CISCO Academy

CCNA Security

Lab - Configure AnyConnect Remote Access SSL VPN Using ASA 5505 ASDM (Instructor Version)

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

Topology



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

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
D4	G0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
RI	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
D2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
R2	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
DO	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
K3	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

IP Addressing Table

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 AnyConnect Client SSL VPN Remote Access Using ASDM

- Start the VPN wizard.
- Specify the VPN encryption protocol.
- Specify the client image to upload to AnyConnect users.
- Configure AAA local authentication.
- Configure the client address assignment.
- Configure the network name resolution.

- Exempt address translation for VPN traffic.
- Review the AnyConnect client deployment details.
- Review the Summary screen and apply the configuration to the ASA.

Part 4: Connecting to an AnyConnect SSL VPN

- Verify the AnyConnect client profile.
- Log in from the remote host.
- Perform platform detection (if required).
- Perform an automatic installation of the AnyConnect VPN Client (if required).
- Manually install the AnyConnect VPN Client (if required).
- Confirm VPN connectivity.

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 A clientless, browser-based VPN that lets users establish a secure, remote-access VPN tunnel to the ASA and use 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 A client-based VPN that 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 an AnyConnect client-based SSL remote access VPN. In Part 4 you will establish a connection and verify connectivity.

Your company has two locations connected to an ISP. R1 represents a CPE device managed by the ISP. R2 represents an intermediate Internet 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 to teleworkers using the ASA as a VPN concentrator. They want you to test the client-based model using SSL and the Cisco AnyConnect client.

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 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.

Instructor Note: AnyConnect Secure Mobility Client release 4.1 or later is recommended. Instructions for installing AnyConnect Client packages to ASA flash are provided in the Chapter 0.0.0.0 lab.

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

Instructor Note: Instructions for erasing switches and routers are provided in the Chapter 0.0.0.0 lab.

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 and are relatively simple for the purposes 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 209.165.200.225 255.255.258.248
```

```
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.

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 conasecurity.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.

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 ssh
 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.

The ASA is the focal point for the network zones, and it has not yet been configured. Therefore, 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 go into Setup mode, repeat Step 2.

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

- a. Use the **show run** command to confirm that there is no previous configuration in the ASA other than the defaults that the ASA automatically inserts.
- 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 <u>https://192.168.1.1</u>. After entering the <u>https://192.168.1.1</u> 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.

Cisco ASDM 7.4(1)	₩ 🛠 🕸
File Edit View Favorites Tools Help	
Coogle Search • More >	> Sign In 🔧 🗸
Cisco ASDM 7.4(1)	
Cisco ASDM 7.4(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.	
Cisco ASDM can run as a local application or as a Java Web Start application.	_
Run Cisco ASDM as a local application	
When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:	
 You can invoke ASDM from a desktop shortcut. No browser is required. One desktop shortcut allows you to connect to <i>multiple</i> security appliances. 	
Install ASDM Launcher	
Run Cisco ASDM as a Java Web Start application	
 Click <i>Run ASDM</i> to run Cisco ASDM. Click <i>Run Startup Wizard</i> to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance. 	
Run ASDM Run Startup Wizard	
Copyright © 2006-2015 Cisco Systems, Inc. All rights reserved.	-

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

📴 Cisco A	SDM-IDM Launcher v1.6(0)	- • •
	Cisco ASDM-IDM Launcher	uhuhu cisco
Enter userr	name and password for 192.168.1.1	
Username:	admin01	
Password:	•••••	
	Remember the username of the specified device on	this computer
	OK Close	
		👙 🔒

Part 3: Configuring AnyConnect SSL VPN Remote Access Using ASDM

Step 1: Start the VPN wizard.

- a. On the ASDM main menu, click Wizards > VPN Wizards > AnyConnect VPN Wizard.
- b. Review the on-screen text and topology diagram. Click **Next** to continue.

anyConnect VPN Connect	ion Setup Wizard
VPN Wizard	Introduction Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the end user's device when a VPN connection is established. VPN Remote Access Cool Cool Cool Cool Cool Cool Cool Cool
	< Back Next > Cancel Help

Step 2: Configure the SSL VPN interface connection profile.

