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

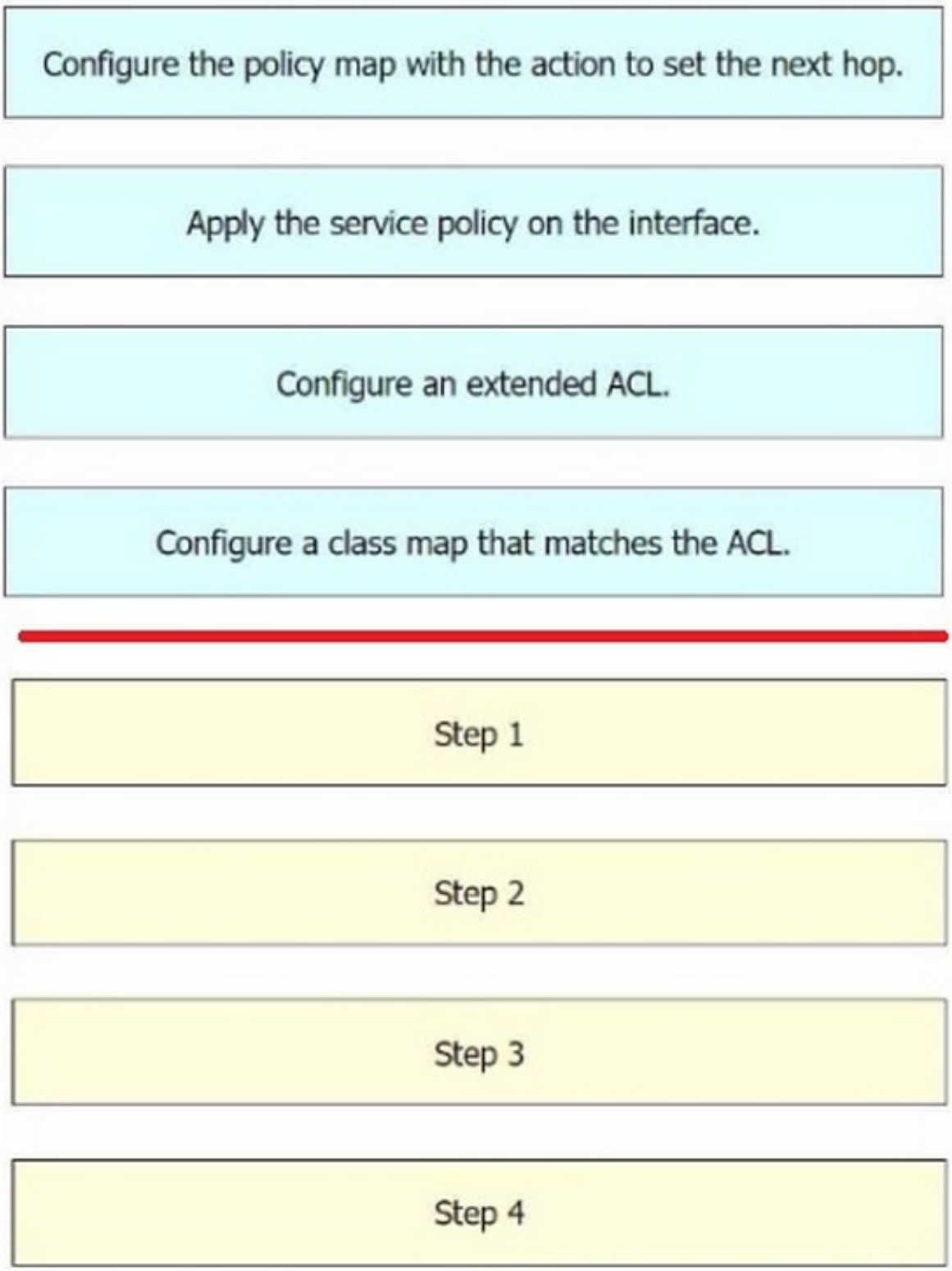
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

