300-440 Q&As

Designing and Implementing Cloud Connectivity (ENCC)

QUESTION 1

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:

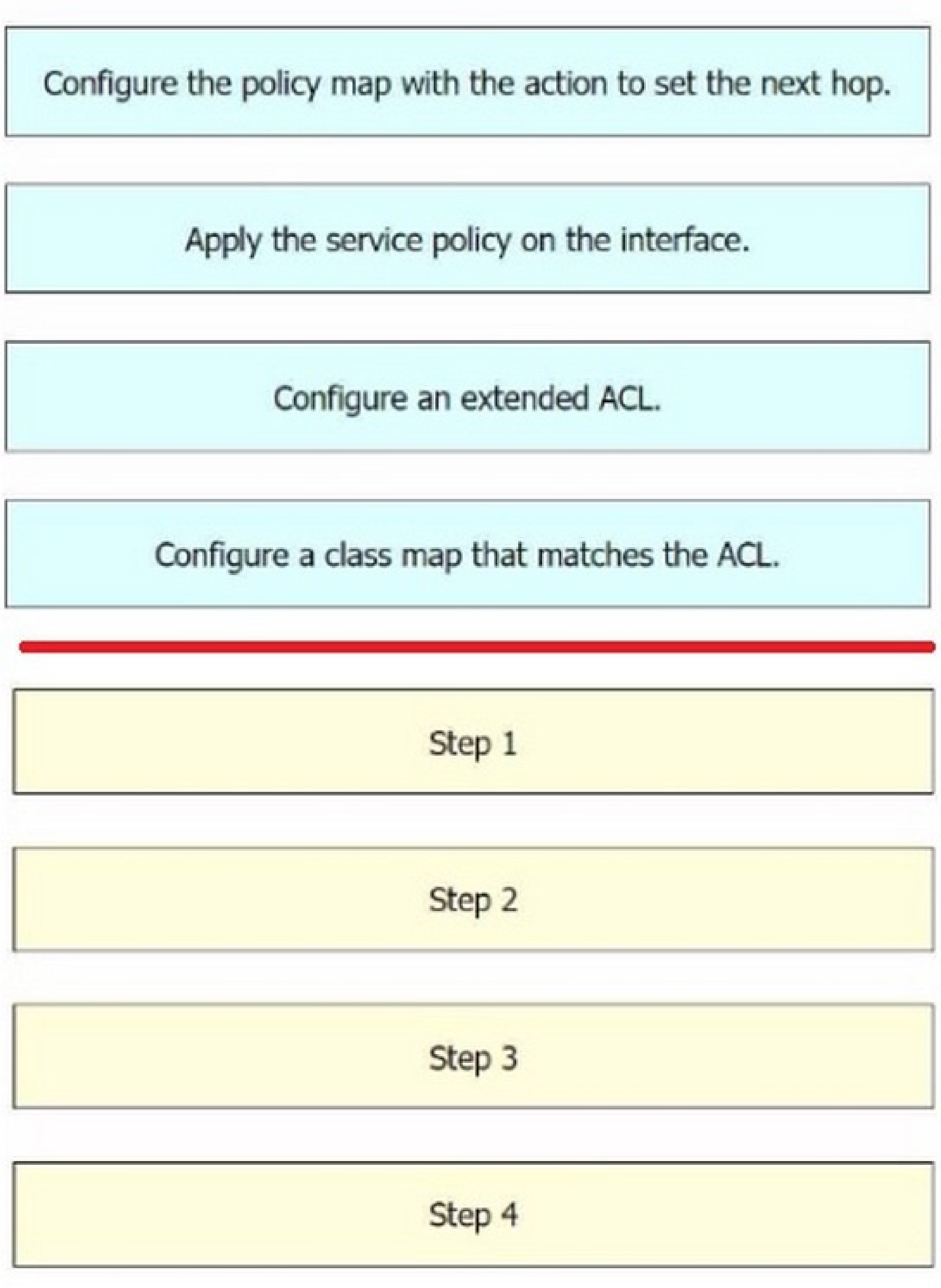
Traditional IPsec Versus Cisco SD-WAN IPsec, SD-WAN vs IPsec VPN\\'s - What\\'s the difference?, SD-WAN vs. VPN: How Do They Compare?, Traditional IPSEC Versus SD-WAN IPSEC

QUESTION 2

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.

