300-440 Q&As

Designing and Implementing Cloud Connectivity (ENCC)

Pass Cisco 300-440 Exam with 100% Guarantee

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

QUESTION 1

A company with multiple branch offices wants a connectivity model to meet its network architecture requirements. The company focuses on ensuring low latency and efficient routing for its critical business applications. Which connectivity model meets these requirements?

A. hub-and-spoke topology with SD-WAN technology, using dynamic routing and OSPF as the routing protocol

B. fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol

C. point-to-point topology using dedicated leased lines and static routing

D. star topology with internet-based VPN connections and static routing

Correct Answer: B

A fully meshed topology with SD-WAN technology, using dynamic routing and BGP as the routing protocol, meets the requirements of the company because it provides the following benefits

It allows direct and secure connectivity between any two branch offices, without the need for a central hub or intermediary devices. This reduces the latency and improves the performance of the critical business applications. It leverages SDWAN technology to optimize the traffic flow and application quality of service (QoS) across the WAN. SD-WAN can dynamically select the best path for each application based on the network conditions and policies. SD- WAN can also provide redundancy, security, and visibility for the WAN. It uses dynamic routing and BGP as the routing protocol to exchange routing information and establish connectivity between the branch offices. BGP is a scalable and flexible protocol that can support multiple address families, such as IPv4 and IPv6, and multiple routing policies, such as local preference and route filtering. BGP can also enable seamless integration with the cloud service providers (CSPs) and internet service providers (ISPs).

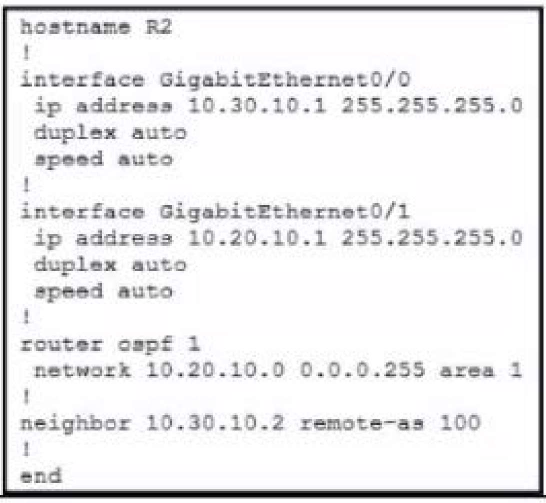
References :

1: Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5) (Cisco U.login required)

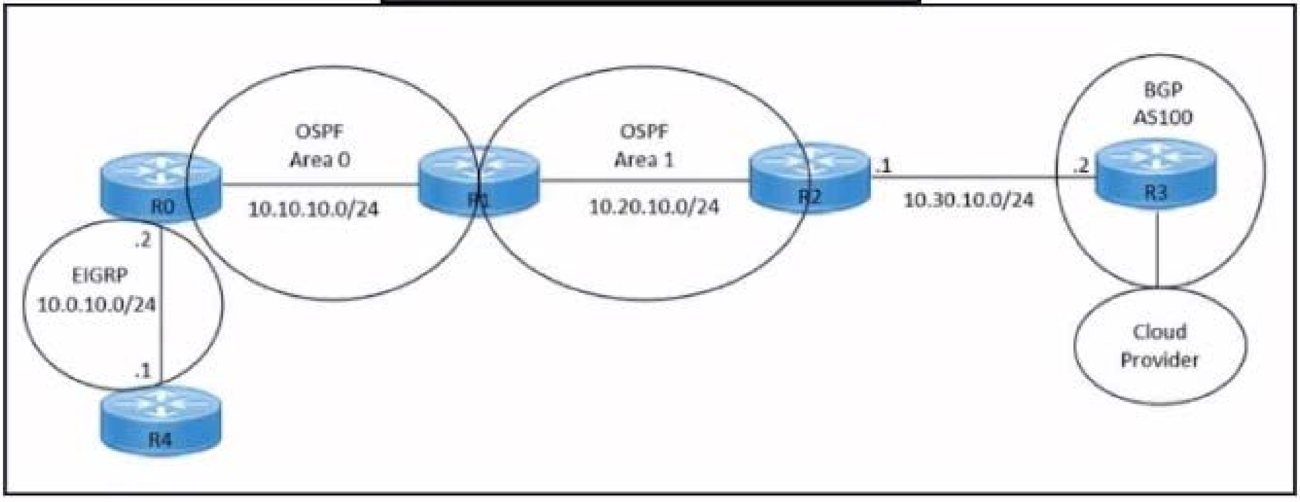
2: Cisco SD-WAN Design Guide

QUESTION 2

Refer to the exhibits.



```
hostname R2
!
interface GigabitEthernet0/0
 ip address 10.30.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 network 10.20.10.0 0.0.0.255 area 1
!
neighbor 10.30.10.2 remote-as 100
!
end
```



An engineer must redistribute OSPF internal routes into BGP to connect an on-premises network to a cloud provider without introducing extra routes. Which two commands must be configured on router R2? (Choose two.)

A. router ospf 1

B. router bgp 100

C. redistribute ospf 1

D. redistribute bgp 100

E. redistribute ospf 1 match internal external

Correct Answer: BE

To redistribute OSPF internal routes into BGP, the engineer needs to configure two commands on router R2. The first command is router bgp 100, which enables BGP routing process and specifies the autonomous system number of 100.

The second command is redistribute ospf 1 match internal external, which redistributes the routes from OSPF process into BGP, and matches both internal and external OSPF routes. This way, the engineer can avoid introducing extra routes

that are not part of OSPF process 1, such as the default route or the connected routes.

References:

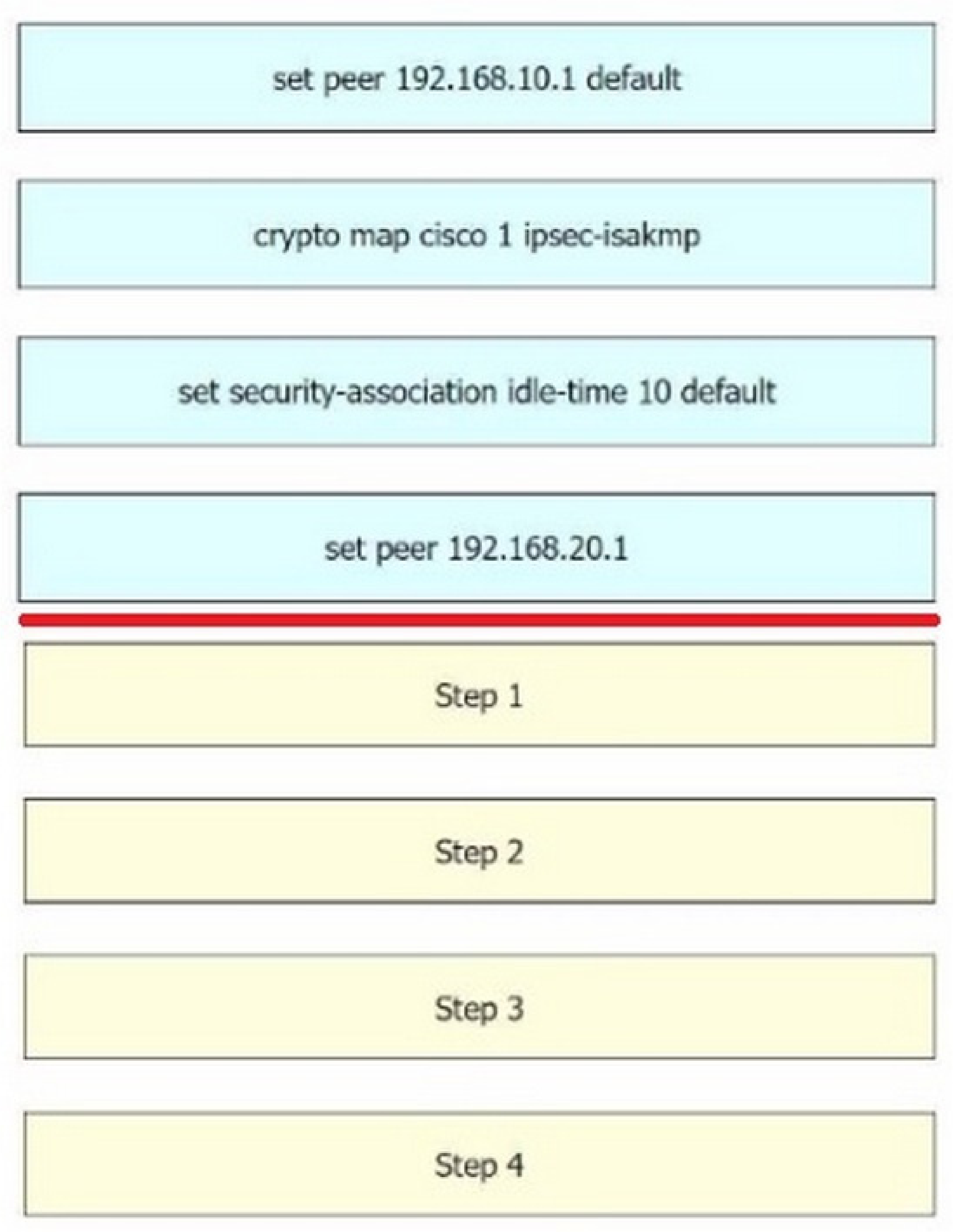
Designing and Implementing Cloud Connectivity (ENCC) v1.0, [ENCC: Configuring IPsec VPN from Cisco IOS XE to AWS], [Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs]