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

Connect VPN Connect	ion Setup Wizard			
Steps	Connection Profile Identification			
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN			
2. Connection Profile Identification	connections.			
3. VPN Protocols	Connection Profile Name: AnyConnect-SSL-VPN			
4. Client Images	VPN Access Interface: outside			
5. Authentication Methods				
6. Client Address Assignme				
 Network Name Resolutio Servers 				
8. NAT Exempt				
 AnyConnect Client Deployment 				
10. Summary				
	< Back Next > Cancel Help			

Step 3: Specify the VPN encryption protocol.

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

Connect VPN Connect	tion Setup Wizard
Steps	VPN Protocols
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support. SSL Device Certificate Device Certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA. Device Certificate: None Manage
	< Back Next > Cancel Help

Step 4: Specify the client image to upload to AnyConnect users.

a. On the Client Images screen, click Add to specify the AnyConnect client image filename.

Connect VPN Connect	ion Setup Wizard			
Steps	Client Images			
1. Introduction	ASA can automatically upload the latest AnyConnect package to the d	ient device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to			
3. VPN Protocols	the top of the list.			
4. Client Images				
5. Authentication Methods				
6. Client Address Assignme	Image	Regular expression to match user-agent		
7. Network Name Resolutio Servers				
8. NAT Exempt				
 AnyConnect Client Deployment 				
10. Summary				
	You can download AnyConnect Client packages from <u>Cisco</u> by searchi	ng 'AnyConnect VPN Client' or <u>click here</u> ,		
	< Back Next >	Cancel Help		

b. In the Add AnyConnect Client Image window, click Browse Flash.

🔄 Add AnyConnect Client Image	—
AnyConnect Image:	Browse Flash Upload
Regular expression to match user-agent	*
OK Cancel Help	

c. In the Browse Flash window, select the AnyConnect package file for Windows (**anyconnect-win-4.1.00028-k9.pkg**, in the example). Click **OK** to return to the AnyConnect Client Image window.

🧧 Browse Flash			×
Folders	Files		
erypto_archive	FileName	Size (bytes)	Date Modified
i∰… i coredumpinfo i∰… i log	Crypto_archive		05/13/15 18:42:24
i sdesktop i odsk1:	ing sdesktop		08/29/11 13:59:36 08/29/11 14:04:12
	anyconnect-linux-2.5.2014-k9.pkg	6,689,498 6,487,517	04/16/15 16:12:18 04/16/15 16:11:26
	anyconnect-win-2.5.2014-k9.pkg	4,678,691	04/16/15 16:10:22
	anyconnect-win-4.1.00028-k9.pkg asa923-k8.bin	16,932,458 30,468,096	02/13/15 15:09:42
	asdm-741.bin csd_3.5.2008-k9.pkg	26,350,916 12,998,641	03/26/15 14:20:14 08/29/11 14:04:10
	upgrade_startup_errors_201505141507.log	100	05/14/15 15:07:38
	upgrade_startup_errors_201505152216.log upgrade_startup_errors_201505191913.log	100	05/19/15 19:13:30
File Name:	anyconnect-win-4.1.00028-k9.pkg		
	OK Cancel Refres	h	

d. Click **OK** again to return to the Client Image window.

🔄 Add AnyConnect Client Image	×
AnyConnect Image: disk0:/anyconnect-win-4.1.00028-k9.pkg	Browse Flash
Regular expression to match user-agent	*
OK Cancel Help	

e. The selected image is now displayed on the Client Image window. Click Next to continue.

E AnyConnect VPN Connec	tion Setup Wizard	—	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the d	ient device when it accesses the enterprise network.	
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to		
3. VPN Protocols	the top of the list.		
4. Client Images	🛧 Add 🖾 Deelaco 🏛 Delato 🔺 🧃		
5. Authentication Methods	T Add C Replace Delete 7 V		
6. Client Address Assignme	Image	Regular expression to match user-agent	
7. Network Name Resolutio Servers	disk0:/anyconnect-win-4.1.00028-k9.pkg		
8. NAT Exempt			
 AnyConnect Client Deployment 			
10. Summary			
	You can download AnyConnect Client packages from <u>Cisco</u> by searchi	ng 'AnyConnect VPN Client' or <u>click here</u> ,	
	<back next=""></back>	Cancel Help	

Step 5: 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 REMOTE-USER with the password cisco12345. Click Add.

