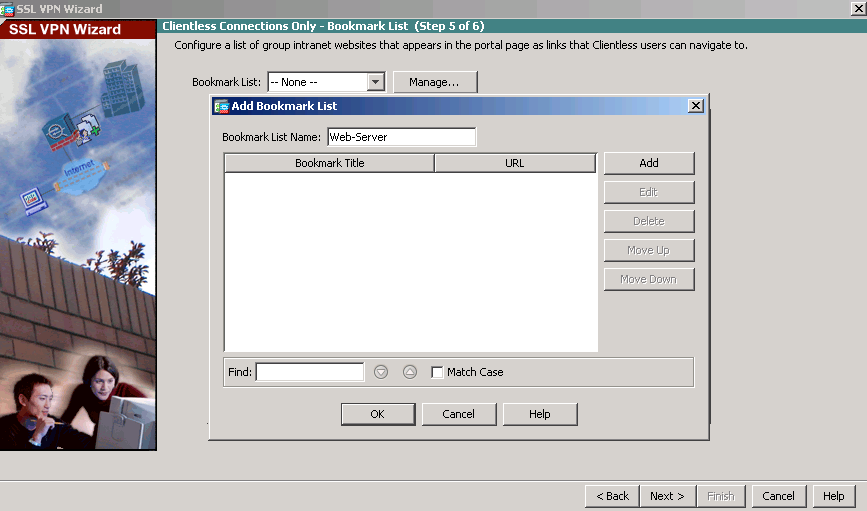


* + - 1. In the Configure GUI Customization Objects window, click **Add** to open the Add Bookmark List window. Name the list **Web-Server**.

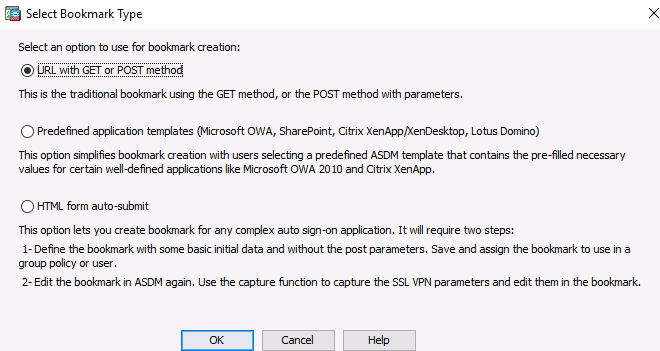
**Note**: If the Web-Server bookmark list is shown as available from a previous configuration, you can delete it in ASDM and re-create it.



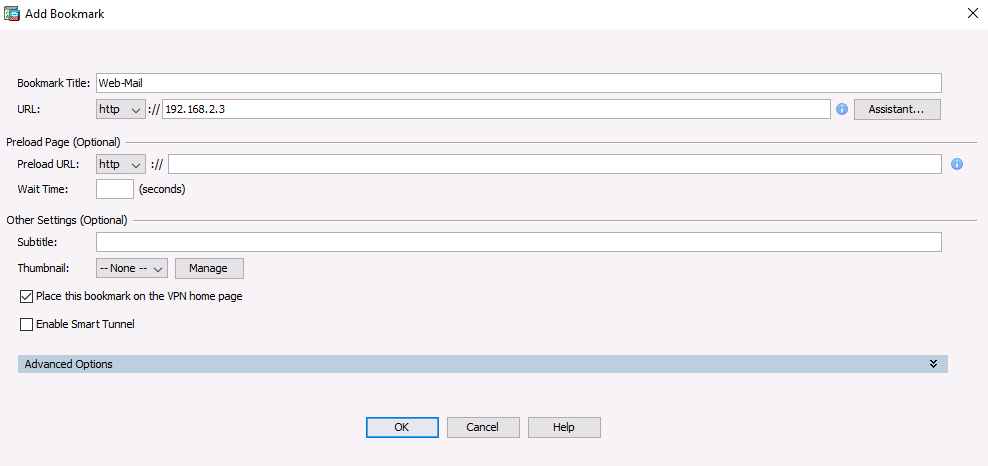
* + - 1. In the Add Bookmark List window, click **Add** to open the Select Bookmark Type window.



