

Cisco

Exam 300-209

Implementing Cisco Secure Mobility Solutions

Version: 10.0

[Total Questions: 213]

Question No : 1

A custom desktop application needs to access an internal server. An administrator is tasked with configuring the company's SSL VPN gateway to allow remote users to work. Which two technologies would accommodate the company's requirement? (Choose two).

- A. AnyConnect client
- B. Smart Tunnels
- C. Email Proxy
- D. Content Rewriter
- E. Portal Customizations

Answer: A,B

Question No : 2

Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

- A. ASDM
- B. Connection-profile CLI command
- C. Host-scan CLI command under the VPN group policy
- D. Pre-login-check CLI command

Answer: A

Question No : 3

Which four activities does the Key Server perform in a GETVPN deployment? (Choose four.)

- A. authenticates group members
- B. manages security policy
- C. creates group keys
- D. distributes policy/keys
- E. encrypts endpoint traffic
- F. receives policy/keys
- G. defines group members

Answer: A,B,C,D

Question No : 4

A user is unable to establish an AnyConnect VPN connection to an ASA. When using the Real-Time Log viewer within ASDM to troubleshoot the issue, which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection? (Choose two.)

- A. Client's public IP address
- B. Client's operating system
- C. Client's default gateway IP address
- D. Client's username
- E. ASA's public IP address

Answer: A,D

Question No : 5

The Cisco AnyConnect client is unable to download an updated user profile from the ASA headend using IKEv2. What is the most likely cause of this problem?

- A. User profile updates are not allowed with IKEv2.
- B. IKEv2 is not enabled on the group policy.
- C. A new profile must be created so that the adaptive security appliance can push it to the client on the next connection attempt.
- D. Client Services is not enabled on the adaptive security appliance.

Answer: C

Question No : 6

Scenario:

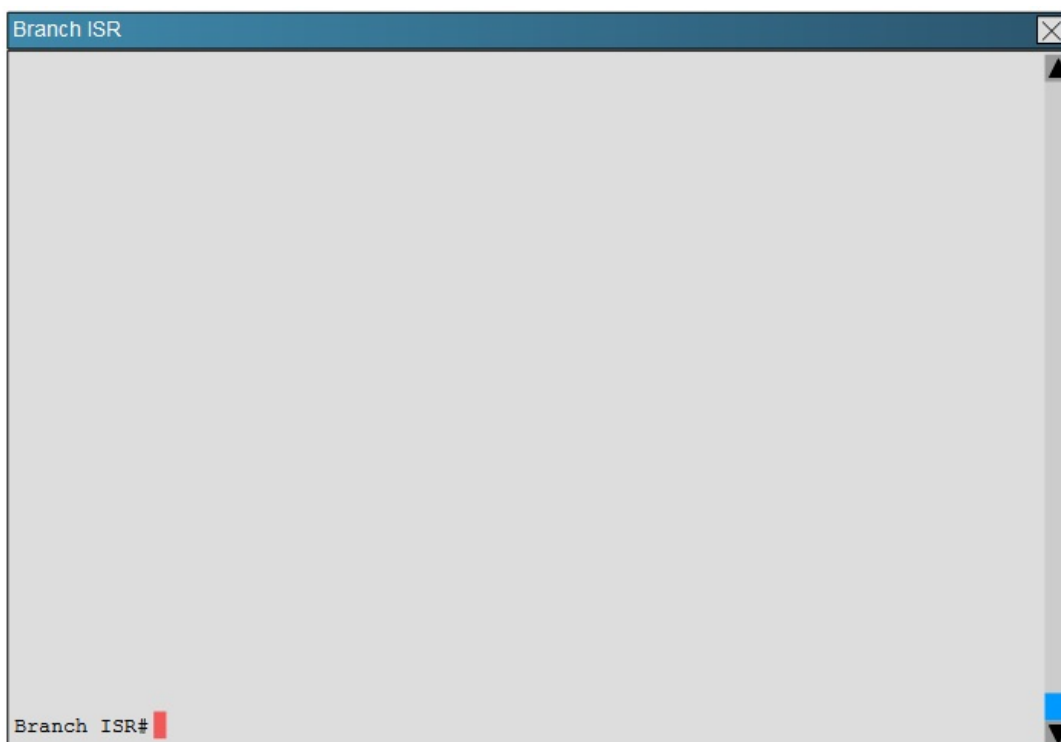
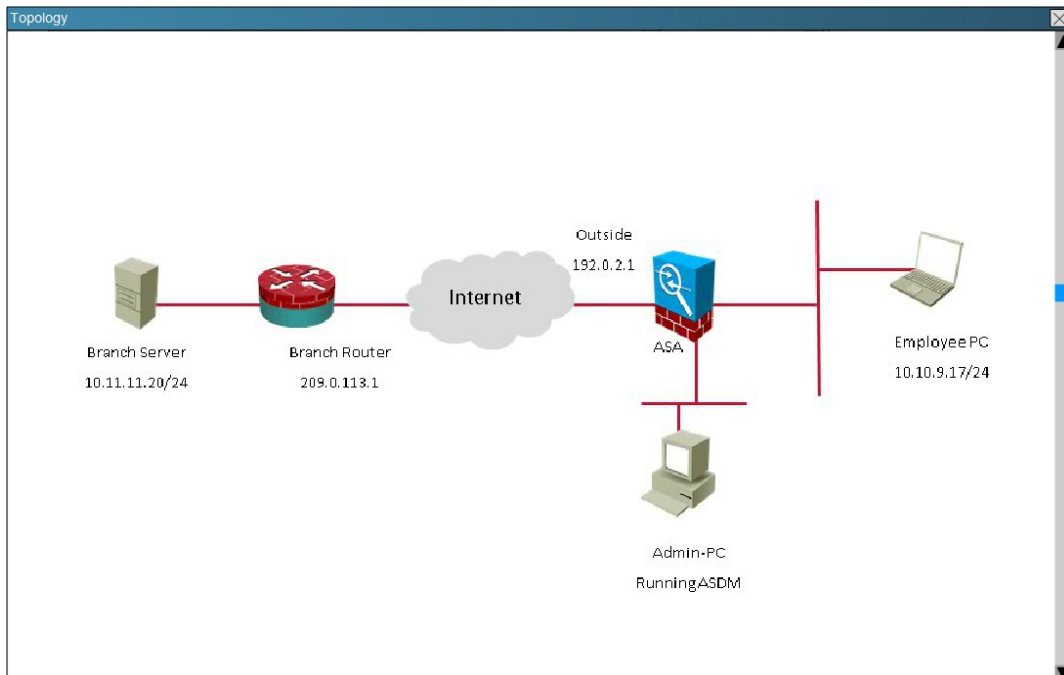
You are the senior network security administrator for your organization. Recently and junior engineer configured a site-to-site IPsec VPN connection between your headquarters Cisco ASA and a remote branch office.