Steps	Authentication Methods	
 Introduction Connection Profile 	This step lets you specify the location of the authentication server. You can dick on the "New" button to create a new server group.	
Identification	AAA Server Group: LOCAL 🗸 New	
4. Client Images		
5. Authentication Methods	Local User Database Details	
6. Client Address Assignme	Liter to be Added	
7. Network Name Resolutio Servers	Username: REMOTE-USER Add >>	
8. NAT Exempt	Password:	
 AnyConnect Client Deployment 	Confirm Password:	
10. Summary		
	< Back Next > Cancel Hel	p

c. Click Next to continue.

Step 6: Configure the client address assignment.

a. In the Client Address Assignment window, click New to create an IPv4 address pool.

The AnyConnect VPN Connect	tion Setup Wizard
Steps	Client Address Assignment
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignment Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect dients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool:Select New Details of the selected address pool
	< Back Next > Cancel Help

b. In the Add IPv4 Pool window, name the pool **Remote-Pool** with a starting IP address of **192.168.1.100**, an ending IP address of **192.168.1.125**, and a subnet mask of **255.255.255.0**. Click **OK** to return to the Client Address Assignment window, which now displays the newly created remote user IP address pool.

🔄 Add IPv4 Pool	X
Name:	Remote-Pool
Starting IP Address:	192.168.1.100
Ending IP Address:	192.168.1.125
Subnet Mask:	255.255.255.0
ОК	Cancel Help

c. The Client Address Assignment window now displays the newly created remote user IP address pool. Click **Next** to continue.

anyConnect VPN Connec	tion Setup Wizard
Steps I. Introduction Connection Profile Identification J. VPN Protocols Client Images L. Authentication Methods Client Address Assignment N. Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment D. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool: Remote-Pool ▼ New Details of the selected address pool Starting IP Address: 192.168.1.100
	< Back Next > Cancel Help

Step 7: Configure the network name resolution.

On the Network Name Resolution Servers screen, enter the IP address of a DNS server (**192.168.2.3**). Leave the current domain name as **ccnasecurity.com**. Click **Next** to continue.

🚡 AnyConnect VPN Connection Setup Wizard				
Steps	Network Name Resolution Servers			
1. Introduction	This step lets yo	u specify how domain names are resolved for the remote user when acces	sing the internal network.	
2. Connection Profile Identification	DNS Servers:	192.168.2.3		
3. VPN Protocols	WINS Servers:			
4. Client Images	Domain Name:	ccnasecurity.com		
5. Authentication Methods				
6. Client Address Assignme				
7. Network Name Resolution Servers				
8. NAT Exempt				
 AnyConnect Client Deployment 				
10. Summary				
	< Back	Vext >	Cancel Help	

Step 8: Exempt address translation for VPN traffic.

On the NAT Exempt screen, click the **Exempt VPN traffic from network address translation** check box. Do not change the default entries for the Inside Interface (**inside**) and the Local Network (**any4**). Click **Next** to continue.

anyConnect VPN Connect	tion Setup Wizard		
Steps	NAT Exempt		
Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers B. NAT Exempt	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. If network address translation Inside Interface is the interface directly connected to your internal network. Inside Interface: inside Local Network is the network address(es) of the internal network that dient can access. Local Network: any4		
9. AnyConnect Client Deployment 10. Summary	The traffic between AnyConnect dient and internal network will be exempt from network address translation.		
	< Back Next > Cancel Help		

Step 9: Review the AnyConnect client deployment details.

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

C AnyConnect VPN Connection Setup Wizard			
Steps	AnyConnect Client Deployment		
1. Introduction	AnyConnect client program can be installed to a client device by one of the following two methods:		
2. Connection Profile Identification	 Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed; Pre-deployment - Manually install the AnyConnect client package. 		
3. VPN Protocols	, , , , , , , , , , , , , , , , , , , ,		
4. Client Images			
5. Authentication Methods			
6. Client Address Assignme			
 Network Name Resolutio Servers 			
8. NAT Exempt			
9. AnyConnect Client Deployment			
10. Summary			
	< Back Next > Cancel Help		

Step 10: Review the Summary screen and apply the configuration to the ASA.