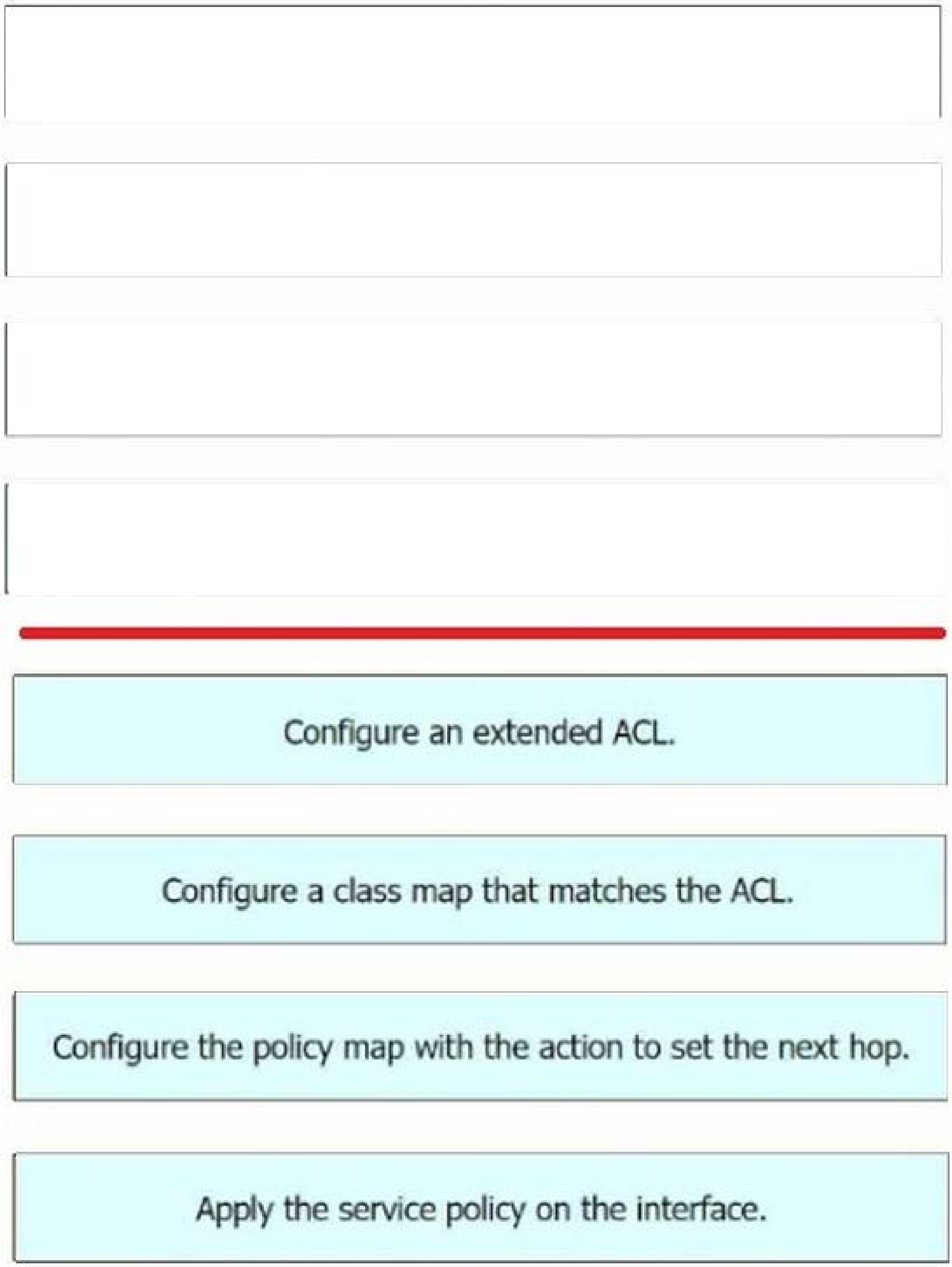
Step 1

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

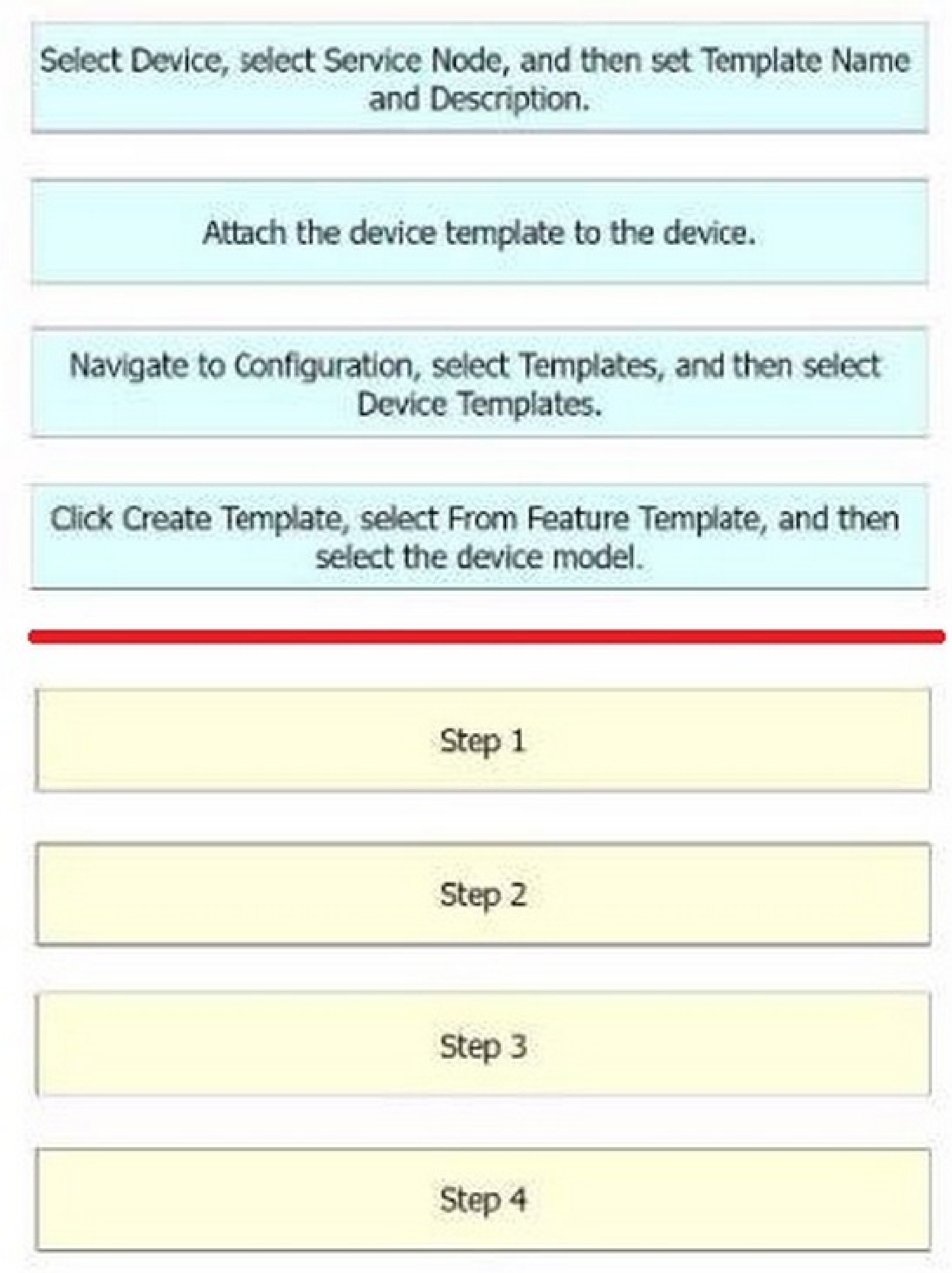
IPv4 traffic from any source to specific hosts. Configure a class map that matches the ACL: Class maps match the parameters in the ACLs. For instance, you can create a class map of type traffic and match it with the previously created ACL. Configure the policy map with the action to set the next hop: 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

QUESTION 3

DRAG DROP

An engineer must configure an AppGoE service node for WAN optimization for applications that are hosted in the cloud using Cisco vManage for C8000V or C8500L-8S4X devices. Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Select Device, select Service Node, and then set Template Name and Description.