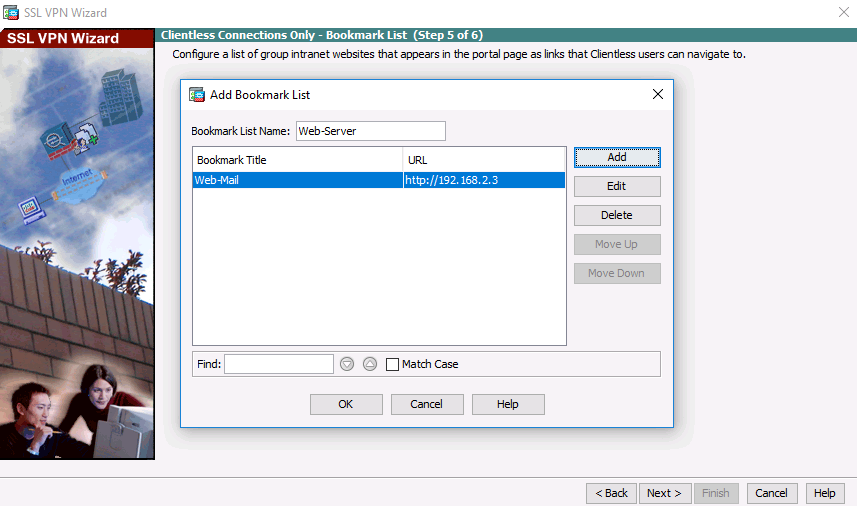
* + - 1. As shown in the figure, the ASDM can create three types of bookmarks. Select the **URL with GET or POST** **method**, click **OK.**



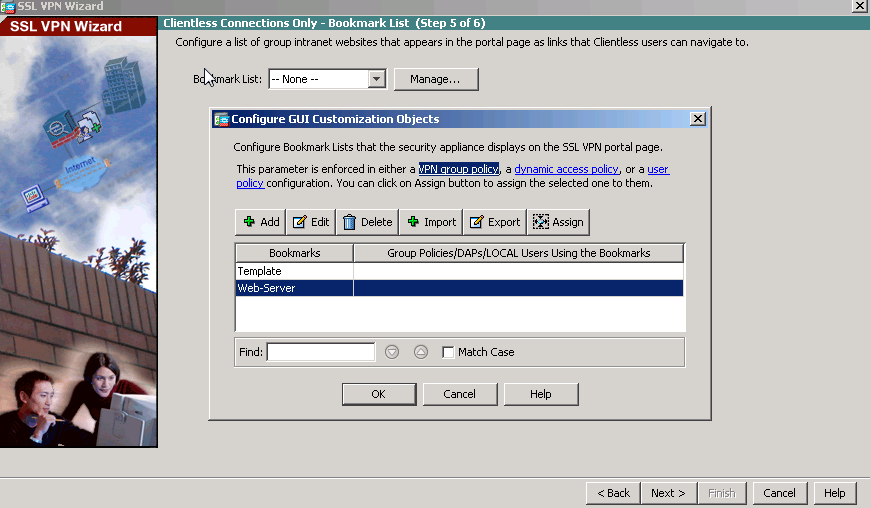
* + - 1. Enter the bookmark title and enter the server destination IP address or hostname as the URL to be used with the bookmark entry. In this example, the Bookmark Title of **Web-Mail** is entered and an internal IP address of **192.168.2.3** (the DMZ server) is specified. If this server has HTTP web services with web mail installed and functional, the outside users are able to access the server from the ASA portal when they connect.



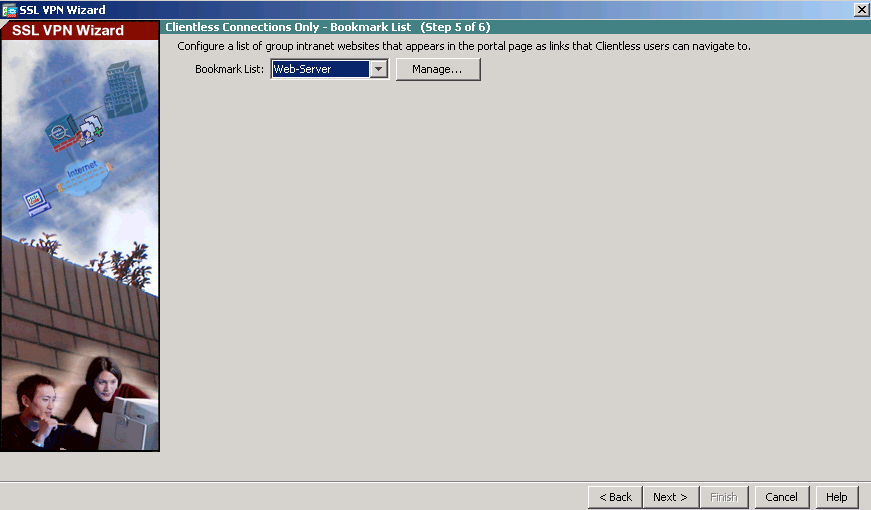
* + - 1. Click **OK** to continue and return to the Add Bookmark List window which now displays the Web-Server bookmark title and URL.



