300-440$^{\text{Q\&As}}$

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 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.

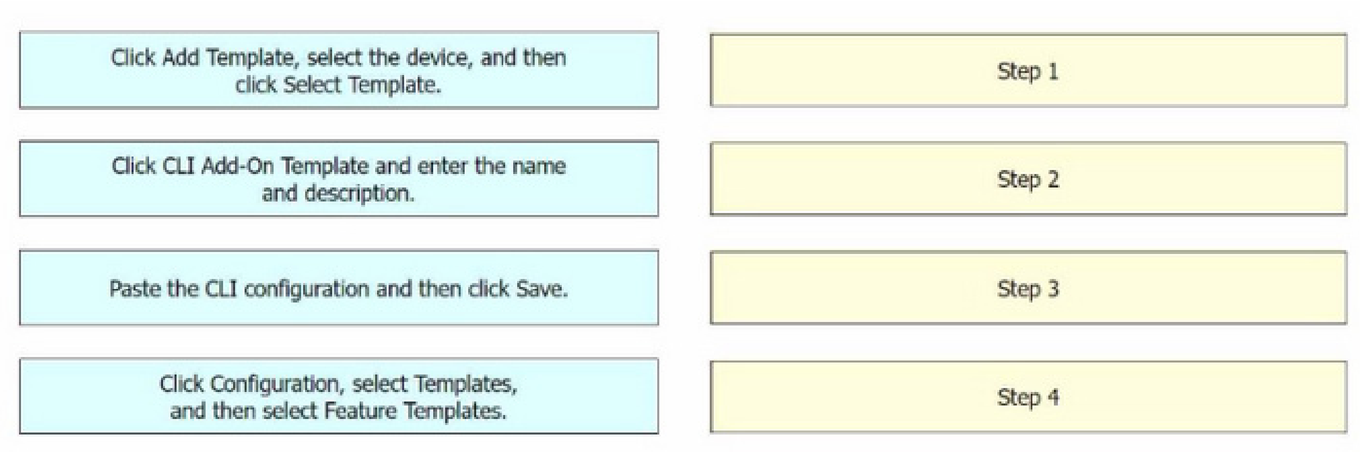
licensing config privacy version false

4.

licensing config utility utility-enable true

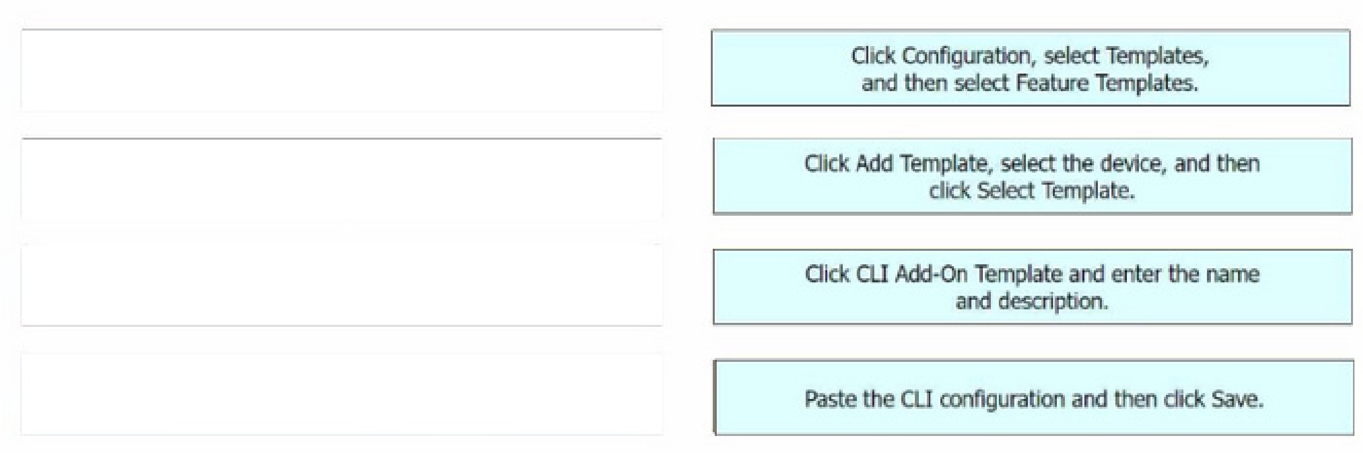
Drag and drop the steps from the left onto the order on the right to complete the configuration.

Select and Place:



Click Add Template, select the device, and then click Select Template.	Step 1
Click CLI Add-On Template and enter the name and description.	Step 2
Paste the CLI configuration and then click Save.	Step 3
Click Configuration, select Templates, and then select Feature Templates.	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:

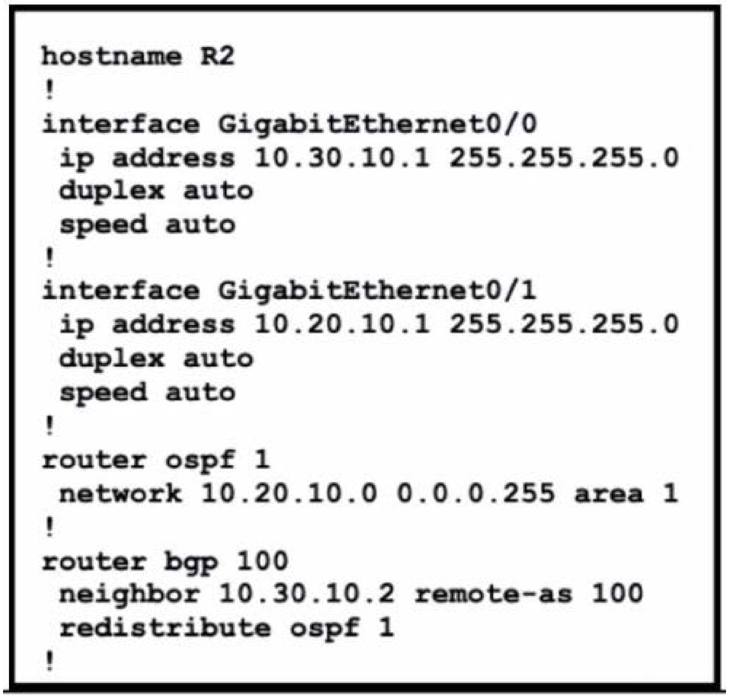
CLI Add-On Feature Templates - Cisco

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

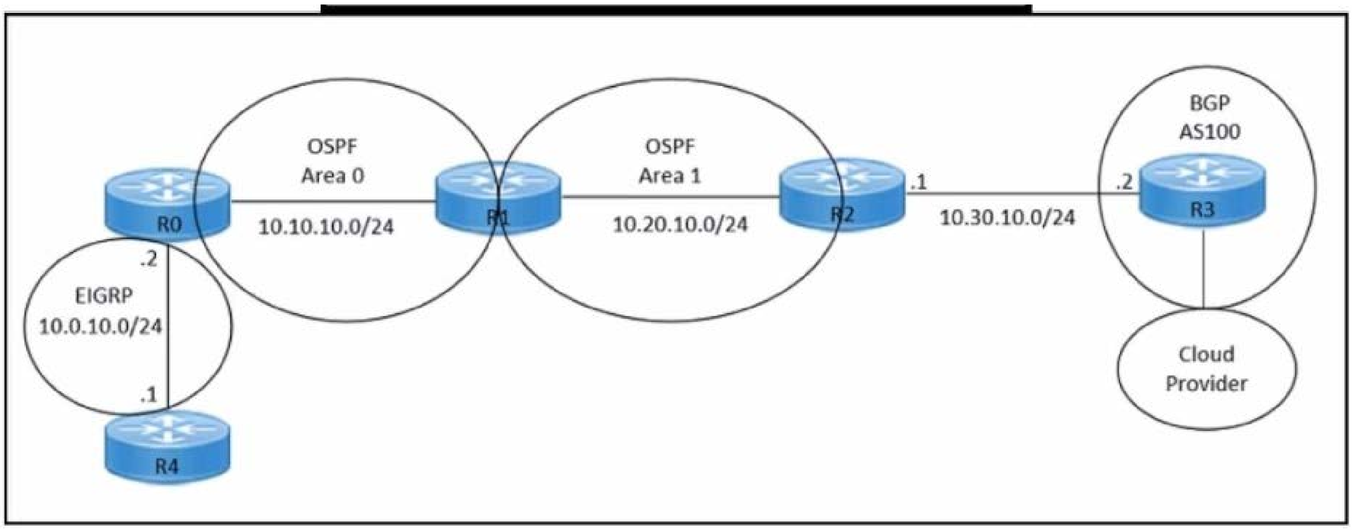
SD-WAN Routers

QUESTION 2

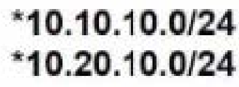
Refer to the exhibits.



```
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
!
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:

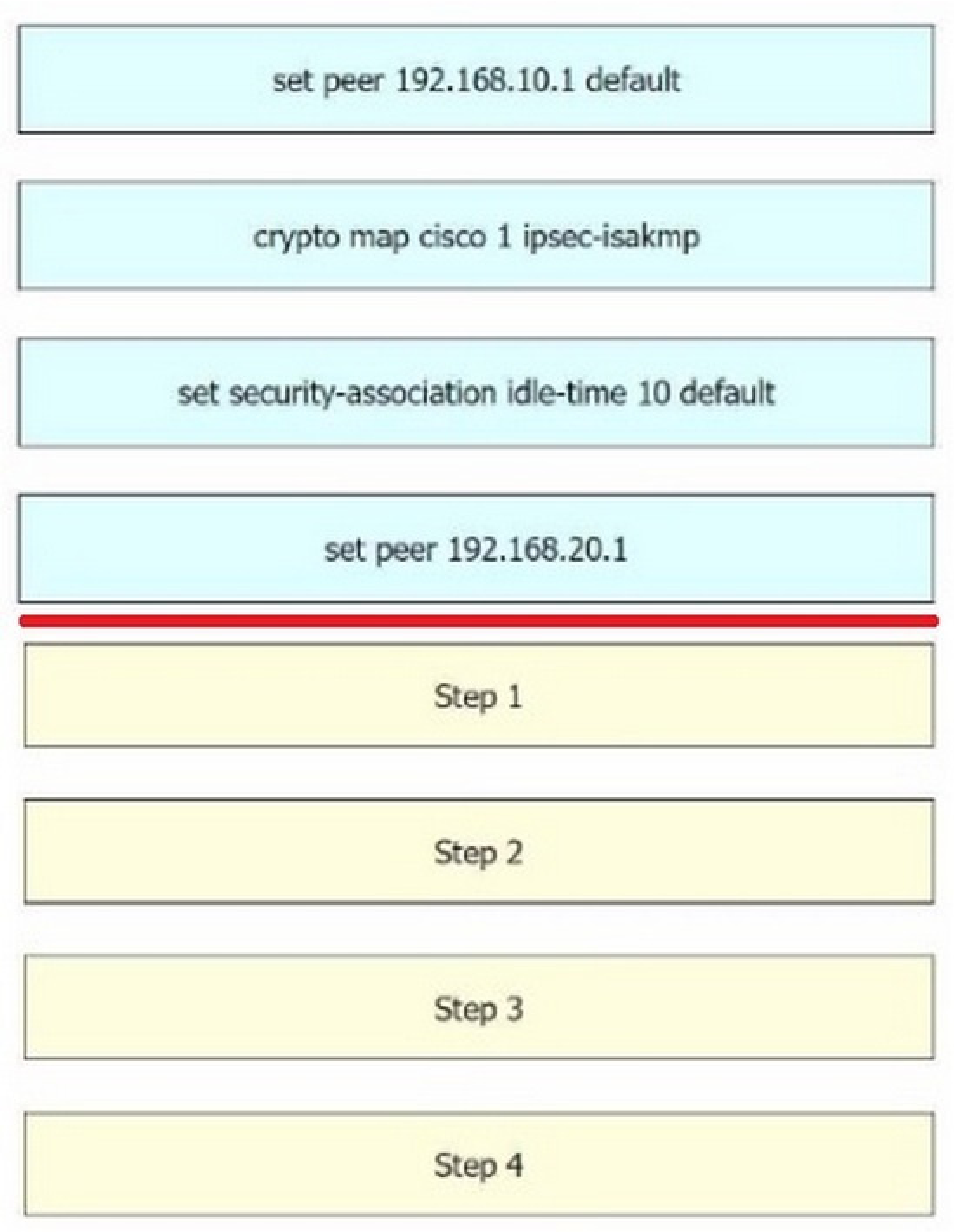
Configuring IPsec VPNs with Dynamic Routing Protocols, Section: Configuring BGP over IPsec VPNs

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

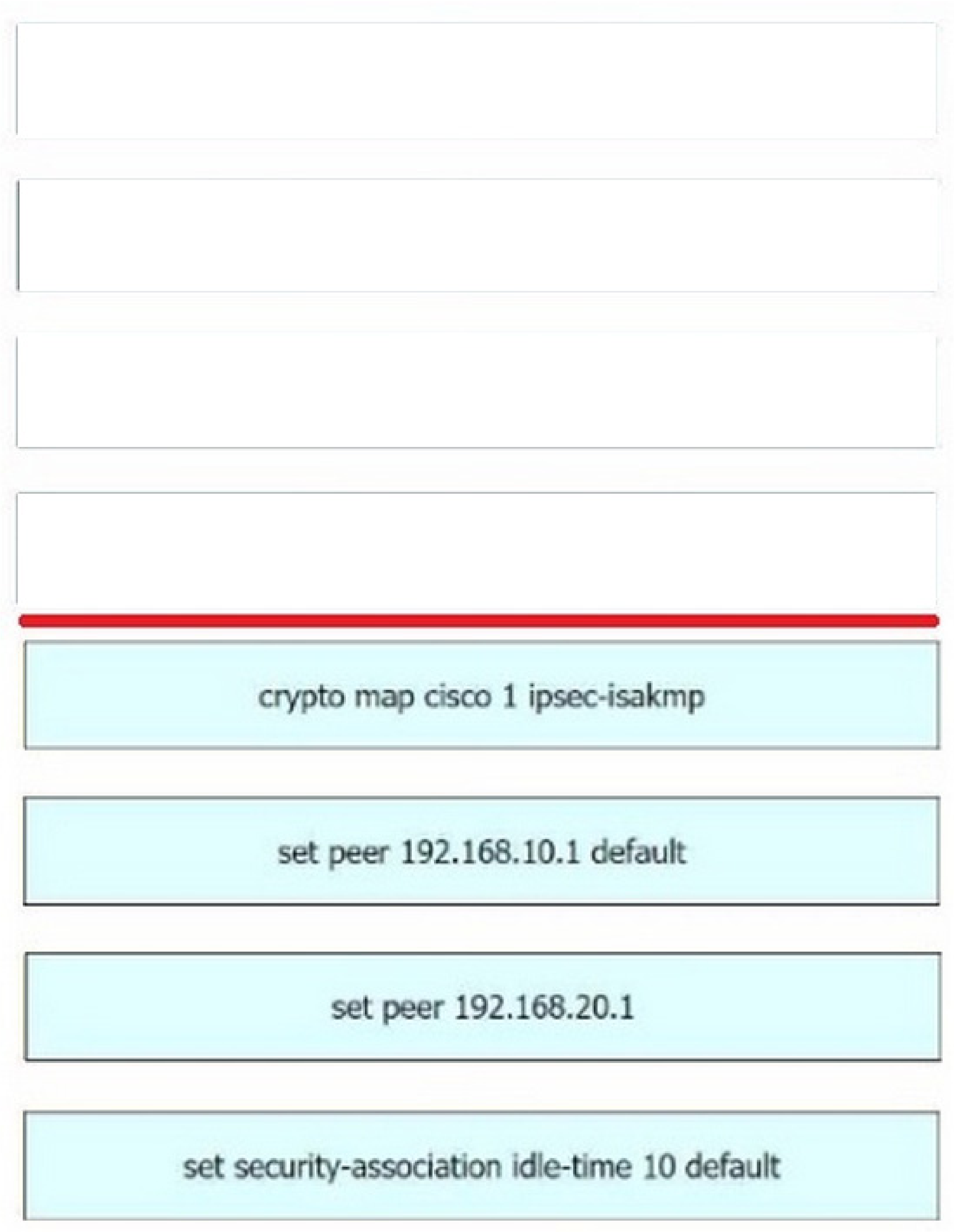
Step 1

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

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 5

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

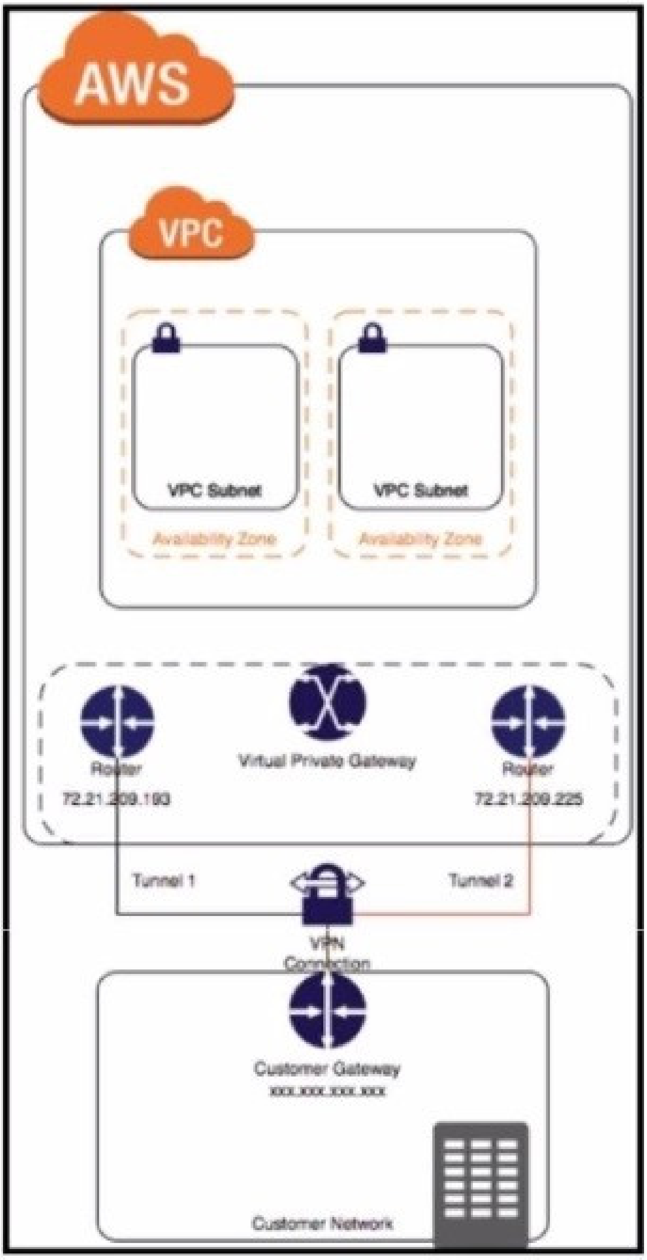
