



300-730^{Q&As}

Implementing Secure Solutions with Virtual Private Networks (SVPN)

Pass Cisco 300-730 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/300-730.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

A user at a company HQ is having trouble accessing a network share at a branch site that is connected with a L2L IPsec VPN. While troubleshooting, a network security engineer runs a packet tracer on the Cisco ASA to simulate the user

traffic and discovers that the encryption counter is increasing but the decryption counter is not. What must be configured to correct this issue?

- A. Adjust the routing on the remote peer device to direct traffic back over the tunnel.
- B. Adjust the preshared key on the remote peer to allow traffic to flow over the tunnel.
- C. Adjust the transform set to allow bidirectional traffic.
- D. Adjust the peer IP address on the remote peer to direct traffic back to the ASA.

Correct Answer: A

QUESTION 2

Which configuration allows a Cisco ASA to receive an IPsec connection from a peer with an unknown IP address?

- A. dynamic crypto map
- B. dynamic tunnel group
- C. dynamic AAA attributes
- D. dynamic access policy

Correct Answer: A

QUESTION 3

Refer to the exhibit.

**IKEv2 SAs:****Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1**

Tunnel-id	Local	Remote	Status	Role
45926289	172.16.1.2/500	172.16.1.1/500	READY	INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/4 sec
Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
remote selector 172.16.2.0/0 - 172.16.2.255/65535
ESP spi in/out: 0xa84caabb/0xf18dce57

A Cisco ASA is configured as a client to a router running as a FlexVPN server. The router is configured with a virtual template to terminate FlexVPN clients. Traffic between networks 192.168.0.0/24 and 172.16.20.0/24 does not work as expected. Based on the show crypto ikev2 sa output collected from the Cisco ASA in the exhibit, what is the solution to this issue?

- A. Modify the crypto ACL on the router to permit network 192.168.0.0/24 to network 172.16.20.0/24.
- B. Modify the crypto ACL on the ASA to permit network 192.168.0.0/24 to network 172.16.20.0/24.
- C. Modify the crypto ACL on the ASA to permit network 172.16.20.0/24 to network 192.168.0.0/24.
- D. Modify the crypto ACL on the router to permit network 172.16.20.0/24 to network 192.168.0.0/24.

Correct Answer: B

QUESTION 4

Refer to the exhibit.

```
IKEv2: (SESSION ID = 16, SA ID = 2):Received Packet [From 192.168.20.25:500/To
192.168.20.26:500/VRF i0:f0]
Initiator SPI : 334586B9AF754E5D - Responder SPI : AC90AD1EE140D901 Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE
Payload contents:
VID IDr AUTH SA TSr NOTIFY(USE_TRANSPORT_MODE) NOTIFY(SET_WINDOW_SIZE)
NOTIFY(ESP_IPC_NO_SUPPORT) NOTIFY(NON_FIRST_FRAGS)
IKEv2: (SESSION ID = 16, SA ID = 2):Process auth response notify
IKEv2: (SESSION ID = 16, SA ID = 2):Searching policy based on peer's identity
'192.168.20.25' of type 'IPv4 address'
IKEv2-ERROR: (SESSION ID = 16, SA ID = 2):: Failed to locate an item in the database
IKEv2: (SESSION ID = 16, SA ID = 2):Verification of peer's authentication data FAILED
IKEv2: (SESSION ID = 16, SA ID = 2):Auth exchange failed
IKEv2-ERROR: (SESSION ID = 16, SA ID = 2):: Auth exchange failed
IKEv2: (SESSION ID = 16, SA ID = 2):Abort exchange
IKEv2: (SESSION ID = 16, SA ID = 2):Deleting SA
IKEv2: (SESSION ID = 10, SA ID = 1):Retransmitting packet
```



An engineer is diagnosing an issue that occurred after a router at a branch site was assigned a new address. Based on the debugs, what must be done to resolve this issue?

- A. Add the remote peer's IP address to the server's IKEv2 keyring.
- B. Ensure that the correct preshared keys are set on both sides.
- C. Ensure that the UDP 500 packets between devices are not dropped.
- D. Add the remote peer's identity to the server's IKEv2 profile.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

The screenshot shows the 'AnyConnect Profile Editor - VPN' window. A 'Server List Entry' dialog box is open, displaying the 'Server' tab. The 'Primary Server' section includes a 'Display Name (required)' field, an 'FQDN or IP Address' field, a 'User Group' field, and a 'Group URL' field. The 'Connection Information' section shows 'Primary Protocol' set to 'IPsec', a checked 'ASA gateway' checkbox, 'Auth Method During IKE Negotiation' set to 'EAP-AnyConnect', and an 'IKE Identity (IOS gateway only)' field. Below these is a 'Backup Servers' section with a 'Host Address' field and buttons for 'Add', 'Move Up', 'Move Down', and 'Delete'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. A 'Help' button is visible at the bottom of the main window.

Which value must be configured in the User Group field when the Cisco AnyConnect Profile is created to connect to an ASA headend with IPsec as the primary protocol?



- A. address-pool
- B. group-alias
- C. group-policy
- D. tunnel-group

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect41/administration/guide/b_AnyConnect_Administrator_Guide_4-1/configure-vpn.html

[300-730 VCE Dumps](#)

[300-730 Practice Test](#)

[300-730 Braindumps](#)