QUESTION 3

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:



set peer 192.168.10.1 default

crypto map cisco 1 ipsec-isakmp

set security-association idle-time 10 default

set peer 192.168.20.1

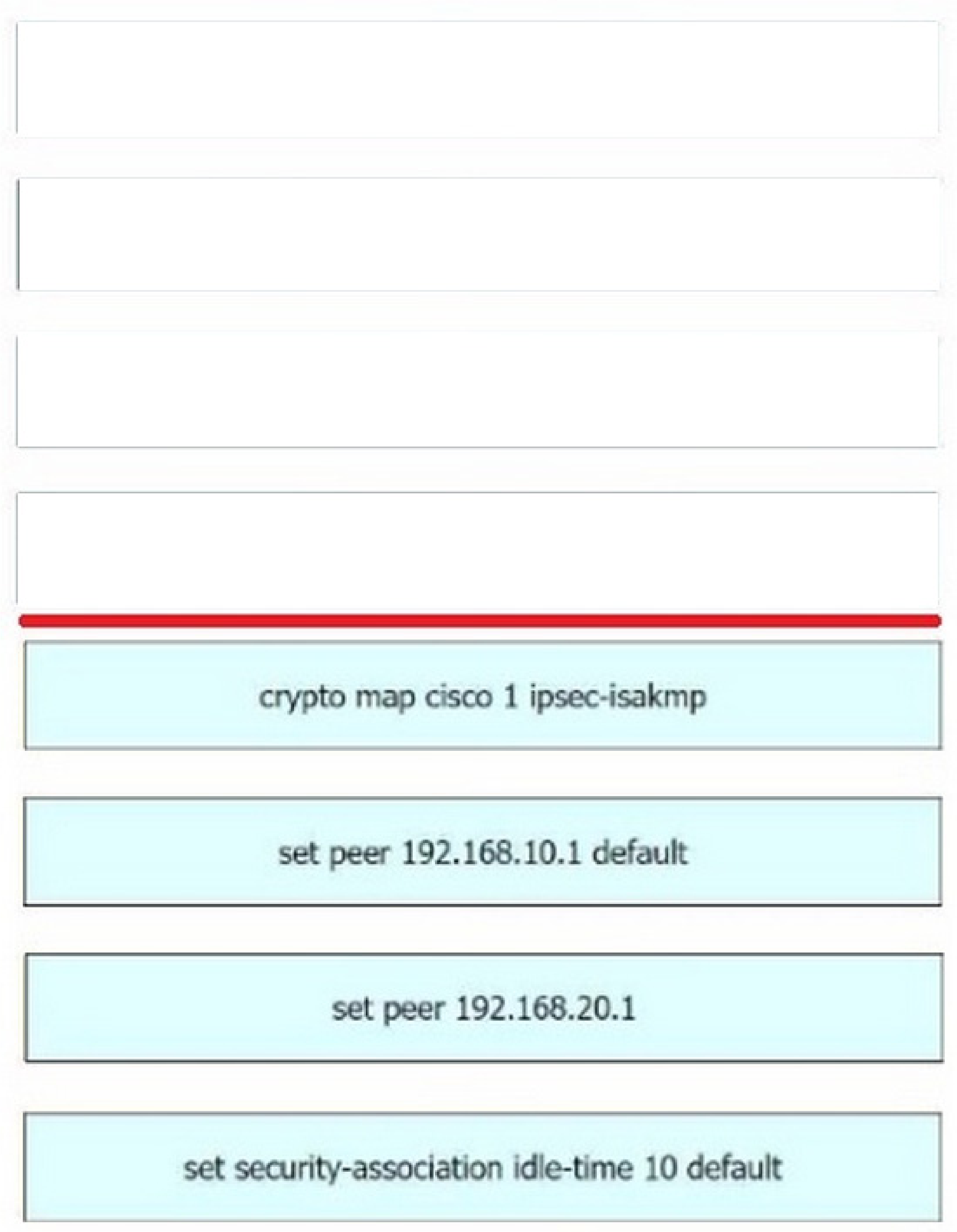
Step 1

Step 2

Step 3

Step 4

Correct Answer:



crypto map cisco 1 ipsec-isakmp

set peer 192.168.10.1 default

set peer 192.168.20.1

set security-association idle-time 10 default

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

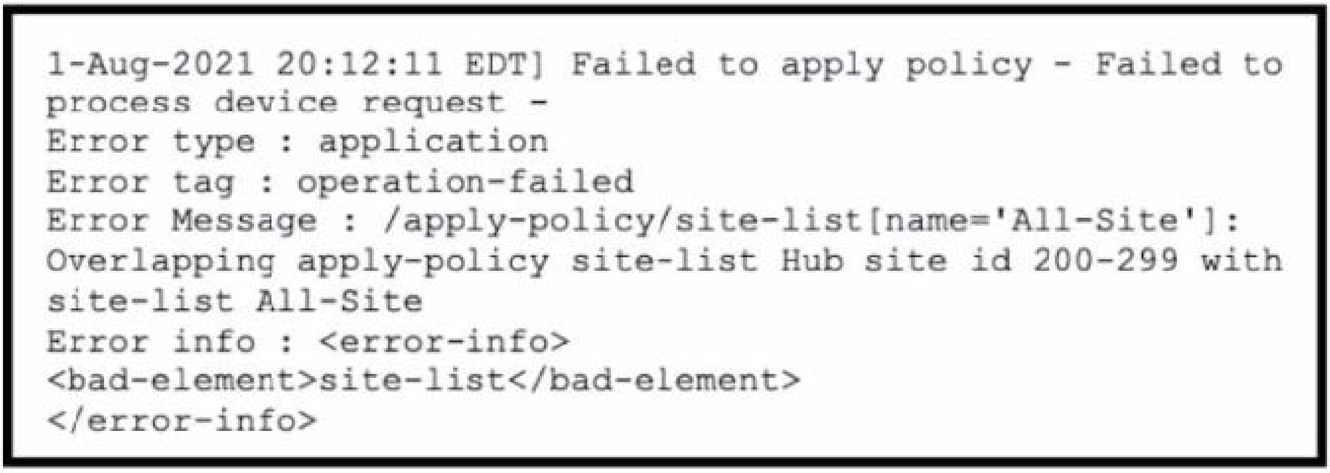
The process of editing the settings of a site-to-site IPsec VPN connection between an on- premises Cisco IOS XE router and Amazon Web Services (AWS), and configuring IPsec to support multiple peers and failover after 120 seconds of idle time on the first entry of the crypto map named Cisco involves several 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 4