On the Summary screen, review the configuration description and then click **Finish**.

The AnyConnect VPN Connection Setup Wizard				
VPN Wizard	Summary			
Branch	Here is the summary of the configuration.			
SEN T	Name	Value		
ISP ISP	Summary			
	Name/Alias of the Connection Profile	AnyConnect-SSL-VPN		
Home	VPN Access Interface	outside		
porate	Device Digital Certificate	none		
Network	VPN Protocols Enabled	SSL only 1 package LOCAL		
	AnyConnect Client Images			
CANAL XE	Authentication Server Group			
	Address Pool for the Client	192.168.1.100 - 192.168.1.125		
	DNS	Server: Domain Name:		
	Network Address Translation	The protected traffic is not subjected to network address translation		
< Back Finish Cancel Help				

Step 11: Verify the AnyConnect client profile.

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

Cisco ASDM 7.4 for ASA - 192.168.1.1						
File View Tools Wizards Window Help Go						
Home 🍪 Configuration 🔯 Monitor	ring 📄 Save 🔇	Refresh 🔇 Bac	k 🕐 Forward 🦓	Help		CISCO
Remote Access VPN 🗗 म	Configuration > I	Remote Access VF	PN > Network (Client)	Access > AnyConn	ect Connection Profiles	
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software Dynamic Access Policies Group Policies	The security appl end-user adminisi Security (DTLS) tr Access Interfaces Imable Cisco SSL access must l	iance automatically d trative rights. The Ci unneling options. AnyConnect VPN Clie be enabled if you allo	eploys the Cisco AnyCo sco AnyConnect VPN Cli ent access on the interfa w AnyConnect client to	nnect VPN Client to rem ent supports IPsec (IKE ces selected in the tabl be launched from a bro	note users upon connection. The ir iv2) tunnel as well as SSL tunnel w le below wser (Web Launch) .	nitial client deployment requires A ith Datagram Transport Layer
IPsec(IKEv1) Connection Profiles		SSL Access		IPsec (IKEv2) Acc	ess	
Address Assignment	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate
⊕-행 Advanced 편 Clientless SSL VPN Access G Easy VPN Remote	outside dmz					Port Settings
B Host Scan Image Scure Desktop Manager Cartificate Management Cartificate Localization M DHGP E Localization M DHGP Ever R DNS B Advanced	Bypass interf Access lists from Login Page Setting Allow user to Shutdown po	ace access lists for ir group policy and use select connection pr rtal login page.	bound VPN sessions r policy always apply to ofile on the login page.	the traffic.		
< III ►	Connection Profiles Connection profi connection profil	le (tunnel group) spe e <u>here</u> ,	cifies how user is auther	nticated and other para	ameters. You can configure the ma	apping from certificate to
Firewall	💠 Add 🗹 Ed	dit <u>î</u> Delete Find	i:	🔘 🔘 🕅 Match Ca	ase	
Remote Access VPN	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
Site-to-Site VPN	DefaultRAGroup		I dee enabled ▼		AAA(LOCAL)	DfltGrpPolicy +
Device Management	•		ſ		set	4
×			ac	Imin01 2		5/5/15 4:55:33 PM UTC

Part 4: Connecting to an AnyConnect SSL VPN

Step 1: Log in from the remote host.

- a. 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. In the address field of the browser, enter https://209.165.200.226 for the SSL VPN. SSL is required to connect to the ASA, therefore, use secure HTTP (HTTPS).
- b. Enter the previously created username **REMOTE-USER** with the password **cisco12345**. Click **Logon** to continue.

٩	Logon
	Group AnyConnect-SSL-VPN -
	Username REMOTE-USER
	Password ••••••
	Logon

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

Step 2: Perform platform detection (if required).

If the AnyConnect client must be downloaded, a security warning will display on the remote host. The ASA will detect whether ActiveX is available on the host system. In order for ActiveX to operate properly with the Cisco ASA, it is important that the security appliance is added as a trusted network site.