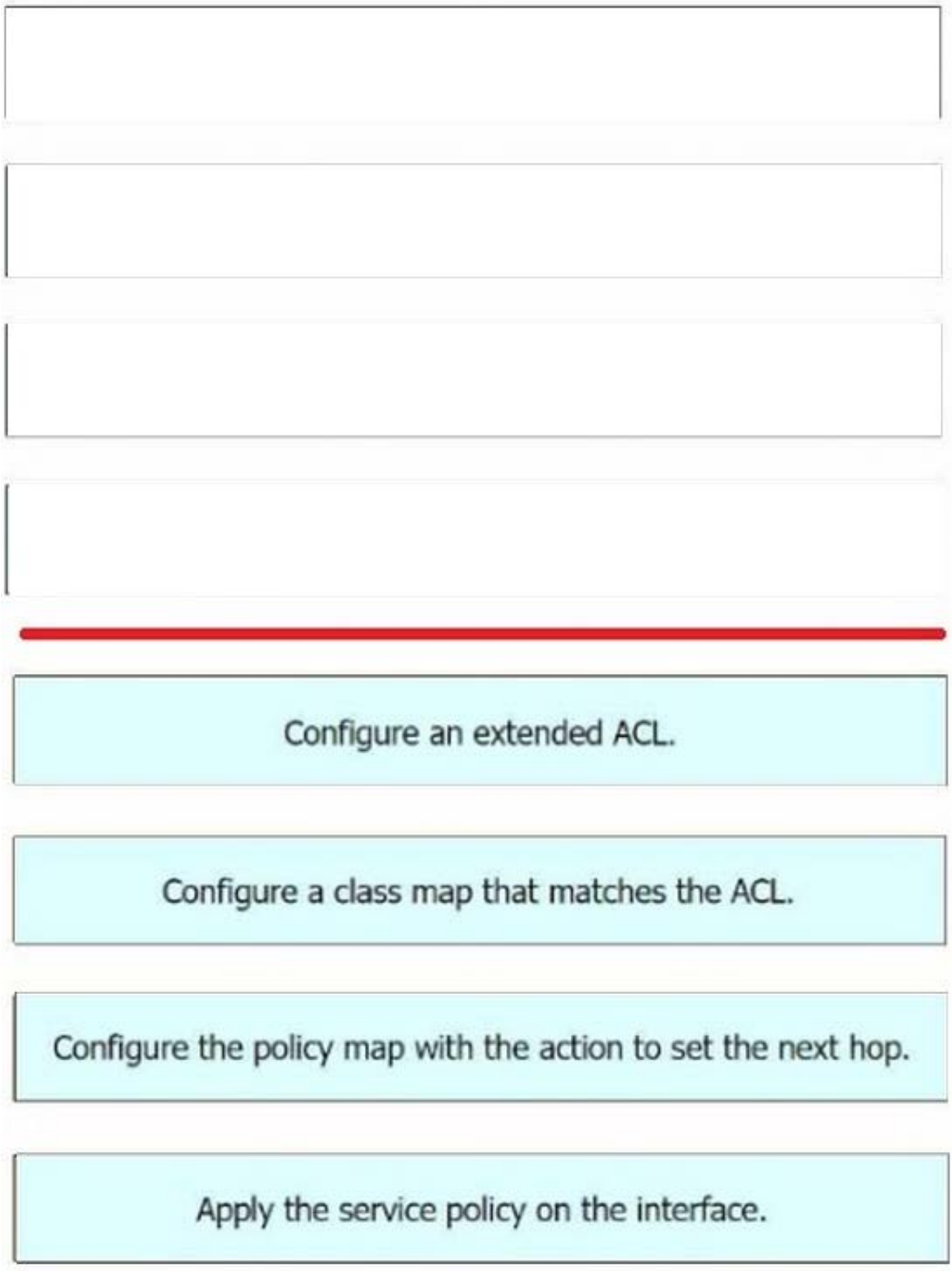
DRAG DROP

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:



Correct Answer:



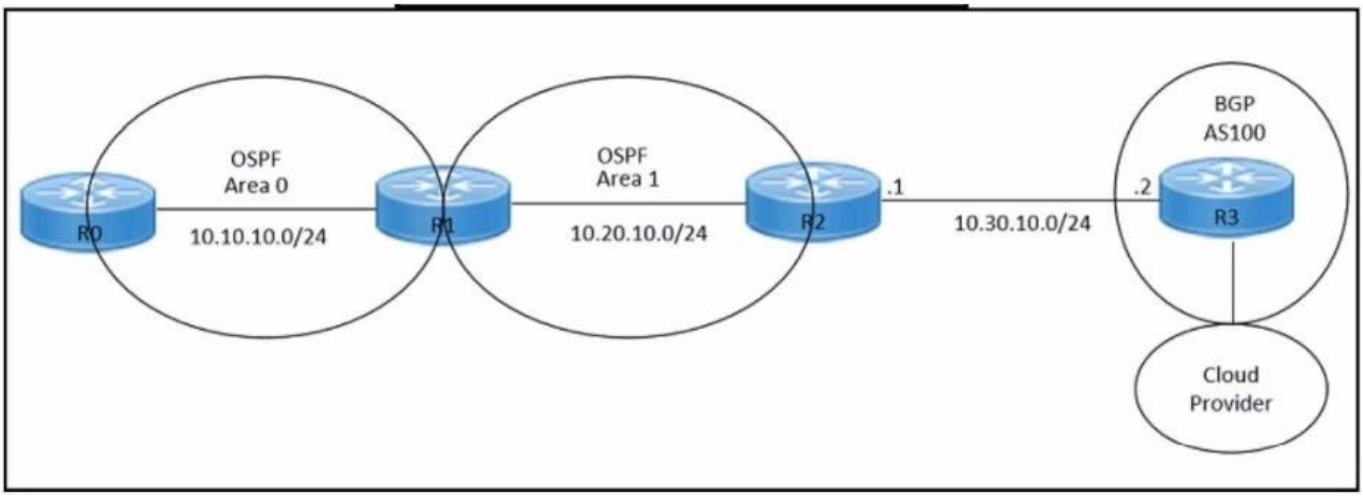
Enhanced Policy-Based Routing (ePBR) is used to direct packets that arrive at an interface to a specified next-hop. It is very useful in managing a large number of configured access lists more efficiently. In ePBR, the router drops the traffic packets if the next hop configured in the PBR policy is not 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 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. Which two commands should the engineer run on router R2? (Choose two.)

A. router bgp 100

B. redistribute bgp 100

C. router ospf 1

D. redistribute ospf 1

E. redistribute ospf 100

Correct Answer: AD

QUESTION 3

Which method is used to create authorization boundary diagrams (ABDs)?