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:

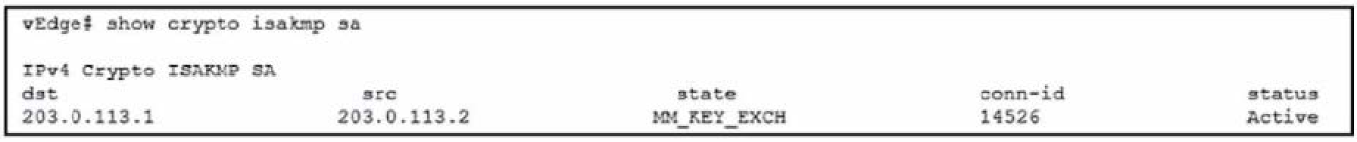
Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3:

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

QUESTION 5

Refer to the exhibit.



```
vEdge# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst                  src                  state                conn-id            status
203.0.113.1          203.0.113.2          MM_KEY_EXCH          14526              Active
```

While troubleshooting an IPsec connection between a Cisco WAN edge router and an Amazon Web Services (AWS) endpoint, a network engineer observes that the security association status is active, but no traffic flows between the devices What is the problem?

A. wrong ISAKMP policy

B. identity mismatch

C. wrong encryption

D. IKE version mismatch

Correct Answer: B

An identity mismatch occurs when the local and remote identities configured on the IPsec peers do not match. This can prevent the establishment of an IPsec tunnel or cause traffic to be dropped by the IPsec policy. In this case, the network

engineer should verify that the local and remote identities configured on the Cisco WAN edge router and the AWS endpoint match the values expected by each peer. The identities can be an IP address, a fully qualified domain name (FQDN),

or a distinguished name (DN). The identities are exchanged during the IKE phase 1 negotiation and are used to authenticate the peers. If the identities do not match, the peers will reject the IKE proposal and the IPsec tunnel will not be

established or will be torn down.

References: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services, Topic:Troubleshooting

Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:

Implementing Cloud Connectivity, Lesson 2: Implementing Cisco SD-WAN Cloud OnRamp for IaaS, Topic: Troubleshooting Cisco SD-WAN Cloud OnRamp for IaaS Cisco IOS Security Configuration Guide, Release 15MandT, Chapter:

Configuring IPsec Network Security, Topic: Configuring IPsec Identity and Peer Addressing

QUESTION 6

DRAG DROP

An engineer must configure a CLI add-on feature template in Cisco vManage for enhanced policy-based routing (ePBR) for IPv4. These configurations were deleted:

1.

licensing config enable false

2.

licensing config privacy hostname true

3.

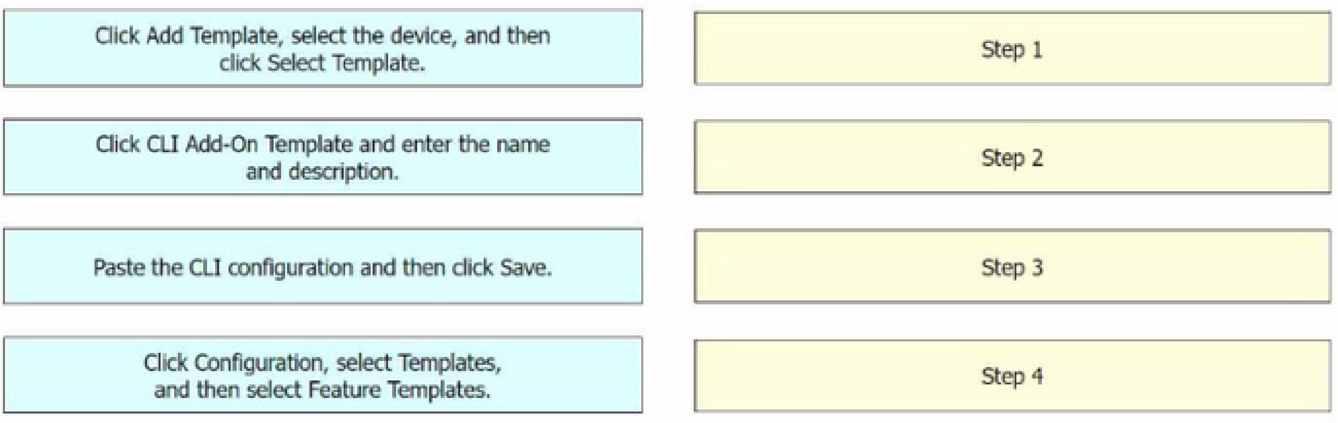
licensing config privacy version false

4.

licensing config utility utility-enable true

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

Select and Place:



Click Add Template, select the device, and then click Select Template.

Click CLI Add-On Template and enter the name and description.

Paste the CLI configuration and then click Save.

Click Configuration, select Templates, and then select Feature Templates.

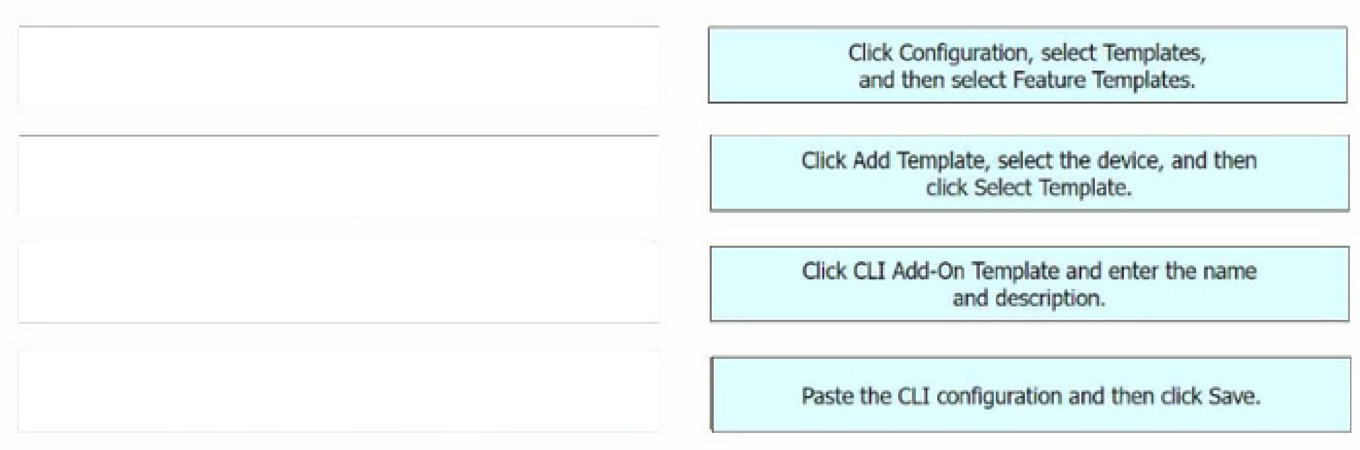
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Click Configuration, select Templates, and then select Feature Templates.