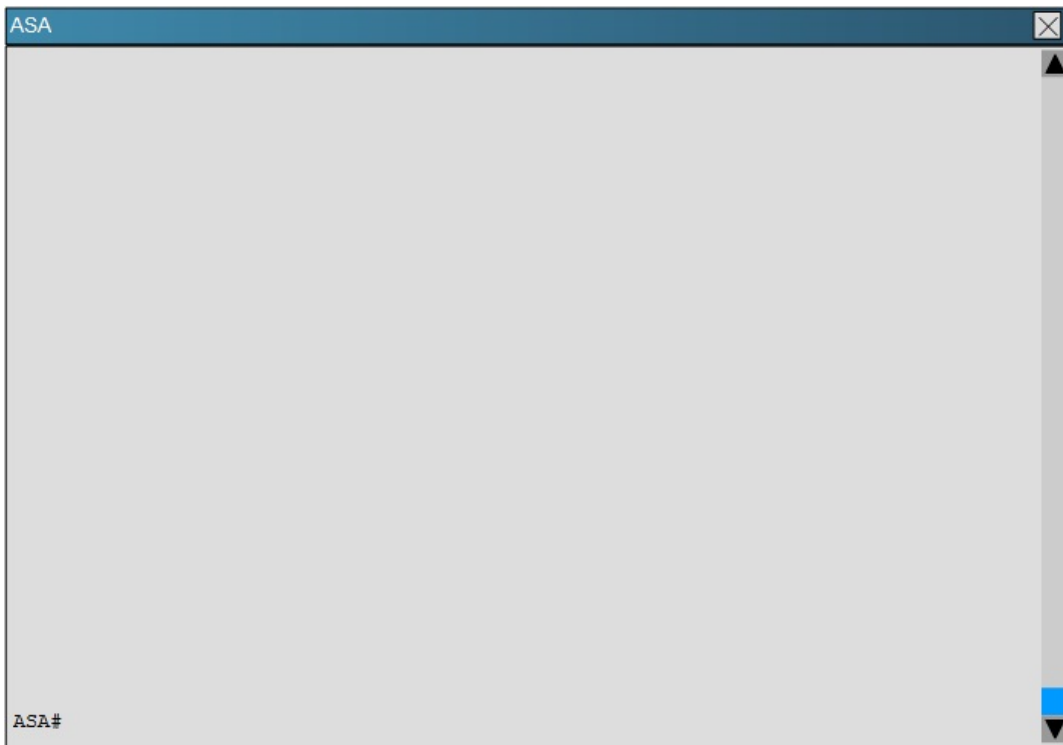
Cisco 300-209 : Practice Test

You are now tasked with verifying the IKEv1 IPsec installation to ensure it was properly configured according to designated parameters. Using the CLI on both the Cisco ASA and branch ISR, verify the IPsec configuration is properly configured between the two sites.

NOTE: the show running-config command cannot be used for this exercise.

Topology:





Which transform set is being used on the branch ISR?

- A. Default
- B. ESP-3DES ESP-SHA-HMAC
- C. ESP-AES-256-MD5-TRANS mode transport
- D. TSET

Answer: B

Explanation:

This can be seen from the “show crypto ipsec sa” command as shown below:

Branch ISR

```
Branch ISR#show crypto ipsec sa
interface: GigabitEthernet0/1
  Crypto map tag: VPN-to-ASA, local addr 203.0.113.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
  #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xCE89192A(3465091370)
  transform: esp-3des esp-sha-hmac ,
```

Branch ISR

```
protected vrf: (none)
local ident (addr/mask/prot/port): (10.11.11.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.9.0/255.255.255.0/0/0)
current_peer 192.0.2.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 569, #pkts encrypt: 569, #pkts digest: 569
  #pkts decaps: 681, #pkts decrypt: 681, #pkts verify: 681
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 203.0.113.1, remote crypto endpt.: 192.0.2.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0x8E47598C(2387040652)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xCE89192A(3465091370)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Tunnel, }
Branch ISR#
Branch ISR#
```

Question No : 7

Which three commands are included in the command show dmvpn detail? (Choose three.)

- A. show ip nhrp nhs
- B. show dmvpn
- C. show crypto session detail
- D. show crypto ipsec sa detail
- E. show crypto sockets
- F. show ip nhrp

Answer: A,B,C

Question No : 8

A network is configured to allow clientless access to resources inside the network. Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?