Note: If ActiveX is not detected, the AnyConnect client software must be manually downloaded and installed. Skip to **Step 3** for instructions on how to manually download the AnyConnect client software.

a. 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.

cisco AnyC	onnect Secure Mobility Client
WebLaunch Platform Detection - ActiveX	Attempting to use Java for Installation Sun Java applet has started. This could take up to 60 seconds. Please wait
Java Detection	
🗌 - Java	
- Download	
Connected	
	Help Download

b. If you are presented with the AnyConnect Downloader window that indicates the 209.165.200.226 AnyConnect server could not be verified, click the **Change Setting** button.



c. The AnyConnect Downloader will present a verification window to change the setting that blocks untrusted connections. Click **Apply Change**.

AnyConnect Do	ownloader 💌
Â	Change the setting that blocks untrusted connections? Changing this Preference may result in a severe security compromise! You must retry the connection after the setting is changed.
	Apply Change Cancel

d. If you receive the Security Waning: Untrusted Server Certificate message, Click Connect Anyway.



e. The AnyConnect Secure Mobility Client Downloader window counts down the download time.



f. After the download is complete, the software will automatically start to install. Click **Yes** when asked to allow the program to make changes to the computer.

🕘 Usei	r Account Control	×	
٢	Do you want to allow the following program from an unknown publisher to make changes to this computer?		
	Program name: Publisher: File origin:	C:\Users\NetAc\WinSetup-Release-web-deploy.msi Unknown Hard drive on this computer	
🕑 si	how details	Yes No	
		Change when these notifications appear	

g. When installation is complete, the AnyConnect client will establish the SSL VPN connection.

AnyConnect Secure Mobility Client							
 WebLaunch Platform Detection - ActiveX - Java Detection - Java - Download - Connected 	Connection Established The Cisco AnyConnect Secure Mobility Client has successfully connected. The connection can be controlled from the tray icon, circled in the image below: $\boxed{\textcircled{OP} \textcircled{OP} \textcircled{OP}} \textcircled{OP} 12:56 \text{ PM}$						
	Help Download						

h. If the Connected option in the panel on the left is checked, skip to **Step 5**. If the Connect option is not checked, continue to **Step 3**.

Step 3: Install the AnyConnect VPN Client (if required).

If ActiveX is not detected, the AnyConnect client software must be manually downloaded and installed.



- a. On the Manual Installation screen, click Windows 7/Vista/64/XP.
- b. Click Run to install the AnyConnect VPN client.
- c. After the download is complete, the Cisco AnyConnect VPN Client Setup starts. Click Next to continue.



d. Read the End-User License Agreement. Select I accept the terms in the License Agreement and click Next to continue.

🗒 Cisco AnyConnect VPN Client Setup
End-User License Agreement Please read the following license agreement carefully
Client Software License Agreement of Cisco Systems THE SOFTWARE TO WHICH YOU ARE REQUESTING ACCESS IS THE PROPERTY OF CISCO SYSTEMS. THE USE OF THIS SOFTWARE IS GOVERNED BY THE TERMS AND CONDITIONS OF THE AGREEMENT SET FORTH BELOW. YOU (ON BEHALF OF YOURSELF AND THE BUSINESS ENTITY YOU REPRESENT) MUST AGREE TO THE FOLLOWING TERMS AND CONDITIONS IN ORDER TO USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE FOLLOWING TERMS AND CONDITIONS THEN YOU ARE NOT I do not accept the terms in the License Agreement Advanced Installer
<pre>Advanced installer</pre> <pre></pre>

e. The Ready to Install window is displayed. Click Install to continue.

🗒 Cisco AnyConnect VPN Client Setup	×
Ready to Install The Setup Wizard is ready to begin the Typical installation	2
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.	
Advanced Installer < Back install Cancel	el

Note: If a security warning is displayed, click Yes to continue.

f. Click **Finish** to complete the installation.



Step 4: Establish an AnyConnect SSL VPN Connection.

a. When the AnyConnect VPN client has been installed, manually start the program by clicking **Start** > **Cisco AnyConnect VPN Client**.



b. When prompted to enter the secure gateway address, enter **209.165.200.226** in the Connect to field, and click **Select**.