Click Add Template, select the device, and then click Select Template.

Click CLI Add-On Template and enter the name and description.

Paste the CLI configuration and then click Save.

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

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

Step 3 = Click CLI Add-On Template and enter the name and description.

Step 4 = Paste the CLI configuration and then click Save.

The process of configuring a CLI add-on feature template in Cisco vManage for enhanced policy-based routing (ePBR) for IPv4 involves several steps1234. 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 vManage.

Click Add Template, select the device, and then click Select Template: In this step, you add a new template for the device.

Click CLI Add-On Template and enter the name and description: After setting up the template, you select the CLI Add-On Template option, and then enter the name and description for the template.

Paste the CLI configuration and then click Save: Finally, you paste the CLI configuration into the template and save the changes.

References:

CLI Add-On Feature Templates - Cisco

Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - CLI Add-On Feature Templates Cisco SD-WAN vSmart CLI Template - NetworkLessons.com CLI Templates for Cisco XE

SD-WAN Routers

QUESTION 7

An engineer must configure an IPsec tunnel to the cloud VPN gateway. Which Two actions send traffic into the tunnel? (Choose two.)

A. Configure access lists that match the interesting user traffic.

B. Configure a static route.

C. Configure a local policy in Cisco vManage.

D. Configure an IPsec profile and match the remote peer IP address.

E. Configure policy-based routing.

Correct Answer: AE

To send traffic into an IPsec tunnel to the cloud VPN gateway, the engineer must configure two actions:

Configure access lists that match the interesting user traffic. This is the traffic that needs to be encrypted and sent over the IPsec tunnel. The access lists are applied to the crypto map that defines the IPsec parameters for the tunnel.

Configure policy-based routing (PBR). This is a technique that allows the engineer to override the routing table and forward packets based on a defined policy. PBR can be used to send specific traffic to the IPsec tunnel interface, regardless

of the destination IP address. This is useful when the cloud VPN gateway has a dynamic IP address or when multiple cloud VPN gateways are available for load balancing or redundancy.

References:

Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:

Implementing Cloud Connectivity, Lesson 3: Implementing IPsec VPNs to the Cloud, Topic: Configuring IPsec VPNs on Cisco IOS XE Routers Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter:

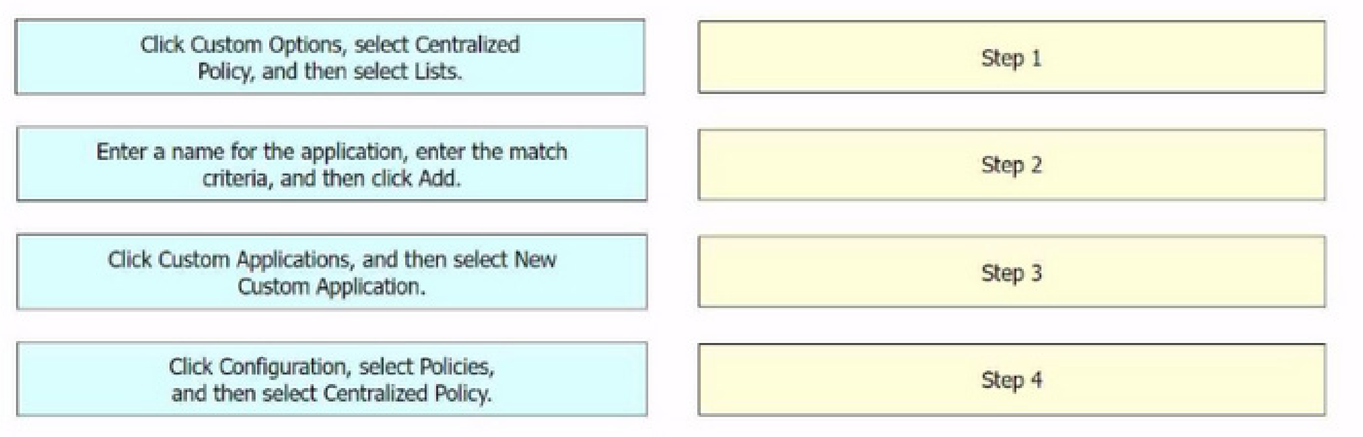
Configuring IPsec VPNs, Topic: Configuring Crypto Maps [Cisco IOS XE Gibraltar 16.12.x Feature Guide], Chapter: Policy-Based Routing, Topic: Policy-Based Routing Overview

QUESTION 8

DRAG DROP

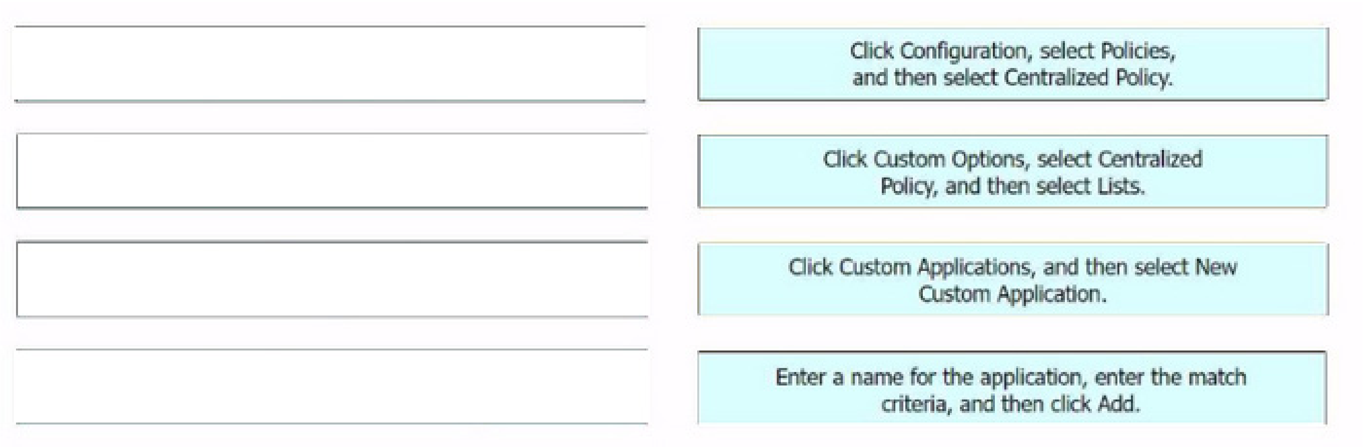
An engineer signs in to Cisco vManage and needs to configure a custom application with a Cisco SD-WAN centralized policy. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Click Custom Options, select Centralized Policy, and then select Lists.	Step 1
Enter a name for the application, enter the match criteria, and then click Add.	Step 2
Click Custom Applications, and then select New Custom Application.	Step 3
Click Configuration, select Policies, and then select Centralized Policy.	Step 4

Correct Answer:



Click Configuration, select Policies, and then select Centralized Policy.

Click Custom Options, select Centralized Policy, and then select Lists.

Click Custom Applications, and then select New Custom Application.

Enter a name for the application, enter the match criteria, and then click Add.

The process of configuring a custom application with a Cisco SD-WAN centralized policy using Cisco vManage involves several steps.

Click Configuration, select Policies, and then select Centralized Policy: This is the first step where you navigate to the Policies section in the Configuration menu of Cisco vManage.

Click Custom Options, select Centralized Policy, and then select Lists: In this step, you select the Custom Options, then select Centralized Policy, and finally select Lists.

Click Custom Applications, and then select New Custom Application: After setting up the Lists, you click on Custom Applications and then select New Custom Application.

Enter a name for the application, enter the match criteria, and then click Add:

Finally, you enter a name for the application, specify the match criteria, and then click Add to complete the configuration.