According to the FedRAMP Authorization Boundary Guidance document, the method used to create authorization boundary diagrams (ABDs) is to identify all tools as either external orinternal to the boundary. The ABD is a visual representation of the components that make up the authorization boundary, which 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 6

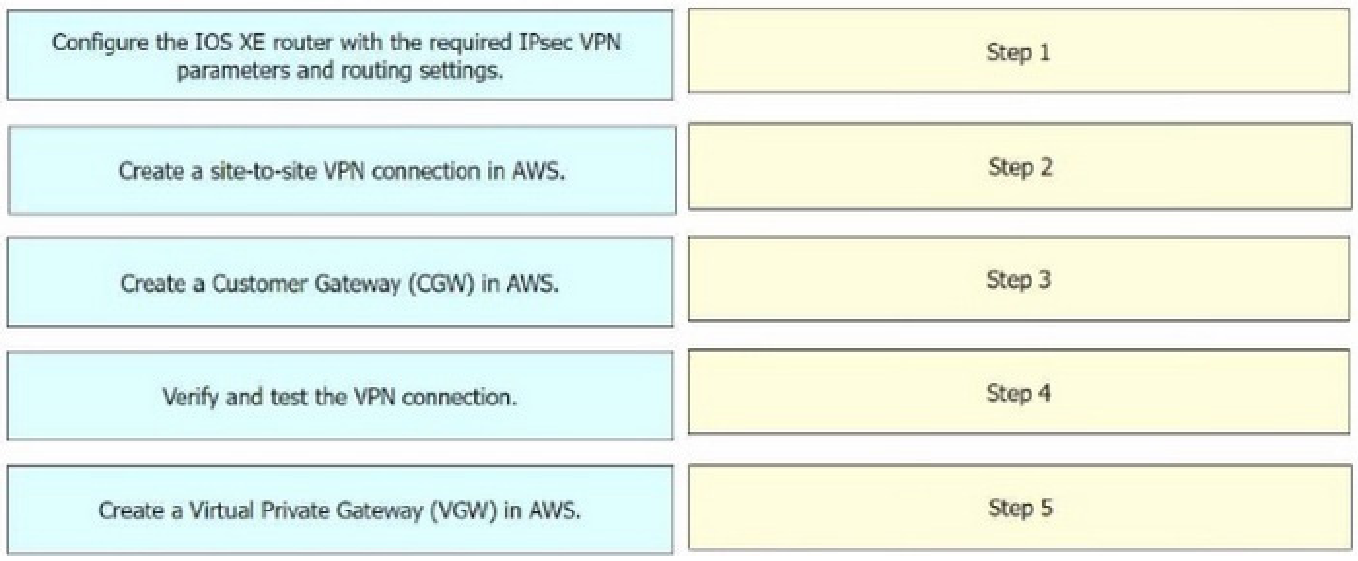
DRAG DROP

Refer to the exhibit.



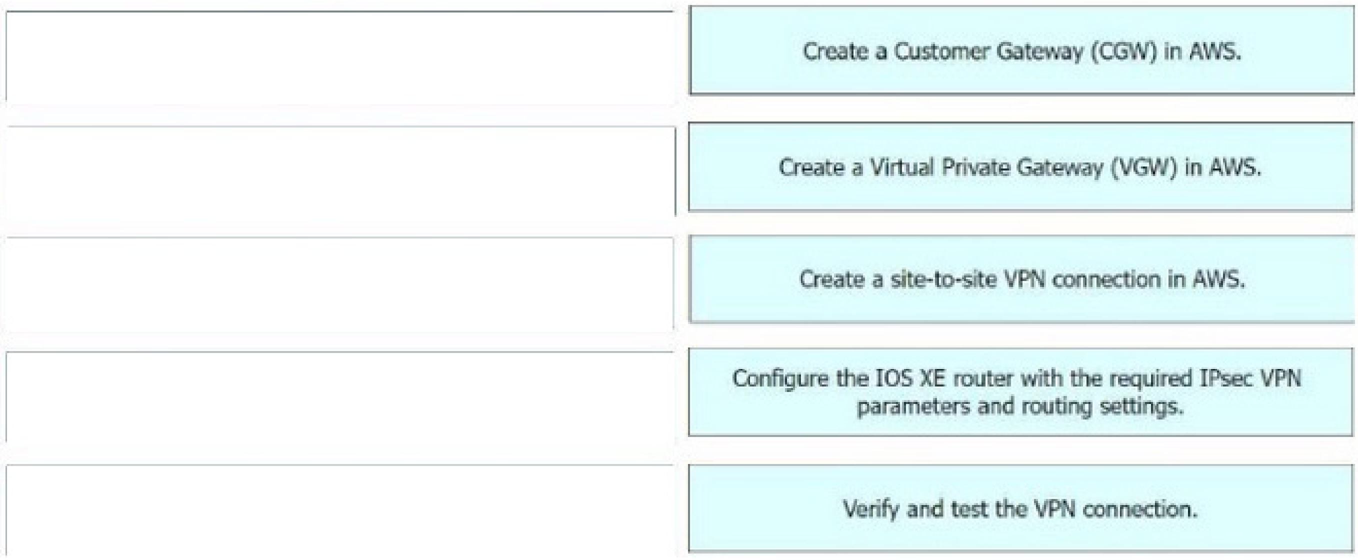
Drag and drop the steps from the left onto the order on the right to configure a site-to-site VPN connection between an on-premises Cisco IOS XE router and Amazon Web Services (AWS).

Select and Place:



Configure the IOS XE router with the required IPsec VPN parameters and routing settings.	Step 1
Create a site-to-site VPN connection in AWS.	Step 2
Create a Customer Gateway (CGW) in AWS.	Step 3
