300-440 Q&As

Designing and Implementing Cloud Connectivity (ENCC)

Pass Cisco 300-440 Exam with 100% Guarantee

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

https://www.leads4pass.com/300-440.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which architecture model establishes internet-based connectivity between on-premises networks and AWS cloud resources?

A. That establishes an iPsec VPN tunnel with Internet Key Exchange (IKE) for secure key negotiation and encrypted data transmission

B. That relies on AWS Elastic Load Balancing (ELB) for traffic distribution and uses SSL/TLS encryption for secure data transmission.

C. That employs AWS Direct Connect for a dedicated network connection and uses private IP addresses tor secure communication.

D. That uses Amazon CloudFrontfor caching and distributing content globally and uses HTTPS for secure data transfer.

Correct Answer: A

The architecture model that establishes internet-based connectivity between on-premises networks and AWS cloud resources is the one that establishes an iPsec VPN tunnel with Internet Key Exchange (IKE) for secure key negotiation and encrypted data transmission. This model is also known as the VPN CloudHub model. It allows multiple remote sites to connect to the same virtual private gateway in AWS, creating a hub-and- spoke topology. The VPN CloudHub model provides the following benefits: It enables secure communication between remote sites and AWS over the public internet, using encryption and authentication protocols such as IPsec and IKE. It supports dynamic routing protocols such as BGP, which can automatically adjust the routing tables based on the availability and performance of the VPN tunnels. It allows for redundancy and load balancing across multiple VPN tunnels, increasing the reliability and throughput of the connectivity. It simplifies the management and configuration of the VPN connections, as each remote site only needs to establish one VPN tunnel to the virtual private gateway in AWS, rather than multiple tunnels to different VPCs or regions. The other options are not correct because they do not establish internet-based connectivity between on-premises networks and AWS cloud resources. Option B relies on AWS Elastic Load Balancing (ELB) for traffic distribution and uses SSL/TLS encryption for secure data transmission. However, ELB is a service that distributes incoming traffic across multiple targets within a VPC, not across different networks. Option C employs AWS Direct Connect for a dedicated network connection and uses private IP addresses for secure communication. However, AWS Direct Connect is a service that establishes a private connection between on-premises networks and AWS, bypassing the public internet. Option D uses Amazon CloudFront for caching and distributing content globally and uses HTTPS for secure data transfer. However, Amazon CloudFront is a service that delivers static and dynamic web content to end users, not to on-premises networks.

References:

1: Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5)

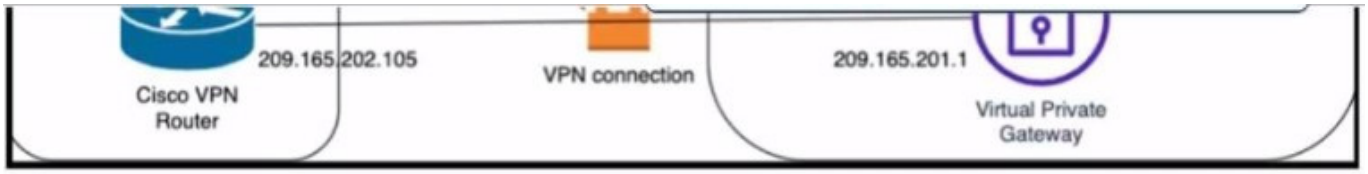
2: Cisco ASA Site-to-Site VPN

3: What Is Elastic Load Balancing?

4: What is AWS Direct Connect?

QUESTION 2

Refer to the exhibit.



Which Cisco IKEv2 configuration brings up the IPsec tunnel between the remote office router and the AWS virtual private gateway?