A. identify only interconnected systems that are FedRAMP-authorized

B. show all networks in CIDR notation only

C. identify all tools as either external or internal to the boundary

D. show only minor or small upgrade level software components

Correct Answer: C

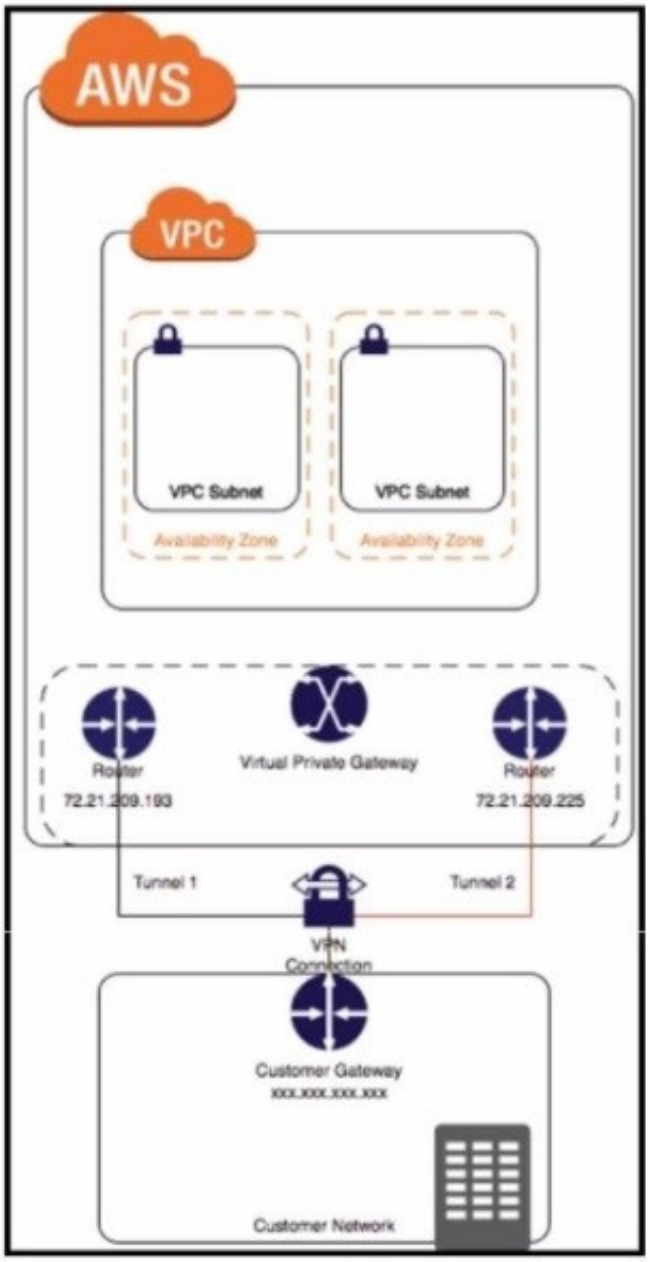
According to the FedRAMP Authorization Boundary Guidance document, the method used to create authorization boundary diagrams (ABDs) is to identify all tools as either external orinternal to the boundary. The ABD is a visual representation of the components that make up the authorization boundary, which includes all technologies, external and internal services, and leveraged systems and accounts for all federal information, data, and metadata that a Cloud Service Offering (CSO) is responsible for. The ABD should illustrate a CSP\\'s scope of control over the system and show components or services that are leveraged from external services or controlled by the customer. The other options are incorrect because they do not capture the full scope and details of the authorization boundary as required by FedRAMP.

References: FedRAMP Authorization Boundary Guidance document

QUESTION 4

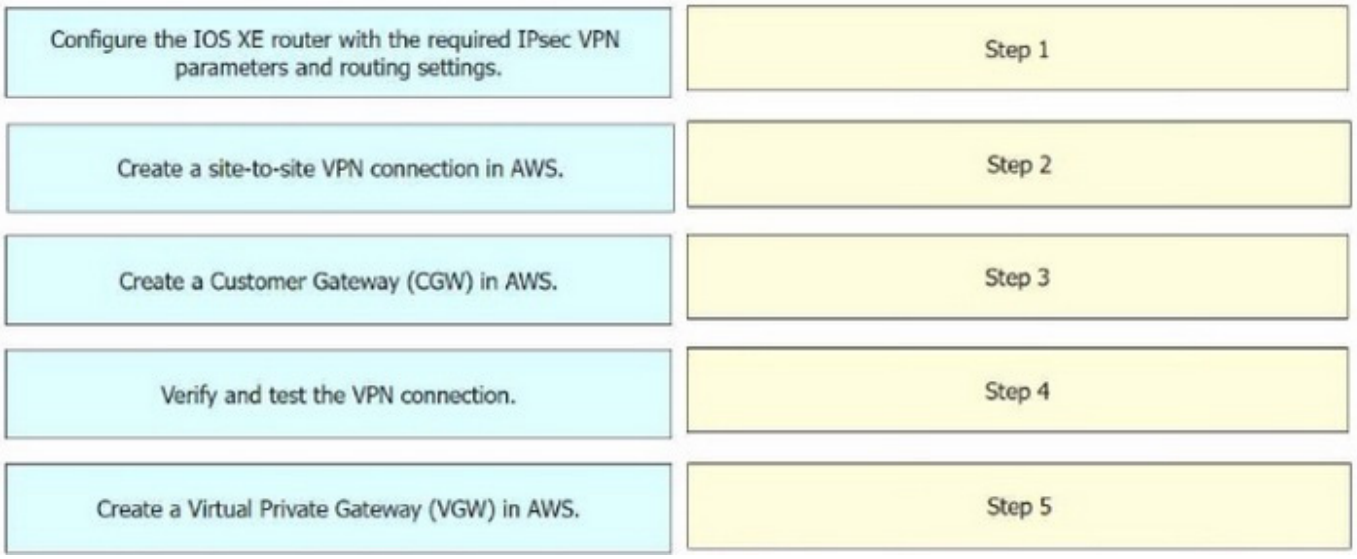
DRAG DROP

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.