Verify and test the VPN connection.	Step 4
Create a Virtual Private Gateway (VGW) in AWS.	Step 5

Correct Answer:



	Create a Customer Gateway (CGW) in AWS.
	Create a Virtual Private Gateway (VGW) in AWS.
	Create a site-to-site VPN connection in AWS.
	Configure the IOS XE router with the required IPsec VPN parameters and routing settings.
	Verify and test the VPN connection.

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.

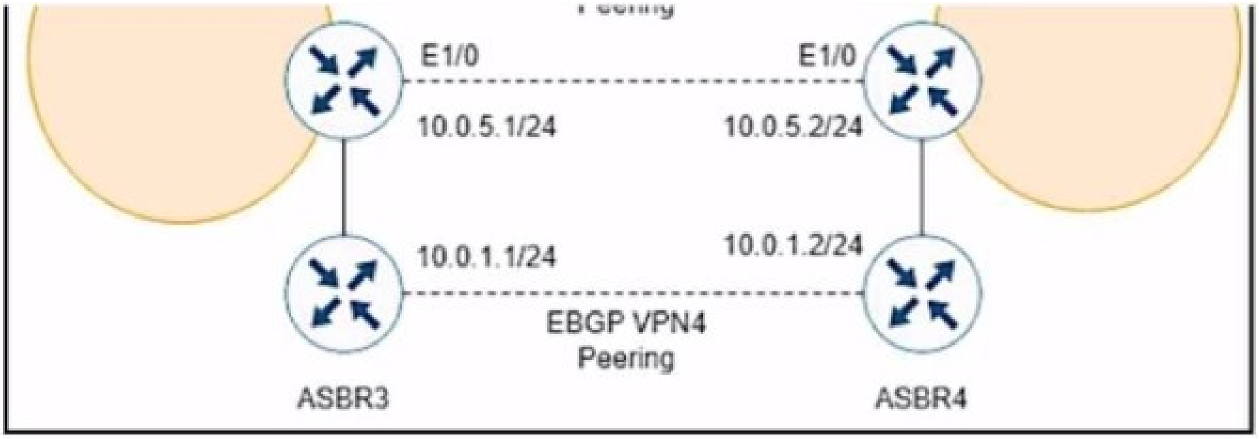
References:

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

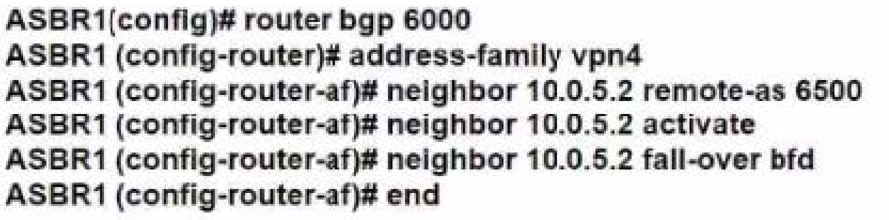
SD-WAN Configuration Example: Site-to-site (LAN to LAN) IPSec between vEdge and Cisco IOS - Cisco Community

QUESTION 7

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 8

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