References:

Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE

QUESTION 9

A cloud engineer is setting up a new set of nodes in the AWS EKS cluster to manage database integration with Mongo Atlas. The engineer set up security to Mongo but now wants to ensure that the nodes are also secure on the network side. Which feature in AWS should the engineer use?

A. EC2 Trust Lock

B. security groups

C. tagging

D. key pairs

Correct Answer: B

Security groups are a feature in AWS that allow you to control the inbound and outbound traffic to your instances. They act as a virtual firewall that can filter the traffic based on the source, destination, protocol, and port. You can assign one or more security groups to your instances, and each security group can have multiple rules. Security groups are stateful, meaning that they automatically allow the response traffic for any allowed inbound traffic, and vice versa. Security groups are essential for securing your nodes in the AWS EKS cluster, as they can prevent unauthorized access to your Mongo Atlas database or other resources.

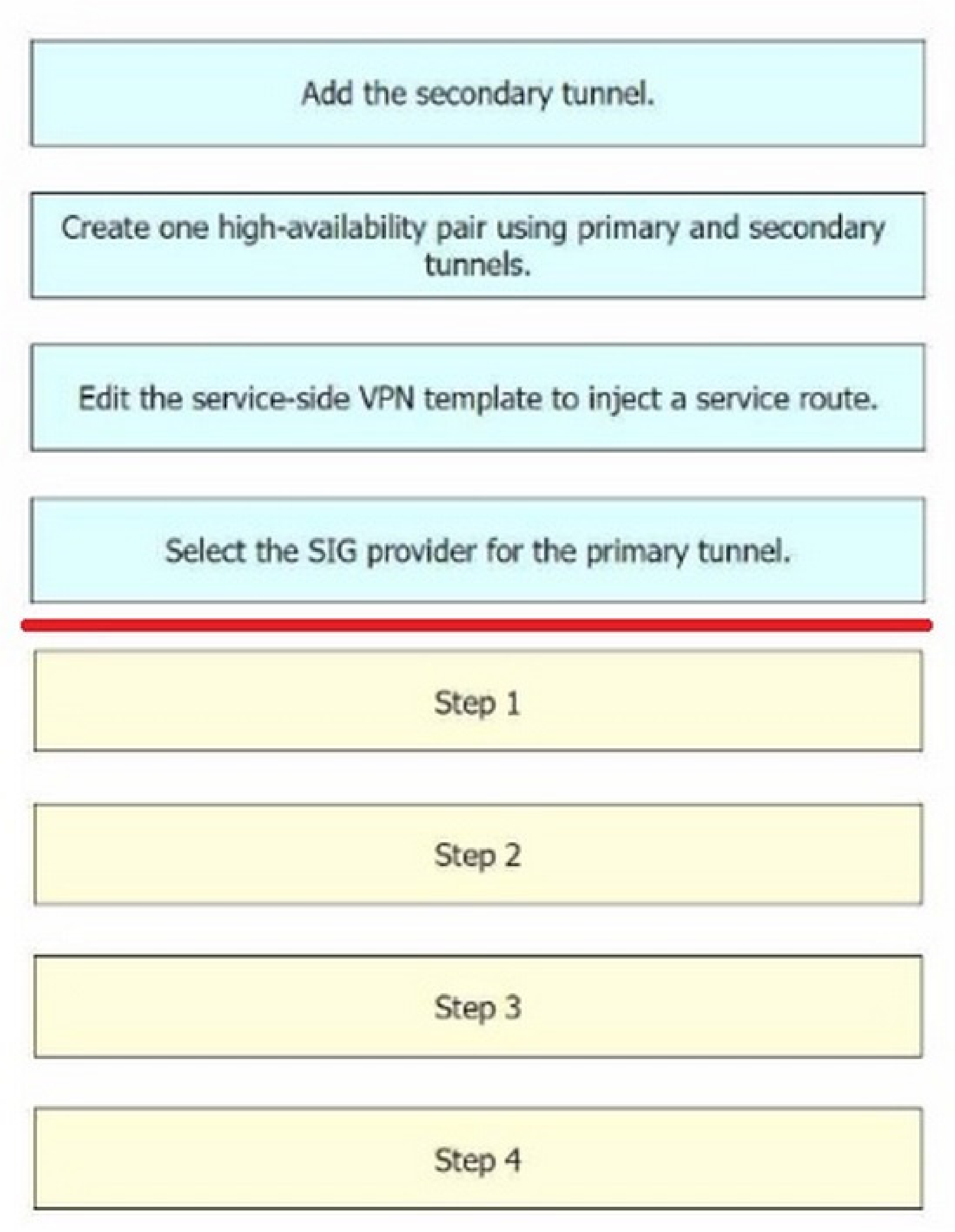
References: AWS Security Groups Security Groups for Your VPC Security Groups for Your Amazon EC2 Instances Security Groups for Your Amazon EKS Cluster

QUESTION 10

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:



Add the secondary tunnel.

Create one high-availability pair using primary and secondary tunnels.

Edit the service-side VPN template to inject a service route.

Select the SIG provider for the primary tunnel.

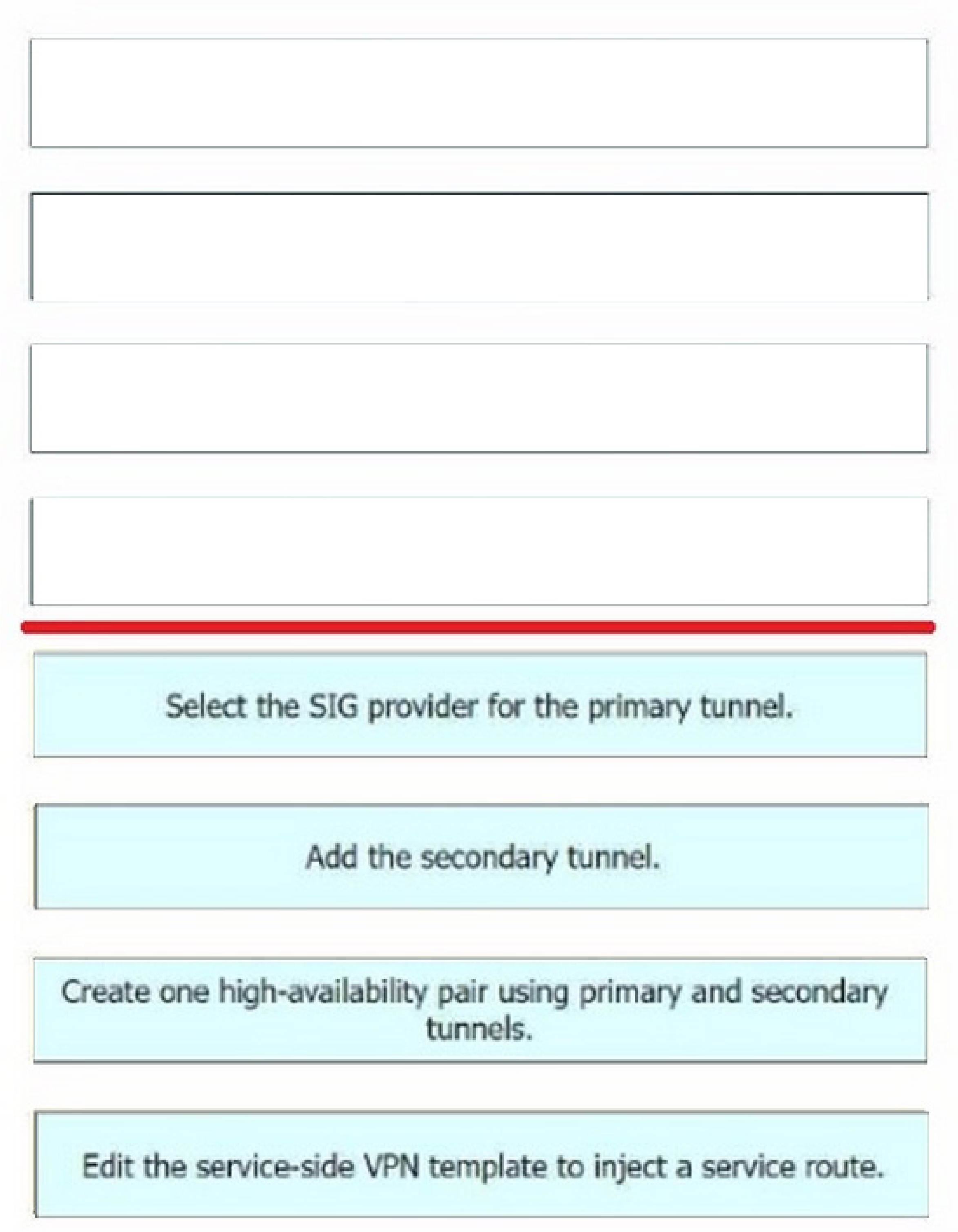
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Select the SIG provider for the primary tunnel.