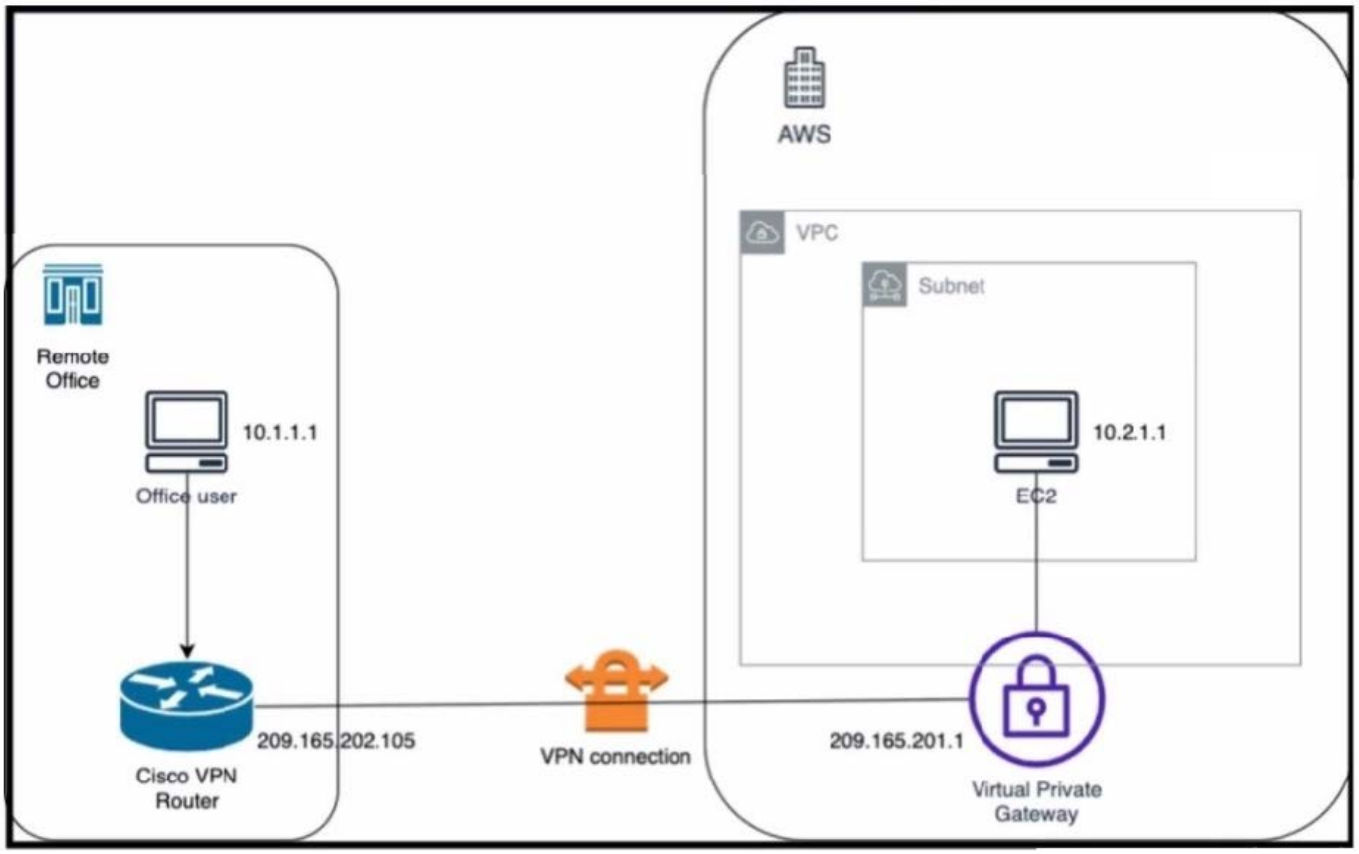
References:

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 5

Refer to the exhibit.



An engineer successfully brings up the site-to-site VPN tunnel between the remote office and the AWS virtual private gateway, and the site-to-site routing works correctly. However, the end-to-end ping between the office user PC and the AWS EC2 instance is not working.

Which two actions diagnose the loss of connectivity? (Choose two.)

A. Check the network security group rules on the host VNET.

B. Check the security group rules for the host VPC.

C. Check the IPsec SA counters.

D. On the Cisco VPN router, configure the IPsec SA to allow ping packets.

E. On the AWS private virtual gateway, configure the IPsec SA to allow ping packets.

Correct Answer: BC

The end-to-end ping between the office user PC and the AWS EC2 instance is not working because either the security group rules for the host VPC are blocking the ICMP traffic or the IPsec SA counters are showing errors or drops. To

diagnose the loss of connectivity, the engineer should check both the security group rules and the IPsec SA counters. The network security group rules on the host VNET are not relevant because they apply to Azure, not AWS. The IPsec SA

configuration on the Cisco VPN router and the AWS private virtual gateway are not likely to be the cause of the problem because the site- to-site VPN tunnel is already up and the site-to-site routing works correctly.