A.
```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-POC
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.202.105
  match identity remote address 209.165.201.1 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

B.
```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-DEMO
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.202.105
  match identity remote address 209.165.201.1 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

C.
```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-DEMO
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
 !
!
crypto ikev2 profile PROFILE-PoC
  match address local 209.165.201.1
  match identity remote address 209.165.202.105 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local DEMO-Keyring
!
```

A. Option A

B. Option B

C. Option C

Correct Answer: C

Option C is the correct answer because it configures the IKEv2 profile with the correct match identity, authentication, and keyring parameters. It also configures the IPsecprofile with the correct transform set and lifetime parameters. Option A is incorrect because it does not specify the match identity remote address in the IKEv2 profile, which is required to match the AWS virtual private gateway IP address. Option B is incorrect because it does not specify the authentication preshare in the IKEv2 profile, which is required to authenticate the IKEv2 peers using a pre-shared key. Option C also matches the configuration example provided by AWS and Cisco for setting up an IKEv2 IPsec site-to- site VPN between a Cisco IOS-XE router and an AWS virtual private gateway.

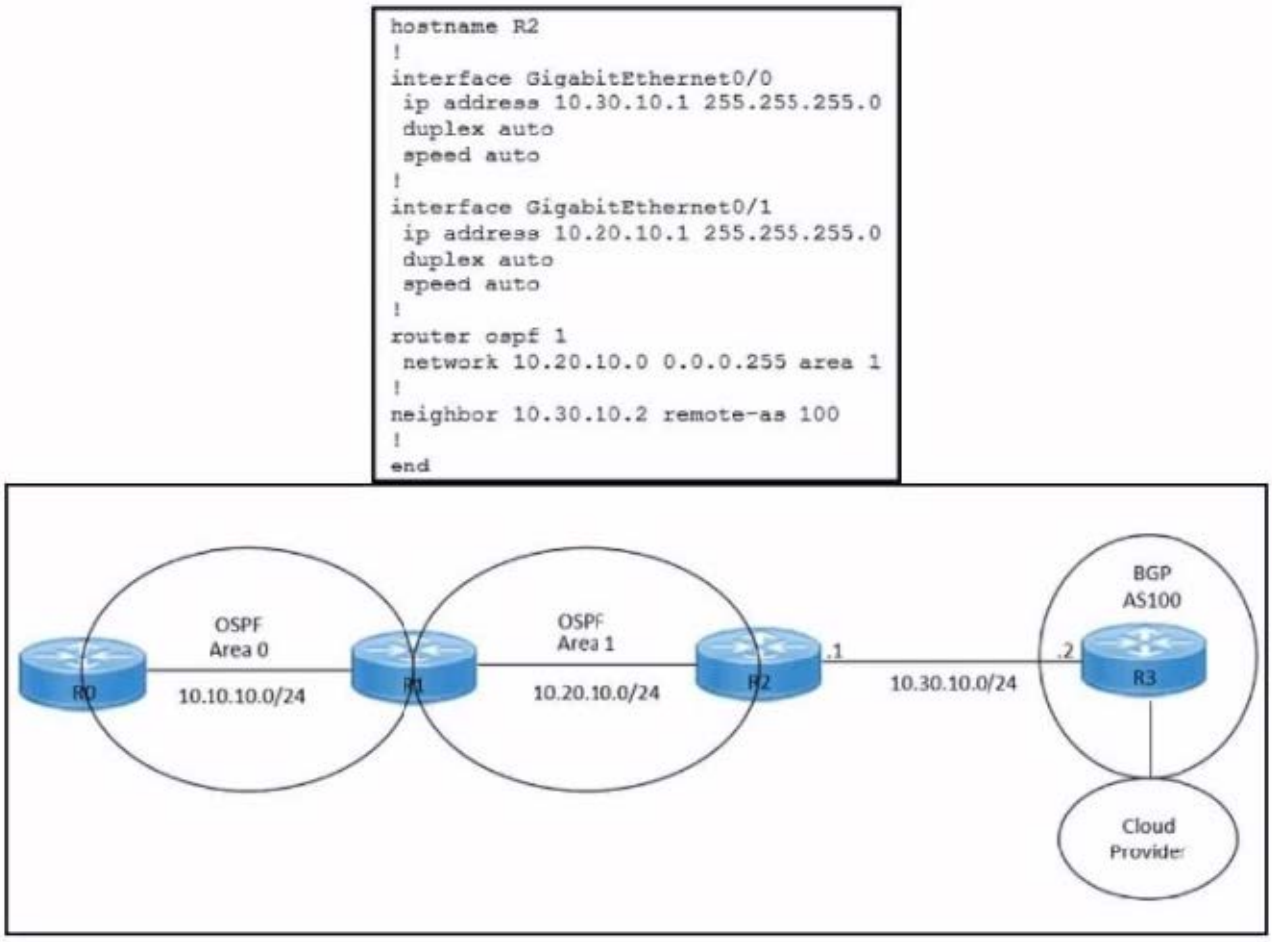
References:

1: AWS VPN Configuration Guide for Cisco IOS-XE

2: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services

QUESTION 3

Refer to the exhibit.



An engineer must redistribute IBGP routes into OSPF to connect an on-premises network to a cloud provider. Which command must be configured on router R2?

A. redistribute ospf 1

B. redistribute bgp 100 ospf 1

C. redistribute bgp 100 subnets

D. bgp redistrlbute-Internal

Correct Answer: B

References: Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) Exam Prep Designing and Implementing Cloud Connectivity (ENCC) v1.0 Cisco Multiprotocol Label Switching Exploring Cisco Cloud OnRamp for Colocation ENCC: Configuring IPsec VPN from Cisco IOS XE to AWS : [Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs]

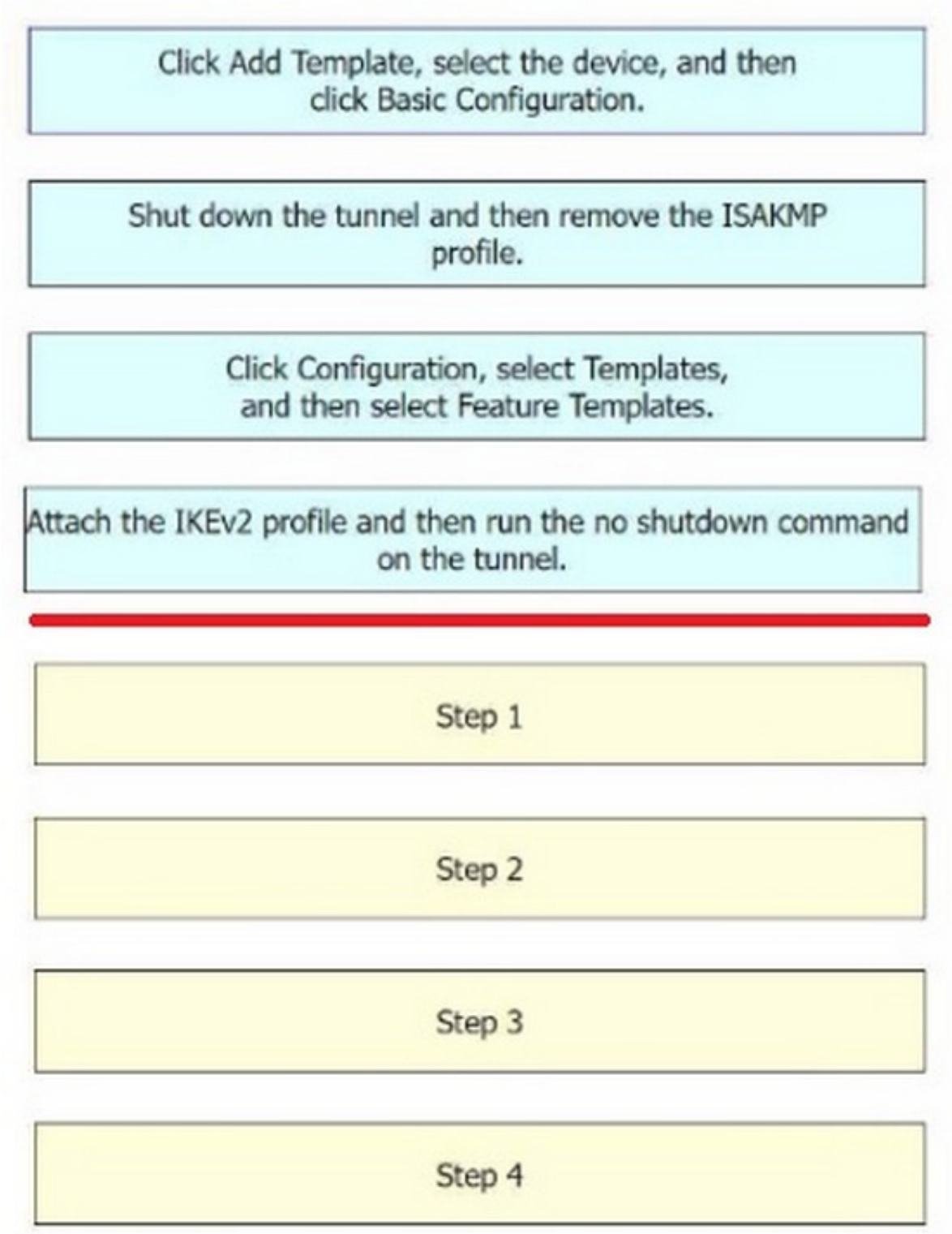
QUESTION 4

DRAG DROP

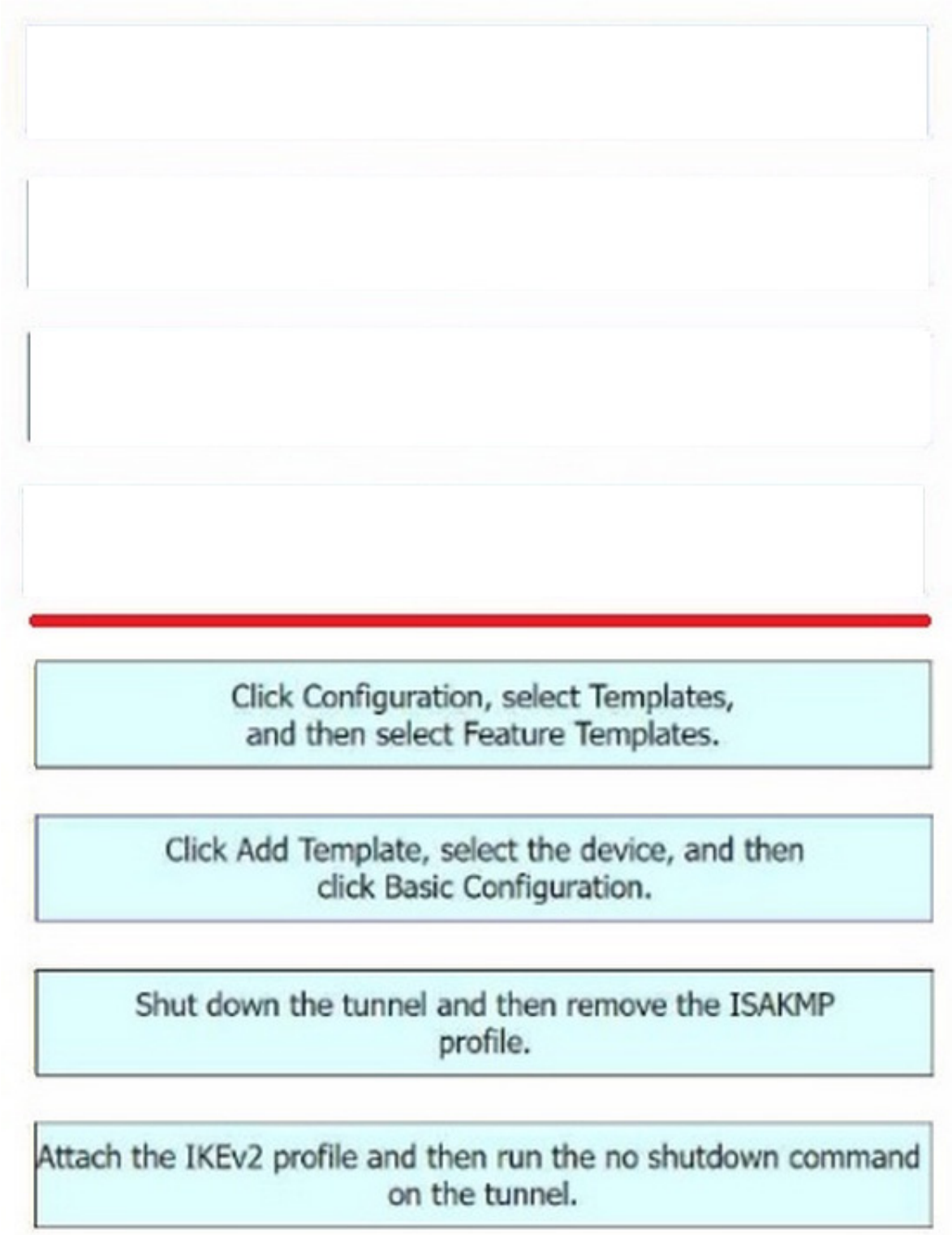
An engineer must configure a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router In Controller mode and AWS. The IKE version must be changed from IKEv1to IKEv2 in Cisco vManage. Drag and drop the

steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:



Step 1 = Click Configuration, select Templates, and then select Feature Templates.

Step 2 = Click Add Template, select the device, and then click Basic Configuration.

Step 3 = Shut down the tunnel and then remove the ISAKMP profile.

Step 4 = Attach the IKEv2 profile and then run the no shutdown command on the tunnel.

The process of configuring a site-to-site IPsec VPN connection between an on-premises Cisco IOS XE router in Controller mode and AWS, and changing the IKE version from IKEv1 to IKEv2 in Cisco vManage involves several steps123. Click

Configuration, select Templates, and then select Feature Templates: This is the first step where you navigate to the Templates section in the Configuration menu of Cisco vManage1.

Click Add Template, select the device, and then click Basic Configuration: In this step, you add a new template for the device and proceed with the basic configuration.

Shut down the tunnel and then remove the ISAKMP profile: Before changing the IKE version, you need to shut down the existing tunnel and remove the ISAKMP profile that is configured for IKEv12.

Attach the IKEv2 profile and then run the no shutdown command on the tunnel:

Finally, you attach the newly created IKEv2 profile to the tunnel and bring the tunnel back up.

References:

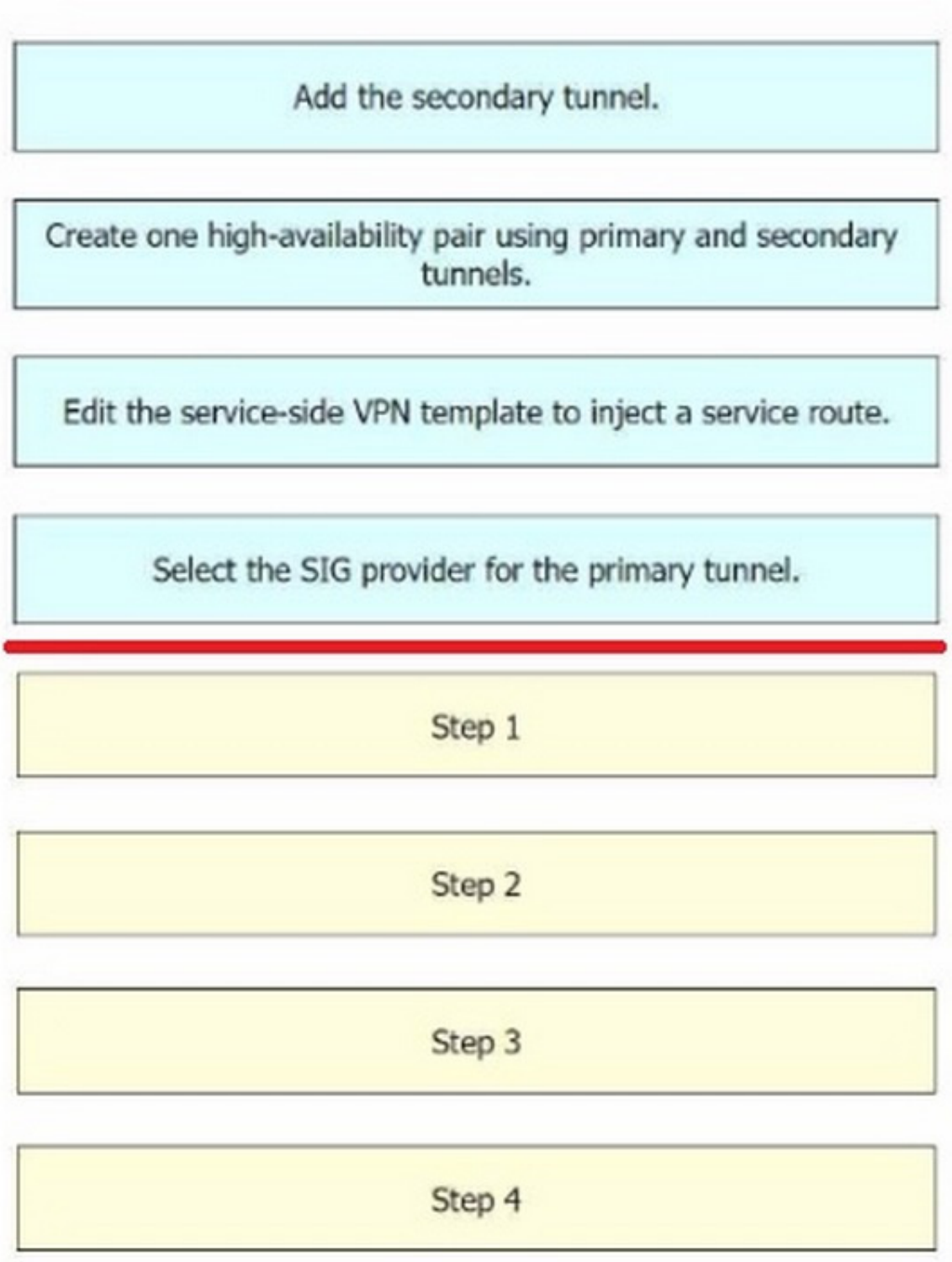
Configuring Internet Key Exchange Version 2 (IKEv2) - Cisco Switch from IKEv1 to IKEv2 on Cisco Routers - Cisco Community Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

