Free Questions for 300-730 by actualtestdumps

Shared by Ochoa on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company is setting up a dynamic crypto map on the Cisco ASA at the headquarters to accept connections from the branch offices. There will be no IP subnet overlap between the branch offices, but the engineer does not know which encryption domains will be requested by the branch offices. Additionally, the company security policy states that routing protocol traffic should not leave the HQ network. Which solution should be used to route traffic back to the branches from the Cisco ASA with minimal administrative effort?

Options:

A- Configure Reverse Route Injection on the dynamic crypto map.

B- Configure a default route with the tunneled keyword on all branch routers.

C- Configure static routes for remote subnets.

D- Configure snapshot routing with EIGRP to send out of band routing updates.

Answer:

A

Question 2

Question Type: MultipleChoice

Which parameter in IPsec VPN tunnel configurations is optional?

Options:

A- hash

B- lifetime

C- encryption

D- Perfect Forward Secrecy

Answer:

D

Question 3

Question Type: MultipleChoice

A router is being configured for IKEv2 AnyConnect using AnyConnect-EAP. How would the administrator separate profiles for administrators and employees so that authorization differs when they connect?

Options:

A- Define group aliases on the headend and have the user pick the appropriate alias when they connect

B- Define group-urls on the headend and create two XML profiles to match the administrator and user group urls

C- Create a certificate map and match on the appropriate certificate fields

D- Define key-ids on the headend and create two XML profiles to match the administrator and user key-ids.

Answer:

B

Explanation:

According to the documentConfigure FlexVPN: AnyConnect IKEv2 Remote Access with Local User Database, one way to separate profiles for administrators and employees is to use group-urls on the headend and create two XML profiles to match the administrator and user group urls. This allows the headend to assign different group-policies and tunnel-groups based on the group-url that the user connects to. For example:

webvpn enable outside anyconnect image disk0:/anyconnect-win-4.6.03049-webdeploy-k9.pkg 1 anyconnect enable tunnel-group-list enable group-policy Admin internal group-policy Admin attributes vpn-tunnel-protocol ikev2 ssl-client address-pools value AdminPool group-policy User internal group-policy User attributes vpn-tunnel-protocol ikev2 ssl-client address-pools value UserPool tunnel-group Admin type remote-access tunnel-group Admin general-attributes default-group-policy Admin tunnel-group Admin webvpn-attributes

group-url https://10.0.0.1/Admin enable tunnel-group User type remote-access tunnel-group User general-attributes default-group-policy User tunnel-group User webvpn-attributes group-url https://10.0.0.1/User enable

The XML profiles can be created with the AnyConnect Profile Editor and uploaded to the headend. The profile for administrators should have the server list entry as:

<ServerList> <HostEntry> <HostName>Admin</HostName> <HostAddress>10.0.0.1</HostAddress> <PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>Admin</UserGroup> </HostEntry> </ServerList>

The profile for users should have the server list entry as:

<ServerList> <HostEntry> <HostName>User</HostName> <HostAddress>10.0.0.1</HostAddress> <PrimaryProtocol>IPsec</PrimaryProtocol> <UserGroup>User</UserGroup> </HostEntry> </ServerList>

This way, when the user connects to the headend, they can choose either Admin or User from the drop-down list and get the appropriate authorization based on their group-url.

Question 4

Question Type: **MultipleChoice**

An engineer has configured Cisco AnyConnect VPN using IKEv2 on a Cisco IOS router. The user cannot connect in the Cisco AnyConnect client, but receives an alert message "Use a browser to gain access." Which action does the engineer take to resolve this issue?

Options:

A- Reset user login credentials.

B- Correct the URL address.

C- Connect using HTTPS.

D- Disable the HTTP server.

Answer:

D

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115755-flexvpn-ike-eap-00.html

Question 5

Question Type: MultipleChoice

Why must a network engineer avoid usage of the default X.509 certificate when implementing clientless SSLVPN on an ASA?

Options:

A- The certificate must be managed by the local CA.

B- The certificate is regenerated at each reboot.

C- The default X.509 certificate is not supported for SSLVPN.

D- The certificate is too weak to provide adequate security.

Answer:

B

Explanation:

By default, the ASA generates a self-signed X.509 certificate upon startup. This certificate is used in order to serve client connections by default. It is not recommended to use this certificate because its authenticity cannot be verified by the browser. Furthermore, this certificate is regenerated upon each reboot so it changes after each reboot. https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html

Question 6

Question Type: MultipleChoice

What are two advantages of using GETVPN to traverse over the network between corporate offices? (Choose two.)

Options:

A- It has unique session keys for improved security.

B- It supports multicast.

C- It has QoS support.

D- It is a highly scalable any to any mesh topology.

E- It supports a hub-and-spoke topology.

Answer:

B, D

Question 7

Question Type: MultipleChoice

An organization wants to distribute remote access VPN load across 12 VPN headend locations supporting 25,000 simultaneous users. Which load balancing method meets this requirement?