References:

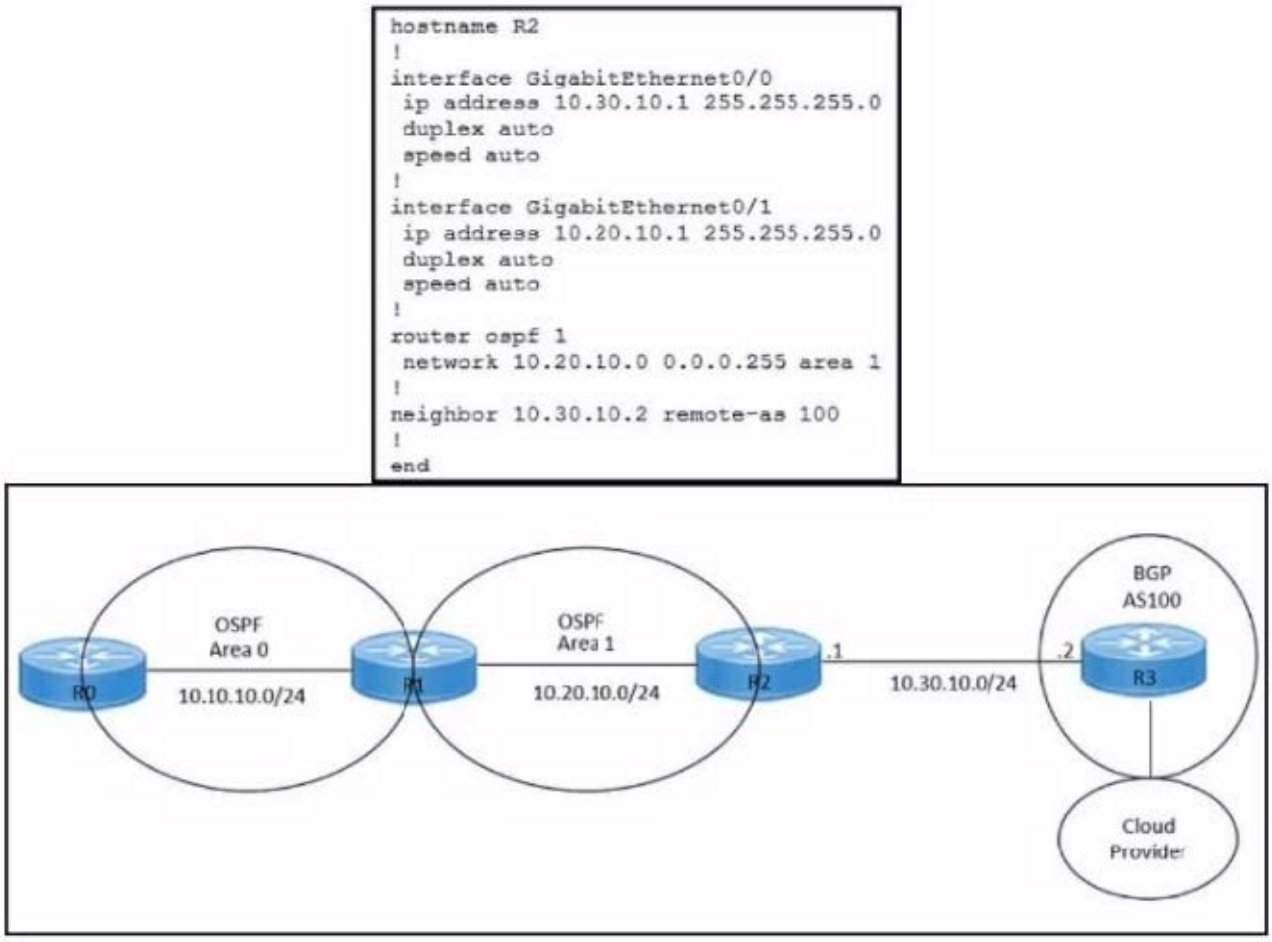
Designing and Implementing Cloud Connectivity (ENCC, Track 1 of 5), Module 3:

Configuring IPsec VPN from Cisco IOS XE to AWS, Lesson 3: Verify IPsec VPN Connectivity

Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter: IPsec VPN Overview, Section: IPsec Security Association AWS Documentation, User Guide for AWS VPN, Section: Security Groups for Your VPC

QUESTION 6

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 7

What is the role of service providers to establish private connectivity between on-premises networks and Google Cloud resources?

A. facilitate direct, dedicated network connections through Google Cloud Interconnect

B. enable intelligent routing and dynamic path selection using software-defined networking

C. provide end-to-end encryption for data transmission using native IPsec

D. accelerate content delivery through integration with Google Cloud CDN

Correct Answer: A

The role of service providers to establish private connectivity between on- premises networks and Google Cloud resources is to facilitate direct, dedicated network connections through Google Cloud Interconnect. Google Cloud Interconnect is

a service that allows customers to connect their on-premises networks to Google Cloud through a service provider partner. This provides low latency, high bandwidth, and secure connectivity to Google Cloud services, such as Google

Compute Engine, Google Cloud Storage, and Google BigQuery. Google Cloud Interconnect also supports hybrid cloud scenarios, such as extending on-premises networks to Google Cloud regions, or connecting multiple Google Cloud

regions together. Google Cloud Interconnect offers two types of connections: Dedicated Interconnect and Partner Interconnect. Dedicated Interconnect provides physical connections between the customer\\'s network and Google\\'s network at

a Google Cloud Interconnect location. Partner Interconnect provides virtual connections between the customer\\'s network and Google\\'s network through a supported service provider partner. Both types of connections use VLAN attachments

to establish private connectivity to Google Cloud Virtual Private Cloud (VPC) networks.

