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.pass4itsure.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

An engineer is implementing a highly securemultitierapplication in AWS that includes S3. RDS, and some additional private links. What is critical to keep the traffic safe?

A. VPC peering and bucket policies

B. specific routing and bucket policies

C. EC2 super policies and specific routing policies

D. gateway load balancers and specific routing policies

Correct Answer: B

A highly secure multitier application in AWS that includes S3, RDS, and some additional private links requires specific routing and bucket policies to keep the traffic safe. The reasons are as follows:

Specific routing policies are needed to ensure that the traffic between the tiers is routed through the private links, which provide secure and low-latency connectivity between AWS services and on-premises resources12. The private links can

also prevent the exposure of the data and the application logic to the public internet12. Bucket policies are needed to control the access to the S3 buckets that store the application data34. Bucket policies can specify the conditions under

which the requests are allowed or denied, such as the source IP address, the encryption status, the request time, etc.34. Bucket policies can also enforce encryption in transit and at rest for the data in S334.

References:

1: AWS PrivateLink

2: AWS PrivateLink FAQs

3: Using Bucket Policies and User Policies

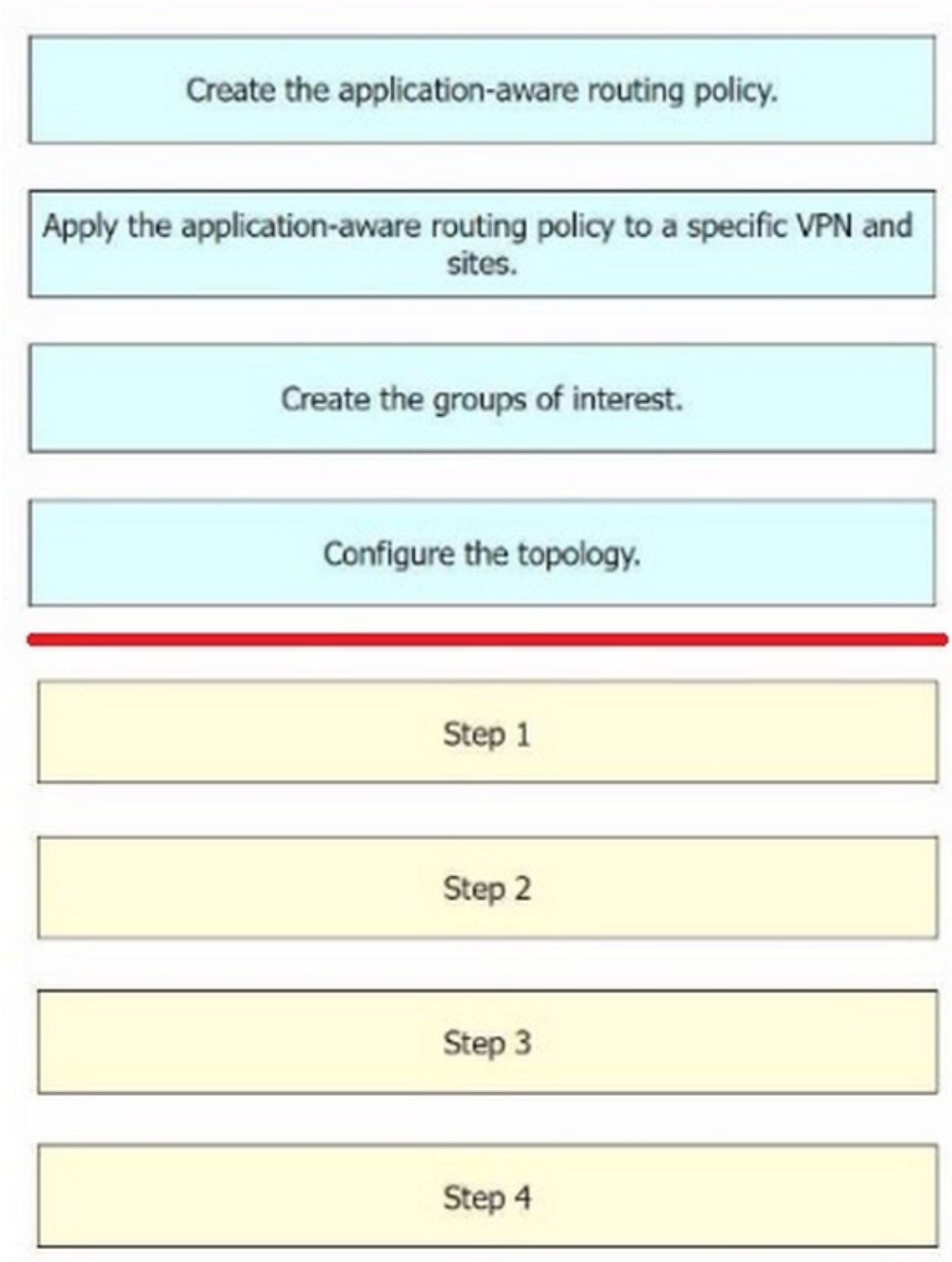
4: Bucket Policy Examples

QUESTION 2

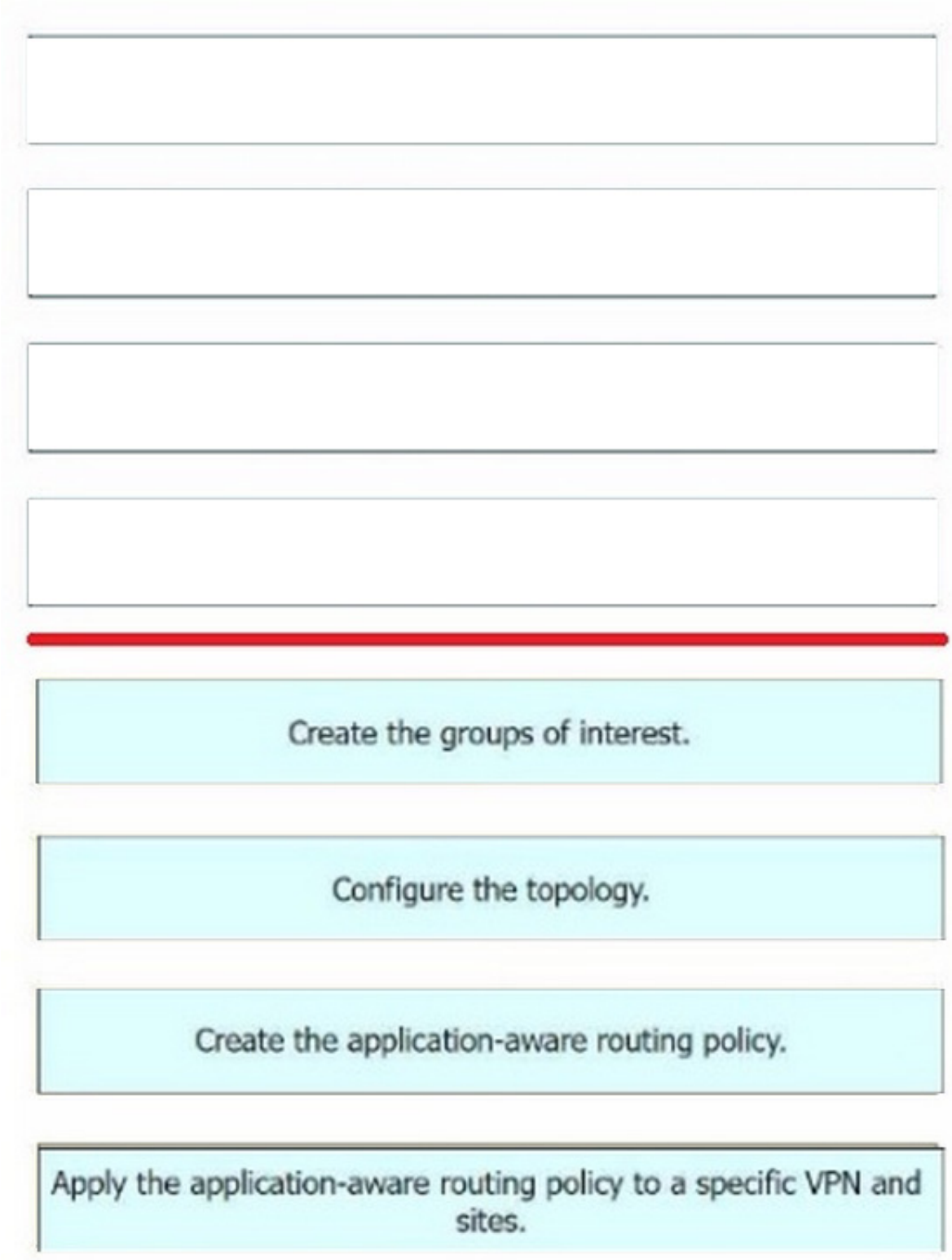
DRAG DROP

An engineer must use Cisco vManage to configure an application-aware routing policy 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 = Create the groups of interest.

Step 2 = Configure the topology.

Step 3 = Create the application-aware routing policy.

Step 4 = Apply the application-aware routing policy to a specific VPN and sites.

The process of configuring an application-aware routing policy in Cisco vManage involves several steps.

Create the groups of interest: This is the first step where you define the applications or groups that the policy will affect. Configure the topology: This involves setting up the network topology that the policy will operate within.

Create the application-aware routing policy: After setting up the groups and topology, you then create the application-aware routing policy. This policy tracks network and path characteristics of the data plane tunnels between Cisco SD-WAN

devices and uses the collected information to compute optimal paths for data traffic.

Apply the application-aware routing policy to a specific VPN and sites: Finally, the created policy is applied to a specific VPN and sites. This allows the policy to affect the desired network traffic.

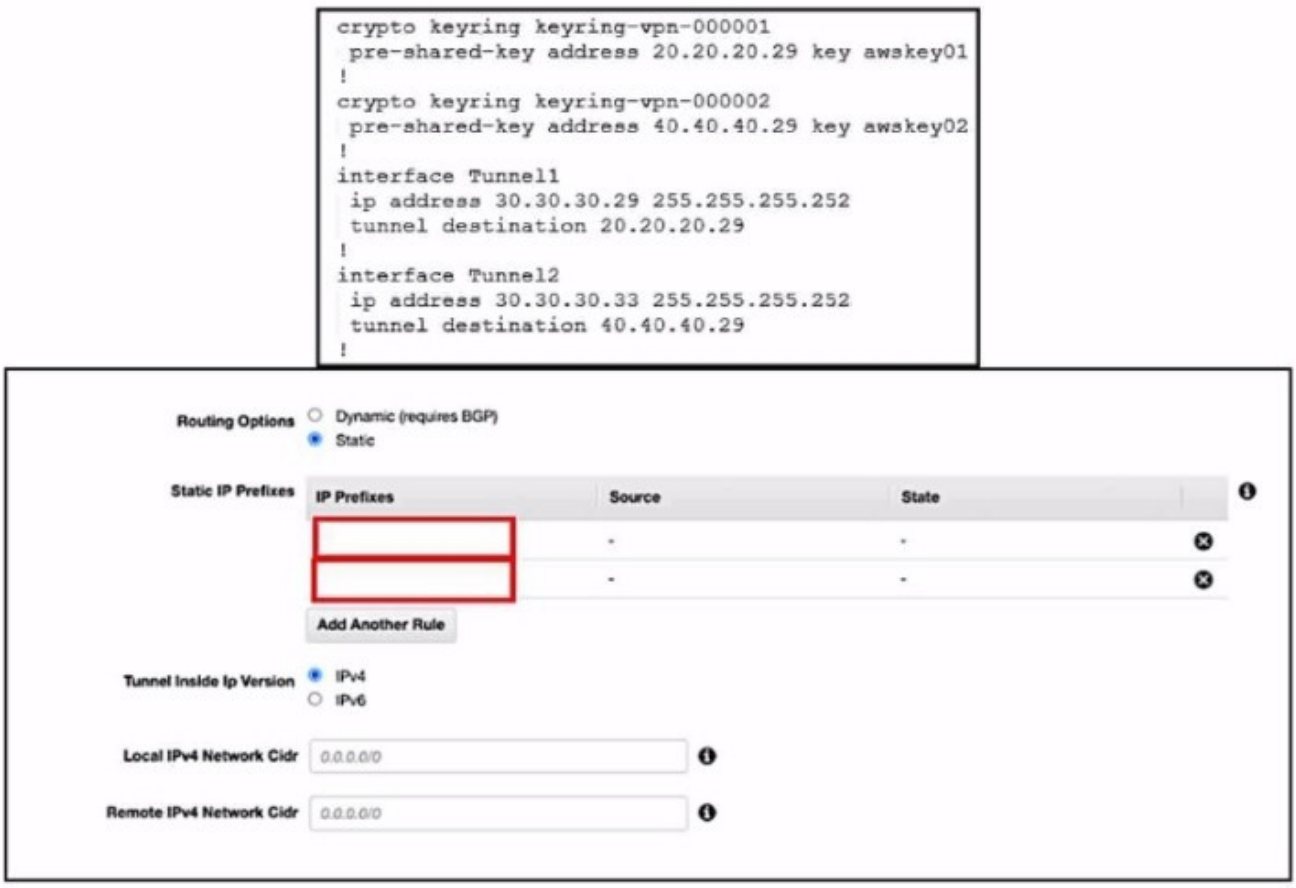
References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0 Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300- 440)