* + - 1. Click **OK** to continue and return to the Configure GUI Customization Objects window which now displays the Web-Server bookmark.

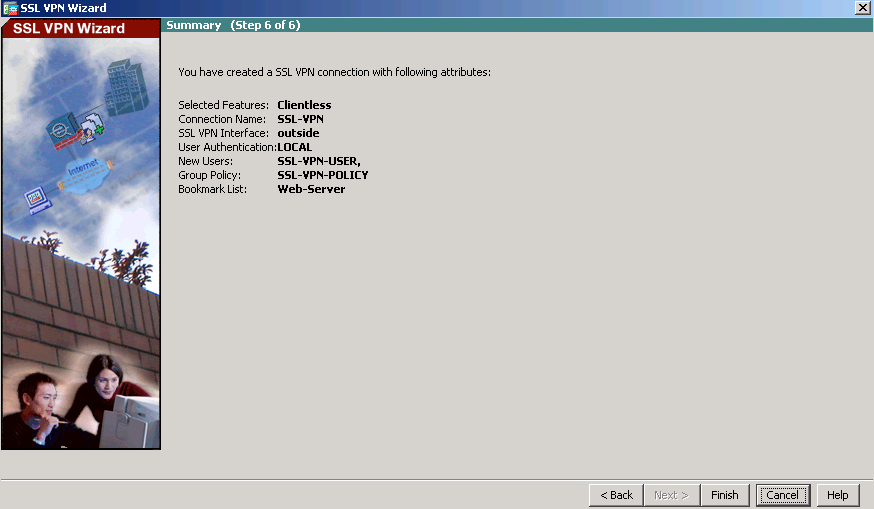


* + - 1. Click **OK** to continue and return to the Bookmark List window and click **Next** to continue.



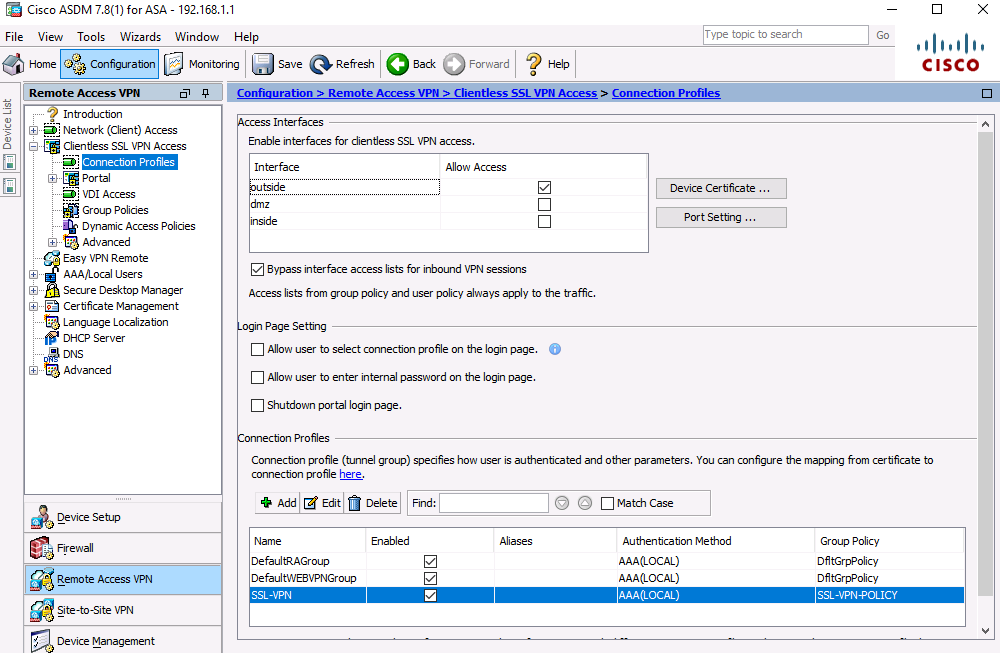
* + 1. Review the configuration summary and deliver the commands to the ASA.