Add the secondary tunnel.

Create one high-availability pair using primary and secondary tunnels.

Edit the service-side VPN template to inject a service route.

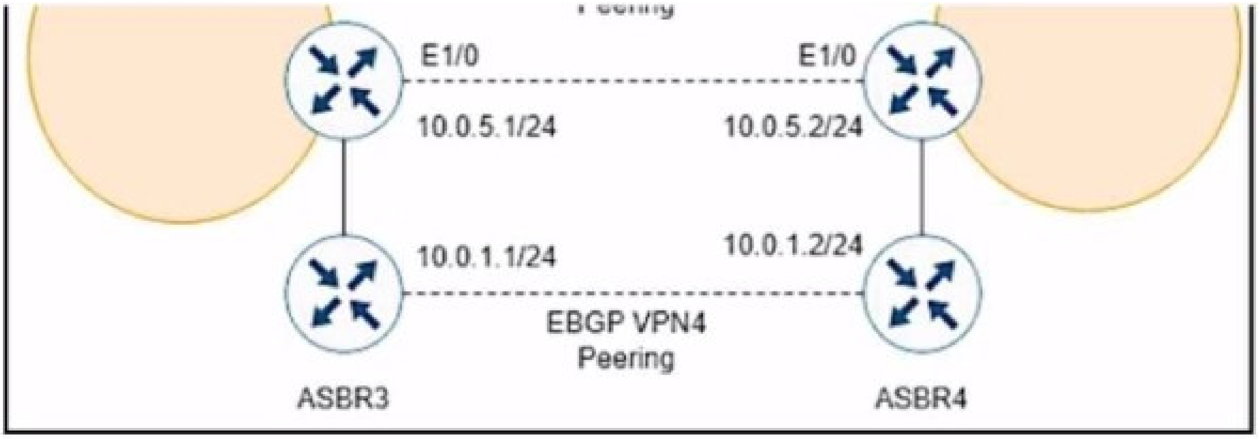
The configuration of cloud connectivity with Cisco Umbrella Secure Internet Gateway (SIG) in active/backup mode involves several steps. After configuring the SIG Credentials and SIG Feature Templates, the engineer must: Select the SIG provider for the primary tunnel: This is the first step in setting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

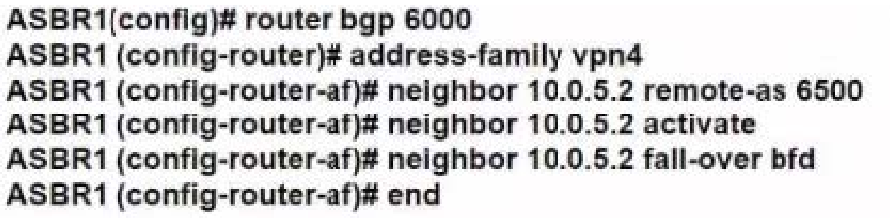
References: Designing and Implementing Cloud Connectivity (ENCC) v1.01 Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300- 440) Exam Prep2 Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios - Cisco

QUESTION 11

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

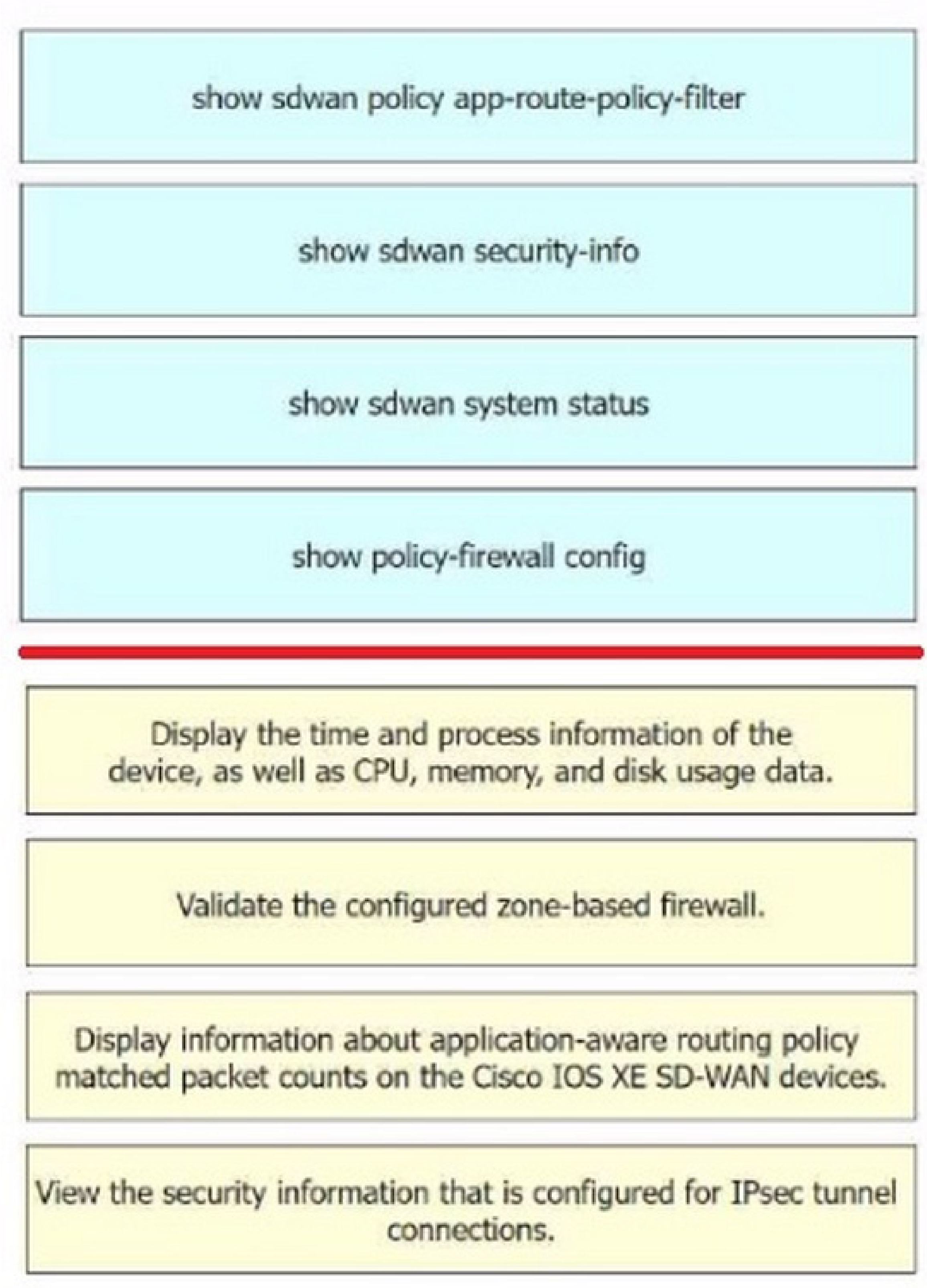
The bgp advertise-best-external command is used to enable the advertisement of the best external path to internal BGP peers. This command is useful when there are multiple exit points from the local AS to other ASes, and the local AS wants to use the closest exit point for each destination. By default, 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 12

DRAG DROP

Drag and drop the commands from the left onto the purposes on the right to identify issues on a Cisco IOS XE SD-WAN device.