Attach the device template to the device.

Navigate to Configuration, select Templates, and then select Device Templates.

Click Create Template, select From Feature Template, and then select the device model.

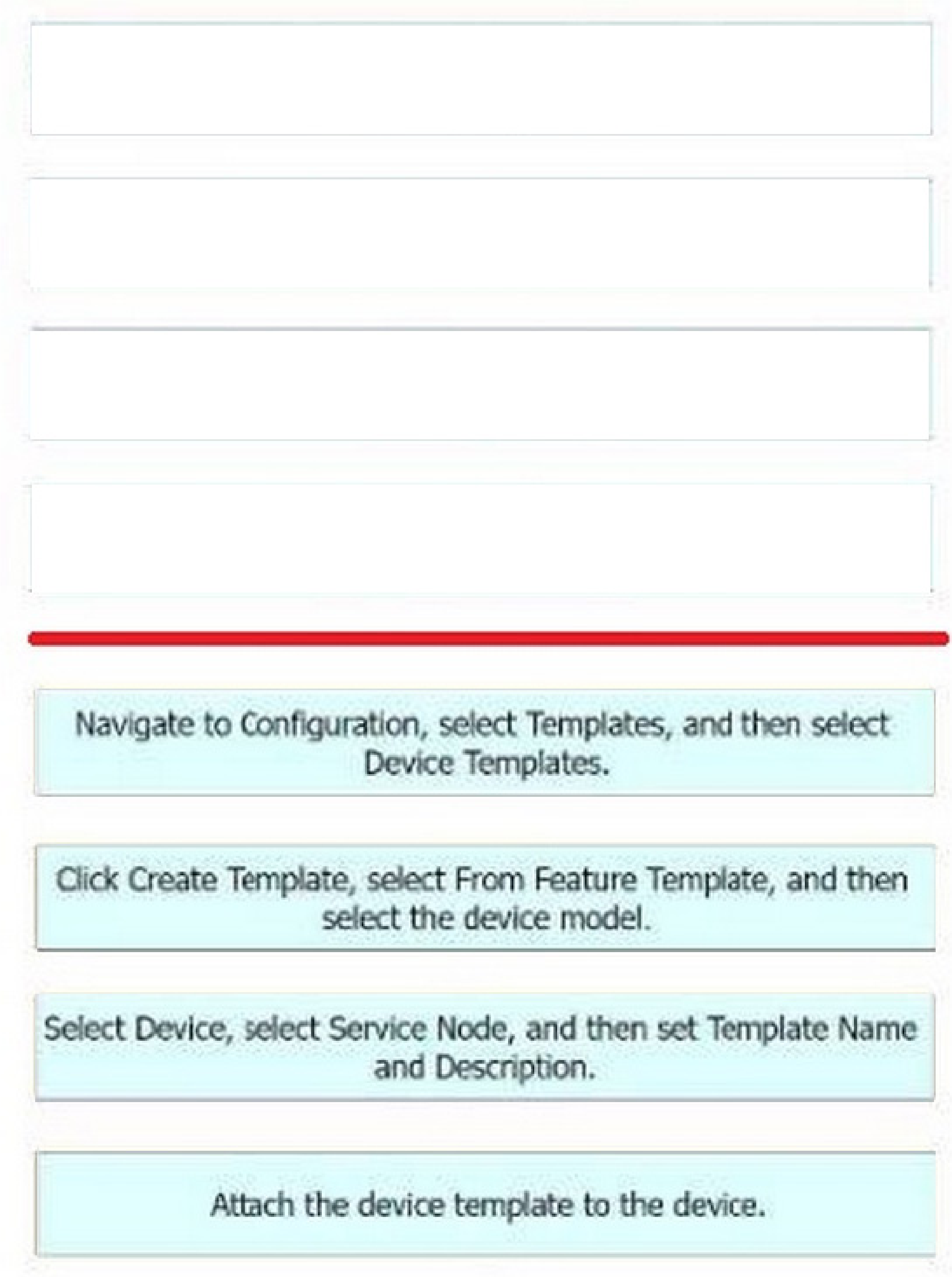
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Navigate to Configuration, select Templates, and then select Device Templates.