References:

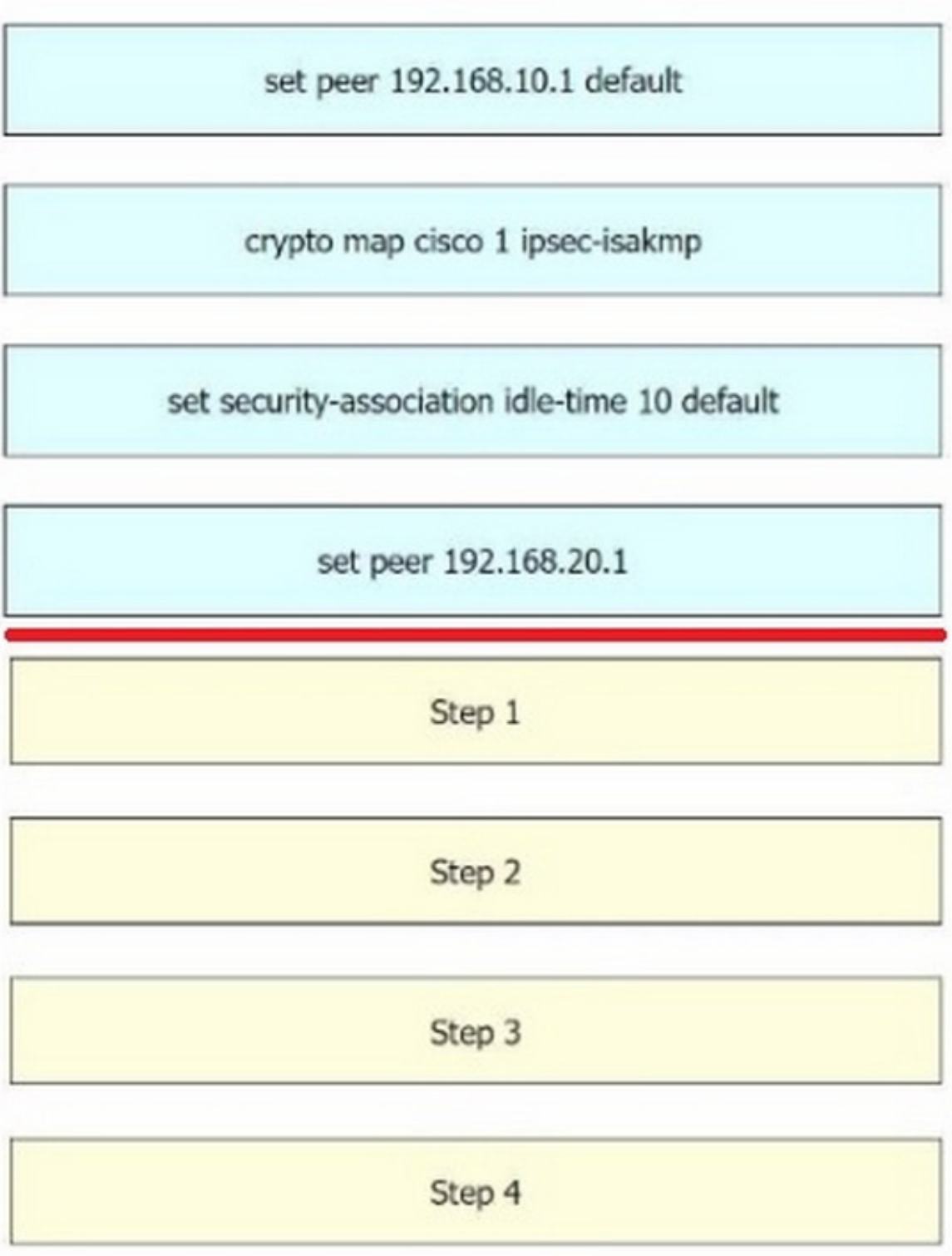
Designing and Implementing Cloud Connectivity (ENCC) v1.0 [Google Cloud Interconnect Overview] [Google Cloud Interconnect Documentation]