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



* + 1. 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.



* + 1. Verify VPN access from the remote host.
       1. 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.

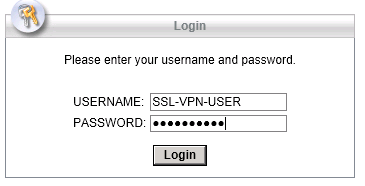
**Note**: If you encounter a prompt stating that the connection is not trusted or secure, accept the self-signed certificate to continue.

* + - 1. The Logon window should display. Enter the previously configured username **SSL-VPN-USER** and password **cisco12345*,*** and click **Logon** to continue.

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

**Note:** If the AnyConnect client fails authentication, reset the password.

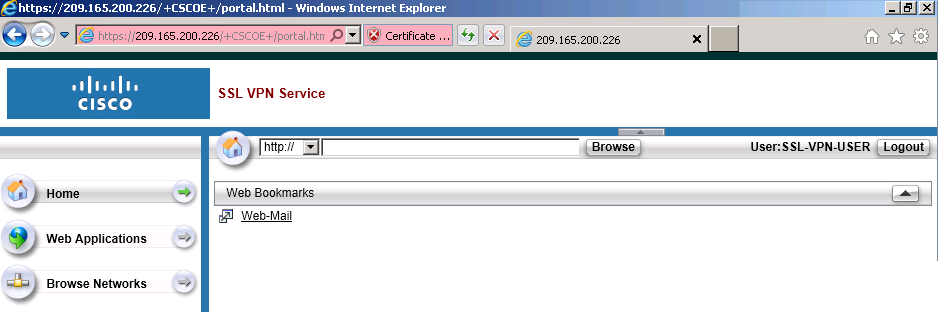
**Configuration > Remote Access VPN > Local Users > SSL-VPN-USER > Edit > Identity > Change user password** (retype in the correct username and password combo).Click **OK** followed by clicking **Apply**.



* + 1. 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.

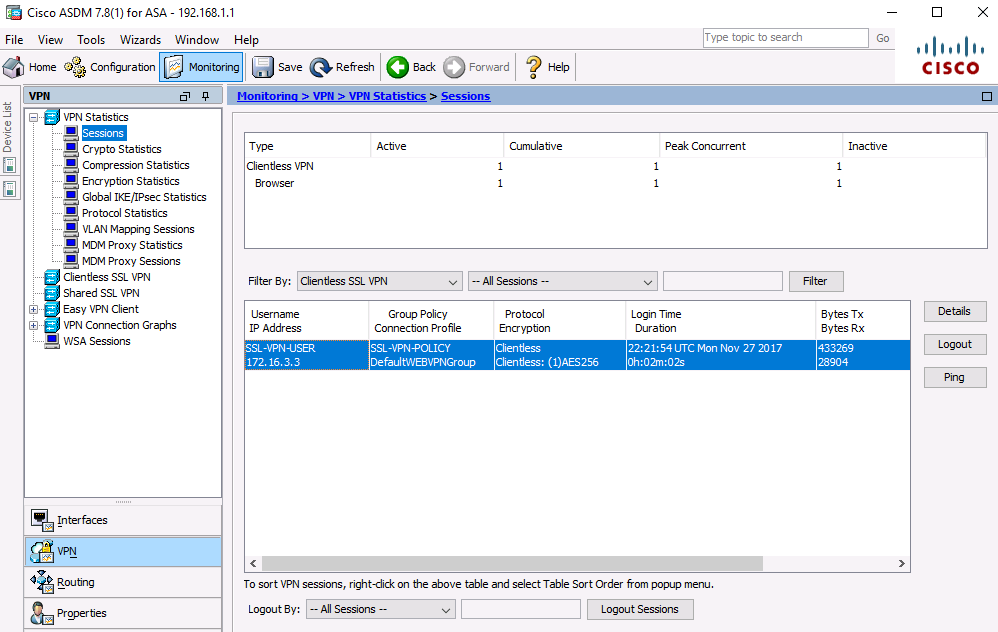


* + 1. View the clientless remote user session using the ASDM Monitor.

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.