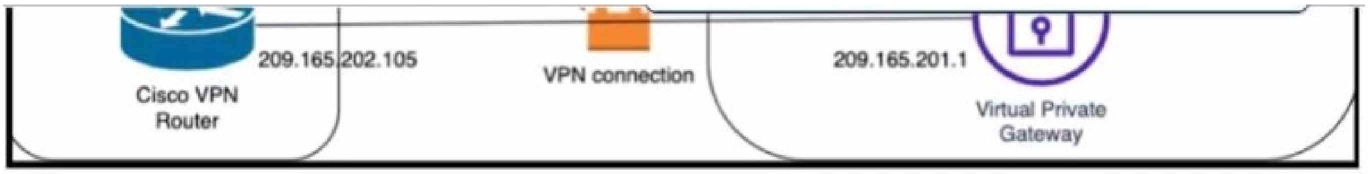
to establish private connectivity to Google Cloud Virtual Private Cloud (VPC) networks.

References:

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

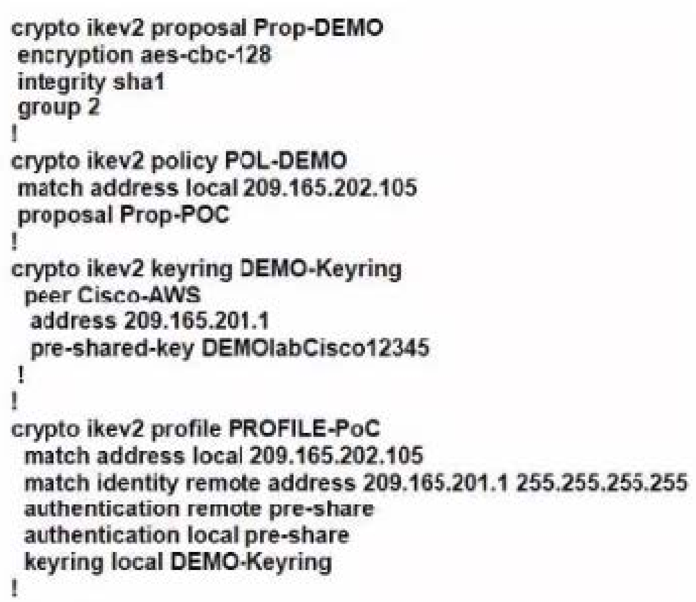
QUESTION 9

Refer to the exhibit.



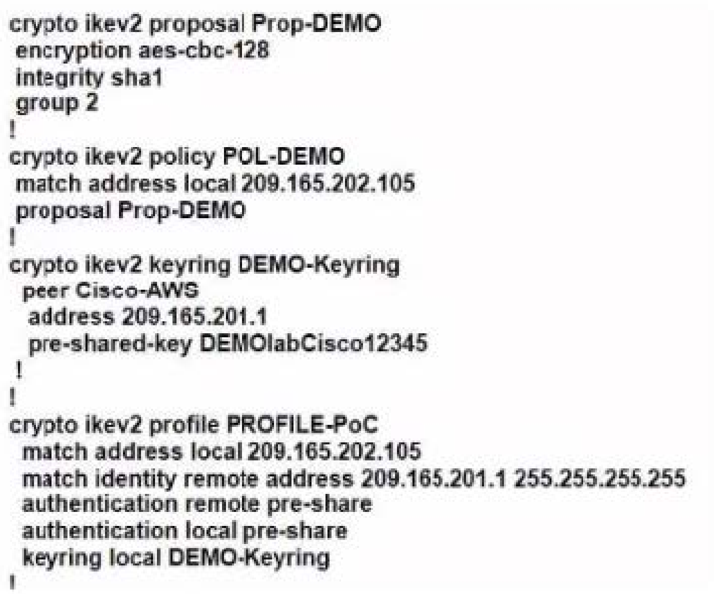
Which Cisco IKEv2 configuration brings up the IPsec tunnel between the remote office router and the AWS virtual private gateway?

A.



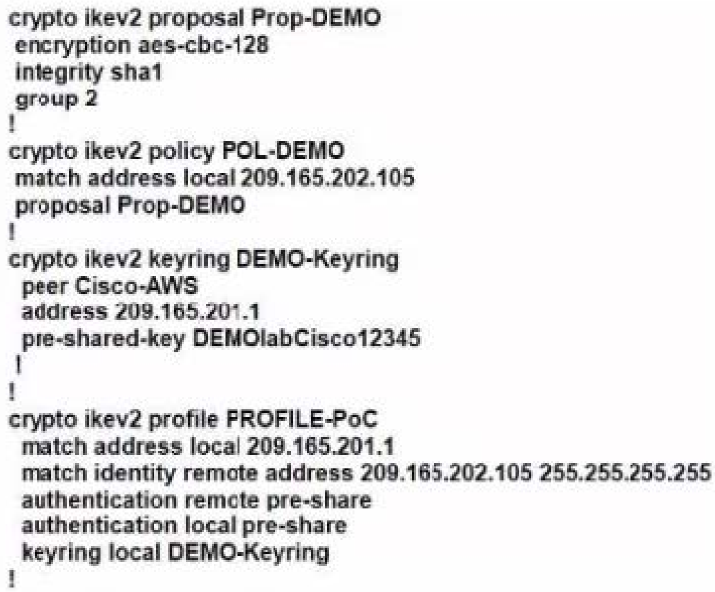
```
crypto ikev2 proposal Prop-DEMO
 encryption aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy POL-DEMO
 match address local 209.165.202.105
 proposal Prop-POC
!
crypto ikev2 keyring DEMO-Keyring
  peer Cisco-AWS
   address 209.165.201.1
   pre-shared-key DEMOlabCisco12345
  !
!
crypto ikev2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