Options:

A- one VPN profile per site

B- DNS-based load balancing

C- AnyConnect native load balancing

D- equal cost, multipath load balancing

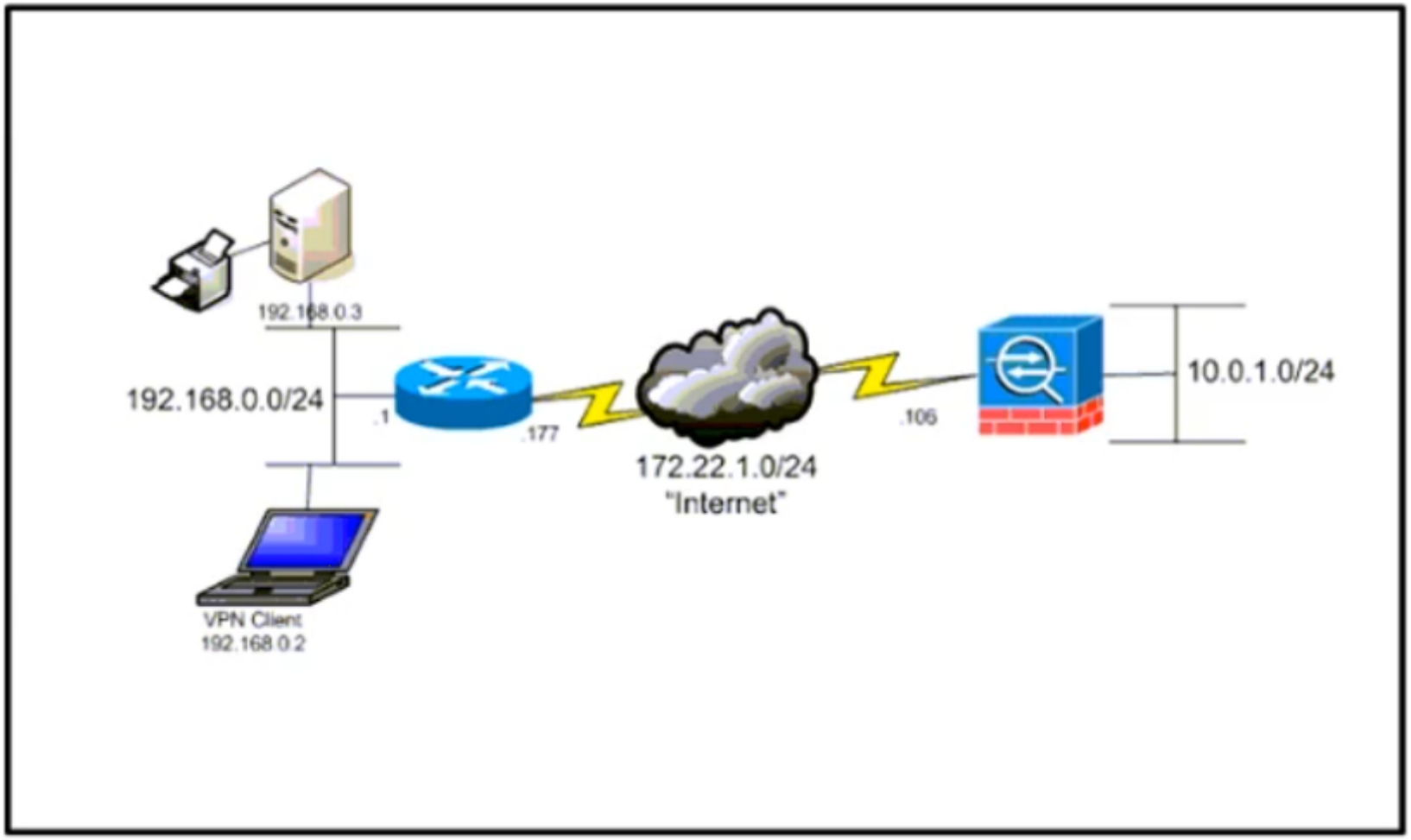
Answer:

B

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.



The network administrator must allow the Cisco AnyConnect Secure Mobility Client to securely access the corporate resources via IKEv2 and print locally. Traffic that is destined for the Internet must still be tunneled to the Cisco AS

Options:

A- Which configuration does the administrator use to accomplish this goal?

A- Split exclude policy with a deny for 192.168.0.3/32.

B- Split exclude policy with a permit for 0.0.0.0/32.

C- Tunnel all policy.

D- Split include policy with a permit for 192.168.0.0/24.

Answer:

B

Explanation:

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html

Question 9

Question Type: MultipleChoice

Which two components are required in a Cisco IOS GETVPN key server configuration? (Choose two.)

Options:

A- RSA key

B- IKE policy

C- SSL cipher

D- GRE tunnel

E- L2TP protocol

Answer:

A, B

Question 10

Question Type: **MultipleChoice**

Over the weekend, an administrator upgraded the Cisco ASA image on the firewalls and noticed that users cannot connect to the headquarters site using Cisco AnyConnect. What is the solution for this issue?

Options:

A- Upgrade the Cisco AnyConnect client version to be compatible with the Cisco ASA software image.

B- Upgrade the Cisco AnyConnect Network Access module to be compatible with the Cisco ASA software image.

C- Upgrade the Cisco AnyConnect client driver to be compatible with the Cisco ASA software image.

D- Upgrade the Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

Answer:

A

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asa-vpn-compatibility.html#Cisco_Reference.dita_60cec583-01b8-4cb2-a6e3-2fe87a6b0f82

Question 11

Question Type: MultipleChoice

Which remote access VPN technology requires the use of the IPsec-proposal configuration option?

Options:

A- clientless SSLVPN

B- SSLVPN Full Tunnel

C- IKEv2-based VPN

D- IKEv1-based VPN

Answer:

C

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/vpn/asa-96-vpn-config/vpn-remote-access.html The IPsec-proposal configuration option is used to specify the encryption, integrity, and authentication algorithms that will be used in the IPsec protocol. In the case of IKEv2-based VPN, this option is used to configure the IPsec security associations (SA) that will be established between the VPN client and the VPN gateway during IKEv2 negotiation. IKEv2 uses IPsec as its underlying encryption and authentication protocol, so the IPsec-proposal configuration is essential to establishing a secure VPN tunnel using IKEv2