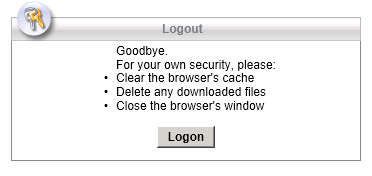
From the ASDM menu bar on PC-B, click **Monitoring** and then select **VPN** > **VPN Statistics** > **Sessions**. Click the **Filter By** pull-down list and select **Clientless SSL VPN**. You should see the SSL-VPN-USER session logged in from PC-C (172.16.3.3).

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



* + 1. 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.



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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

They are easier to setup because only a browser is required and no client software needs to be installed. They can be used to limit access to very specific resources based on URLs that are defined by network administration.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Client-based VPNs can offer a more secure tunnel, if using IPsec, but are somewhat more complex to configure.

1. 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. | | | | |

1. Device Configs
2. ASA 5506 Final Config
3. CCNAS-ASA# show run
4. : Saved
5. :
6. : Serial Number: JAD2002064E
7. : Hardware: ASA5506W, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
8. :
9. ASA Version 9.8(2)
10. !
11. hostname CCNAS-ASA
12. domain-name ccnasecurity.com
13. enable password $sha512$5000$CQjFkol8u9efEcwrY9udDQ==$HeOdwc6BbBO/yKUnl4mUfw== pbkdf2
14. xlate per-session deny tcp any4 any4
15. xlate per-session deny tcp any4 any6
16. xlate per-session deny tcp any6 any4
17. xlate per-session deny tcp any6 any6
18. xlate per-session deny udp any4 any4 eq domain
19. xlate per-session deny udp any4 any6 eq domain
20. xlate per-session deny udp any6 any4 eq domain
21. xlate per-session deny udp any6 any6 eq domain
22. names
23. !
24. interface GigabitEthernet1/1
25. nameif outside
26. security-level 0
27. ip address 209.165.200.226 255.255.255.248
28. !
29. interface GigabitEthernet1/2
30. nameif inside
31. security-level 100
32. ip address 192.168.1.1 255.255.255.0
33. !
34. interface GigabitEthernet1/3
35. nameif dmz
36. security-level 70
37. ip address 192.168.2.1 255.255.255.0
38. !
39. interface GigabitEthernet1/4
40. shutdown
41. no nameif
42. no security-level
43. no ip address
44. !
45. interface GigabitEthernet1/5
46. shutdown
47. no nameif
48. no security-level
49. no ip address
50. !
51. interface GigabitEthernet1/6
52. shutdown
53. no nameif
54. no security-level
55. no ip address
56. !
57. interface GigabitEthernet1/7
58. shutdown
59. no nameif
60. no security-level
61. no ip address
62. !
63. interface GigabitEthernet1/9
64. shutdown
65. no nameif
66. no security-level
67. no ip address
68. !
69. interface Management1/1
70. management-only
71. shutdown
72. no nameif
73. no security-level
74. no ip address
75. !
76. ftp mode passive
77. dns server-group DefaultDNS
78. domain-name ccnasecurity.com
79. object network inside-net
80. subnet 192.168.1.0 255.255.255.0
81. object network dmz-server
82. host 192.168.2.3
83. access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
84. pager lines 24
85. mtu outside 1500
86. mtu inside 1500
87. mtu dmz 1500
88. icmp unreachable rate-limit 1 burst-size 1
89. no asdm history enable
90. arp timeout 14400
91. no arp permit-nonconnected
92. arp rate-limit 16384
93. !
94. object network inside-net
95. nat (inside,outside) dynamic interface
96. object network dmz-server
97. nat (dmz,outside) static 209.165.200.227
98. access-group OUTSIDE-DMZ in interface outside
99. route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
100. timeout xlate 3:00:00
101. timeout pat-xlate 0:00:30
102. timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
103. timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
104. timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
105. timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
106. timeout tcp-proxy-reassembly 0:01:00
107. timeout floating-conn 0:00:00
108. timeout conn-holddown 0:00:15
109. timeout igp stale-route 0:01:10
110. user-identity default-domain LOCAL
111. aaa authentication telnet console LOCAL
112. aaa authentication ssh console LOCAL
113. aaa authentication http console LOCAL
114. aaa authentication login-history
115. http server enable
116. http 192.168.1.0 255.255.255.0 inside
117. no snmp-server location
118. no snmp-server contact
119. service sw-reset-button
120. crypto ipsec security-association pmtu-aging infinite
121. crypto ca trustpool policy
122. telnet 192.168.1.0 255.255.255.0 inside
123. telnet timeout 10
124. ssh stricthostkeycheck
125. ssh 192.168.1.0 255.255.255.0 inside
126. ssh timeout 10
127. ssh key-exchange group dh-group1-sha1
128. console timeout 0
129. threat-detection basic-threat
130. threat-detection statistics access-list
131. no threat-detection statistics tcp-intercept
132. webvpn
133. enable outside
134. cache
135. disable
136. error-recovery disable
137. group-policy SSL-VPN-POLICY internal
138. group-policy SSL-VPN-POLICY attributes
139. vpn-tunnel-protocol ssl-clientless
140. webvpn
141. url-list value Web\_Server
142. dynamic-access-policy-record DfltAccessPolicy
143. username SSL-VPN-USER password $sha512$5000$N1ajK/bSMww9HuD/r6YLFA==$zOJ/ege6l65QAsHLQCgZfA== pbkdf2 privilege 0
144. username SSL-VPN-USER attributes
145. vpn-group-policy SSL-VPN-POLICY
146. username admin01 password $sha512$5000$oEhbf+nhDQXP07KnlaJ2jA==$DA6QQI066mXsAKo4erKlOg== pbkdf2
147. tunnel-group SSL-VPN type remote-access
148. tunnel-group SSL-VPN general-attributes
149. default-group-policy SSL-VPN-POLICY
150. !
151. class-map inspection\_default
152. match default-inspection-traffic
153. !
154. policy-map type inspect dns preset\_dns\_map
155. parameters
156. message-length maximum client auto
157. message-length maximum 512
158. no tcp-inspection
159. policy-map global\_policy
160. class inspection\_default
161. inspect ftp
162. inspect h323 h225
163. inspect h323 ras
164. inspect ip-options
165. inspect netbios
166. inspect rsh
167. inspect rtsp
168. inspect skinny
169. inspect esmtp
170. inspect sqlnet
171. inspect sunrpc
172. inspect tftp
173. inspect sip
174. inspect xdmcp
175. inspect dns preset\_dns\_map
176. inspect icmp
177. policy-map type inspect dns migrated\_dns\_map\_2
178. parameters
179. message-length maximum client auto
180. message-length maximum 512
181. no tcp-inspection
182. policy-map type inspect dns migrated\_dns\_map\_1
183. parameters
184. message-length maximum client auto
185. message-length maximum 512
186. no tcp-inspection
187. !
188. service-policy global\_policy global
189. prompt hostname context
190. no call-home reporting anonymous
191. call-home
192. profile CiscoTAC-1
193. no active
194. destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
195. destination address email callhome@cisco.com
196. destination transport-method http
197. subscribe-to-alert-group diagnostic
198. subscribe-to-alert-group environment
199. subscribe-to-alert-group inventory periodic monthly
200. subscribe-to-alert-group configuration periodic monthly
201. subscribe-to-alert-group telemetry periodic daily
202. Cryptochecksum:e875444854165549c9bb97a5a0116a75
203. : end
204. Router R1