🖓 Cisco AnyConnect VPN Client 📃 💷 📧							
🔌 Connection	🚯 Statistics						
Connect to:	209.165.200.226 👻 🧬						
	Select						

Note: If a security warning is displayed, click Yes to proceed.

c. When prompted, enter **REMOTE-USER** for the username and **cisco12345** as the password.

省 Cisco AnyConnec	省 Cisco AnyConnect VPN Client 📃 💷 💌						
🗞 Connection 🚯	Statistics 🔒 About						
Connect to:	209.165.200.226 🗸						
Group:	AnyConnect-SSL-VPN -						
Username:	REMOTE-USER						
Password:	******						
Connect Please enter your username and password.							
all all and a series of a passion of all all all all all all all all all al							

Step 5: 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.

 Display connection statistics and information by double-clicking the AnyConnect icon in the system tray. You will be able to disconnect the SSN VPN session from here. Do Not click Disconnect at this time. Click the gear icon at the bottom left corner of the Cisco AnyConnect Secure Mobility client window.

🕥 Cisco AnyCo	onnect Secure Mobility Client		×
	VPN: Connected to 209.165.200.226. 209.165.200.226	▼ Disconnect	
00:14:16		I	Pv4
\$ (i)			alialia cisco

b. Use the scroll bar on the right side of the Virtual Private Network (VPN) – Statistics tab for additional connection information.

9	Cis	co AnyConne	ect Secure	Mobility Clien	t				
	••	li.ili. Isco	AnyC	Connect	Seci	ure Mo	bility Clier	nt	()
		Virtual Pri	vate Ne	twork (VPN	1)				
		Preferences	Statistics	Route Details	Firewall	Message His	tory		
		Connect	tion Inform	nation					- •
		State:		Con	nected				
		Tunnel Mo	de (IPv4):	Tun	nel All Tra	ffic			=
		Tunnel Mo	de (IPv6):	Dro	p All Traffi	c			
		Duration:		00:	09:06				
		Address	Informatio	on					- ^
		Client (IPv	(4):	192	. 168. 1. 10	0			
		Client (IPv	·6):	Not	Available				
		Server:		209	. 165. 200.	226			
		Bytes —							- •
		Sent:		276	18				
		Received:		206	51				
		Frames							- • -
1							Reset	Export	Stats
1									

Note: The inside IP address that is assigned to the client from the VPN pool is 192.168.1.100-125.

c. From a command prompt on the remote host PC-C, verify the IP addressing by using the **ipconfig** command. Notice that there are 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 to the SSL VPN tunnel (192.168.1.100).

C:\Windows\system32\cmd.exe	×
C:\Users\NetAcad>ipconfig	
Windows IP Configuration	
Ethernet adapter Local Area Connection 3: Connection-specific DNS Suffix .: ccnasecurity.com IPv4 Address	Ш
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: Link-local IPv6 Address : fe80::70f5:f35c:59de:53a7%11 IPv4 Address : 172.16.3.3 Subnet Mask : 255.255.255.0 Default Gateway : 172.16.3.1	
C:\Users\NetAcad>	-

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

C:\Windows\system32\cmd.exe	
C:\Users\NetAcad>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=9ms 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 = 9ms, Average = 5ms C:\Users\NetAcad>	Ŧ

Step 6: Use the ASDM Monitor to view the AnyConnect remote user session.

Note: Future SSL VPN sessions can be launched through the web portal or through the installed Cisco AnyConnect SSL VPN client. While the remote user at PC-C is still logged in using the AnyConnect client, you can view the session statistics by using the ASDM monitor.

On the ASDM menu bar, click **Monitoring** and then select **VPN** > **VPN Statistics** > **Sessions**. Click the **Filter By** pull-down list and select **AnyConnect Client**. You should see the **VPN-User** session logged in from PC-C, which has been assigned an inside network IP address of 192.168.1.100 by the ASA.