Information About Application-Aware Routing - Cisco Configuring Application-Aware Routing (AAR) Policies | NetworkAcademy.io Policies Configuration Guide, Cisco IOS XE SD-WAN Releases 16.11, 16.12

QUESTION 3

Refer to the exhibits.



An engineer needs to configure a site-to-site IPsec VPN connection between an on premises Cisco IOS XE router and Amazon Web Services (AWS). Which two IP prefixes should be used to configure the AWS routing options? (Choose two.)

A. 30.30.30.0/30

B. 20.20.20.0/24

C. 30.30.30.0/24

D. 50.50.50.0/30

E. 40.40.40.0/24

Correct Answer: AE

The correct answer is A and E because they are the IP prefixes that match the tunnel interfaces on the Cisco IOS XE router. The AWS routing options should include the local and remote IP prefixes that are used for the IPsec tunnel endpoints. The other options are either the public IP addresses of the routers or the LAN subnets that are not relevant for the IPsec tunnel configuration. References= Designing and Implementing Cloud Connectivity (ENCC) v1.0, Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services, Site-to-Site VPN with Amazon Web Services

QUESTION 4

Which feature is unique to Cisco SD-WAN IPsec tunnels compared to native IPsec VPN tunnels?

A. real-time dynamic path selection

B. tunneling protocols

C. end-to-end encryption

D. authentication mechanisms

Correct Answer: A

Cisco SD-WAN IPsec tunnels are different from native IPsec VPN tunnels in several ways. One of the unique features of Cisco SD-WAN IPsec tunnels is that they support real-time dynamic path selection, which means that they can

automatically choose the best path for each application based on the network conditions and policies. This feature improves the performance, reliability, and efficiency of the network traffic. Native IPsec VPN tunnels, on the other hand, do not

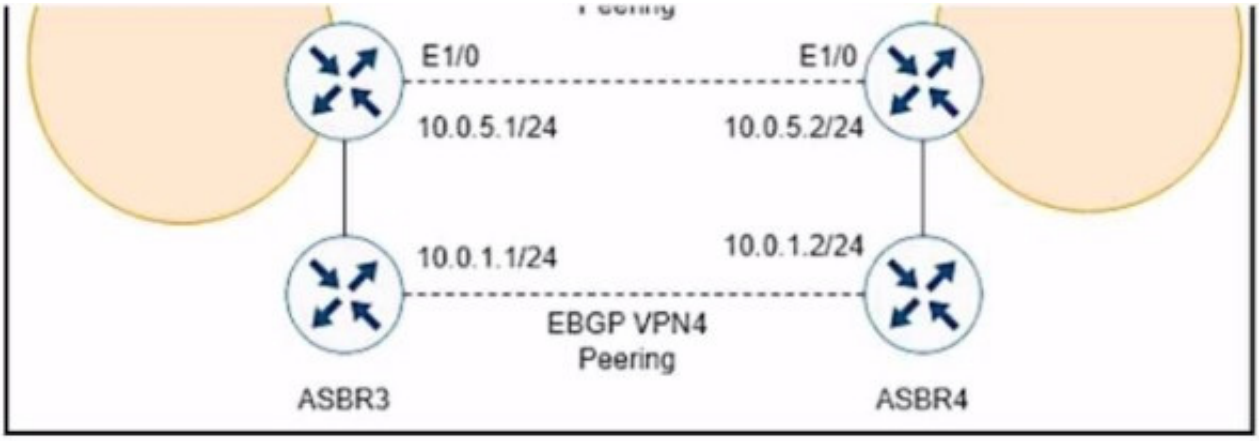
have this capability and rely on static routing or manual configuration to select the path for each tunnel. This can result in suboptimal performance, increased latency, and higher costs.

References:

Traditional IPsec Versus Cisco SD-WAN IPsec, SD-WAN vs IPsec VPN\\'s - What\\'s the difference?, SD-WAN vs. VPN: How Do They Compare?, Traditional IPSEC Versus SD-WAN IPSEC

QUESTION 5

Refer to the exhibits.