R1#show run

Building configuration...

Current configuration : 2116 bytes

!

! Last configuration change at 21:04:09 UTC Tue Jan 6 2015

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$NxjzpK6dd08tuk$QDF7wpeiijoH80x.yVc2pwsODmSbabN5d0OQmOgHgEk

!

no aaa new-model

memory-size iomem 15

!

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

voice-card 0

!

license udi pid CISCO2911/K9 sn FTX1713ALKC

license accept end user agreement

license boot module c2900 technology-package securityk9

license boot module c2900 technology-package uck9

license boot module c2900 technology-package datak9

!

username admin01 secret 9 $9$bv0p..7dLnvX0k$ho53wilFSM.lBCd.P97.PqbWhZMYqPMTDwBQ3lbcO8g

!

redundancy

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 209.165.200.225 255.255.255.248

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/2

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

clock rate 125000

!

interface Serial0/0/1

no ip address

shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

!

control-plane

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none

mgcp behavior comedia-check-media-src disable

mgcp behavior comedia-sdp-force disable

!

mgcp profile default

!

gatekeeper

shutdown

!

line con 0

exec-timeout 5 0

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1  
line vty 0 4  
 exec-timeout 5 0  
 logging synchronous  
 login local  
 transport input ssh  
!  
scheduler allocate 20000 1000  
!end

1. Router R2

R2#show run

Building configuration...