QUESTION 5

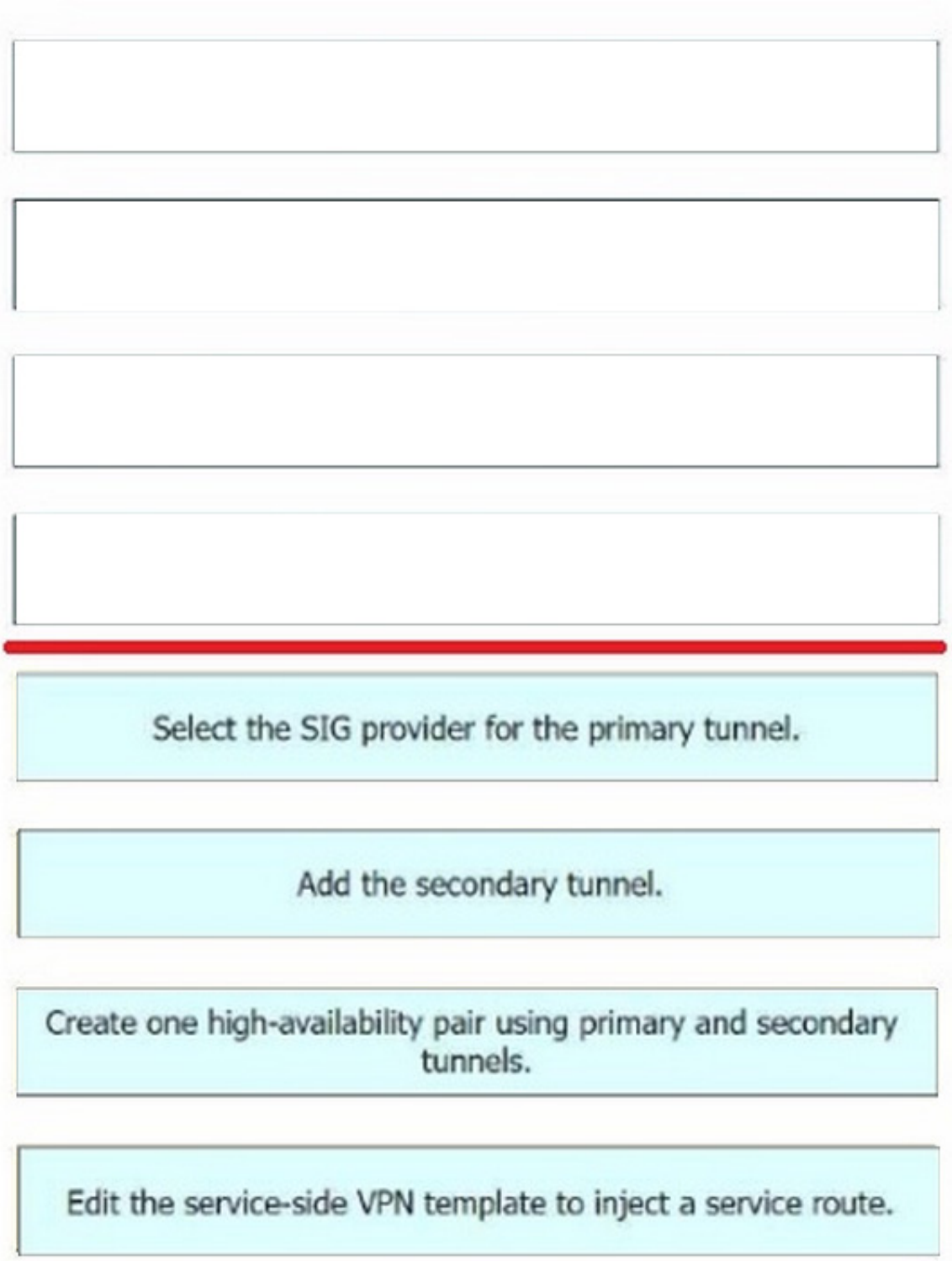
DRAG DROP

An engineer must configure cloud connectivity with Cisco Umbrella Secure Internet Gateway (SIG) in active/backup mode. The engineer already configured the SIG Credentials and SIG Feature Templates. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Correct Answer:



The configuration of cloud connectivity with Cisco Umbrella Secure Internet Gateway (SIG) in active/backup mode involves several steps. After configuring the SIG Credentials and SIG Feature Templates, the engineer must: Select the SIG provider for the primary tunnel: This is the first step in setting up the active/backup mode. The primary tunnel is the main connection path for the cloud connectivity.

Add the secondary tunnel: The secondary tunnel serves as a backup in case the primary tunnel fails. It ensures that the cloud connectivity remains uninterrupted even if there are issues with the primary tunnel. Create one high-availability pair using primary and secondary tunnels: This step involves pairing the primary and secondary tunnels to create a high-

availability pair. Thisensures that the cloud connectivity will switch over to the secondary tunnel seamlessly if the primary tunnel fails. Edit the service-side VPN template to inject a service route: The final step involves modifying the VPN template on the service side to include a service route. This ensures that the traffic is correctly routed through the primary or secondary tunnel as needed.

References: Designing and Implementing Cloud Connectivity (ENCC) v1.01 Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300- 440) Exam Prep2 Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios - Cisco