While troubleshooting, a network engineer discovers that the backup path fails between ASBR3 and ASBR4 for traffic between BGP AS6000 and BGP AS6500 when the connection between ASBR1 and ASBR2 goes down. The following configurations were performed on ASBR1:

```
ASBR1(config)# router bgp 6000
ASBR1 (config-router)# address-family vpn4
ASBR1 (config-router-af)# neighbor 10.0.5.2 remote-as 6500
ASBR1 (config-router-af)# neighbor 10.0.5.2 activate
ASBR1 (config-router-af)# neighbor 10.0.5.2 fall-over bfd
ASBR1 (config-router-af)# end
```

Which command is missing?

A. bgp additional-paths Install

B. bgp additional-paths select

C. redistribute static

D. bgp advertise-best-external

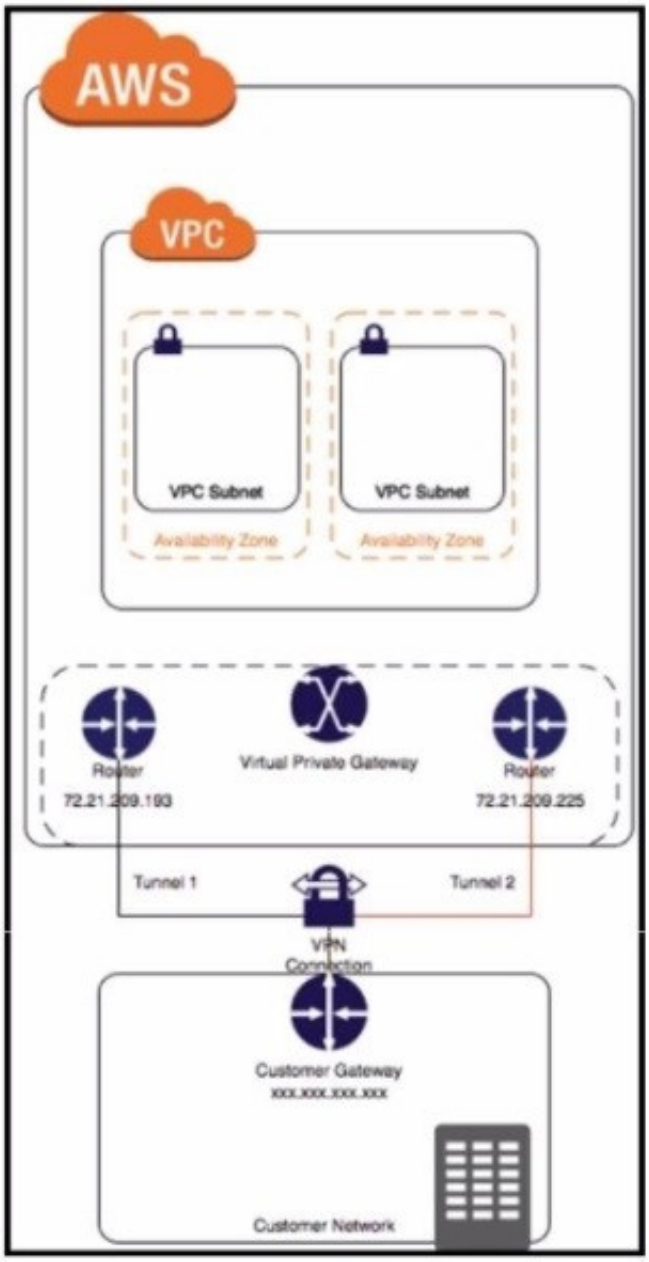
Correct Answer: D

The bgp advertise-best-external command is used to enable the advertisement of the best external path to internal BGP peers. This command is useful when there are multiple exit points from the local AS to other ASes, and the local AS wants to use the closest exit point for each destination. By default, BGP only advertises the best path to its peers, and the best path is usually the one with the lowest IGP metric to the next hop. However, this may not be the optimal path for traffic leaving the local AS, as it may result in suboptimal hot-potato routing or MED oscillations. The bgp advertise-best-external command allows BGP to advertise the best external path, which is the path with the lowest MED among the paths from different neighboring ASes, in addition to the best path. This way, the internal BGP peers can choose the best exit point based on the MED value, rather than the IGP metric. In this scenario, ASBR1 is configured to receive additional paths from ASBR2, which is a route reflector. ASBR2 receivestwo paths for the same prefix from AS6500, one from ASBR3 and one from ASBR4. ASBR2 selects the best path based on the IGP metric to the next hop, and advertises it to ASBR1. However, this path may not be the best external path, as it may have a higher MED value than the other path. If the connection between ASBR1 and ASBR2 goes down, ASBR1 will not have any backup path to reach AS6500, as it does not know the other path from ASBR4. To prevent this situation, ASBR1 should be configured with the bgp advertise-best-external command, so that it can receive the best external path from ASBR2, along with the best path. This way, ASBR1 will have a backup path to reach AS6500, in case the primary path fails.