Select and Place:



show sdwan policy app-route-policy-filter

show sdwan security-info

show sdwan system status

show policy-firewall config

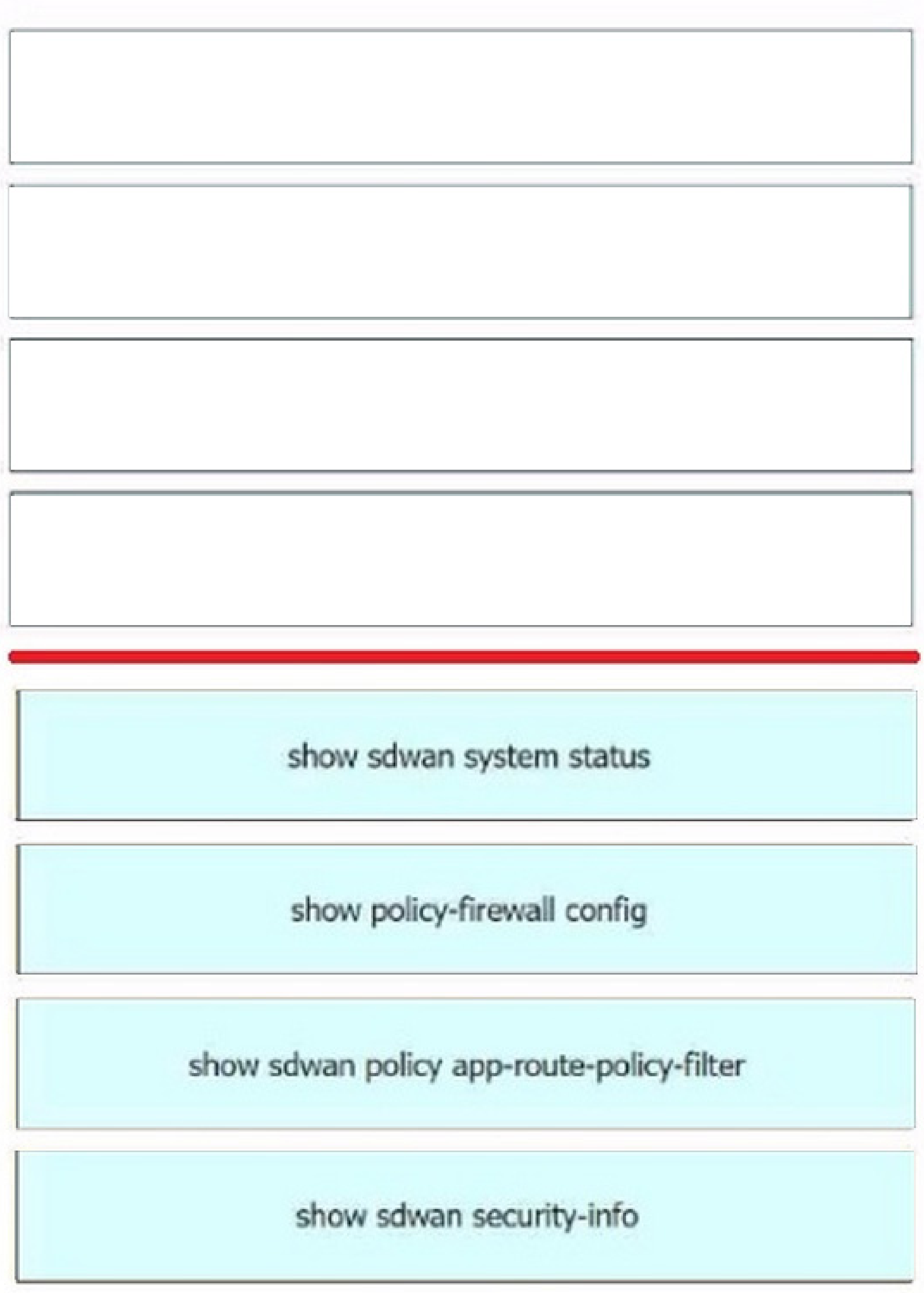
Display the time and process information of the device, as well as CPU, memory, and disk usage data.

Validate the configured zone-based firewall.

Display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices.

View the security information that is configured for IPsec tunnel connections.

Correct Answer:



show sdwan system status

show policy-firewall config

show sdwan policy app-route-policy-filter

show sdwan security-info

Display the time and process information of the device, as well as CPU, memory, and disk usage data. = show sdwan system status Validate the configured zone-based firewall. = show policy-firewall config1 Display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices. = show sdwan policy app-route-policy- filter View the security information that is configured for IPsec tunnel connections. = show sdwan security-info The commands used to identify issues on a Cisco IOS XE SD-WAN device are as follows show sdwan system status: This command is used to display the time and process information of the device, as well as CPU, memory, and disk usage data. show policy-firewall config: This command is used to validate the configured zone-based firewall. show sdwan policy app-route-policy-filter: This command is used to display information about application-aware routing policy matched packet counts on the Cisco IOS XE SD-WAN devices. show sdwan security-info: This command is used to view the security information that is configured for IPsec tunnel connections