QUESTION 8

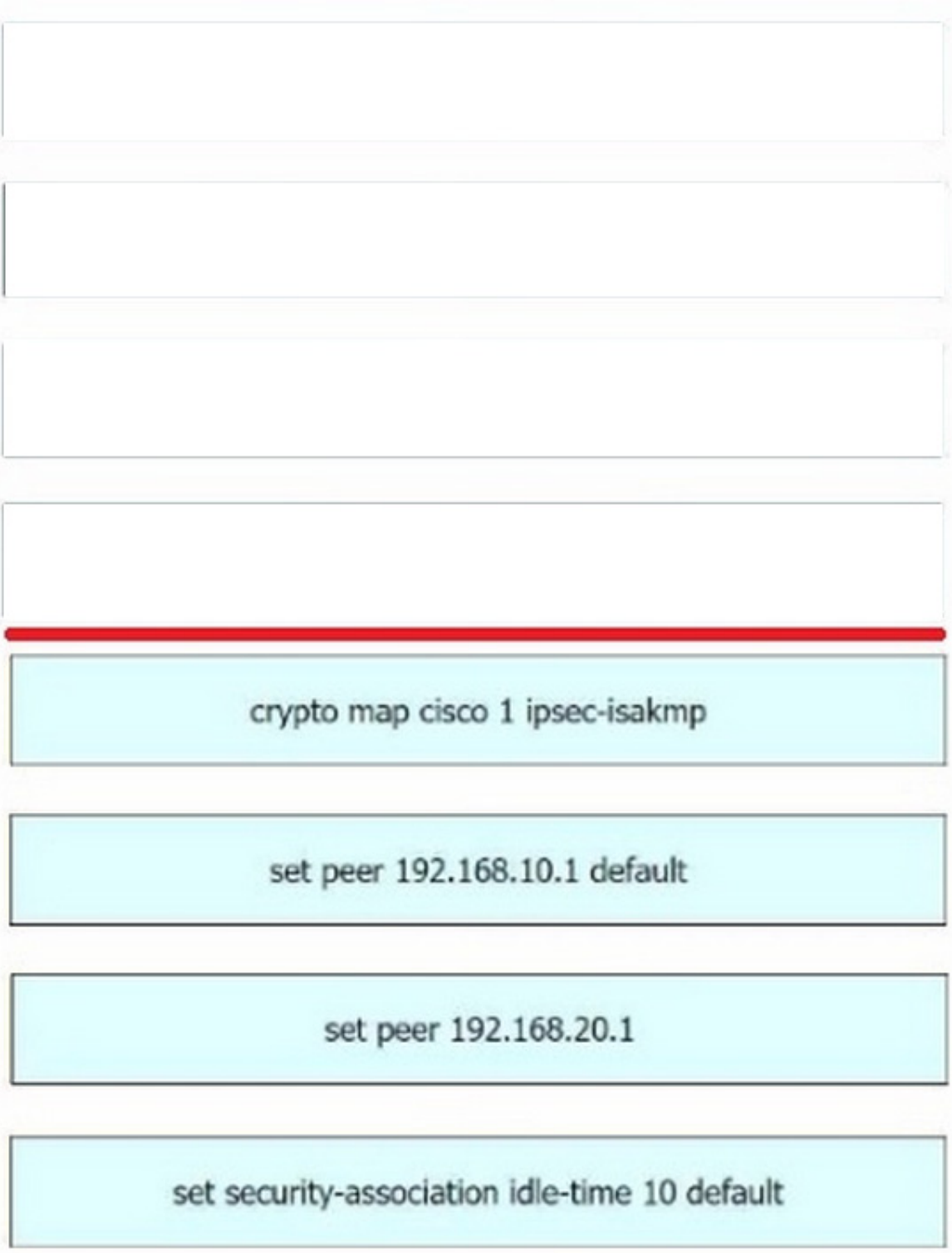
DRAG DROP

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.

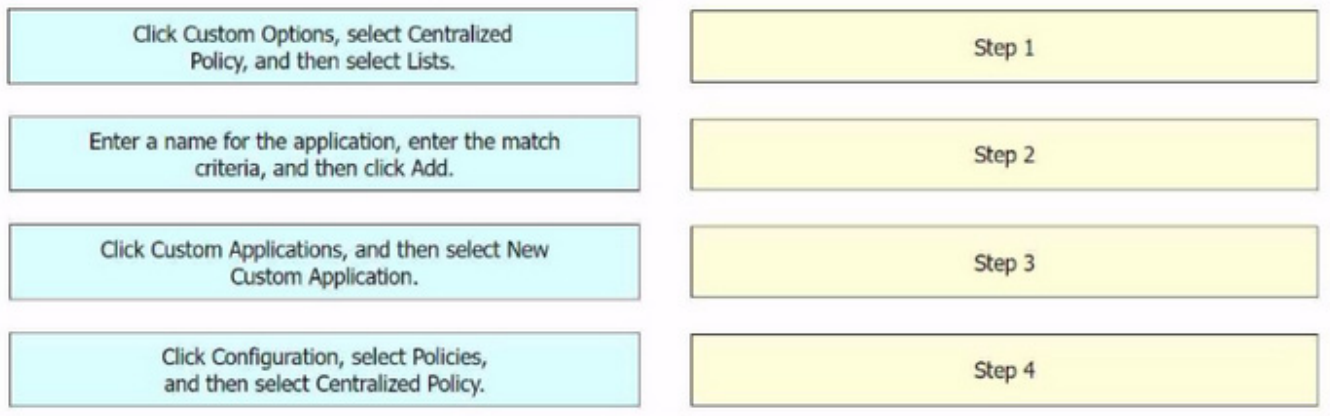
References: Configure a Site-to-Site IPSec IKEv1 Tunnel Between an ASA and a Cisco IOS Router - Cisco Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services - Cisco Community Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers Configure Failover for IPSec Site-to-Site Tunnels 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