QUESTION 6

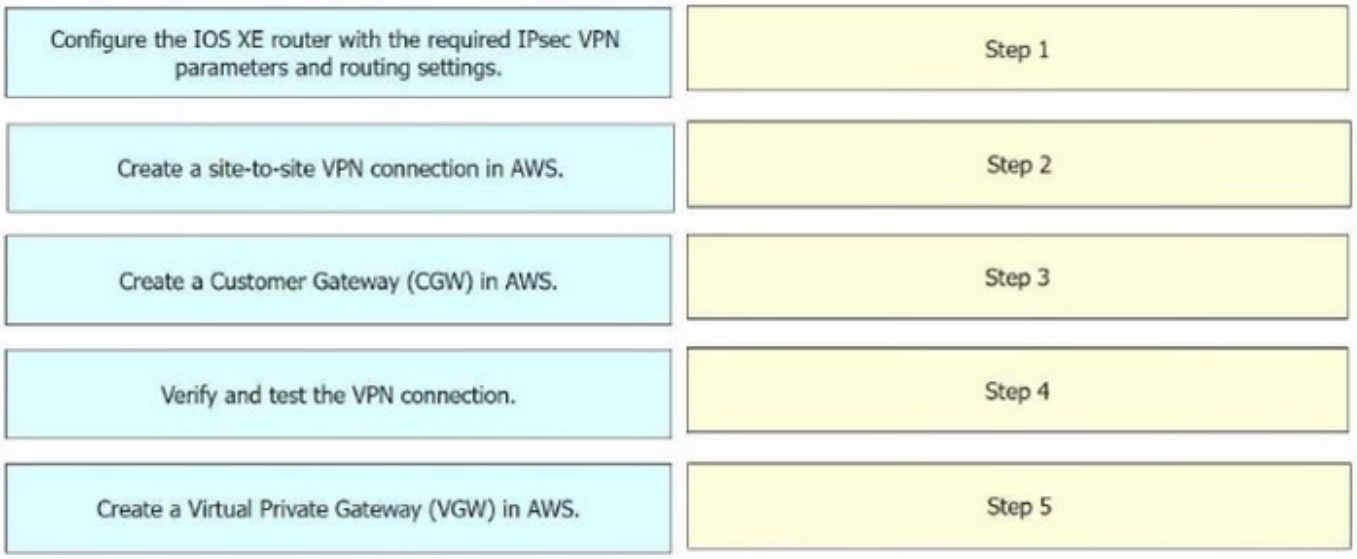
DRAG DROP

Refer to the exhibit.



Drag and drop the steps from the left onto the order on the right to configure a site-to-site VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS).

Select and Place:



Correct Answer:

Step 1 = Create a Customer Gateway (CGW) in AWS.

Step 2 = Create a Virtual Private Gateway (VGW) in AWS.

Step 3 = Create a site-to-site VPN connection in AWS.

Step 4 = Configure the IOS XE router with the required IPsec VPN parameters and routing settings.

Step 5 = Verify and test the VPN connection.

The process of configuring a site-to-site VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS) involves several steps

Create a Customer Gateway (CGW) in AWS: This is the first step where you define the public IP address of your on-premises Cisco IOS XE router in AWS. Create a Virtual Private Gateway (VGW) in AWS: This involves creating a VGW and

attaching it to the VPC in AWS.

Create a site-to-site VPN connection in AWS: After setting up the CGW and VGW, you then create a site-to-site VPN connection in AWS. This involves specifying the CGW, VGW, and the static IP prefixes for your on-premises network.

Configure the IOS XE router with the required IPsec VPN parameters and routing settings: After the AWS side is set up, you configure the on-premises Cisco IOS XE router with the required IPsec VPN parameters and routing settings. Verify

and test the VPN connection: Finally, you verify and test the VPN connection to ensure that it is working correctly.

References:

Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

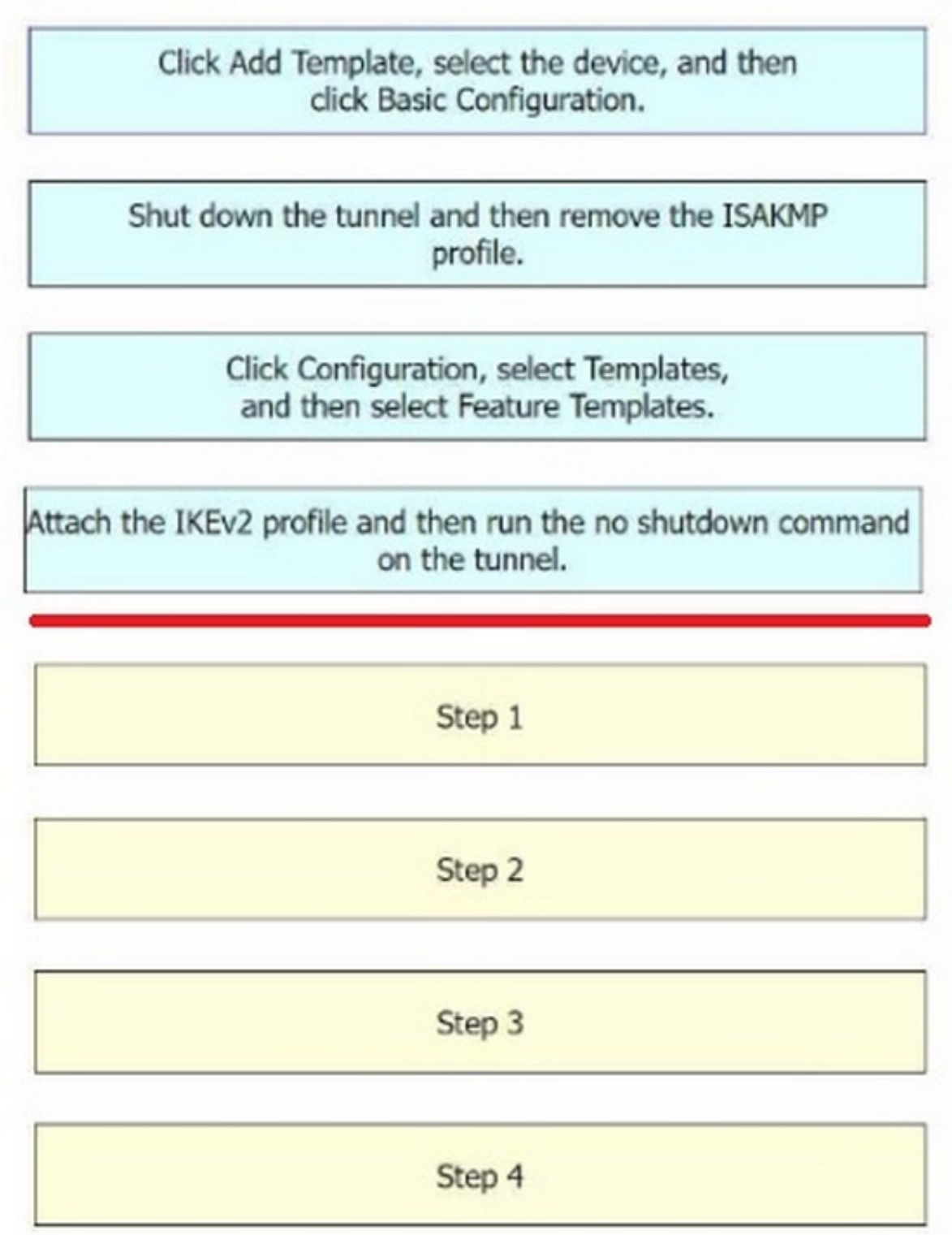
SD-WAN Configuration Example: Site-to-site (LAN to LAN) IPSec between vEdge and Cisco IOS - Cisco Community