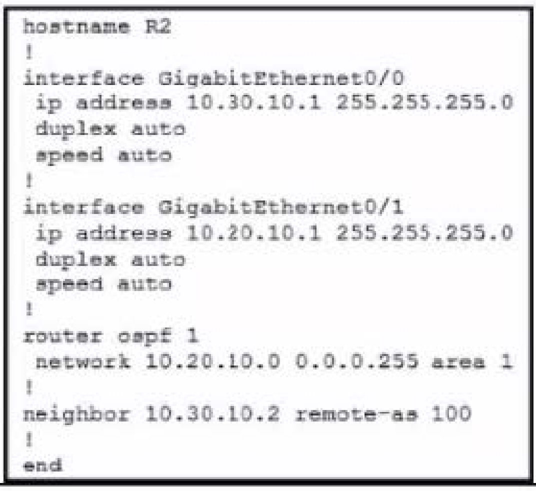
References:

1: AWS VPN Configuration Guide for Cisco IOS-XE

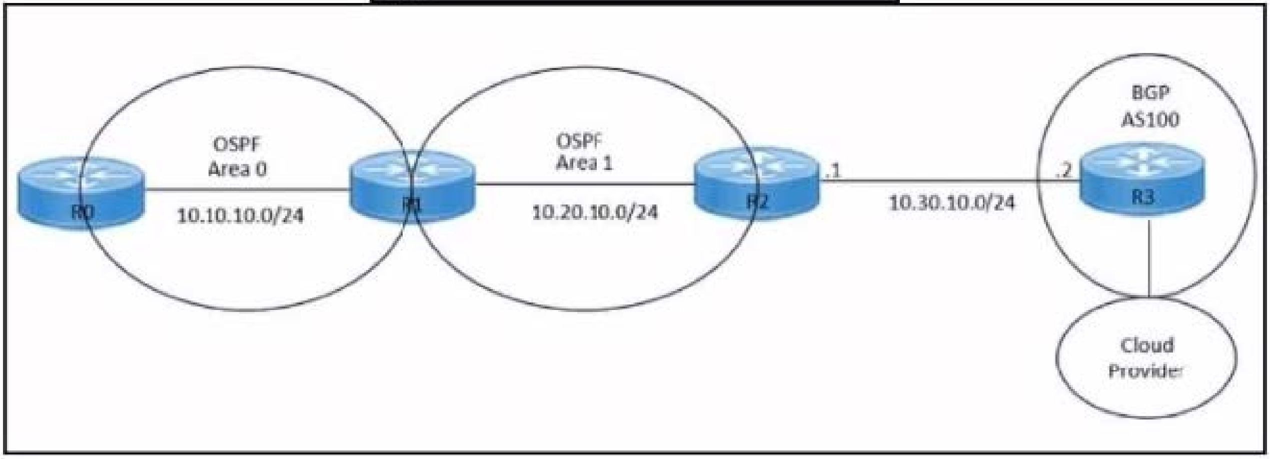
2: Configure IOS-XE Site-to-Site VPN Connection to Amazon Web Services