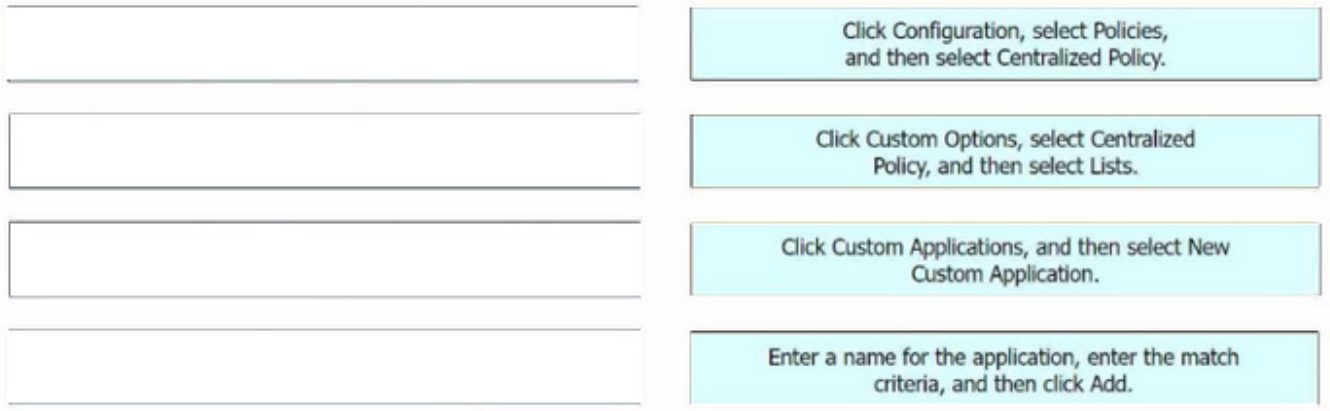
DRAG DROP

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:



Correct Answer:



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.

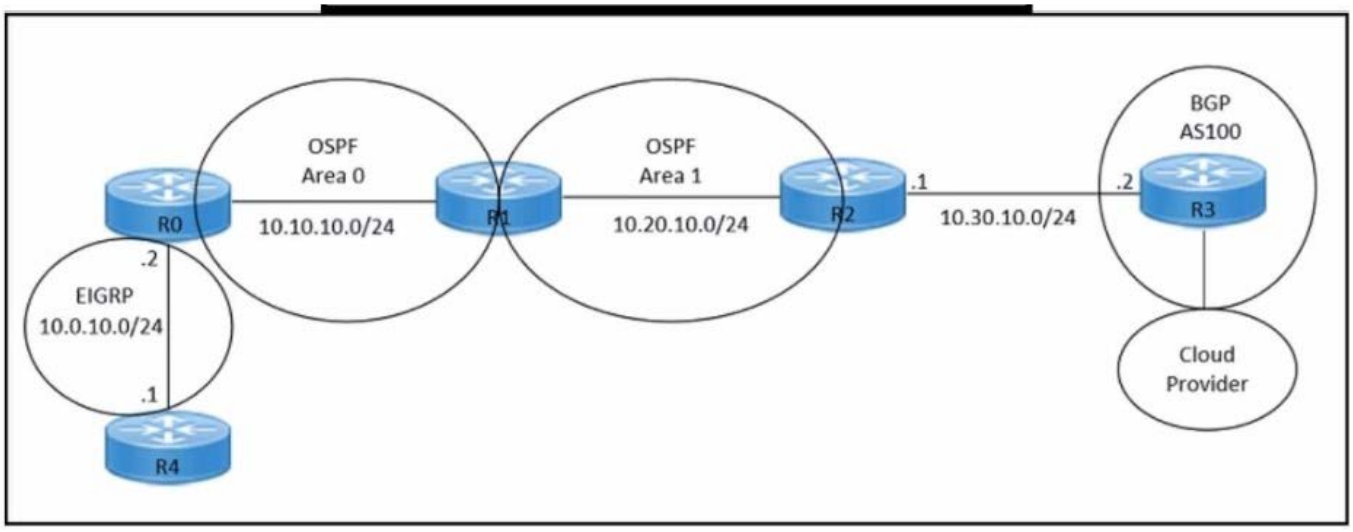
References:

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

QUESTION 10

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
!
router bgp 100
 neighbor 10.30.10.2 remote-as 100
 redistribute ospf 1
!
```



An engineer must redistribute only the 10.0.10.0/24 network into BGP to connect an on-premises network to a public cloud provider. These routes are currently redistributed:

```
*10.10.10.0/24
*10.20.10.0/24
```

Which command is missing on router R2?

A. neighbor 10.0.10.2 remote-as 100

B. redistribute ospf 1 match internal

C. redistribute ospf 1 match external

D. neighbor 10.0.10.0/24 remote-as 100

Correct Answer: C

The command redistribute ospf 1 match external is missing on router R2. This command is needed to redistribute only the external OSPF routes into BGP. The external OSPF routes are those that are learned from another routing protocol or

redistributed into OSPF. In this case, the 10.0.10.0/24 network is an external OSPF route, as it is redistributed from EIGRP into OSPF on router R1. The other commands are either already present or not relevant for this scenario.

References:

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

Implementing Cloud Connectivity, Lesson 3.1: Implementing IPsec VPN from Cisco IOS XE to AWS, Topic 3.1.2: Configure BGP on the Cisco IOS XE Router Security for VPNs with IPsec Configuration Guide, Cisco IOS XE, Chapter:

Configuring IPsec VPNs with Dynamic Routing Protocols, Section: Configuring BGP over IPsec VPNs