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

	Cisco ASDM 7.4 for ASA - 192.168.1.1						- • •
<u>F</u> ile	<u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> indow	<u>H</u> elp			Type top	oic to search Go	ababa
) Home 🦓 Configuration 🔯 Monitori	ng 🔒 Save 🔇 Refre	sh 🔇 Back 🔘 F	Forward 🧖 Help			CISCO
	VPN 급 무	Monitoring > VPN > VP	<u>N Statistics</u> > <u>Sessi</u>	ons			
Device Lis	Crypto Statistics Sessions Crypto Statistics Compression Statistics Global IXE/IPsec Statistics Protocol Statistics VLAN Mapping Sessions Clentless SSL VPN	Type AnyConnect Client SSL/TLS/DTLS Clientless VPN Browser	Active	Cumulative 1 1 0 0	Peak Concurrent	Inactive 1 1 1 1 1	0
	Easy VPN Client VPN Connection Graphs WSA Sessions	Filter By: AnyConnect	Client 🗸	All Sessions	•	Filter	
	kine i	Username	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Details
		REMOTE-USER	GroupPolicy_AnyCon AnyConnect-SSL-VPN	ne 192. 168. 1. 100 I 172. 16.3. 3	AnyConnect-Parent SSL AnyConnect-Parent: (1)	-Tunnel DTLS 18:59:25 UTC Tue RC4_SSL-Tun. 0h:03m:05s	Logout
	- Annual Annua						
	Interfaces						
		To sort VPN sessions, rig	nt-click on the above ta	able and select Table Sort Ord	ler from popup menu.	,	
	Properties	Logout By: All Sessio	ns 🔹	Lo	gout Sessions		
				Ref	iresh		
	, , , , , , , , , , , , , , , , , , ,					Last Updated: 5	/5/15 12:05:59 PM
Data	Refreshed Successfully.			admin01	2	5/5	5/15 4:55:33 PM UTC

Reflection

1. Describe at least two benefits of client-based vs. clientless VPNs?

Users have access to the same internal network resources as if they were on the LAN. Client-based VPN solutions, such as AnyConnect, can be configured to automatically download the proper client software based on the client platform characteristics.

2. Describe at least one difference between using SSL 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.

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 (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)				
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.

Device Configs

ASA 5505 Config – After Part 4 – Clientless VPN

CCNAS-ASA# show running-config

```
: Saved
:
: Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
:
ASA Version 9.2(3)
1
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password 9D8jmmmgkfNZLETh encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

names ip local pool Remote-Pool 192.168.1.100-192.168.1.125 mask 255.255.255.0 1 interface Ethernet0/0 switchport access vlan 2 1 interface Ethernet0/1 ! interface Ethernet0/2 switchport access vlan 3 1 interface Ethernet0/3 shutdown 1 interface Ethernet0/4 shutdown 1 interface Ethernet0/5 shutdown ! interface Ethernet0/6 shutdown ! interface Ethernet0/7 shutdown 1 interface Vlan1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 1 interface Vlan2 nameif outside security-level 0 ip address 209.165.200.226 255.255.258.248 ļ interface Vlan3 no forward interface Vlan1 nameif dmz security-level 70 ip address 192.168.2.1 255.255.255.0 ! ftp mode passive dns server-group DefaultDNS domain-name ccnasecurity.com object network inside-net subnet 192.168.1.0 255.255.255.0 object network dmz-server host 192.168.2.3

object network NETWORK OBJ 192.168.1.96 27 subnet 192.168.1.96 255.255.255.224 access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3 pager lines 24 mtu inside 1500 mtu outside 1500 mtu dmz 1500 icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 no arp permit-nonconnected nat (inside,outside) source static any any destination static NETWORK OBJ 192.168.1.96 27 NETWORK OBJ 192.168.1.96 27 no-proxy-arp route-lookup T. 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 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy user-identity default-domain LOCAL 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 no snmp-server location no snmp-server contact crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet 192.168.1.0 255.255.255.0 inside telnet timeout 10 ssh stricthostkeycheck ssh 192.168.1.0 255.255.255.0 inside ssh timeout 10 ssh key-exchange group dh-group1-sha1 console timeout 0 threat-detection basic-threat