Click Create Template, select From Feature Template, and then select the device model.

Select Device, select Service Node, and then set Template Name and Description.

Attach the device template to the device.

Step 1 = Navigate to Configuration, select Templates, and then select Device Templates.

Step 2 = Click Create Template, select From Feature Template, and then select the device model.

Step 3 = Select Device, select Service Node, and then set Template Name and Description.

Step 4 = Attach the device template to the device.

The process of configuring an AppGoE service node for WAN optimization for applications that are hosted in the cloud using Cisco vManage for C8000V or C8500L-8S4X devices involves several steps.

Navigate to Configuration, select Templates, and then select Device Templates:

This is the first step where you navigate to the Templates section in the Configuration menu of Cisco vManage.

Click Create Template, select From Feature Template, and then select the device model: In this step, you create a new template for the device model from the feature template.

Select Device, select Service Node, and then set Template Name and Description:

After setting up the template, you select the device and the service node, and then set the template name and description.

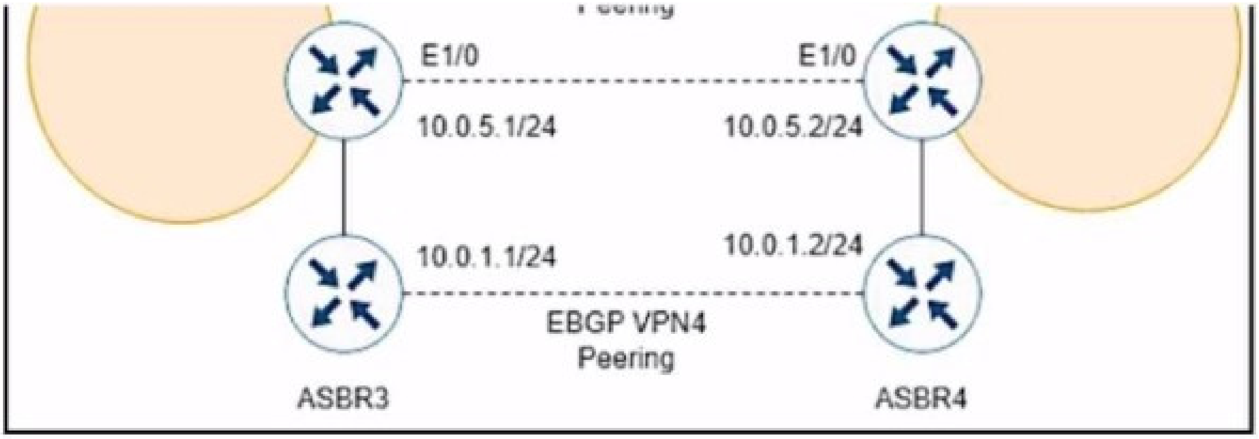
Attach the device template to the device: Finally, you attach the created device template to the device.

References:

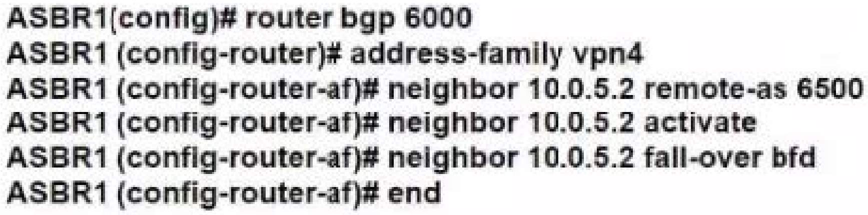
AppQoE - Step-by-Step Configuration - Cisco Community Cisco Catalyst SD-WAN AppQoE Configuration Guide, Cisco IOS XE Catalyst SD- WAN Release 17.x

QUESTION 4

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 5

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

300-440 PDF Dumps 300-440 Study Guide 300-440 Braindumps