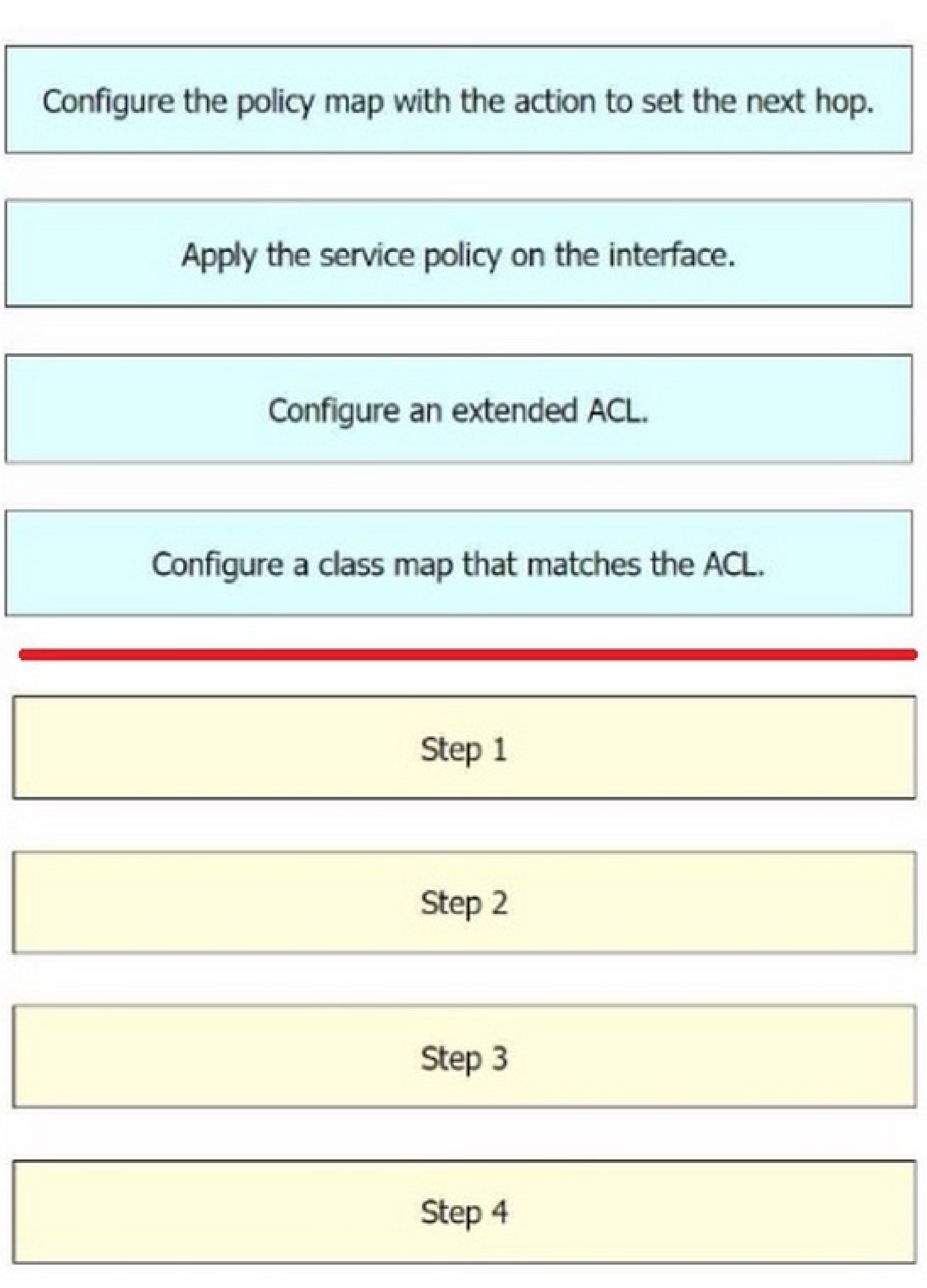
References: Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Cisco Catalyst SD-WAN Command Reference Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE SD-WAN Tunnel Interface Commands - Cisco

QUESTION 13

DRAG DROP

An engineer needs to configure enhanced policy-based routing (ePBR) for IPv4 by using Cisco vManage. Drag and drop the steps from the left onto the order on the right to complete the configuration of the ePBR using the CLI add-on template.

Select and Place:



Configure the policy map with the action to set the next hop.

Apply the service policy on the interface.

Configure an extended ACL.

Configure a class map that matches the ACL.

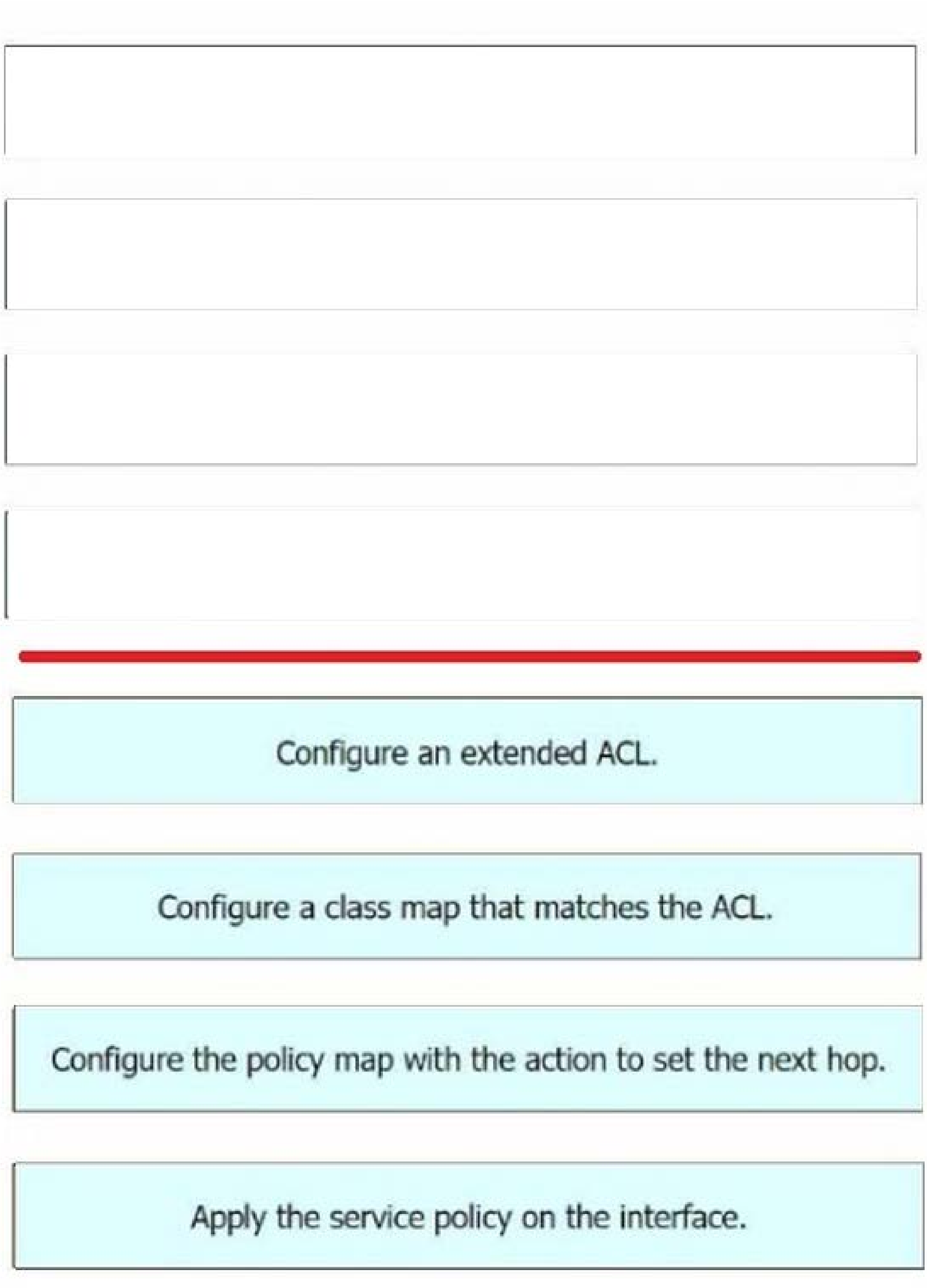
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Configure an extended ACL.

Configure a class map that matches the ACL.

Configure the policy map with the action to set the next hop.

Apply the service policy on the interface.

Enhanced Policy-Based Routing (ePBR) is used to direct packets that arrive at an interface to a specified next-hop. It is very useful in managing a large number of configured access lists more efficiently. In ePBR, the router drops the traffic packets if the next hop configured in the PBR policy is not reachable. To avoid packet loss in such scenarios, you must configure multiple next hops for each access control entry. Here are the steps to configure ePBR for IPv4 using Cisco vManage: Configure an extended ACL: This step involves defining the network or the host. For example, you can permit

IPv4 traffic from any source to specific hosts. Configure a class map that matches the ACL: Class maps match the parameters in the ACLs. For instance, you can create a class map of type traffic and match it with the previously created ACL. Configure the policy map with the action to set the next hop: Policy maps with ePBR then take detailed actions based on the set statements configured. You can configure an ePBR policy map with the class map and set the next hop. Apply the service policy on the interface: Finally, you apply the ePBR policy map to the interface. For example, you can apply the policy map to a GigabitEthernet interface. References : Implementing Enhanced Policy Based Routing - Cisco Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE How to configure PBR - Cisco Community