QUESTION 10

Refer to the exhibit.



```
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 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-lnternal

Correct Answer: B

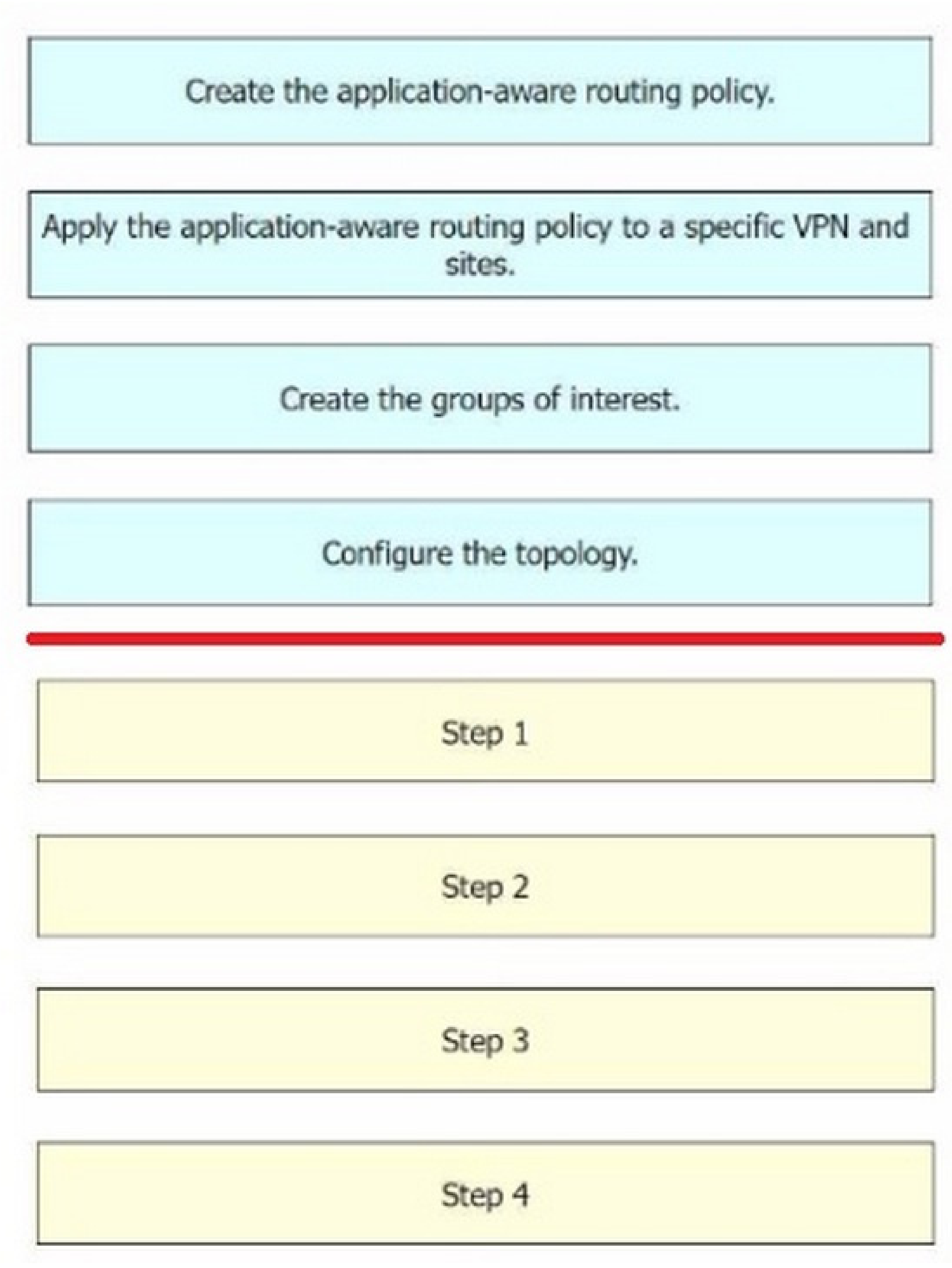
References: Learning Plan: Designing and Implementing Cloud Connectivity v1.0 (ENCC 300-440) Exam Prep Designing and Implementing Cloud Connectivity (ENCC) v1.0 Cisco Multiprotocol Label Switching Exploring Cisco Cloud OnRamp for Colocation ENCC: Configuring IPsec VPN from Cisco IOS XE to AWS : [Deploying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

QUESTION 11

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:



Create the application-aware routing policy.

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

Create the groups of interest.

Configure the topology.