Current configuration : 2138 bytes

!

! Last configuration change at 17:05:46 UTC Thu Nov 30 2017

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9 $9$F9BnTpKC4XoNcE$rMzDpGtwCFY24D6hdyppkKAUVE/DZjNiVG9Yj4OWhrc

!

no aaa new-model

memory-size iomem 15

!

ip domain name ccnasecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

voice-card 0

!

license udi pid CISCO2911/K9 sn FTX1713ALJP

license boot module c2900 technology-package securityk9

license boot module c2900 technology-package uck9

license boot module c2900 technology-package datak9

!

username admin01 secret 9 $9$XeXYLYiVZL9FZ.$FzD3Tx4zhvG1QUsKAD1MxebR2sKn2IFj9gS4BJy5gFg

!

redundancy

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/2

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 125000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 172.16.3.0 255.255.255.0 Serial0/0/1

ip route 209.165.200.224 255.255.255.248 Serial0/0/0

!

control-plane

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none

mgcp behavior comedia-check-media-src disable

mgcp behavior comedia-sdp-force disable

!

mgcp profile default

!

gatekeeper

shutdown

!

line con 0

exec-timeout 5 0

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

exec-timeout 5 0

logging synchronous

login local

transport input ssh

!

scheduler allocate 20000 1000

!

end

1. Router R3
2. R3#show run
3. Building configuration...
4. Current configuration : 2149 bytes  
   !  
   ! Last configuration change at 21:04:34 UTC Tue Jan 6 2015  
   !  
   version 15.4  
   service timestamps debug datetime msec  
   service timestamps log datetime msec  
   no service password-encryption  
   !  
   hostname R3  
   !  
   boot-start-marker  
   boot-end-marker  
   !  
   security passwords min-length 10  
   enable secret 9 $9$qGZYsq994ywdHk$N9cQxG82ViaHFjPzNn/mngPNdjK7MZhzRxcTcEvlWZw  
   !  
   no aaa new-model  
   memory-size iomem 15  
   !  
   ip domain name ccnasecurity.com  
   ip cef  
   no ipv6 cef  
   !  
   multilink bundle-name authenticated  
   !   
   cts logging verbose  
   !  
   voice-card 0  
   !  
   license udi pid CISCO2911/K9 sn FTX1713ALJV  
   license accept end user agreement  
   license boot module c2900 technology-package securityk9  
   license boot module c2900 technology-package uck9  
   license boot module c2900 technology-package datak9  
   !   
   vtp domain TSHOOT  
   vtp mode transparent  
   username admin01 secret 9 $9$ymTtFX0dTRK.eE$FnqHHtnGk0I8QXUSycOThp5bGj2wFREstIhuYcgRoJk  
   !  
   redundancy  
   !  
   interface Embedded-Service-Engine0/0  
    no ip address  
    shutdown  
   !  
   interface GigabitEthernet0/0  
    no ip address  
    shutdown  
    duplex auto  
    speed auto  
   !  
   interface GigabitEthernet0/1  
    ip address 172.16.3.1 255.255.255.0  
    duplex auto  
    speed auto  
   !  
   interface GigabitEthernet0/2  
    no ip address  
    shutdown  
    duplex auto  
    speed auto  
   !  
   interface Serial0/0/0  
    no ip address  
    shutdown   
    clock rate 125000  
   !  
   interface Serial0/0/1  
    ip address 10.2.2.1 255.255.255.252  
   !  
   ip forward-protocol nd  
   !  
   no ip http server  
   no ip http secure-server  
   !  
   ip route 0.0.0.0 0.0.0.0 Serial0/0/1  
   !  
   control-plane  
   !  
   mgcp behavior rsip-range tgcp-only  
   mgcp behavior comedia-role none  
   mgcp behavior comedia-check-media-src disable  
   mgcp behavior comedia-sdp-force disable  
   !  
   mgcp profile default  
   !  
   gatekeeper  
    shutdown  
   !  
   line con 0  
    exec-timeout 5 0  
    logging synchronous  
    login local  
   line aux 0  
   line 2  
    no activation-character  
    no exec  
    transport preferred none  
    transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh  
    stopbits 1  
   line vty 0 4  
    exec-timeout 5 0  
    logging synchronous  
    login local  
    transport input none  
   !  
   scheduler allocate 20000 1000  
   !  
   end
5. Switches S1, S2 and S3 – Use default configs, except for host name