- A. auto applet download
- B. port forwarding
- C. web-type ACL
- D. HTTP proxy

Answer: B

Question No : 9

Scenario

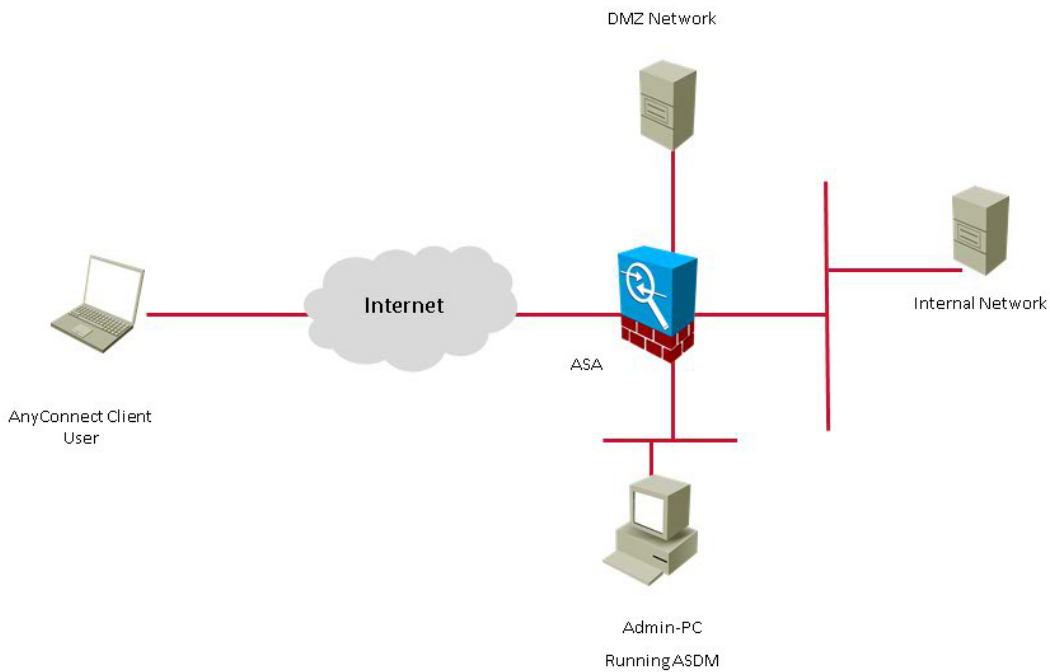
Your organization has just implemented a Cisco AnyConnect SSL VPN solution. Using Cisco ASDM, answer the questions regarding the implementation.

Note: Not all screens or option selections are active for this exercise.

Instructions

- Navigate the ASDM GUI on the device to verify network operation and answer for multiple-choice questions.
- You may have to use the scroll bars to view the entire ASDM Configuration screens.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- **NOT ALL SCREENS AND SELECTIONS ARE AVAILABLE FOR THIS EXERCISE.**
- Click on the Admin PC on the topology page to gain ASDM to the ASA. No passwords are required for this exercise.
- You may also click on the Default Home tab to access ASDM or return to the ASDM home screen at any time.
- There are **four (4)** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.
- To access the multiple-choice questions, click on the Questions tab and then numbered boxes on the left of the panel to view each question.

Topology



Default_Home

Cisco 300-209 : Practice Test

Device Information

Host Name:	HQ-ASA.secure-x.local		
ASA Version:	9.1(1)4	Device Uptime:	16d 12h 29m 22s
ASDM Version:	7.1(2)	Device Type:	ASA 5515, IPS
Firewall Mode:	Routed	Context Mode:	Single
Environment Status:	OK		
		Total Flash:	8192 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
DMZ	172.16.1.1/24	up	up	0
Guest	10.10.250.1/24	up	up	0
Site-To-Site	172.16.2.1/24	up	up	0
inside	10.10.1.1/24	up	up	0
management	10.10.2.1/24	up	up	4
outside	192.0.2.1/24	up	up	0

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage | Total CPU Usage | Core Usage | Details

Memory Usage (MB)

772MB

14:33:25

Traffic Status

Connections Per Second Usage

14:29 14:30 14:31 14:32 14:33

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

14:29 14:30 14:31 14:32 14:33

Input Kbps: 0 Output Kbps: 0

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group
GigabitEthernet0/0	outside	Enabled	0	192.0.2.1	255.255.255.0	native	
GigabitEthernet0/1	inside	Enabled		100 10.10.1.1	255.255.255.0	native	
GigabitEthernet0/1.250	Guest	Enabled		30 10.10.250.1	255.255.255.0	vlan250	
GigabitEthernet0/2	DMZ	Enabled		50 172.16.1.1	255.255.255.0	native	
GigabitEthernet0/3	Site-To...	Enabled		60 172.16.2.1	255.255.255.0	native	
GigabitEthernet0/4		Enabled				native	
GigabitEthernet0/5		Enabled				native	
Management0/0	manage...	Enabled		90 10.10.2.1	255.255.255.0	native	

Enable traffic between two or more interfaces which are configured with same security levels
 Enable traffic between two or more hosts connected to the same interface
 Enable jumbo frame reservation

Apply Reset

Cisco 300-209 : Practice Test