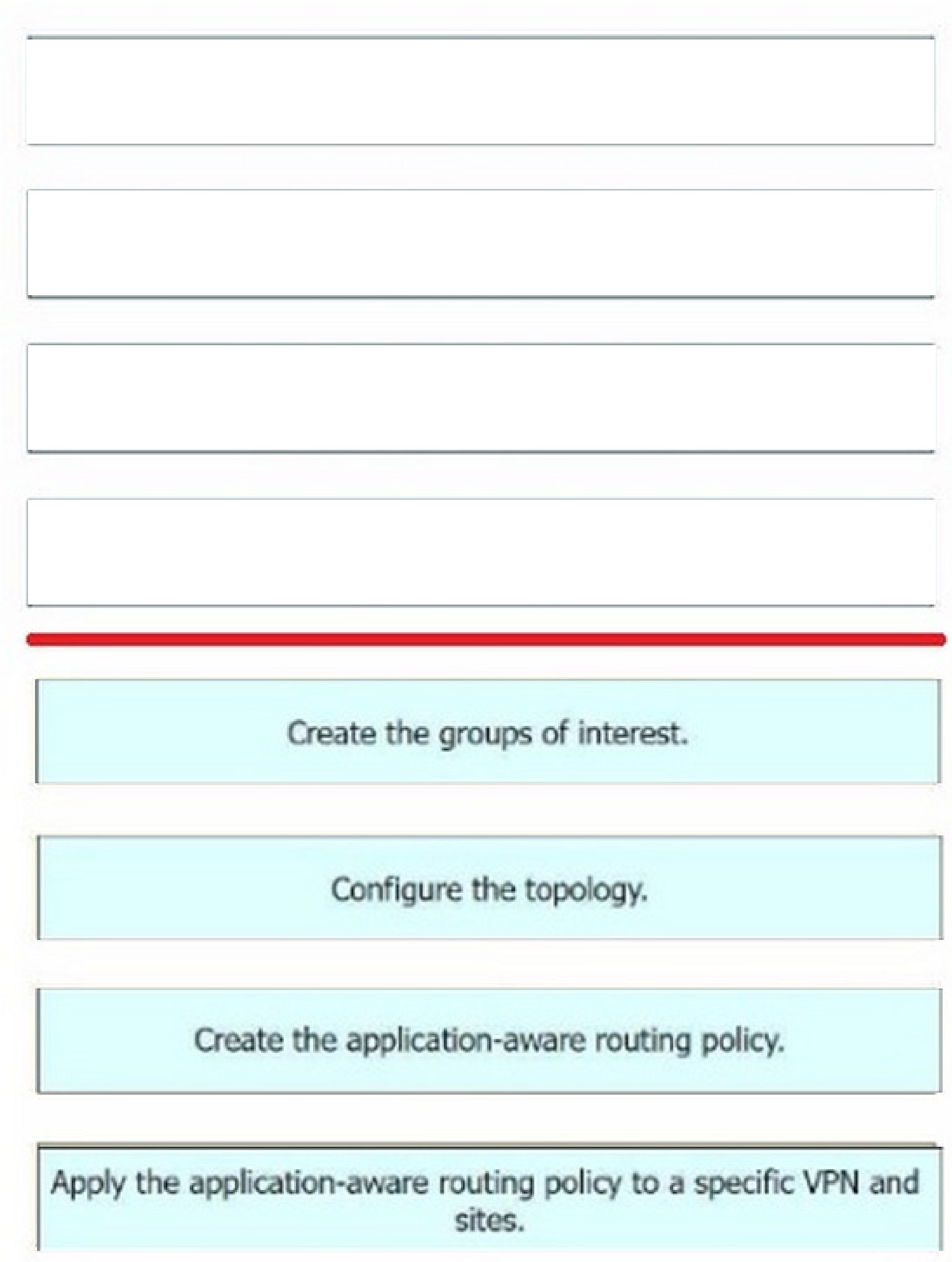
Step 1

Step 2

Step 3

Step 4

Correct Answer:



Create the groups of interest.

Configure the topology.

Create the application-aware routing policy.

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

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.

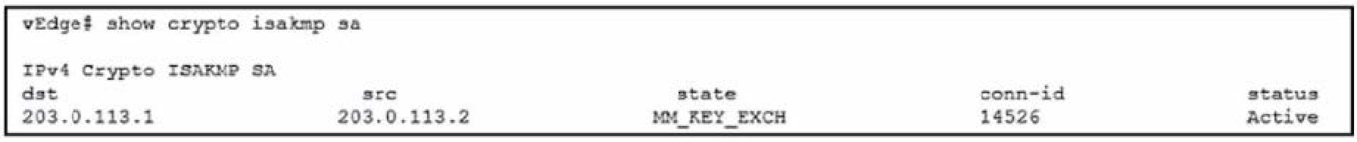
References:

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 12

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 13

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 14

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:

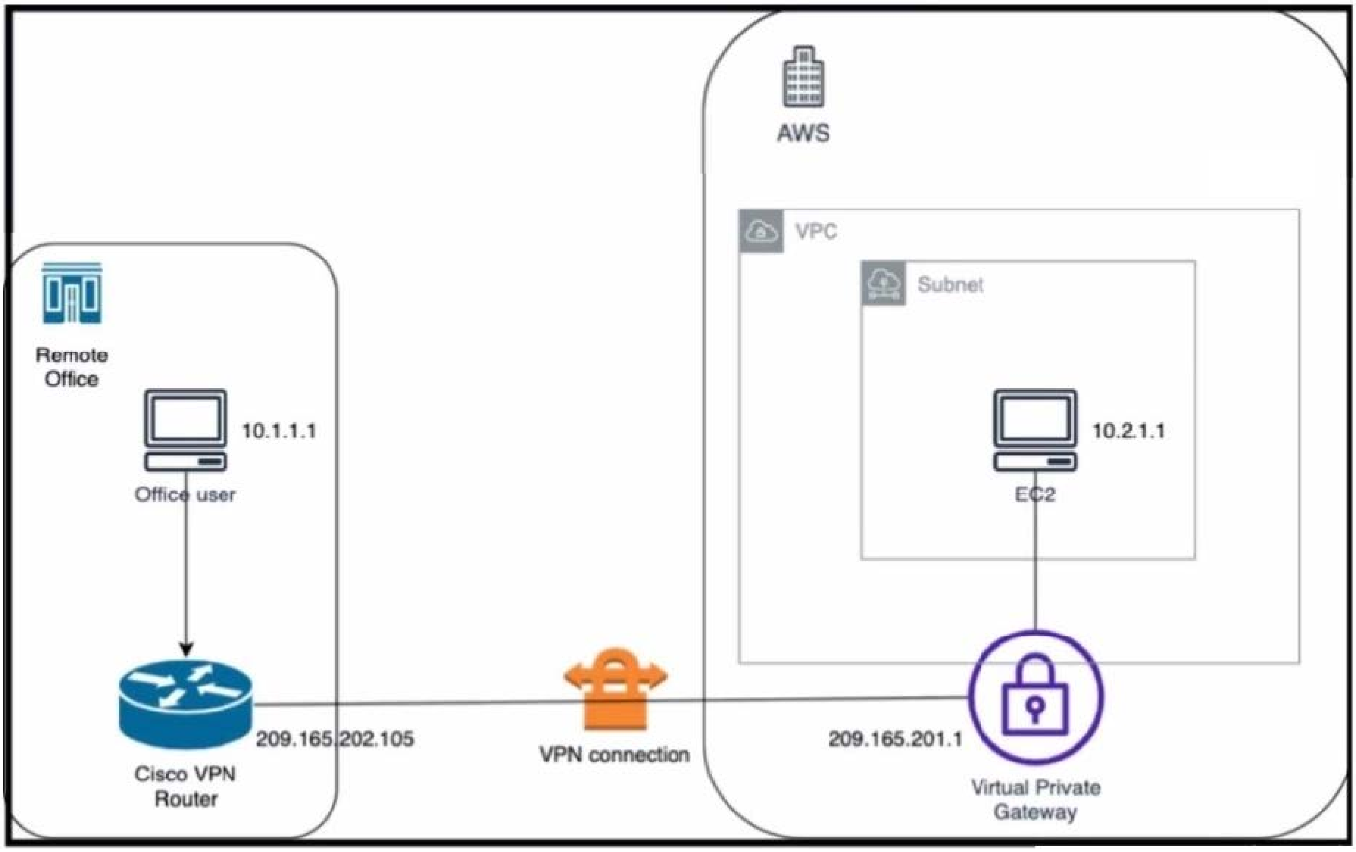
Designing and Implementing Cloud Connectivity (ENCC) v1.0, Module 3:

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 15

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