```
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
webvpn
enable outside
 anyconnect image disk0:/anyconnect-win-4.1.0028-k9.pkg 1
anyconnect enable
tunnel-group-list enable
group-policy GroupPolicy AnyConnect-SSL-VPN internal
group-policy GroupPolicy AnyConnect-SSL-VPN attributes
wins-server none
 dns-server value 192.168.2.3
vpn-tunnel-protocol ssl-client
default-domain value ccnasecurity.com
username admin01 password UsMZmktANM6Z2Y9I encrypted
username REMOTE-USER password llxyqnhIpZuYtaix encrypted
tunnel-group AnyConnect-SSL-VPN type remote-access
tunnel-group AnyConnect-SSL-VPN general-attributes
address-pool Remote-Pool
default-group-policy GroupPolicy AnyConnect-SSL-VPN
tunnel-group AnyConnect-SSL-VPN webvpn-attributes
group-alias AnyConnect-SSL-VPN enable
Ţ.
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 dns preset dns map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect ip-options
  inspect netbios
 inspect rsh
  inspect rtsp
 inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
 inspect xdmcp
 inspect icmp
ļ
service-policy global policy global
prompt hostname context
```

```
call-home reporting anonymous prompt 2
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:fcdbd09708c62316445fdae183145b2b
; end
```

Router R1

```
R1# show run
Building configuration...
Current configuration : 1694 bytes
1
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
ļ
hostname R1
1
boot-start-marker
boot-end-marker
1
security passwords min-length 10
enable secret 9 $9$40V1VQCgcg5HRU$9JbJ5WpsOTBRm8H1cyIPLqGmTG3t3AFS9bx1151tsnE
1
no aaa new-model
memory-size iomem 15
ip cef
no ipv6 cef
Ţ.
multilink bundle-name authenticated
cts logging verbose
1
username admin01 secret 9
$9$5GtoxBiNFw5p9k$up1/WwRQGzsvRp6m4PWRoti1TWCR5G97MxBKnugrW6M
!
redundancy
```

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
1
interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.248
duplex auto
speed auto
1
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
1
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 2000000
1
interface Serial0/0/1
no ip address
shutdown
1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
1
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
control-plane
1
line con O
exec-timeout 5 0
logging synchronous
login local
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output 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 telnet
```

```
1
scheduler allocate 20000 1000
!
end
Router R2
R2# show run
Building configuration...
Current configuration : 1678 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
1
hostname R2
1
boot-start-marker
boot-end-marker
1
security passwords min-length 10
enable secret 9 $9$Nb4BPAMsmT24y.$4bn2kyZCwulndKiaU14531zF4n3ge95hfoFIKrucvpI
1
no aaa new-model
memory-size iomem 15
1
ip cef
no ipv6 cef
1
multilink bundle-name authenticated
1
cts logging verbose
Ţ.
username admin01 secret 9
$9$6PSI5.sujsrgN.$LFz4TeeqS/1FtxvK23Le8jxUAY9sjeedVmyF/PA9sPo
1
redundancy
!
interface Embedded-Service-Engine0/0
no ip address
interface Embedded-Service-Engine0/0
no ip address
shutdown
1
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
```

```
speed auto
ļ
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
1
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 2000000
ļ
ip forward-protocol nd
1
no ip http server
no ip http secure-server
1
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
ļ
control-plane
!
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 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 telnet
!
scheduler allocate 20000 1000
!
end
```

Router R3

R3# **show run** Building configuration...

```
Current configuration : 1655 bytes
1
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
1
hostname R3
1
boot-start-marker
boot-end-marker
1
security passwords min-length 10
enable secret 9 $9$5Mho73ipFPMgWE$yJiMb2sLFmK1P2mWClFwuB3gtdlQWqyjhAZNruqHyrk
1
no aaa new-model
memory-size iomem 15
1
ip cef
no ipv6 cef
1
multilink bundle-name authenticated
1
cts logging verbose
1
vtp domain TSHOOT
vtp mode transparent
username admin01 secret 9
$9$JXN7EcHDQcdh2k$9qnRjzJxhSGJK3KGF9F0piZU6HpDCGdWFRUdfg6QIVY
!
redundancy
1
interface Embedded-Service-Engine0/0
no ip address
shutdown
1
interface GigabitEthernet0/0
no ip address
 shutdown
duplex auto
speed auto
1
interface GigabitEthernet0/1
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
1
interface Serial0/0/0
```

```
no ip address
 shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
1
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
1
line con O
exec-timeout 5 0
logging synchronous
login local
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output 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 telnet
!
scheduler allocate 20000 1000
1
end
```

Switches S1, S2 and S3 – Use default configs, except for host name