QUESTION 7

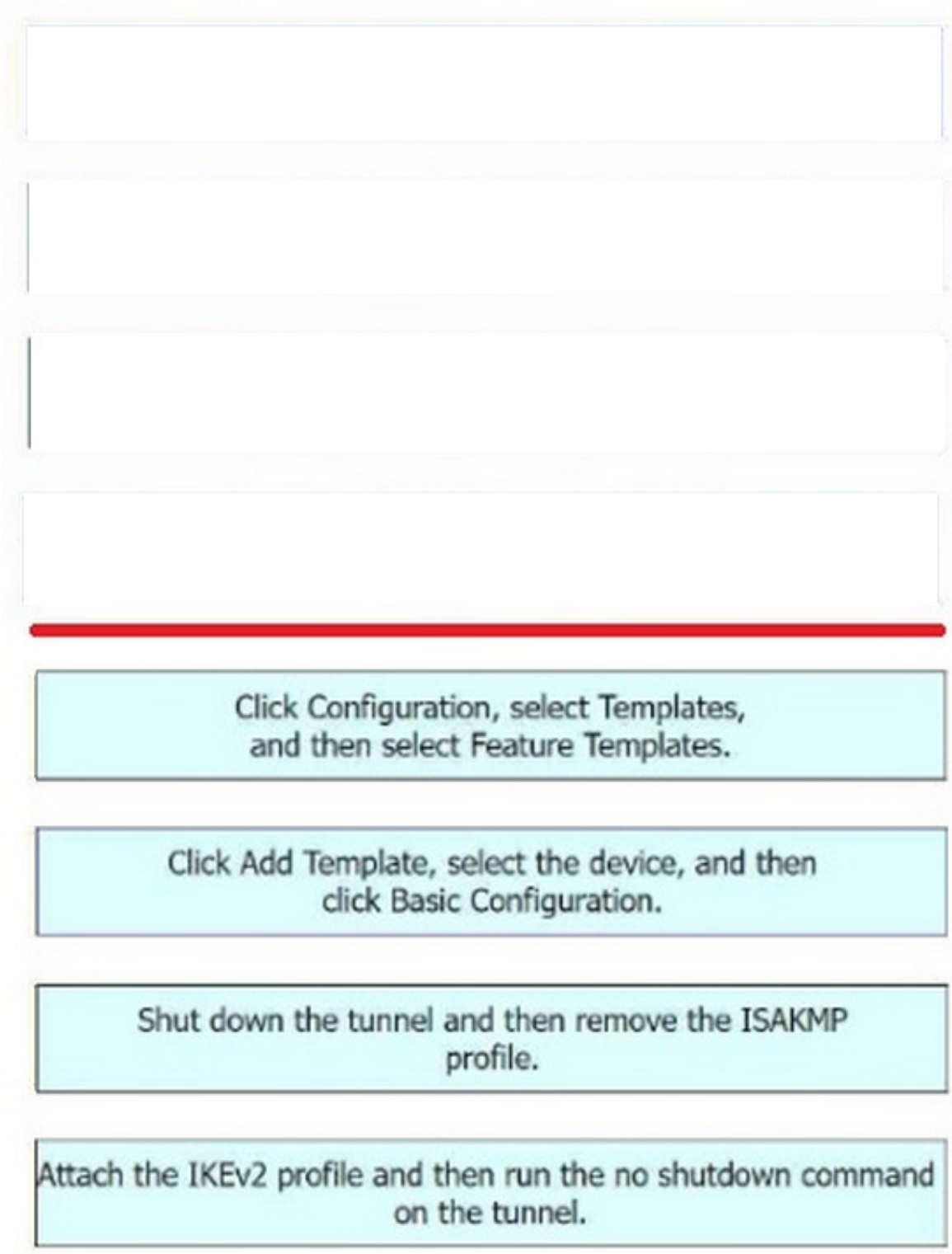
DRAG DROP

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:

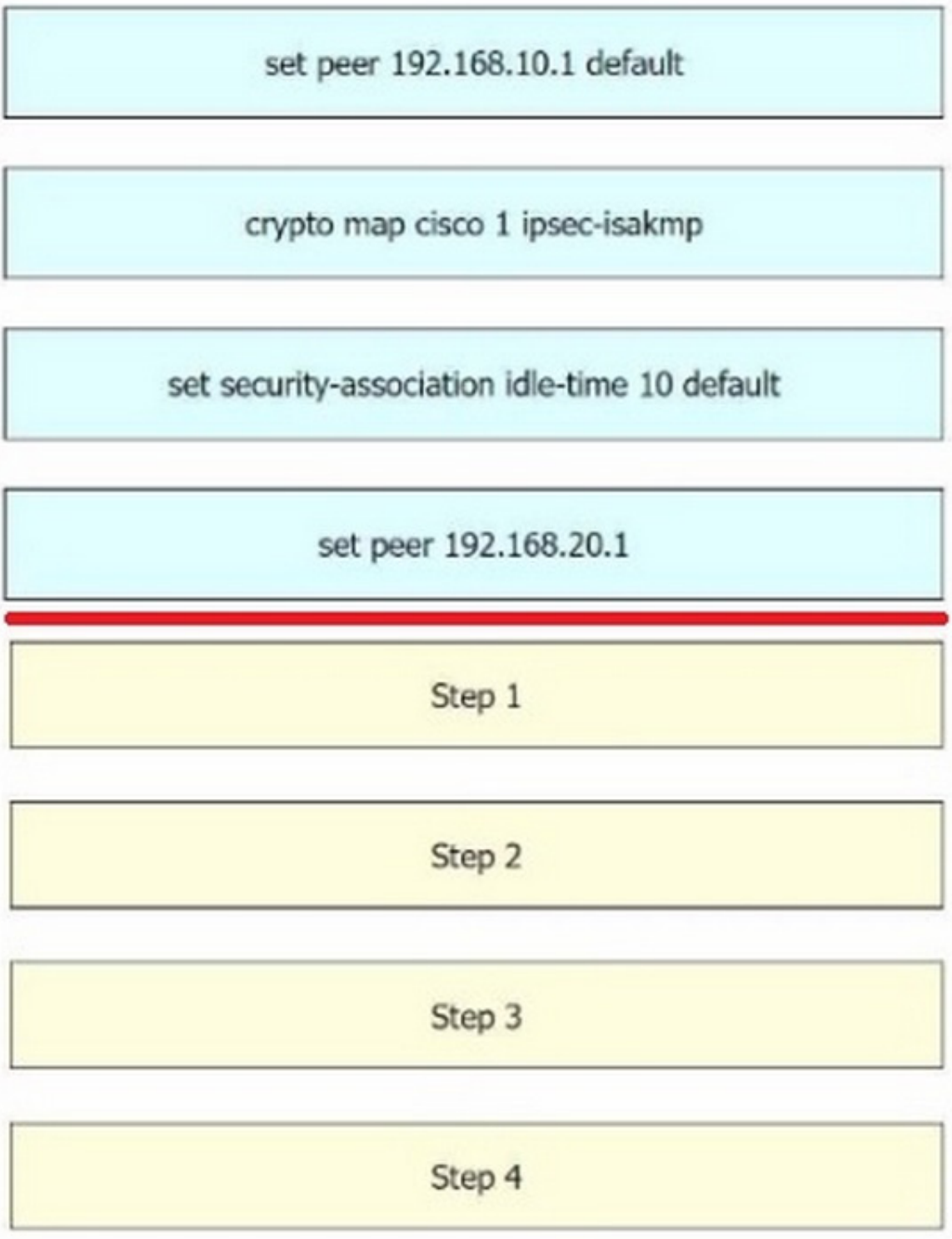
Configuring Internet Key Exchange Version 2 (IKEv2) - Cisco Switch from IKEv1 to IKEv2 on Cisco Routers - Cisco Community Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community

QUESTION 8

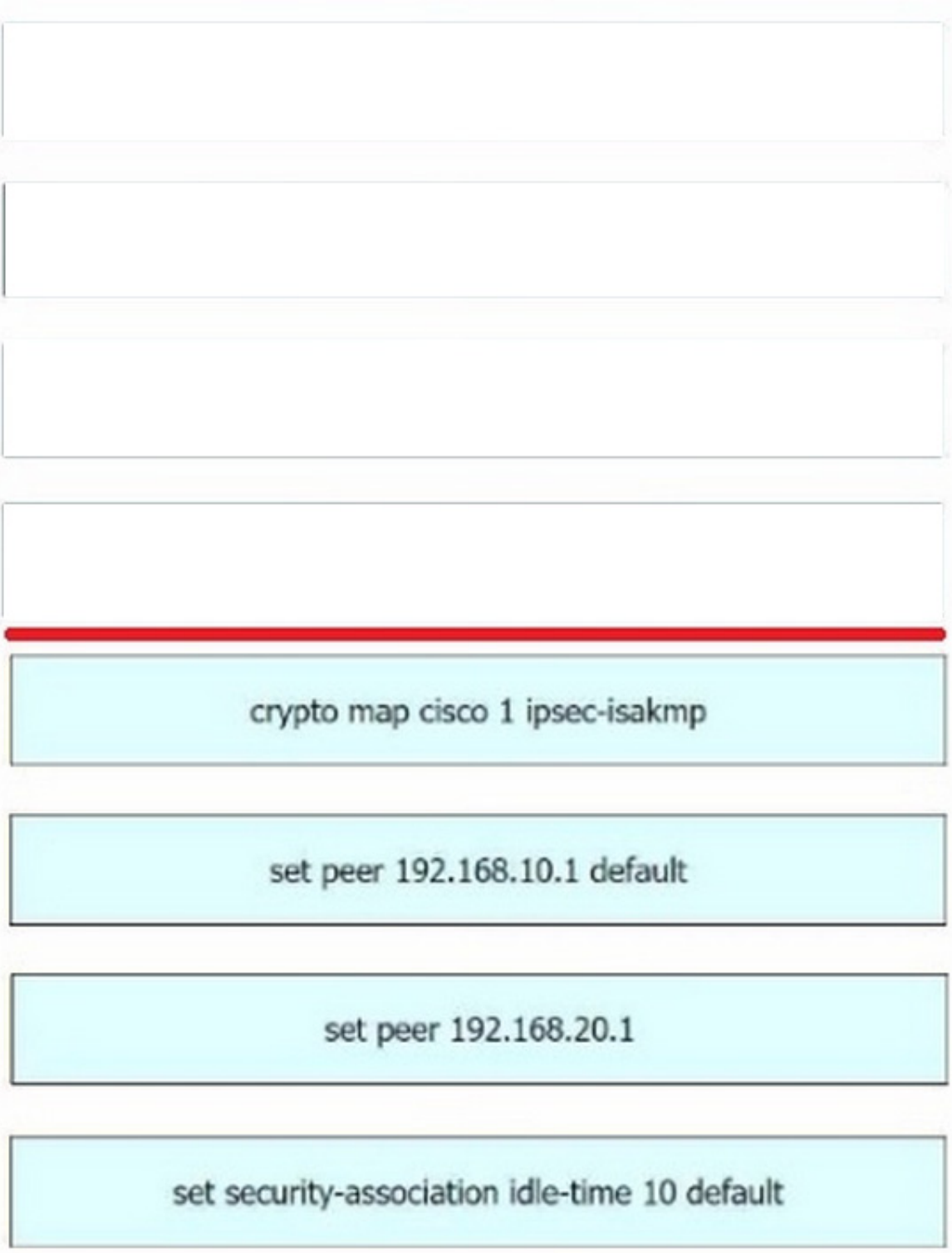
DRAG DROP

An engineer must edit the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS). IPsec must be configured to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco. Drag and drop the commands from the left onto the order on the right.

Select and Place:



Correct Answer:



Step 1 = crypto map cisco 1 ipsec-isakmp Step 2 = set peer 192.168.10.1 default Step 3 = set peer 192.168.20.1 Step 4 = set security-association idle-time 120 default

The process of editing the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS), and configuring IPsec to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco involves several steps123456. crypto map cisco 1 ipsec-isakmp: This command is used to create a new entry in the crypto map named "cisco". The "1" is the sequence number of the entry, and "ipsec-isakmp" specifies that the IPSec security associations (SAs) should be established using the

Internet Key Exchange (IKE) protocol13. set peer 192.168.10.1 default: This command is used to specify the IP address of the default peer for the crypto map entry. In this case, the default peer is at IP address 192.168.10.115. set peer 192.168.20.1: This command is used to add an additional peer to the crypto map entry. In this case, the additional peer is at IP address 192.168.20.1. This allows the IPsec VPN to support multiple peers56. set security-association idle-time 120 default: This command is used to set the idle time for the security association. If no traffic is detected over the VPN for the specified idle time (in this case, 120 seconds), the security association is deleted, and the VPN connection fails over to the next peer46.

References: Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router - Cisco Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers Configure Failover for IPSec Site-to-Site Tunnels with Backup ISP Links on FTD Managed by FMC - Cisco Does Setting Multiple Peers in a Crypto Map Also Support Parallel IPSec Connections - Cisco Community Multiple WAN Connections -- IPsec in Multi-WAN Environments | pfSense Documentation Multiple Set Peer for VPN Failover - Server Fault

QUESTION 9

Which approach does a centralized internet gateway use to provide connectivity to SaaS applications?

A. A cloud-based proxy server routes traffic from the on-premises infrastructure to the SaaS provider data center.

B. Internet traffic from the on-premises infrastructure is routed through a centralized gateway that provides access controls for SaaS applications.

C. VPN connections are used to provide secure access to SaaS applications from the on- premises infrastructure.

D. A dedicated, private connection is established between the on-premises infrastructure and the SaaS provider data center using colocation services.

Correct Answer: B

A centralized internet gateway is a network design that routes all internet- bound traffic from the on-premises infrastructure through a single point of egress, typically located at the data center or a regional hub1. This approach allows the enterprise to apply consistent security policies and access controls for SaaS applications, as well as optimize the bandwidth utilization and performance of the WAN links. A centralized internet gateway can use various technologies to provide connectivity to SaaS applications, such as proxy servers, firewalls, web filters, and WAN optimizers. However, a cloud-based proxy server (option A) is not a part of the centralized internet gateway, but rather a separate service that can be used to route traffic from the on-premises infrastructure to the SaaS provider data center4. VPN connections (option C) and dedicated, private connections (option D) are also not related to the centralized internet gateway, but rather alternative ways of providing secure and reliable access to SaaS applications from the on- premises infrastructure5. Therefore, the correct answer is option B, which describes the basic function of a centralized internet gateway.

QUESTION 10

Refer to the exhibit.

```
1-Aug-2021 20:12:11 EDT] Failed to apply policy - Failed to
process device request -
Error type : application
Error tag : operation-failed
Error Message : /apply-policy/site-list[name='All-Site']:
Overlapping apply-policy site-list Hub site id 200-299 with
site-list All-Site
Error info : <error-info>
<bad-element>site-list</bad-element>
</error-info>
```

A company uses Cisco SD-WAN in the data center. All devices have the default configuration. An engineer attempts to add a new centralized control policy in Cisco vManage but receives an error message. What is the problem?

A. A centralized control policy is already applied to the specific site ID and direction

B. The policy for "Hub" should be applied in the outbound direction, and the policy for "All- Site" should be applied inbound.

C. Apply an additional outbound control policy to override the site ID overlaps.

D. Site-list "All-Site" should be configured with a new match sequence that is lower than the sequence for site-list "Hub*.

Correct Answer: D

The problem is that the site-list "All-Site" has a higher match sequence than the site-list "Hub", which means that the policy for "All-Site" will take precedence over the policy for "Hub" for any site that belongs to both lists. This creates a conflict

and prevents the engineer from adding a new centralized control policy in Cisco vManage. To resolve this issue, the site-list "All-Site" should be configured with a new match sequence that is lower than the sequence for site-list "Hub", so that

the policy for "Hub" will be applied first and then the policy for "All-Site" will be applied only to the remaining sites that are not in the "Hub" list.

References:

Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3:

Cisco SD-WAN Cloud OnRamp for Colocation, Lesson 3: Cisco SD-WAN Cloud OnRamp for Colocation - Centralized Control Policies Cisco SD-WAN Cloud OnRamp for Colocation Deployment Guide, Chapter 4:

Configuring Centralized Control Policies Cisco SD-WAN Configuration Guide, Release 20.3, Chapter: Centralized Policy Framework, Section: Policy Configuration Overview